



Comcast Wireless Cable Modem Gateway

SMCD3GNV3 User Manual

FastFind Links

[Getting to Know the Gateway](#)

[Installing the Gateway](#)

[Preconfiguration Guidelines](#)

[Configuring the Gateway](#)

[Configuring the Gateway's mso Interface](#)

SMC Networks
20 Mason
Irvine, CA. 92618
U.S.A.

Copyright © 2012 SMC Networks
All Rights Reserved

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, or for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of SMC.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Apple and Macintosh are registered trademarks of Apple, Inc. All other brands, product names, trademarks, or service marks are property of their respective owners.

This product (Model :SMCD3GNV3) includes software code developed by third parties, including software code subject to the GNU General Public License ("GPL") or GNU Lesser General Public License (LGPL). As applicable, the terms of the GPL and LGPL, and information on obtaining access to the GPL code and LGPL used in this product, are available to you at <http://gpl.smc.com/>. The GPL code and LGPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, see the GPL Code and LGPL Code for this product and the terms of the GPL and LGPL.

SMCD3GNV3 Wireless Cable Modem Gateway User Manual
November 20, 2012

Contents

Preface	vii
Key Features	viii
Document Organization	ix
Document Conventions	ix
Safety and Warnings	ix
Typographic Conventions	x
1 Getting to Know the Gateway.....	11
Unpacking Package Contents	12
System Requirements	12
Front Panel.....	13
Rear Panel	15
Top Panel.....	16
Bottom Panel.....	16
Using the Reset Button	17
2 Installing the Gateway	18
Finding a Suitable Location.....	19
Installing a Battery.....	20
Connecting to the LAN.....	21
Connecting the WAN.....	22
Connecting to the Public Telephone Network	22
Powering on the Gateway.....	23
3 Preconfiguration Guidelines	24
Configuring Your Computer for TCP/IP	25
Configuring Microsoft Windows 2000	25
Configuring Microsoft Windows XP	26
Configuring Microsoft Windows Vista	27
Configuring Microsoft Windows 7	30
Configuring an Apple [®] Macintosh [®] Computer	33
Disabling Proxy Settings	34
Disabling Proxy Settings in Internet Explorer	34
Disabling Proxy Settings in Firefox	34
Disabling Proxy Settings in Safari.....	35
Disabling Firewall and Security Software	35
Confirming the Gateway's Online Status.....	35

Confirming Your Computer's Link Status	35
4 Configuring the Gateway	36
Accessing the Gateway's Web Management	37
Understanding the Web Management Interface Menus	38
Web Management Interface Menus	40
Viewing Information About Your Network and Connected Devices	42
Viewing Information About Your Network and Connections	43
Viewing the Gateway's Connection Status	44
Viewing Comcast Network Information	46
Viewing and Editing Your Local IP Configuration	47
Viewing and Editing Wireless Configuration	49
Configuring Firewall Settings	53
Viewing System Software Settings	55
Configuring System Hardware	56
Viewing System Hardware Settings	56
Viewing Battery Settings	57
Viewing LAN Ethernet Settings	58
Viewing Wi-Fi Settings	59
Configuring Your Home Network	60
Working with Connected Devices	64
Manually Adding Computers with Static IP Addresses to the Wireless Network	65
Configuring Parental Controls	68
Blocking Sites and Keywords, and Selecting Trusted Computers	68
Blocking Services	75
Managing Devices and Access Types	78
Generating Reports	82
Using Advanced Features	84
Enabling or Disabling Port Forwarding	84
Enabling or Disabling Port Triggering	87
Enabling or Disabling Port Blocking	91
Discovering Devices	92
Troubleshooting the Gateway	94
Defining Log Filters	94
Testing Connectivity to Destination and IP Addresses	96
Restoring or Rebooting the Gateway	98
Changing the Login Password	99
5 Configuring the Gateway's mso Interface	100
Accessing the Gateway's Web Management	101
Understanding the Web Management Interface Menus	102

Web Management Interface Menus	104
Configuring the Gateway Settings	106
Viewing At-a-Glance Configuration Settings	107
Configuring Email Notifications.....	108
Configuring Connections.....	110
Viewing the Gateway's Connection Status.....	111
Viewing and Editing Your Local IP Configuration.....	112
Viewing and Editing Wireless Configuration.....	114
Viewing XFINITY Network Information.....	121
Configuring Firewall Settings	123
Viewing System Software Settings.....	125
Configuring Hardware	126
Viewing System Hardware Settings	127
Viewing Battery Settings	128
Viewing LAN Ethernet Settings.....	129
Viewing Wi-Fi Settings	130
Configuring Your Home Network.....	131
Working with Connected Devices	135
Manually Adding Computers with Static IP Addresses	136
Manually Adding Wireless Clients	139
Configuring Parental Controls.....	142
Blocking Sites and Keywords, and Selecting Trusted Computers.....	142
Blocking Services and Selecting Trusted Computers	148
Managing Devices and Access Types.....	152
Generating Reports.....	156
Using Advanced Features.....	157
Enabling or Disabling Port Forwarding.....	157
Enabling or Disabling Port Triggering.....	160
Remote Management	163
Configuring DMZ Settings.....	165
Configuring Routing Settings	167
Configuring Dynamic DNS Settings.....	169
Discovering Devices.....	171
Troubleshooting the Gateway	173
Generating Logs.....	174
Testing Connectivity to Destination and IP Addresses	175
Restoring or Rebooting the Gateway	177
Changing the Login Password.....	178
6 Troubleshooting Procedures.....	179
Basic Troubleshooting Procedures.....	180
Advanced Troubleshooting Procedures	182

Troubleshooting Physical Network Problems	182
Troubleshooting Configuration Problems	183
Determining Your IP Address	183
Troubleshooting Software-Interaction Problems	187
Specific Troubleshooting Procedures	188
Unable to Log In to Gateway	188
Local Networked Devices Unable to Access the Gateway	188
Unable to Access the Internet.....	189
Unable to Access Networked Devices.....	191
Using the Ping Utility to Troubleshoot	191
Testing the Path from a Computer to the Gateway	191
Testing the Path from a Computer to the Internet.....	192
Using Ping on a Macintosh	193
Gateway Disconnects from the Internet	194
Slow Web Browsing	195
Unable to Configure Port Forwarding.....	195
Unable to Use Pass-thru VPN.....	195
Gateway is Not Passing DHCP Address to a computer.....	195
Determining a Computer's MAC Address.....	196
Microsoft Windows	196
Apple Macintosh Windows OS X.....	197
Wireless Troubleshooting	198
Checking the Gateway's Wireless Connection.....	198
Wireless Range is Low	198
Unable to Connect to a Wireless Network Using Windows XP and Vista	199
Achieving Optimal Wireless Performance	201
Guidelines for Improving Your Wireless Network.....	201
Wireless IEEE 802.11n Guidelines.....	202
Application and Gaming Troubleshooting.....	204
Connecting to Messenger Services Behind the Gateway	204
Connecting to America Online Behind the Gateway	204
Connecting to XBox Live, PSP, and Nintendo WFC	204
Appendix A - Specifications	錯誤! 尚未定義書籤。
Appendix B - Compliances	錯誤! 尚未定義書籤。
Index	207

Preface

The SMCD3GNV3 Wireless Cable Modem Gateway is the ideal all-in-one wired and wireless solution for the home or business environment. SMC is proud to provide you with a powerful, yet simple communication device for connecting your local-area network (LAN) to the Internet.

This user manual contains all the information you need to install and configure your new SMCD3GNV3 Wireless Cable Modem Gateway.



Key Features

The following list summarizes the Gateway's key features.

- Integrated, CableLabs-compliant DOCSIS 1.1/ 2.0 /3.0 cable modem.
- Integrated cable modem port for Internet connection to cable modem service.
- Four 10/100/1000 Mbps Auto-Sensing LAN ports with Auto-MDI/MDIX.
- High-speed 300 Mbps IEEE 802.11n Wireless Access Point.
- Dynamic Host Configuration Protocol (DHCP) for dynamic IP configuration, and Domain Name System (DNS) for domain name mapping.
- One USB 2.0 port.
- Two Plain Old Telephone System (POTS) RJ-11 telephone ports to allow Public Switch Telephone Network (PSTN) analog phone connections.
- IEEE 802.11 b/g/n interoperability with multiple vendors.
- Wireless WEP, WPA, and WPA2 encryption, Hide SSID, and MAC Filtering.
- VPN pass-through support using PPTP, L2TP, or IPSec.
- Advanced SPI firewall Gateway for enhanced network security from attacks over the Internet:
 - Firewall protection with Stateful Packet Inspection
 - Client privileges
 - Hacker prevention
 - Protection from denial of service (DoS) attacks
 - Network Address Translation (NAT)
- Universal Plug and Play (UPnP) enables any UPnP device seamlessly.
- Quality of Service (QoS) ensures high-quality performance with existing networks.
- Effortless plug-and-play installation.
- Intuitive graphical user interface (GUI) configuration, regardless of operating system.
- Comprehensive front panel LEDs for network status and troubleshooting.
- Compatible with all popular Internet applications.

Document Organization

This document consists of four chapters and two appendices.





- **Chapter 1** - describes the contents in the Gateway package, system requirements, and an overview of the Gateway's front, rear, top, and bottom panels.
- **Chapter 2** - describes how to install the Gateway.
- **Chapter 3** - describes how to configure TCP/IP settings on the computer you will use to configure the Gateway.
- **Chapter 4** - describes how to configure the Gateway.
- **Chapter 6** – provides troubleshooting information you can use in the unlikely event you encounter a problem with the Gateway.
- lists the Gateway's specifications.
contains compliance information.

Document Conventions

This document uses the following conventions to draw your attention to certain information.

Safety and Warnings

This document uses the following symbols to draw your attention to certain information.

Symbol	Meaning	Description
	Note	Notes emphasize or supplement important points of the main text
	Tip	Tips provide helpful information, guidelines, or suggestions for performing tasks more effectively.
	Warning	Warnings indicate that failure to take a specified action could result in damage to the device.
	Electric Shock Hazard	This symbol warns users of electric shock hazard. Failure to take appropriate precautions such as not opening or touching hazardous areas of the equipment could result in injury or death.

Typographic Conventions

This document also uses the following typographic conventions.

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels.
<i>Italic</i>	Indicates a variable, which is a placeholder for actual text provided by the user or system. Angled brackets (< >) are also used to indicate variables.
screen/code	Indicates text that is displayed on screen or entered by the user.
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Italic font is also used to indicate variables.
[] square brackets	Indicates optional values.
{ } braces	Indicates required or expected values.
vertical bar	Indicates that you have a choice between two or more options or arguments.

1 Getting to Know the Gateway

Before you install your SMCD3GNV3 Wireless Cable Modem Gateway, check the package contents and become familiar with the Gateway's front and back panels.

The topics covered in this chapter are:

- Unpacking Package Contents (page 12)
- System Requirements (page 12)
- Front Panel (page 13)
- Rear Panel (page 15)
- Top Panel (page 16)
- Bottom Panel (page 16)
- Using the Reset Button (page 17)

Unpacking Package Contents

Unpack the items in your SMCD3GNV3 Wireless Cable Modem Gateway contents and confirm that no items are missing or damaged. Your package should include:

- One SMCD3GNV3 Wireless Cable Modem Gateway
- One 2600 mAh battery
- One Category 5E Ethernet cable
- One CD that contains this User Manual

If any items are missing or damaged, please contact your cable service provider. Keep the carton, including the original packing material, in case you need to store the product or return it.

System Requirements

To complete your installation, you will need the following items:

- Provisioned Internet access on a cable network that supports cable modem service.
- A computer with a wired network adapter with TCP/IP installed.
- A Java-enabled Web browser, such as Microsoft Internet Explorer 5.5 or above.
- Microsoft® Windows® 2000 or higher for USB driver support.
- An analog telephone and two RJ-11 cables if you want to connect the Gateway to an analog telephone and PSTN telephone line.

Front Panel

The front panel of your SMCD3GNV3 Wireless Cable Modem Gateway contains a set of light-emitting diode (LED) indicators. These LEDs show the status of the Gateway and simplify troubleshooting.

Figure 1 shows the front panel of the SMCD3GNV3 Wireless Cable Modem Gateway. Table 1 describes the front panel LEDs.



Figure 1. Front Panel of the SMCD3GNV3 Wireless Cable Modem Gateway

Table 1. Front Panel LEDs

LED	Color	Description
POWER	White	ON = power is supplied to the Gateway. OFF = power is not supplied to the Gateway.
US/DS	White	Blinking = ranging is in progress. ON = ranging is complete on 1 channel only. OFF = scanning for DS channel.
DS	White	Blinking = scanning for DS channel. ON = synchronized on 1 channel only.
US and DS		Both US and DS blinking together = operator is performing maintenance.
Online	White	Blinking = cable interface is acquiring IP, ToD, CM configuration. ON = Gateway is operational. OFF = Gateway is offline.
WiFi	White	Blinking = data is transmitting over the Gateway's Wi-Fi interface. ON = Wi-Fi is enabled. OFF = Wi-Fi is disabled.
Tel ¹	White	Blinking = telephone line 1 is in use. ON = Gateway's telephone 1 port is online. OFF = Gateway's telephone 1 port is not online.
Tel ²	White	Blinking = telephone line 2 is in use. ON = Gateway's telephone 2 port is online. OFF = Gateway's telephone 2 port is not online.
Battery	White	Blinking = Gateway battery power is low. Please apply AC power as soon as possible. ON = Gateway is operating from battery power. OFF = Gateway is operating from AC power.

Rear Panel

The rear panel of your SMCD3GNV3 Wireless Cable Modem Gateway contains a reset button and the ports for attaching the supplied power adapter and making additional connections. Figure 2 shows the rear panel components and Table 2 describes their meanings.

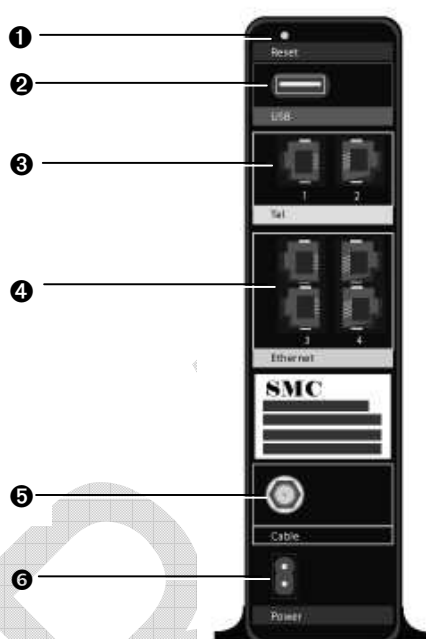


Figure 2. Rear View of the SMCD3GNV3 Wireless Cable Modem Gateway

Table 2. SMCD3GNV3 Wireless Cable Modem Gateway Rear Panel Components

	Item	Description
❶	Reset button	Use this button to reset the power or restore the default factory settings (see “Using the Reset Button” on page 17).
❷	USB	USB 2.0 high-speed port for USB-enabled peripherals.
❸	Tel 1-2	Connect an analog telephone to one port and an analog (PSTN) telephone line to the other port.
❹	Ethernet 1-4	Four 10/100/1000 auto-sensing RJ-45 switch ports. Connect devices on your LAN such as a computer, hub, or switch to these ports.
❺	Cable	Connect your coaxial cable line to this port.
❻	Power 110 VAC	Connect the supplied power cord.

Top Panel

The top panel of your SMCD3GNV3 Wireless Cable Modem Gateway has a **WPS** button for configuring wireless security automatically. Figure 3 shows the **WPS** button.



Figure 3. Top View of the SMCD3GNV3 Wireless Cable Modem Gateway

Bottom Panel

The bottom panel of your SMCD3GNV3 Wireless Cable Modem Gateway contains a panel for installing the Gateway's battery. For information about installing the battery, see "Installing a Battery" on page 20.

Using the Reset Button

Using the reset button on the rear panel (see Figure 2 on page 15), you can perform two types of reset operations with the Gateway:

- Software reset – this reset operation power-cycles the Gateway and retains its current configuration settings.
- Factory default reset – this operation remove all overrides made to the Gateway's factory default configuration and returns the Gateway to its original factory default settings.

The number of seconds you press the reset button determines which reset operation is performed. To protect against accidental resets, the reset button is recessed on the Gateway rear panel.



Note: You can also reset the Gateway and retain its current configuration settings using the RESET method described under “Restoring or Rebooting the Gateway” on page 98.

To use the reset button to perform a software or factory default reset:

1. Leave power plugged into the Gateway.
2. Find the reset button at the top of the back panel, then use a thin object to press and hold the reset button as follows:
 - To perform a software reset, press the reset button for at least 10 seconds.
 - To perform a factory default reset, press the reset button for at least 15 seconds.
3. Release the reset button.

2 Installing the Gateway

This chapter describes how to install your SMCD3GNV3 Wireless Cable Modem Gateway. The topics covered in this chapter are:

- Finding a Suitable Location (page 19)
- Installing a Battery (page 20)
- Connecting to the LAN (page 21)
- Connecting the WAN (page 22)
- Powering on the Gateway (page 23)

DRAFT

Finding a Suitable Location

Your SMCD3GNV3 Wireless Cable Modem Gateway can be installed in any location with access to the cable network. All of the cables connect to the rear panel of the Gateway for better organization and utility. The LED indicators on the front panel are easily visible to provide you with information about network activity and status.

For optimum performance, the location you choose should:

- Be close to a working AC power outlet when powering the Gateway using AC power.
- Allow at least one foot of space around the sides and top of the Gateway to provide sufficient air flow around the device.
- Not expose the Gateway to a dusty or wet environment.
- Be an elevated location such as a high shelf, keeping the number of walls and ceilings between the Gateway and your other devices to a minimum.
- Be away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, or the base for a cordless phone.
- Be away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal. For more information about selecting an optimum location for wireless operation, see “Guidelines for Improving Your Wireless Network” on page 201.

Installing a Battery

To install a battery into the Gateway, use the following procedure.

1. Place the Gateway on its side on a table.
2. Remove battery compartment door on the bottom panel and set it aside (see Figure 4).



Figure 4. Removing the Battery Compartment Door

3. Insert the battery into the battery compartment (see Figure 5).



Figure 5. Installing the Battery

4. Close the battery compartment.



Note: Using the Battery menu in the Gateway's Web interface, you can view status information about the battery (see "Viewing Battery Settings" on page 57).

Connecting to the LAN

Using an Ethernet LAN cable, you can connect the Gateway to a desktop computer, notebook, hub, or switch. The Gateway supports auto-MDI/MDIX, so you can use either a standard straight-through or crossover Ethernet cable.

1. Connect either end of an Ethernet cable to one of the four **Ethernet** ports on the rear panel of the Gateway (see Figure 6).

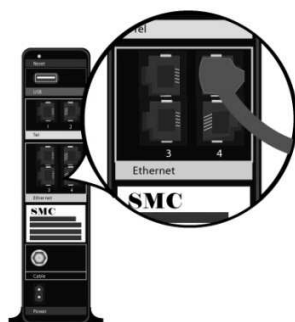


Figure 6. Connecting to an Ethernet Port on the Gateway Rear Panel

2. Connect the other end of the cable to your computer's network-interface card (NIC) or to another network device (see Figure 7).

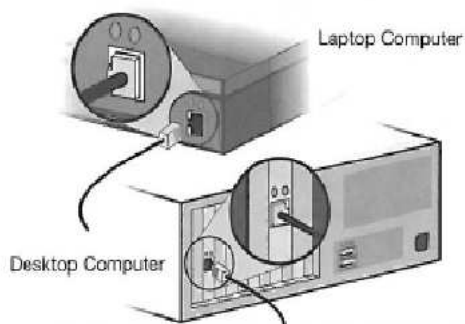


Figure 7. Connecting the Gateway to a Laptop or Desktop Computer

Connecting the WAN

To connect the Gateway to a Wide Area Network (WAN) interface:

3. Connect a coaxial cable to the port labeled **Cable** on the rear panel of the Gateway from a cable port in your home or office (see Figure 2 on page 15). Use only manufactured coaxial patch cables with F-type connectors at both ends for all connections.
4. Hand-tighten the connectors to secure the connection.
5. If the modem was not installed by your cable provider (ISP) or is replacing another cable modem, contact your cable operator to register the SMCD3GNV3. If the modem is not registered with your cable operator, it will be unable to connect to the cable network system.

Connecting to the Public Telephone Network

The rear panel of the Gateway has two RJ-11 telephone-style connectors labeled **Tel 1** and **Tel 2**. Each of these connectors can provide telephone service to multiple telephones, fax machines, and analog modems.

The maximum number of telephone devices connected to each RJ-11 port is limited by the total Ringing Load of the telephone devices that are connected. Many telephone devices are marked with a Ringer Equivalent Number (REN). Each telephone port on the Gateway can support up to a 5 REN load. The sum of the REN load on all of the telephone devices attached to each port must not exceed 5 REN.

Before you use the Gateway's RJ-11 connectors to power the analog devices in your home or office, disconnect the telephone lines from any other provider at the demarcation point. If the incoming phone line is connected to another provider, such as an incumbent telephone company, it can result in potentially harmful voltage to the analog telephone line.



Note: The customer or the customer's wire contractor is responsible for adhering to all local codes for wiring.

To set up the ability to place calls using a regular analog telephone line (PSTN), perform the following procedure.

1. Disconnect the phone lines from any other provider at the demarcation point, if appropriate.
2. Connect the RJ-11 cable on an analog device to the **Tel 1** connector on the rear panel of the Gateway.
3. Connect the RJ-11 cable on another analog device to the **Tel 2** connector on the rear panel of the Gateway.

Powering on the Gateway

After making your connections, use the following procedure to power on the Gateway:

1. Connect the supplied power cord to the power port on the rear panel of the Gateway (see Figure 2 on page 15).
2. Connect the other end of the power adapter to a working power outlet. The Gateway powers on automatically, the **POWER** LED on the front panel goes ON, and the other front panel LEDs show the Gateway's status (see Table 1 on page 14).



WARNING: Only use the power cord supplied with the Gateway. Using a different power cord can damage the Gateway and void the warranty.

DRAFT

3 Preconfiguration Guidelines

After you install your SMCD3GNV3 Wireless Cable Modem Gateway, use the information in this chapter to configure the TCP/IP settings on the computer that will be used to configure the Gateway. This chapter also covers other preconfiguration guidelines you should review before configuring the Gateway.

The topics covered in this chapter are:

- Configuring Your Computer for TCP/IP (page 25)
- Disabling Proxy Settings (page 34)
- Disabling Firewall and Security Software (page 35)
- Confirming the Gateway's Online Status (page 35)
- Confirming Your Computer's Link Status (page 35)

Configuring Your Computer for TCP/IP

Before you configure the Gateway using its Web management interface, configure TCP/IP settings on the computer that will be used to configure the Gateway. The TCP/IP procedure to use depends on the operating system installed on the computer.

- For Microsoft Windows 2000, see the procedure below
- For Microsoft Windows XP, see page 26
- For Microsoft Windows Vista, see page 27
- For Microsoft Windows 7, see page 30
- For Apple Macintosh, see page 33

Configuring Microsoft Windows 2000

Use the following procedure to configure your computer if your computer has Microsoft Windows 2000 installed.

1. On the Windows taskbar, click **Start**, point to **Settings**, and then click **Control Panel**.
2. In the Control Panel window, double-click the **Network and Dial-up Connections** icon. If the Ethernet adapter in your computer is installed correctly, the **Local Area Connection** icon appears.
3. Double-click the **Local Area Connection** icon for the Ethernet adapter connected to the Gateway. The Local Area Connection Status dialog box appears (see Figure 8).

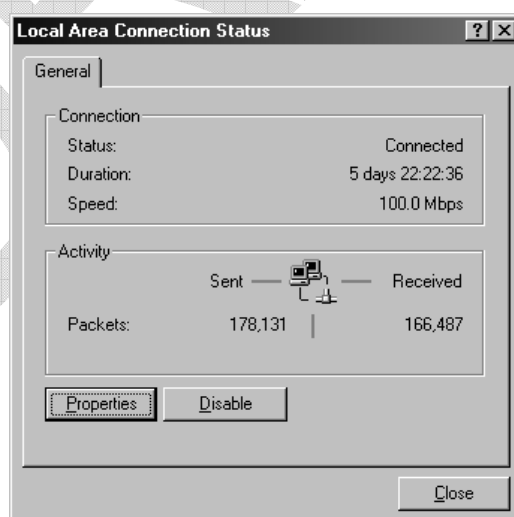


Figure 8. Local Area Connection Status Window

4. In the Local Area Connection Status dialog box, click the **Properties** button. The Local Area Connection Properties dialog box appears.
5. In the Local Area Connection Properties dialog box, verify that **Internet Protocol (TCP/IP)** is checked. Then select **Internet Protocol (TCP/IP)** and click the **Properties** button.
6. Click **Obtain an IP address automatically** to configure your computer for DHCP.
7. Click the **OK** button to save this change and close the Local Area Connection Properties dialog box.
8. Click **OK** button again to save these new changes.
9. Restart your computer.

Configuring Microsoft Windows XP

Use the following procedure to configure your computer if your computer has Microsoft Windows XP installed. If you use the Classic interface, where the icons and menus resemble previous Windows versions, perform the procedure under “Configuring Microsoft Windows 2000” on page 25.

1. On the Windows taskbar, click **Start**, click **Control Panel**, and then click **Network and Internet Connections**.
2. Click the **Network Connections** icon.
3. Click **Local Area Connection** for the Ethernet adapter connected to the Gateway. The Local Area Connection Status dialog box appears.
4. In the Local Area Connection Status dialog box, click the **Properties** button (see Figure 9). The Local Area Connection Properties dialog box appears.

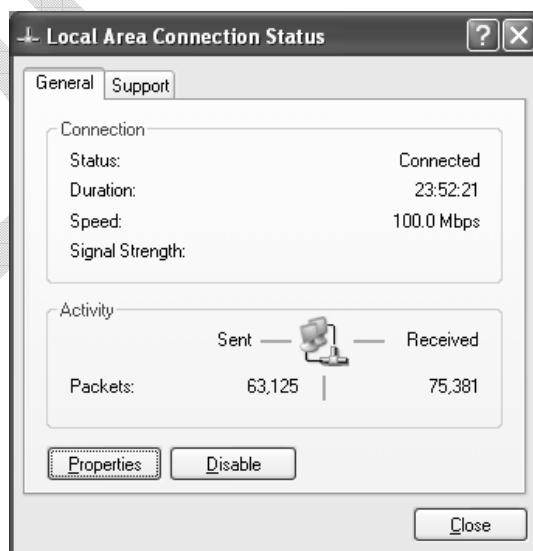


Figure 9. Local Area Connection Status Window

5. In the Local Area Connection Properties dialog box, verify that **Internet Protocol (TCP/IP)** is checked. Then select **Internet Protocol (TCP/IP)** and click the **Properties** button. The Internet Protocol (TCP/IP) Properties dialog box appears.
6. In the Internet Protocol (TCP/IP) Properties dialog box, click **Obtain an IP address automatically** to configure your computer for DHCP. Click the **OK** button to save this change and close the Internet Protocol (TCP/IP) Properties dialog box.
7. Click the **OK** button again to save your changes.
8. Restart your computer.

Configuring Microsoft Windows Vista

Use the following procedure to configure a computer running Microsoft Windows Vista with the default interface. If you use the Classic interface, where the icons and menus resemble previous Windows versions, perform the procedure under “Configuring Microsoft Windows 2000” on page 25.

1. On the Windows taskbar, click Start, click Control Panel, and then select Network and Internet Icon.
2. Click View Networks Status and tasks and then click **Management Networks Connections**.
3. Right-click the **Local Area Connection** icon and click **Properties**.
4. Click **Continue**. The Local Area Connection Properties dialog box appears.
5. In the Local Area Connection Properties dialog box, verify that **Internet Protocol (TCP/IPv4)** is checked. Then select **Internet Protocol (TCP/IPv4)** and click the **Properties** button (see Figure 10). The Internet Protocol Version 4 Properties dialog box appears.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

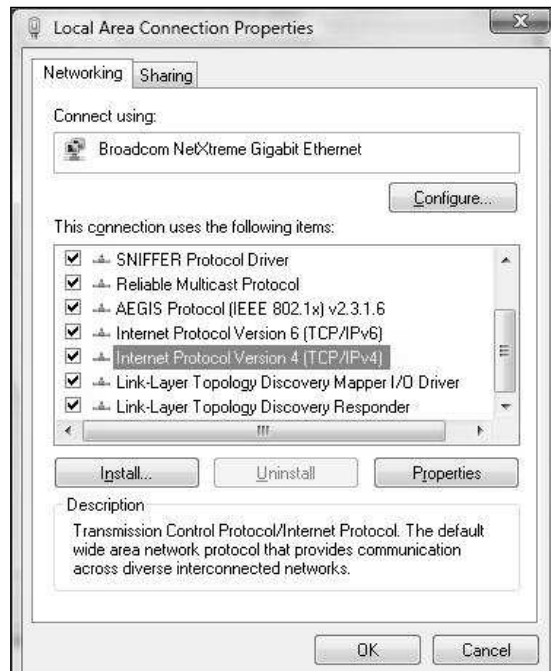


Figure 10. Local Area Connection Properties Window

6. In the Internet Protocol Version 4 Properties dialog box, click **Obtain an IP address automatically** to configure your computer for DHCP (see Figure 11).



Figure 11. Internet Protocol Properties Window

錯誤! 使用 [常用] 索引標籤將 **Heading 1** 套用到您想要在此處顯示的文字。

7. Click the **OK** button to save your changes and close the dialog box.
8. Click the **OK** button again to save your changes.

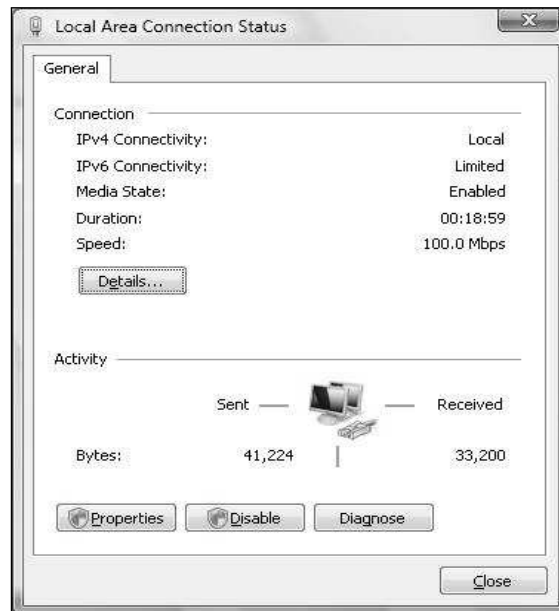


Figure 12. Local Area Connection Status Window

Configuring Microsoft Windows 7

Use the following procedure to configure a computer running Microsoft Windows 7.

1. In the Start menu search box, type: **ncpa.cpl**

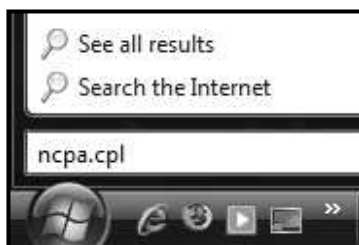


Figure 13. Typing ncpa.cpl in the Start Menu Box

The Network Connections List appears.



Figure 14. Example of Network Connections List

2. Right-click the **Local Area Connection** icon and click **Properties**.
3. In the **Networking** tab, click either **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.

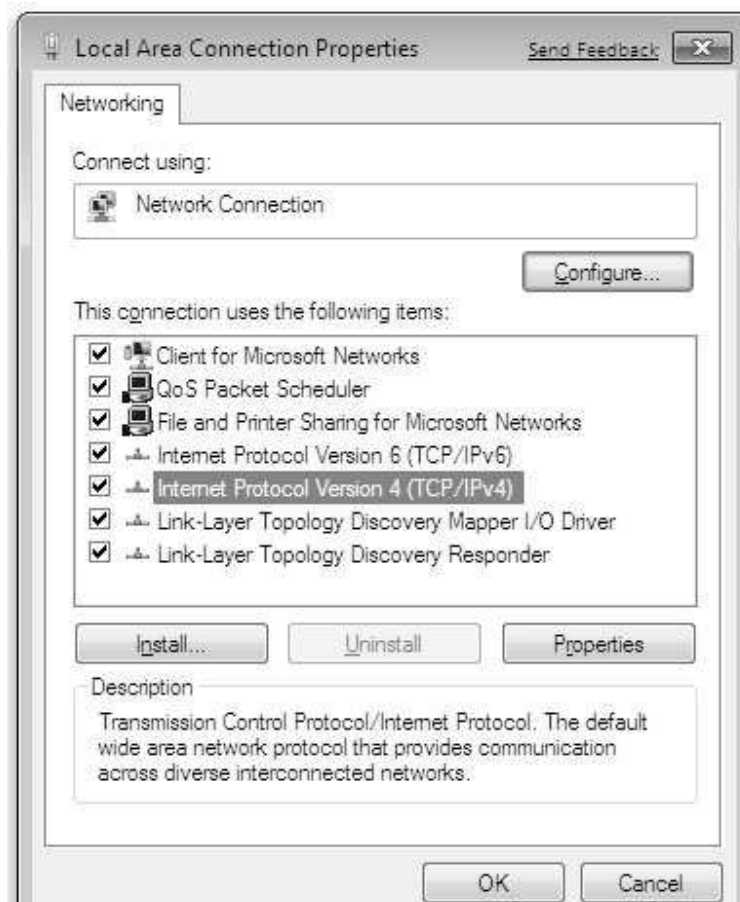


Figure 15. Local Area Network Connection Properties Dialog Box

4. In the properties dialog box, click **Obtain an IP address automatically** to configure your computer for DHCP (see Figure 16).

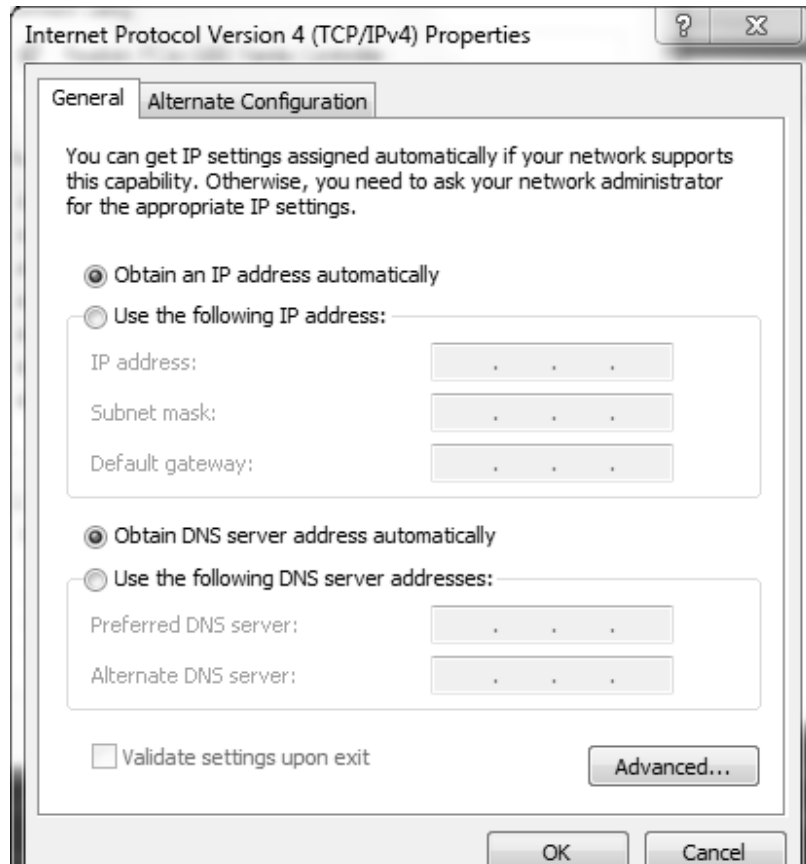


Figure 16. Properties Window

5. Click the **OK** button to save your changes and close the dialog box.
6. Click the **OK** button again to save your changes.

Configuring an Apple® Macintosh® Computer

The following procedure describes how to configure TCP/IP on an Apple Macintosh running Mac OS 10.2. If your Apple Macintosh is running Mac OS 7.x or later, the steps you perform and the screens you see may differ slightly from the following. However, you should still be able to use this procedure as a guide to configuring your Apple Macintosh for TCP/IP.

1. Pull down the Apple Menu, click **System Preferences**, and select **Network**.
2. Verify that NIC connected to the SMCD3GNV3 is selected in the **Show** field.
3. In the **Configure** field on the **TCP/IP** tab, select **Using DHCP** (see Figure 17).
4. Click **Apply Now** to apply your settings and close the TCP/IP dialog box.



Figure 17. Selecting Using DHCP in the Configure Field

Disabling Proxy Settings

Disable proxy settings in your Web browser. Otherwise, you will not be able to view the Gateway's Web-based configuration menus.

Disabling Proxy Settings in Internet Explorer

The following procedure describes how to disable proxy settings in Internet Explorer 5 and later.

1. Start Internet Explorer.
2. On your browser's **Tool** menu, click **Options**. The Internet Options dialog box appears.
3. In the Internet Options dialog box, click the **Connections** tab.
4. In the **Connections** tab, click the **LAN settings** button. The Local Area Network (LAN) Settings dialog box appears.
5. In the Local Area Network (LAN) Settings dialog box, uncheck all check boxes.
6. Click **OK** until the Internet Options window appears.
7. In the Internet Options window, under **Temporary Internet Files**, click **Settings**.
8. For the option **Check for newer versions of stored pages**, select **Every time I visit the webpage**.
9. Click **OK** until you close all open browser dialog boxes.

Disabling Proxy Settings in Firefox

The following procedure describes how to disable proxy settings in Firefox.

1. Start Firefox.
2. On your browser's **Tools** menu, click **Options**. The Options dialog box appears.
3. Click the **Advanced** tab.
4. In the **Advanced** tab, click the **Network** tab.
5. Click the **Settings** button.
6. Click **Direct connection to the Internet**.
7. Click the **OK** button to confirm this change.

Disabling Proxy Settings in Safari

The following procedure describes how to disable proxy settings in Safari.

1. Start Safari.
2. Click the **Safari** menu and select **Preferences**.
3. Click the **Advanced** tab.
4. In the **Advanced** tab, click the **Change Settings** button.
5. Choose your location from the **Location** list (this is generally **Automatic**).
6. Select your connection method. If using a wired connection, select **Built-in Ethernet**. For wireless, select **Airport**.
7. Click the **Proxies** tab.
8. Be sure each proxy in the list is unchecked.
9. Click **Apply Now** to finish.

Disabling Firewall and Security Software

Disable any firewall or security software that may be running on your computer. For more information, refer to the documentation for your firewall. After you configure the Gateway, please re-enable your computer firewall.

Confirming the Gateway's Online Status

Confirm that the **Online** LED on the Gateway front panel is ON (see Figure 1 on page 13). If the LED is OFF, replace the coaxial cable connecting the Gateway to the cable service. If the **Online** LED does not go ON after several minutes, please contact your cable provider to confirm that the service is active.

Confirming Your Computer's Link Status

Be sure there is an Ethernet cable connecting your computer to the Gateway. Then confirm that the LEDs for the Gateway port connected to your computer are blinking. If the LEDs are OFF, the connection between your computer and Gateway is not working properly.

4 Configuring the Gateway

After configuring your computer for TCP/IP and following the preconfiguration guidelines in Chapter 3, use that computer's Web browser to configure your SMCD3GNV3 Gateway. This chapter describes how to use your computer's Web browser to configure the Gateway.

The topics covered in this chapter are:

- Accessing the Gateway's Web Management (page 37)
- Understanding the Web Management Interface Menus (page 38)
- Web Management Interface Menus (page 40)

Accessing the Gateway's Web Management

After configuring your computer for TCP/IP and reviewing the guidelines on the previous page, configure the Gateway using its Web-based management interface. From your Web browser, log in to the interface to define system parameters, change password settings, view status windows to monitor network conditions, and control the Gateway and its ports.

To display the SMCD3GNV3 Wireless Cable Modem Gateway's Web-based management screens, use the following procedure.

1. Launch a Web browser.



Note: Your computer does not have to be online to configure the Gateway.

2. In the browser address bar, type <http://10.0.0.1> and press the Enter key. The Login screen appears (see Figure 18).

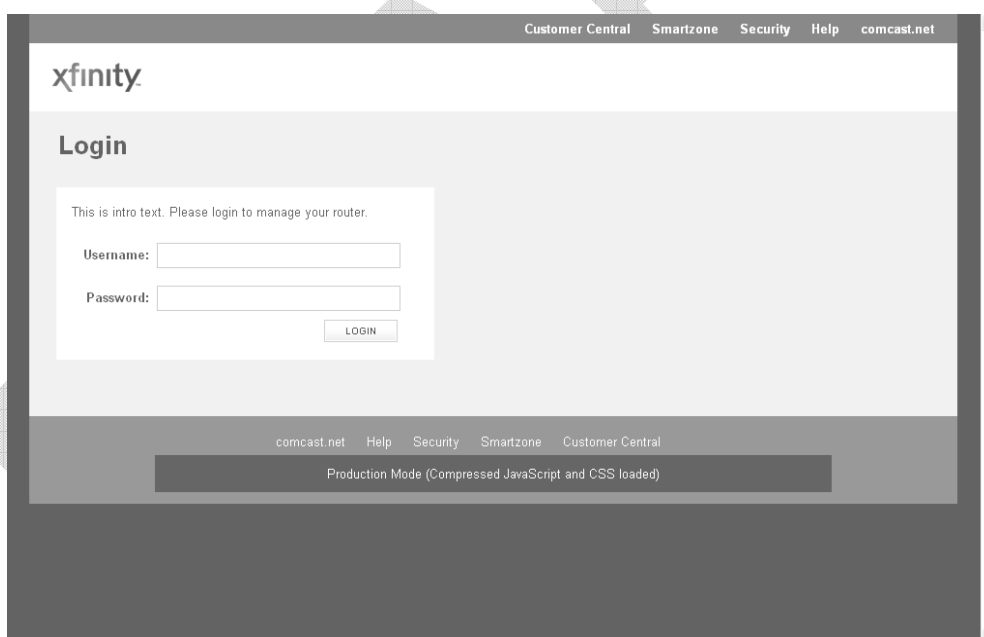


Figure 18. Login Screen

3. In the Login User Password screen, enter the default username **cusadmin** and the default password **highspeed**. Both are case sensitive. For security, each password character appears as a dot (•). After you log in, we recommend you change the default password on the Change Password menu (see "Changing the Login Password" on page 99).



Note: Your cable modem operator may customize the login password, so please check with your operator for the correct password to use.

4. Click the **LOGIN** button to access the Gateway's Web interface. The At a Glance menu appears, showing connection status information about the Gateway. You can also display this menu any time by clicking **At a Glance** in the menu bar.

Understanding the Web Management Interface Menus

The left side of the management interface contains a menu bar for selecting menus to configure the Gateway. When you click a menu, information and any configuration settings associated with the menu appear in the main area (see Figure 19). If the displayed information exceeds the main area, scroll bars appear to the right of the main area so you can scroll up and down through the information.

The top of the main area shows the path (or "breadcrumb") associated with the information displayed in the main area. For example, if you click the **Status** submenu in the **Connection** menu, **Connection > Status** appears at the top of the main area.

The top-right area shows the username used to log in to the Web interface, along with links for changing the login password and logging out of your current session.

Below the login user name and links are status icons that show the:

- Percentage of battery power remaining
- Gateway's Internet access
- Status of the Gateway's wireless connection
- Firewall security level

A control panel at the bottom of the menu provides links for accessing comcast.net, help, security, smartzone, and customer central.

Username 

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

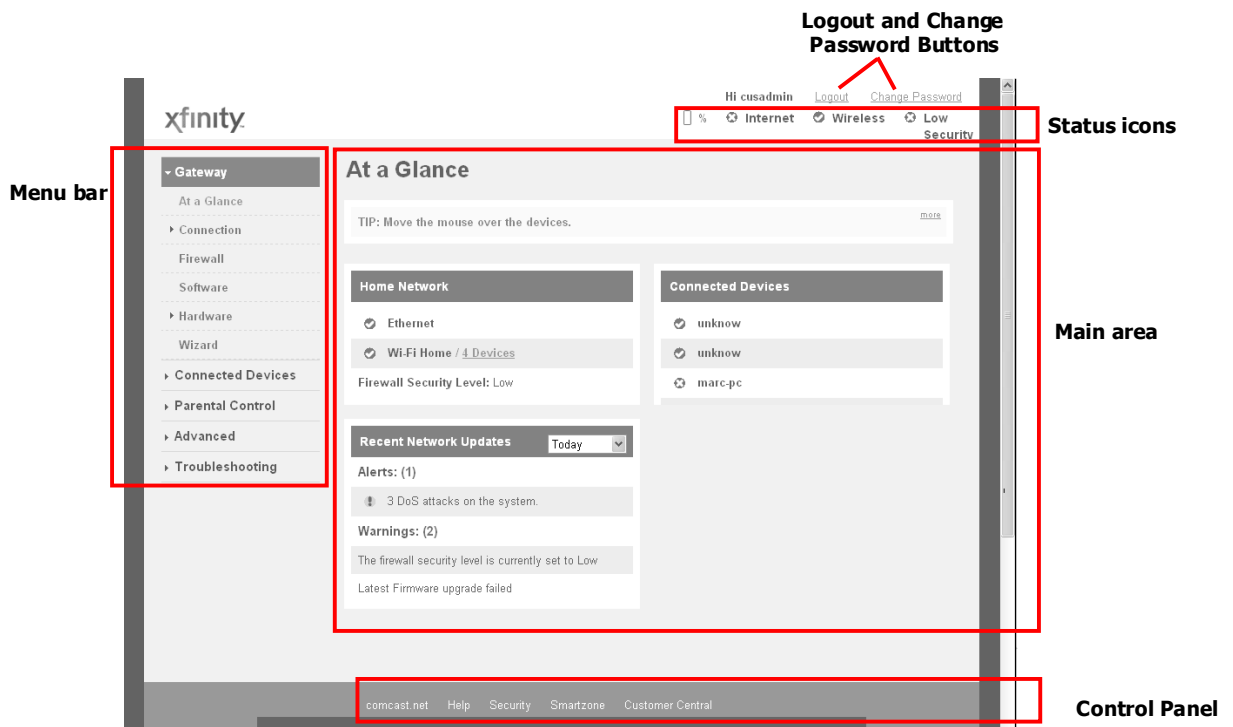


Figure 19. Main Areas on the Web Management Interface

Some menus in the menu bar have submenus associated with them. If you click a menu that has submenus, the submenus appear below the menu. For example, if you click the **Connection** menu, the submenus in Figure 20 appear.

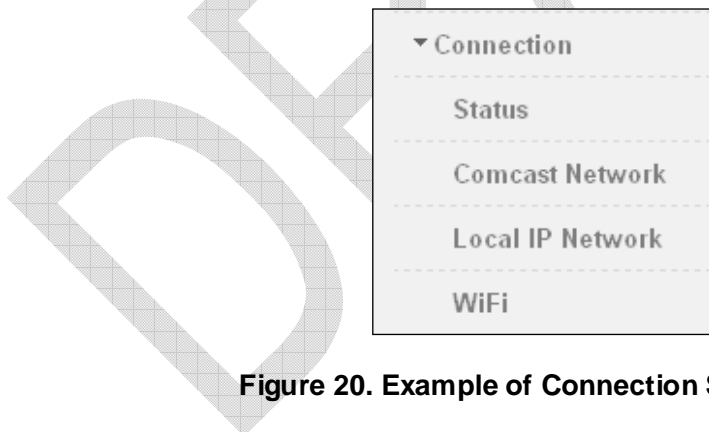


Figure 20. Example of Connection Submenus

Web Management Interface Menus

Table 3 describes the menus in the Web management interface.

Table 3. Web Management Interface Menus and Submenus

Menus and Submenus	Description	See Page
At a Glance	Lets you view information about your home network, connected devices, and recent network updates.	42
Connection	Displays submenus that let you:	
Connection > Status	<ul style="list-style-type: none"> View and edit settings for the local IP network, and view the settings of the Wi-Fi network and Comcast network. 	44
Connection > Comcast Network	<ul style="list-style-type: none"> View Comcast network settings and initialization procedures, including cable modem, downstream, and upstream information. 	46
Connection > Local IP Network	<ul style="list-style-type: none"> View and reset your local IPv4 and IPv6 settings. 	47
Connection > WiFi	<ul style="list-style-type: none"> View and edit the Gateway's basic and advanced wireless settings. 	49
Firewall	<ul style="list-style-type: none"> Configure the security level of the Gateway's internal firewall. 	53
Ssoftware	<ul style="list-style-type: none"> View system software information. 	55
Hardware > System Hardware	<ul style="list-style-type: none"> View information about the Gateway system hardware. 	56
Hardware > Battery	<ul style="list-style-type: none"> View information about the Gateway's internal battery. 	57
Hardware > LAN	<ul style="list-style-type: none"> View the link status and Media Access Control (MAC) address for each of the four Gateway Ethernet ports. 	58
Hardware > WiFi	<ul style="list-style-type: none"> View the status and MAC address of the Gateway's Wi-Fi port. 	59
Wizard	<ul style="list-style-type: none"> Use a wizard to set up your home network. 	60
Connected Devices	Displays the Computer submenu for adding online computers and viewing computers that are offline.	

Table 3. Web Management Interface Menus and Submenus

Menus and Submenus	Description	See Page
Parental Control	Displays submenus that let you configure the Gateway for:	
Parental Control > Managed Sites	<ul style="list-style-type: none"> Blocked sites, blocked keywords, and trusted computers. 	68
Parental Control > Managed Services	<ul style="list-style-type: none"> Blocked services and trusted computers. 	75
Parental Control > Managed Devices	<ul style="list-style-type: none"> Managed and blocked devices. 	78
Parental Control > Reports	<ul style="list-style-type: none"> Generating reports containing selected Log Messages generated during the user-defined timeframe. 	82
Advanced	Displays submenus that let you:	
Advanced > Port Forwarding	<ul style="list-style-type: none"> Enable or disable the Gateway's port forwarding feature. 	84
Advanced > Port Triggering	<ul style="list-style-type: none"> Enable or disable the Gateway's port triggering feature. 	87
Advanced > Port Blocking	<ul style="list-style-type: none"> Enable or disable the Gateway's port blocking feature. 	91
Advanced > Device Discovery	<ul style="list-style-type: none"> Enable or disable the Gateway's Universal Plug and Play (UPnP) feature for dynamic connectivity to devices on the network. 	92
Troubleshooting	Displays submenus that let you:	
Troubleshooting > Logs	Configure log filters, and download and print system logs.	94
Troubleshooting > Diagnostic Tools	Tests connectivity to a destination or IP address.	96
Troubleshooting > Restore/Reboot Gateway	Reset the Gateway, reset the Wi-Fi router only, or restore factory settings.	98
Troubleshooting > Change Password	Change the password used to log in to the Gateway's Web interface.	99

Viewing Information About Your Network and Connected Devices

The At a Glance menu appears when you log in to the Gateway's Web interface. You can also display this menu by clicking **Gateway** in the menu bar. Figure 21 shows an example of the At a Glance menu and Table 4 describes the menu.

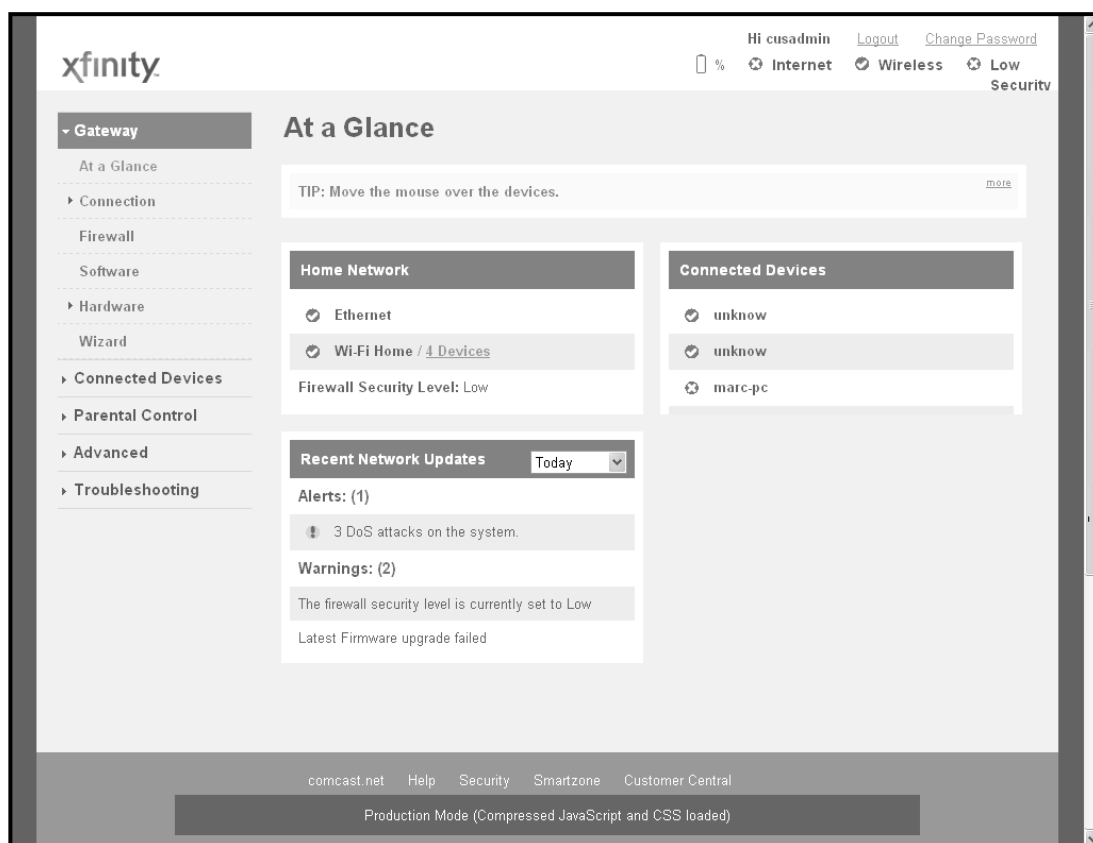


Figure 21. Example of the At a Glance Menu

Table 4. At a Glance Menu

Option	Description
Home Network	Shows the status of your home network's Ethernet and Wi-Fi home status. A green check mark indicates normal operation. This area also shows the Gateway's firewall security level. To change this level, see "Configuring Firewall Settings" on page 53.
Connected Devices	Shows the names of the devices connected to the Gateway. A Connected Devices button opens the Computers menu for viewing devices that the Gateway automatically detects using DHCP (see page 64).
Recent Network Updates	Displays alert and warning information. A drop-down list lets you view this information for today, yesterday, this week, or this month.

Viewing Information About Your Network and Connections

Using the **Gateway** menu, you can:

- View and edit settings for the local IP network, and view Wi-Fi and Comcast network status. See page 44.
- View Comcast network settings and initialization procedures, including cable modem, downstream, and upstream information. See page 46.
- Configure IPv4 or IPv6 settings for the Gateway. See page 47.
- View and edit basic and advanced wireless settings. See page 49.

DRAFT

Viewing the Gateway's Connection Status

The Status menu lets you view and edit the settings for your local IP network. You can also use this menu to view the status of the Wi-Fi network and Comcast network.

To display the Status menu, click **Connection** in the menu bar, and then click the **Status** submenu. Figure 22 shows an example of the Status menu and Table 5 describes the menu.

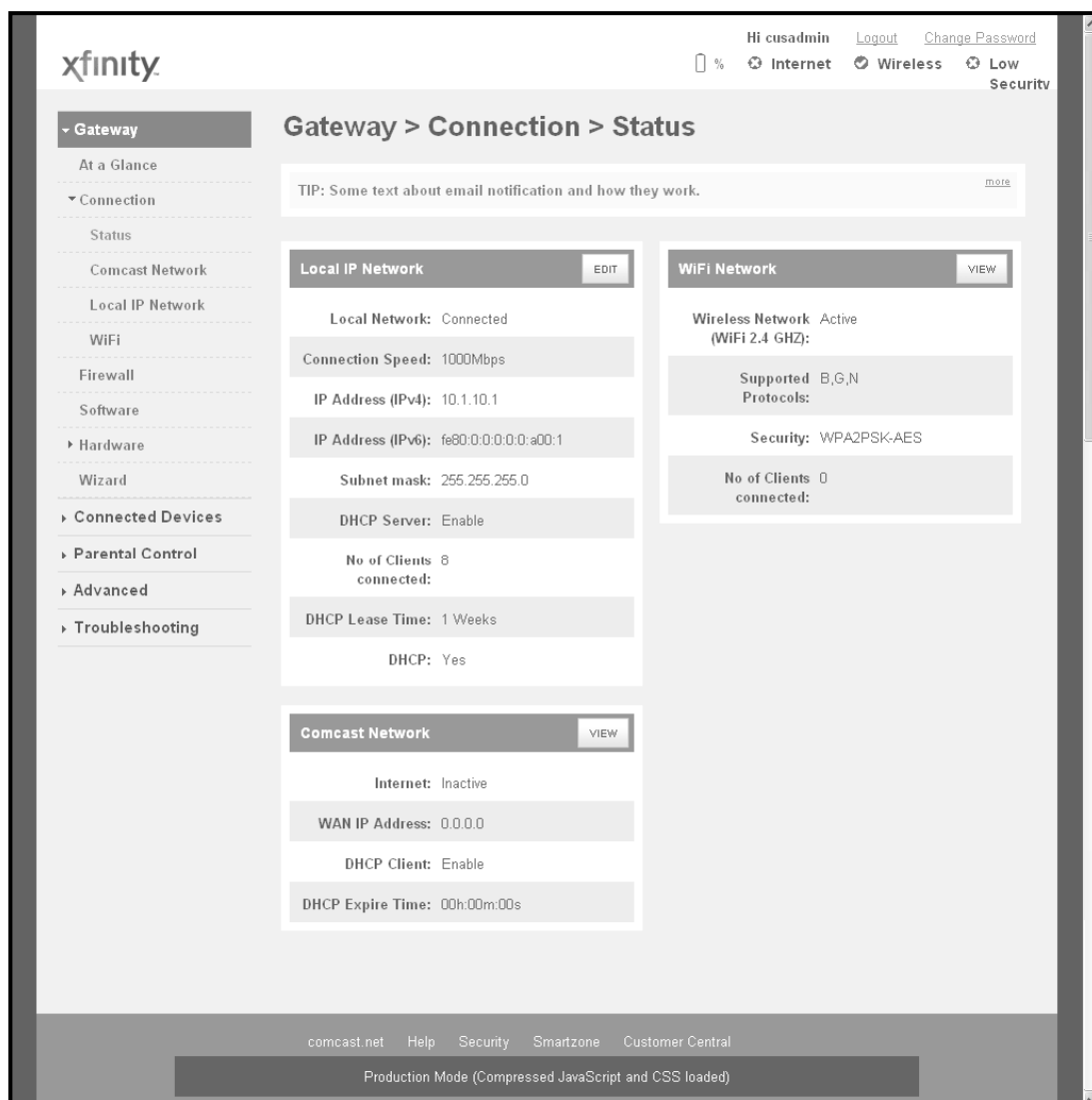


Figure 22. Example of the Status Menu

錯誤! 使用 [常用] 索引標籤將 **Heading 1** 套用到您想要在此處顯示的文字。

Table 5. Status Menu

Option	Description
Local IP Network	Displays information about the local network. The EDIT button opens the Local IP Configuration menu for viewing and changing IPv4 or IPv6 settings (see “Viewing and Editing Your Local IP Configuration” on page 47).
WiFi Network	Lets you view information about your Wi-Fi network. A VIEW button opens the WiFi menu for viewing the link status and MAC address of the Gateway’s WiFi LAN port (see “Viewing Wi-Fi Settings” on page 59).
Comcast Network	Lets you view information about the Comcast network. A VIEW button opens the Comcast Network menu for viewing the initialization procedures, including cable modem, downstream, and upstream information (see “Viewing Comcast Network Information” on page 46).

DRAFT

Viewing Comcast Network Information

The Comcast Network menu lets you view settings for the Comcast network. This menu also shows information about the Gateway's initialization procedures, cable modem settings, and downstream and upstream information. The information shown on this menu automatically updates (refreshes) every 10 seconds.

To display the Comcast Network menu, click **Gateway** in the menu bar, and then click the **Connection** and **Comcast Network** submenus. Figure 23 shows an example of the Comcast Network menu.

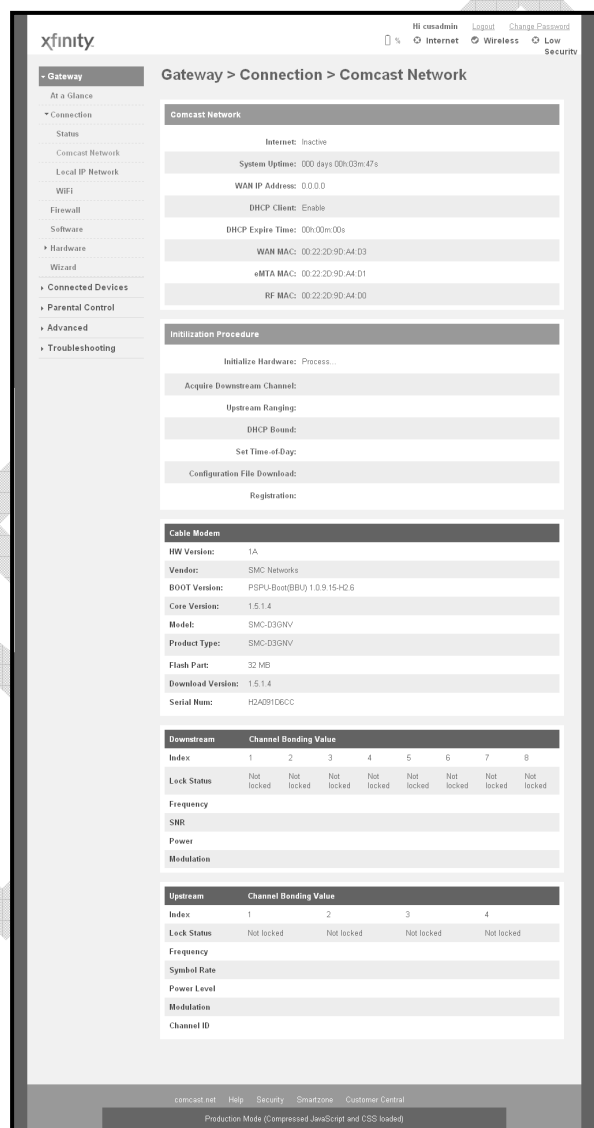


Figure 23. Example of Comcast Network Menu

Viewing and Editing Your Local IP Configuration

The Local IP Configuration menu lets you view and change the Internet Protocol (IP) settings used by the Gateway. Fields are provided for configuring IP version 4 (IPv4) and the newer IP version 6 (IPv6).

To display the Local IP Configuration menu, click **Connection** in the menu bar, and then click the **Local IP Network** submenu. Figure 24 shows an example of the Local IP Configuration menu and Table 6 describes the menu.



Figure 24. Example of Local IP Configuration Menu

Table 6. Local IP Configuration Menu

Option	Description
IPv4 (for computers that use IP v4 Messaging)	
Gateway Address	IPv4 IP address that the Gateway is to use.
Subnet Mask	IPv4 subnet mask that the Gateway is to use.
DHCP Beginning Address	Starting IP address range for the pool of allocated for DHCP IP addresses. The first two fields match the first two octets in the Gateway's IP address and cannot be changed. The last two fields let you enter the final two octets in the starting IP address range.
DHCP Ending Address	Ending IP address range for the pool of allocated for DHCP IP addresses. The first two fields match the first two octets in the Gateway's IP address and cannot be changed. The last two fields let you enter the final two octets in the ending IP address range.
DHCP Lease Time	Amount of time a DHCP network user is allowed connection to the Gateway with their current dynamic IP address. Default is One Week.
SAVE SETTINGS button	After configuring your IPv4 settings, click this button to save them.
RESTORE DEFAULT SETTINGS FOR IPV4 button	Resets the Gateway to the factory default IPv4 settings.
IPv6 (for computers that use IP v6 Messaging)	
Enable IPv6	Check this box to configure the Gateway to use IPv6 settings.
Gateway Address	IPv6 IP address that the Gateway is to use.
Subnet Mask	IPv6 subnet mask that the Gateway is to use.
DHCP Beginning Address	Starting IP address range for the pool of allocated for DHCP IP addresses. The first two fields match the first two octets in the Gateway's IP address and cannot be changed. The last two fields let you enter the final two octets in the starting IP address range.
DHCP Ending Address	Ending IP address range for the pool of allocated for DHCP IP addresses. The first two fields match the first two octets in the Gateway's IP address and cannot be changed. The last two fields let you enter the final two octets in the ending IP address range.
DHCP Lease Time	Amount of time a DHCP network user is allowed connection to the Gateway with their current dynamic IP address. Default is One Week.
IPv6 Mode	Select the IPv6 mode that the Gateway is to use. Choices are: <ul style="list-style-type: none"> • link-local only = allows communication among nodes attached to the same link. Packets are not forwarded outside the site. (<i>default</i>) • site-local only = allows communication among nodes within a site or organization.
SAVE SETTINGS button	After configuring your IPv6 settings, click this button to save them.
RESTORE DEFAULT SETTINGS FOR IPV6 button	Resets the Gateway to the factory default IPv6 settings.

Viewing and Editing Wireless Configuration

The Wireless menu lets you view and change the Gateway's basic and advanced wireless settings. To display the Wireless menu, click **Gateway** in the menu bar, and then click the **Connection** and **WiFi** submenus. Figure 25 shows an example of the Local IP Configuration menu and Table 7 describes the menu.

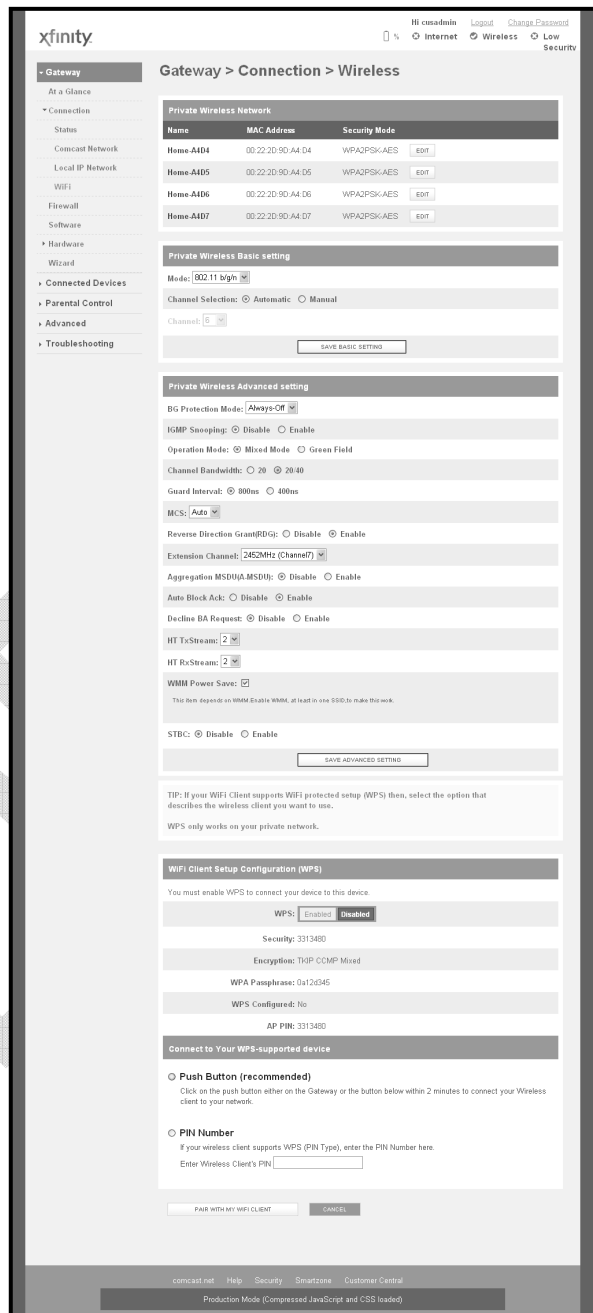


Figure 25. Example of Wireless Menu

Table 7. Wireless Menu

Option	Description
Private Wireless Network	
Name MAC Address Security Mode	Shows the name MAC address, and security setting, if any, for each private wireless network detected. An EDIT button is provided to change these settings.
Private Wireless Basic Setting	
Mode	<p>Choices are:</p> <ul style="list-style-type: none"> • 802.11 b/g = use this setting if you have a combination of IEEE 802.11b and IEEE 802.11g devices on your network. • 802.11n = use this setting if you have only IEEE 802.11n devices on your network or want to limit your network to IEEE 802.11n devices. • 802.11 b/g/n = use this setting if you have a combination of IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n devices on your network. <i>(default)</i>
Channel Selection	<p>Select how the Gateway will select a channel for communicating over the wireless network. Choices are:</p> <ul style="list-style-type: none"> • Automatic = the Gateway selects the channel automatically. <i>(default)</i> • Manual = the Gateway uses the channel specified in the Channel option.
Channel	<p>If the Channel Selection option is Manual, specify the appropriate channel from the list provided to correspond with your network settings. Choices are 1, 6, and 11. The default setting is 6, which refers to radio frequency ranges within the 2.4 GHz range. You can change this setting if necessary; however, all devices in your wireless network must use the same channel to work properly.</p>
SAVE BASIC SETTING button	Click this button to save your changes to the private wireless basic settings.
Private Wireless Advanced Setting	
BG Protection Mode	<p>This mode is a protection mechanism that prevents collisions among 802.11b/g modes. Choices are:</p> <ul style="list-style-type: none"> • Auto = BG protection mode goes on or off automatically as needed. • Always-On = BG protection mode is always on. • Always-Off = BG protection mode is always off. <i>(default)</i>
IGMP Snooping	<p>Enables or disables the Gateway from forwarding multicast traffic intelligently.</p> <ul style="list-style-type: none"> • Enable = Gateway listens to IGMP membership reports, queries, and leave messages to identify the Gateway ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups. • Disable = Gateway does not analyze all IGMP packets. <i>(default)</i>
Operation Mode	<p>Lets you select between Mixed Mode and Green Field.</p> <ul style="list-style-type: none"> • Mixed Mode = provides backward compatibility with IEEE 802.11n/a/g/b devices. <i>(default)</i> • Green Field = used for pure network of 802.11n access points and clients, taking full advantage of the high-throughput capabilities of the 11n multiple-input multiple-output (MIMO) architecture.

錯誤! 使用 [常用] 索引標籤將 **Heading 1** 套用到您想要在此處顯示的文字。

Option	Description
Channel Bandwidth	Select a channel bandwidth of 20 or 20/40. <ul style="list-style-type: none"> • 20 = allows only single-channel operation (e.g., 20 MHz). • 20/40 = allows both single channel operation (20 MHz) and the wider bandwidth operation (40 MHz) by using two or more adjacent (contiguous channels). A 20/40 BSS is a wireless network that allows a wider bandwidth operation mode. (<i>default</i>)
Guard Interval	The guard interval is the period in nanoseconds that the Gateway listens between packets. Choices are: <ul style="list-style-type: none"> • Long = 800 ns guard interval. • Short = 400 ns guard interval. (<i>default</i>)
MCS	Modulation Coding Scheme (MCS) is a specification of PHY parameters consisting of modulation order (BPSK, QPSK, 16-QAM, 64-QAM) and FEC code rate (1/2, 2/3, 3/4, 5/6). MCS is used in the Gateway to define 32 symmetrical settings. MCS provides for potentially greater throughput. High throughput data rates are a function of MCS, bandwidth, and guard interval. Default is auto.
Reverse Direction Grant (RDG)	Speeds up data transmission between the Gateway and 802.11n access points and clients by allowing wireless workstations to send/receive data simultaneously, without contending for shared medium. Default is enable.
Extension Channel	Defines a second 20-MHz channel. 40-MHz stations can use this channel in addition to using the control channel simultaneously.
Aggregation MSDUA (A-MSDU)	Enables or disables aggregation of multiple MSDUs in one MPDU. Default is disable.
Auto-Block Ack	Enables or disables Auto Block ACL function. Default is enable.
Decline BA Request	Enables or disables the BA request function. Default is disable.
HT Tx Stream	Select 1 or 2 from the pull-down menu. Default is 2.
HT Rx Stream	Select 1 or 2 from the pull-down menu. Default is 2.
WMM Power Save	When checked, enables the Gateway's power-management features for optimizing battery life. Default is checked.
STBC	Space Time Block Coding (STBC) is an 802.11n technique intended to improve the reliability of data transmissions. With STBC, the data stream is transmitted on multiple antennas, so the receiving system has a better chance of detecting at least one of the data streams. Choices are: <ul style="list-style-type: none"> • Disable = Gateway does not transmit the same data on multiple antennas. (<i>default</i>) • Enable = Gateway transmits the same data stream on multiple antennas at the same time.
SAVE ADVANCED SETTING button	Click this button to save your changes to the private wireless advanced settings.
WiFi Client Setup Configuration (WP5)	
WPS	Lets you enable or disable Wi-Fi Protected Setup (WPS) on the Gateway. Default is disabled.
Security	A read-only field that shows security information.
Encryption	A read-only field that shows the encryption method, if any, used.
WPA Passphrase	A read-only field that shows the WPA passphrase used by the Gateway. The passphrase is a sequence of words or text that can be used to automatically generate WEP keys.
WPS Configured	A read-only field that whether WPS has been configured.
AP PIN	A read-only field that shows the personal identification number (PIN) for the access point.

錯誤! 使用 [常用] 索引標籤將 **Heading 1** 套用到您想要在此處顯示的文字。

Option	Description
Connect to Your WPS-supported Device	
Push Button	Click this option to use the WPS button on the top panel of the Gateway to configure WPS (see Figure 3).
PIN Number	Click this option if you need to enter a PIN to configure WPS.
Enter Wireless Clients PIN	If you clicked PIN Number , enter the PIN in this field.
Pair with my WiFi Client	Click this button to pair (connect) the Gateway's Wi-Fi settings with your Wi-Fi client.

DRAFT

Configuring Firewall Settings

The Firewall menu lets you view and edit the settings for the Gateway's internal firewall. The setting you select here is displayed at the top-right area of the Gateway's Web interface.

To display the Firewall menu, click **Gateway** in the menu bar, and then click the **Firewall** submenu. Figure 26 shows an example of the Firewall menu and Table 8 describes the menu.

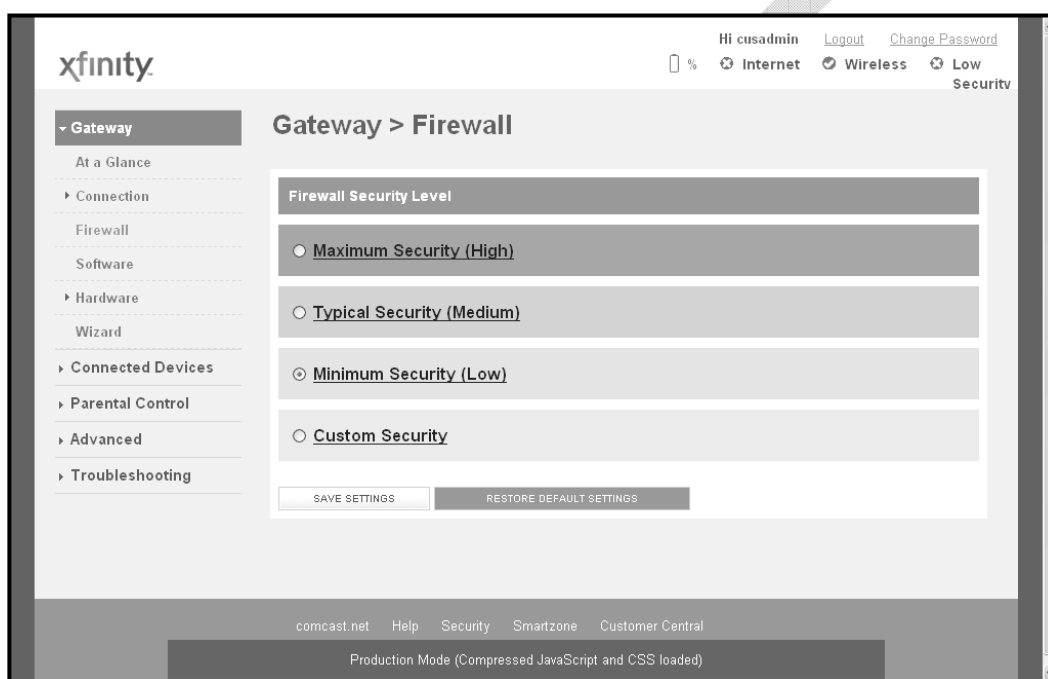


Figure 26. Example of the Firewall Menu

Table 8. Firewall Menu

Option	Description
Maximum Security (High)	Configures the Gateway's firewall to the highest setting. Select this setting for environments where security is critical.
Typical Security (Medium)	Configures the Gateway's firewall for typical (medium) security. Select this setting for environments where security is important.
Minimum Security (Low)	Configures the Gateway's firewall for minimum (low) security. Select this setting for environments where security is not important.
Custom Security	Clicking this option displays the custom security settings in Figure 27. For more information, see Table 9.
SAVE SETTINGS button	After configuring your firewall settings, click this button to save them.
RESTORE DEFAULT SETTINGS button	Resets the Gateway to the factory default firewall settings.

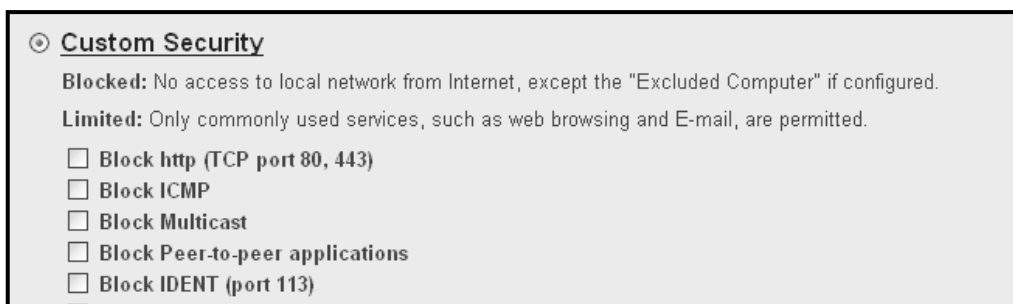


Figure 27. Custom Firewall Security Settings

Table 9. Custom Security Settings

Option	Description
Block http	Blocks Hypertext Transfer Protocol (HTTP) downloads on ports 80 and 443.
Block ICMP	Blocks Internet Control Message Protocol (ICMP) traffic at the outer perimeter of the Gateway to protect against attacks such as cascading ping floods.
Block Multicast	Blocks unsolicited multicast packets.
Block Peer-to-peer application	Blocks peer-to-peer applications
Block IDENT	Blocks identification (Ident) requests from Ident servers on port 113. Note: Port 113 is associated with Ident. If a client program on a computer connected to the Gateway contacts a remote server for services such as POP, IMAP, SMTP, or IRC, the remote server returns a query to the "Ident" server running in many systems listening for these queries on port 113. Essentially, the remote server is asking your system to identify itself and you. This means that port 113 is often probed by attackers as a source of your personal information.
Disable entire firewall	Disables all of the Gateway's firewall settings.

Viewing System Software Settings

The Software menu is a read-only screen that shows the software version and packet cable version associated with the Gateway.

To display the Software menu, click **Gateway** in the menu bar, and then click the **Software** submenu. Figure 28 shows an example of the Software menu.

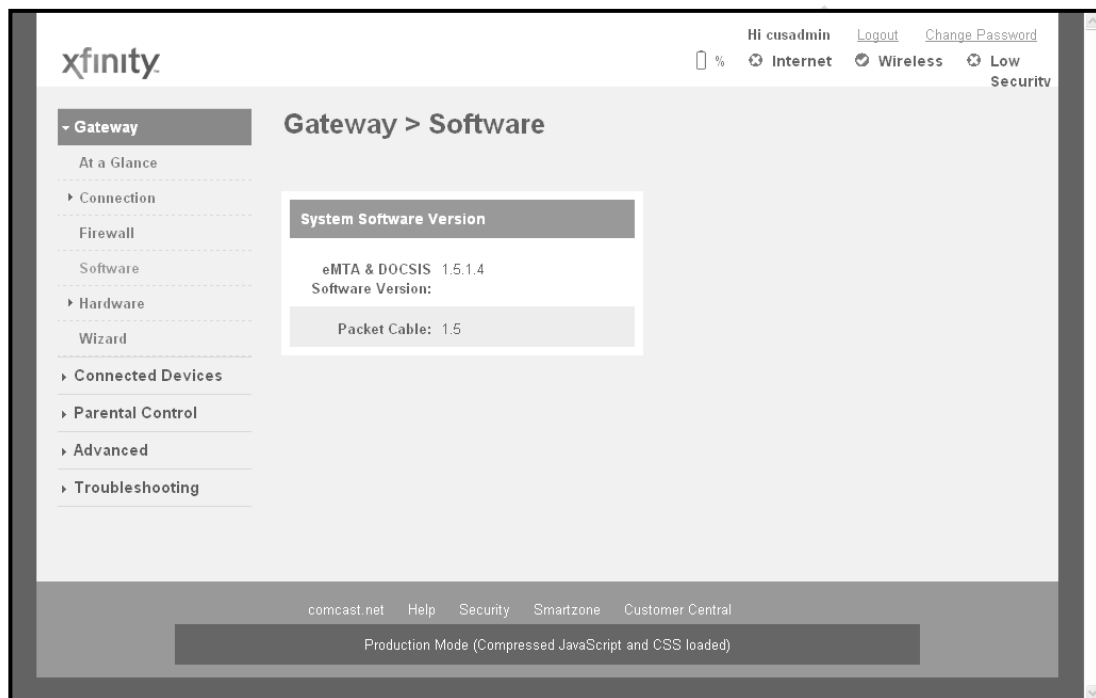


Figure 28. Example of the Software Menu

Configuring System Hardware

Using the Hardware menu, you can:

- View system hardware information. See page 56.
- View information about the Gateway's internal battery. See page 57.
- View the link status and Media Access Control (MAC) address for all four Gateway Ethernet ports. See page 58.
- View the status and MAC address of the Gateway's Wi-Fi port. See page 59.

Viewing System Hardware Settings

The System Hardware menu is a read-only screen that shows the Gateway's system hardware.

To display the System Hardware menu, click **Gateway** in the menu bar, and then click the **Hardware** and **System Hardware** submenus. Figure 29 shows an example of the System Hardware menu.

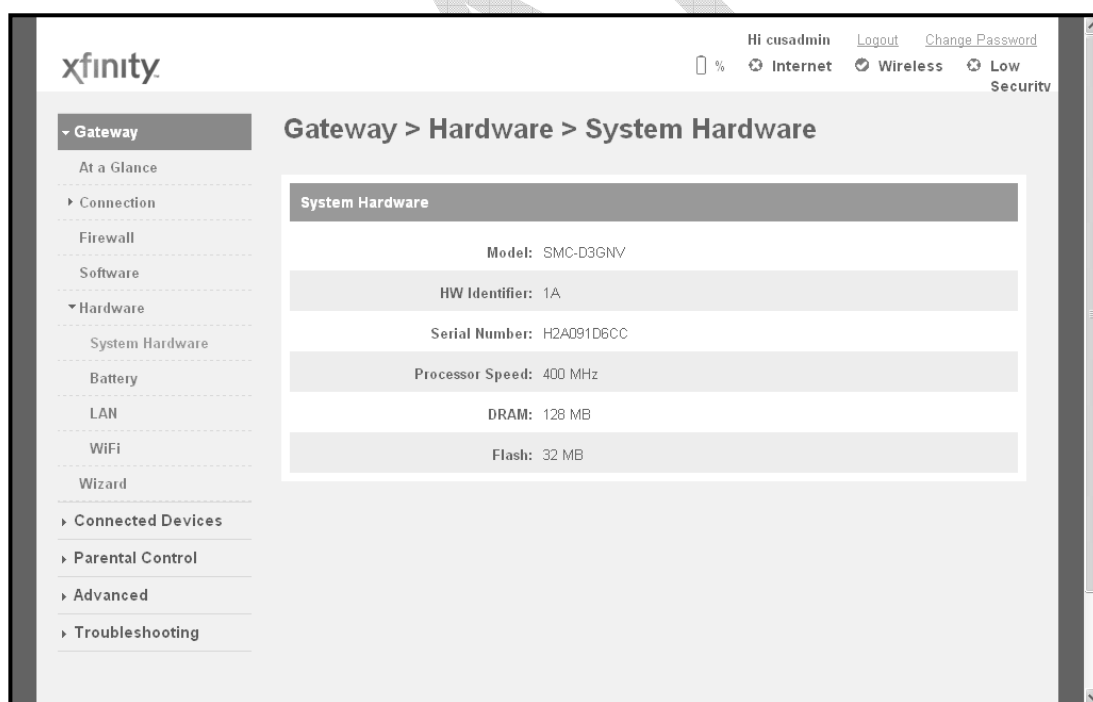


Figure 29. Example of the System Hardware Menu

Viewing Battery Settings

The Battery menu is a read-only screen that shows information about the Gateway's internal battery.

To display the Battery menu, click **Gateway** in the menu bar, and then click the **Hardware** and **Battery** submenus. Figure 30 shows an example of the Battery menu.

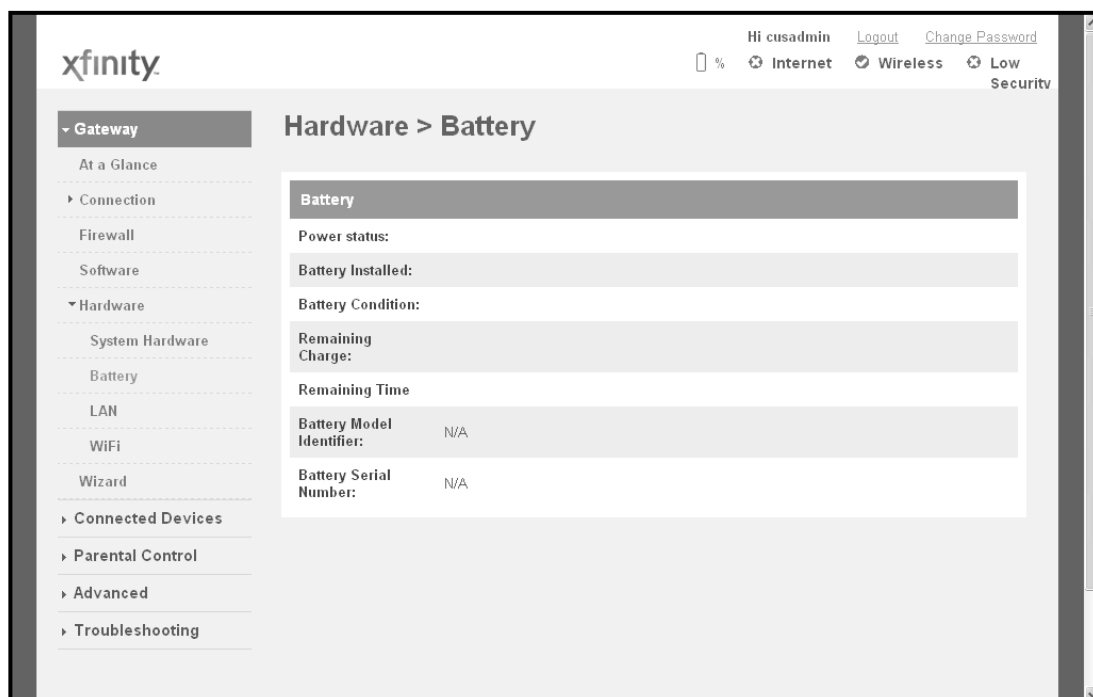


Figure 30. Example of the Battery Menu

Viewing LAN Ethernet Settings

The LAN Ethernet menu is a read-only screen that shows the link status and MAC address of the Gateway's four Ethernet ports.

To display the LAN Ethernet menu, click **Gateway** in the menu bar, and then click the **Hardware** and **LAN** submenus. Figure 31 shows an example of the LAN Ethernet menu.

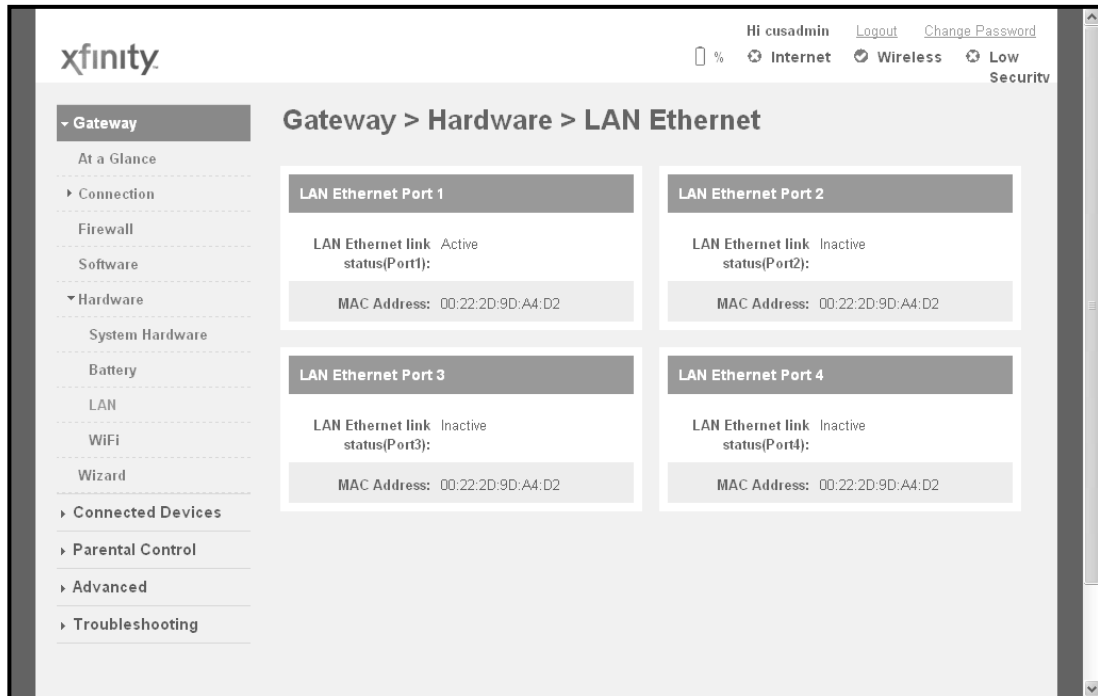


Figure 31. Example of the LAN Ethernet Menu

Viewing Wi-Fi Settings

The WiFi menu is a read-only screen that shows the Wi-Fi link status and MAC address of the Gateway's WiFi port.

To display the WiFi menu, click **Gateway** in the menu bar, and then click the **Hardware** and **WiFi** submenus. Figure 32 shows an example of the WiFi menu.

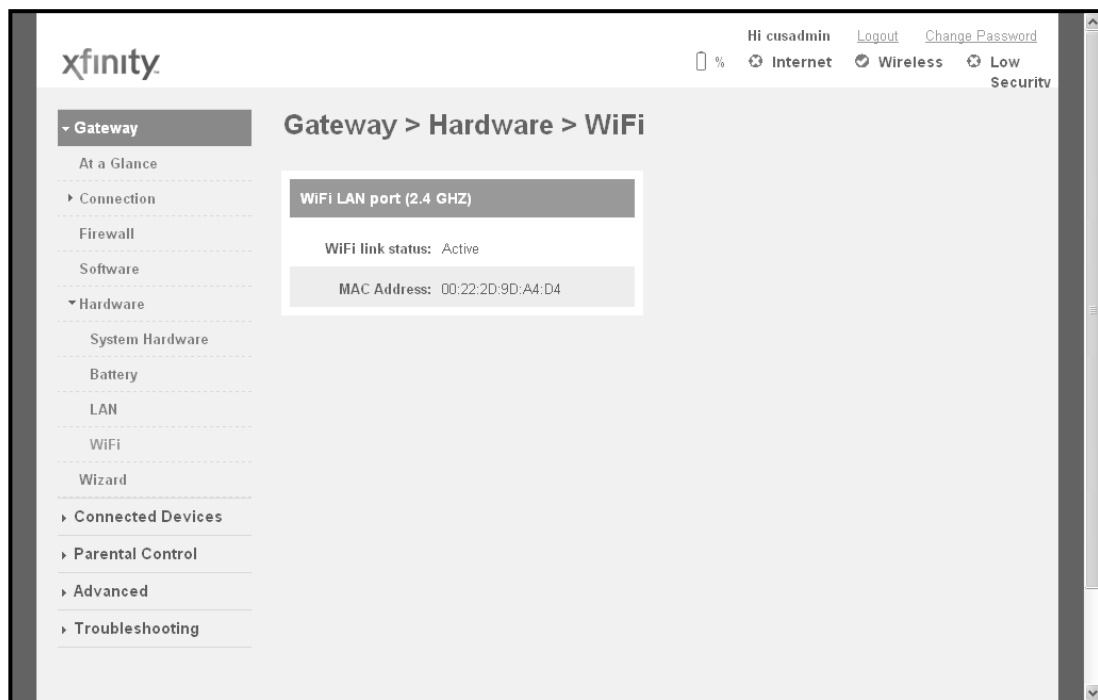


Figure 32. Example of the WiFi Menu

Configuring Your Home Network

The Home Network Wizard menu is part of a 2-page wizard you can use to configure your home network.

To display the first page of the Home Network Wizard, click **Gateway** in the menu bar, and then click the **Wizard** submenu. Figure 33 shows an example of the first page of the Home Network Wizard and Table 10 describes the page.

The screenshot displays the Comcast xfinity Gateway Home Network Wizard interface. At the top left is the xfinity logo. The top right shows the user 'Hi cusaadmin' with links for 'Logout' and 'Change Password'. Below this, there are status indicators for 'Internet', 'Wireless', and 'Low Security'. The main heading is 'Gateway > Home Network Wizard - Step 1'. A left sidebar menu is expanded to 'Gateway', showing sub-items like 'At a Glance', 'Connection', 'Firewall', 'Software', 'Hardware', 'Wizard', 'Connected Devices', 'Parental Control', 'Advanced', and 'Troubleshooting'. The main content area is titled 'Step 1 of 2' and contains a welcome message: 'Welcome to Comcast. To configure your home network, we need some basic information'. Below this are four input fields: 'Gateway Name:', 'Current Password:', 'New Password:', and 'Re-enter New Password:'. A note specifies '8-20 characters. Letter and numbers only. No spaces. Case sensitive.' A 'NEXT STEP' button is located at the bottom of the form. The footer includes 'comcast.net', 'Help', 'Security', 'Smartzone', 'Customer Central', and 'Production Mode (Compressed JavaScript and CSS loaded)'.

Figure 33. Example of the First Page of the Home Network Wizard

Table 10. Home Network Wizard – Step 1

Option	Description
Gateway Name	The name you want to assign to the Gateway. Assign a name so that this device will not be confused with other devices on your wireless network. We recommend you use a name that is meaningful to you so you can identify the Gateway easily. The Gateway name is case sensitive and can contain from 8 to 20 alphanumeric characters, but no spaces.
Current Password	Enter the current case-sensitive password. For security purposes, every typed character appears as a dot (•). The default password is not shown for security purposes. The password is case sensitive and can contain from 8 to 20 alphanumeric characters, but no spaces.
New Password	Enter the new password you want to use. The password is case sensitive and can contain from 8 to 20 alphanumeric characters, but no spaces. Spaces count as password characters. For security purposes, every typed character appears as a dot (•).
Re-enter New Password	Enter the same case-sensitive administrator password you typed in the New Password field. For security purposes, every typed character appears as a dot (•).
NEXT PAGE button	Click this button to display the second page of the Home Network Wizard (see Figure 34 and Table 11).

DRAFT

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

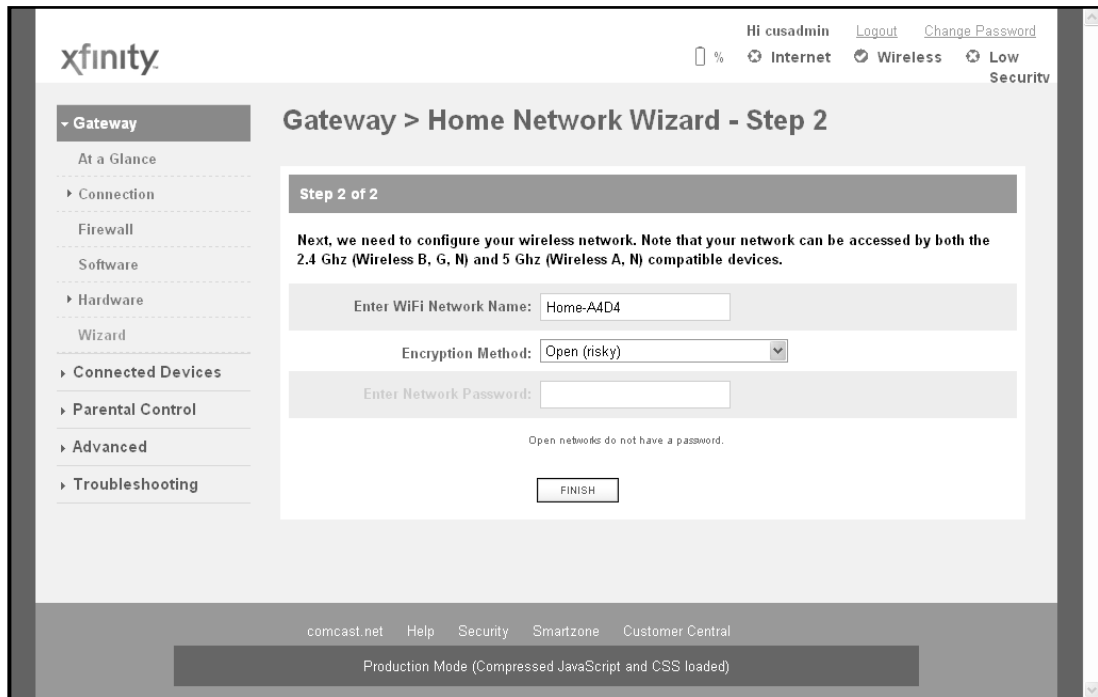


Figure 34. Example of the Second Page of the Home Network Wizard

Table 11. Home Network Wizard – Step 2

Option	Description
Enter WiFi Network Name	Enter the name of your wireless network (typically, the SSID). The Wi-Fi name will make it more obvious for others to know which network they are connecting to.
Encryption Method	<p>The default selection of OPEN means your wireless transmissions are not protected. To prevent other computers in the area from using your Internet connection, secure your wireless network by selecting an encryption method from this drop-down list. There are several encryption methods for wireless settings, including:</p> <ul style="list-style-type: none">• WEP = basic encryption and therefore least secure (i.e., it can be easily cracked, but is compatible with a wide range of devices including older hardware).• WPA (WPA-Personal) = one of the highest levels of wireless security for your network. Select this option if your wireless adapters support WPA.• WPA-2 (Wi-Fi Protected Access version 2) = second generation of WPA. Select this option if your wireless adapters support WPA2.• WPA-Enterprise = provides extremely strong wireless security and adds authentication to WEP's basic encryption. This option is mainly suited for enterprise users, not home users, and can be selected if your wireless adapters support WPA-Enterprise.
Enter Network Password	If you select one of the WEP or WPA encryption settings, enter the password used for encryption and decryption.
Radius Server Address	IP address of the Remote Authentication Dial In User Service (RADIUS) server.
Radius Server Port	Port number that RADIUS uses for authentication. Default is 1812.
FINISH button	Click this button to complete the Home Network Wizard.

Working with Connected Devices

Using the **Computers** menu, you can:

- View the computers that the Gateway has discovered using DHCP or Home Network Administration Protocol (HNAP).
- Manually add computers with static IP addresses to the wireless network.
- Edit computers with static IP addresses
- Disconnect online and offline computers from the wireless network.

To display the **Computers** menu, click **Connected Devices** in the menu bar. Figure 35 shows an example of the Computers menu.

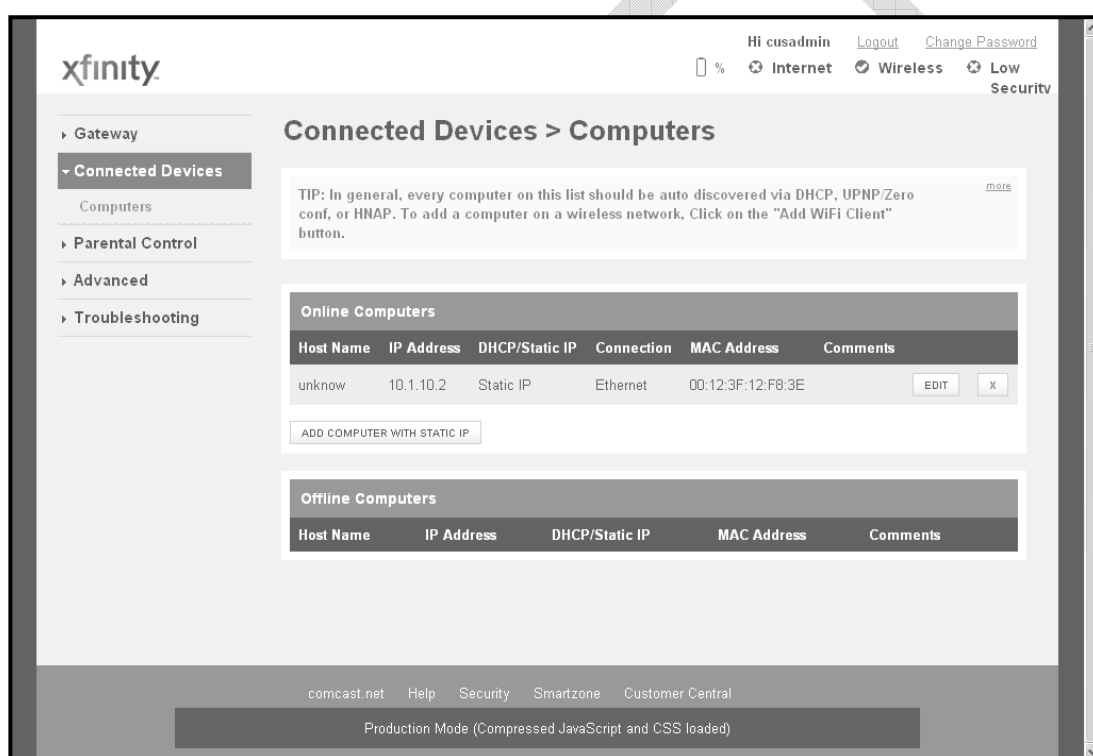
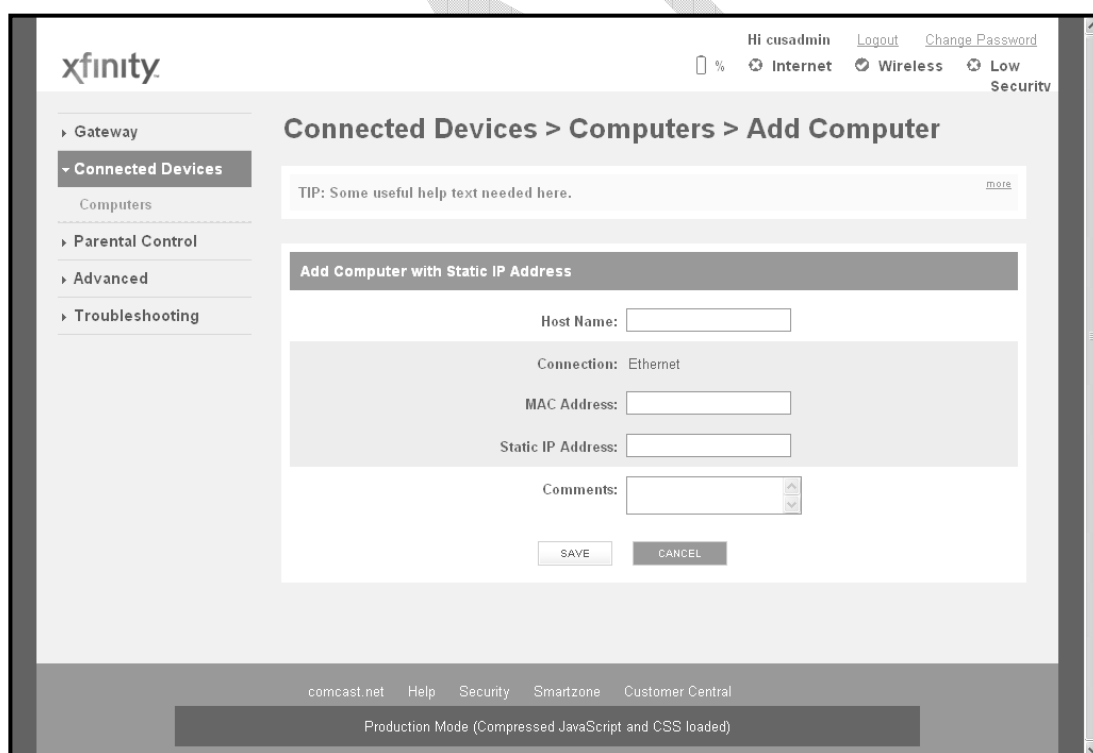


Figure 35. Example of the Computers Menu

Manually Adding Computers with Static IP Addresses to the Wireless Network

To manually add a computer with a static IP address to your wireless network:

5. Under **Online Computers**, click the **ADD COMPUTER WITH STATIC IP** button. The Add Computer menu appears (see Figure 36).
6. Complete the fields in the Add Computer menu (see Table 12).
7. Click **SAVE** to save your settings (or click **CANCEL** to discard them). If you click **SAVE**, the Computer menu reappears, with the computer you added displayed under **Offline Computers**.
8. To add more computers with static IP addresses, repeat steps 1 through 3.
9. To edit an online computer, click the **EDIT** button next to the computer you want to modify, edit the settings on the Edit Computer menu (see Figure 37), and click **SAVE**.
10. To delete an online or offline computer, click the **X** next to the computer. When the Delete Computer message appears, click **OK** to delete the computer or **CANCEL** to retain it. If you clicked **OK**, the computer is removed from the Computers menu.



The screenshot displays the Xfinity web interface for managing connected devices. The breadcrumb trail is "Connected Devices > Computers > Add Computer". The main content area contains a tip: "TIP: Some useful help text needed here." Below this is a form titled "Add Computer with Static IP Address" with the following fields: "Host Name:" (text input), "Connection: Ethernet" (pre-filled), "MAC Address:" (text input), "Static IP Address:" (text input), and "Comments:" (text area with up/down arrows). At the bottom of the form are "SAVE" and "CANCEL" buttons. The left sidebar shows navigation options: Gateway, Connected Devices (selected), Computers, Parental Control, Advanced, and Troubleshooting. The top right shows user information: "Hi cusadmin", "Logout", and "Change Password". The bottom of the page includes links for "comcast.net", "Help", "Security", "Smartzone", and "Customer Central", along with a footer note: "Production Mode (Compressed JavaScript and CSS loaded)".

Figure 36. Example of the Add Computer Menu

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

Table 12. Add Computer Menu

Option	Description
Host Name	Host name of the computer you want to add.
Connection	Read-only field that displays shows the network connection of Ethernet .
MAC Address	MAC address of the computer you want to add. Add a colon between each 2-character ID in the MAC address. For information about obtaining the MAC address of a computer, see "Determining a Computer's MAC Address" on page 196.
Static IP Address	Static IP address of the computer you want to add. Add a period between each octet in the IP address.
Comments	Optional comments about the computer.
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Add Computer menu.

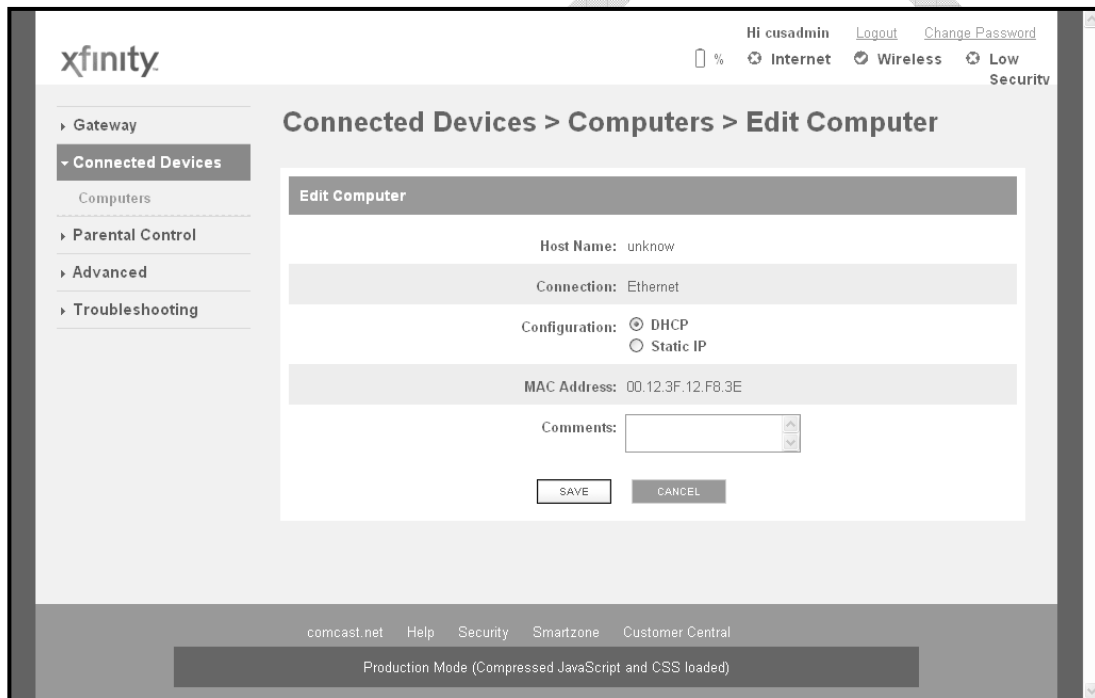


Figure 37. Example of the Edit Computer Menu

Table 13. Edit Computer Menu

Option	Description
HostName	Read-only field that shows the hostname of the computer you selected.
Connection	Read-only field that displays shows the network connection of Ethernet .
Configuration	Select whether the selected computer should be discovered by the Gateway using DHCP or a static IP address. If you select Static IP , enter the static IP address in the Static IP Address field.
MAC Address	Edit the MAC address of the selected computer. Add a colon between each 2-character ID in the MAC address.
Static IP Address	If you selected Static IP for Configuration , enter the computer's static IP address. Add a period between each octet in the IP address.
Comments	Optional comments about the computer.
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Edit Computer menu.

Configuring Parental Controls

Regulating Web browsing can prevent children and workers from accessing dangerous content on the Internet, or having to make judgment calls over suitable relationships in chat-rooms. The fact is, Web sites, chat-room users, and downloaded programs may not have the best interests of you, your family, or your workers at heart. The unscrupulous may try to manipulate the people you care about or try to gain trust, which may result in unacceptable access to your family, your coworkers, your computer, or personal information.

Using the **Parental Controls** menu, you can prevent access to unwanted Web content by:

- Blocking sites and keywords. See page 68.
- Blocking services. See page 75.
- Blocking devices and access types. See page 78.

You can also define report filters and generate reports. See page 82.

Blocking Sites and Keywords, and Selecting Trusted Computers

Using the Managed Sites menu, you can block access to certain Web sites from local computers. To display the Managed Sites menu, click **Parental Control** in the menu bar. Figure 38 shows an example of the Managed Sites menu.

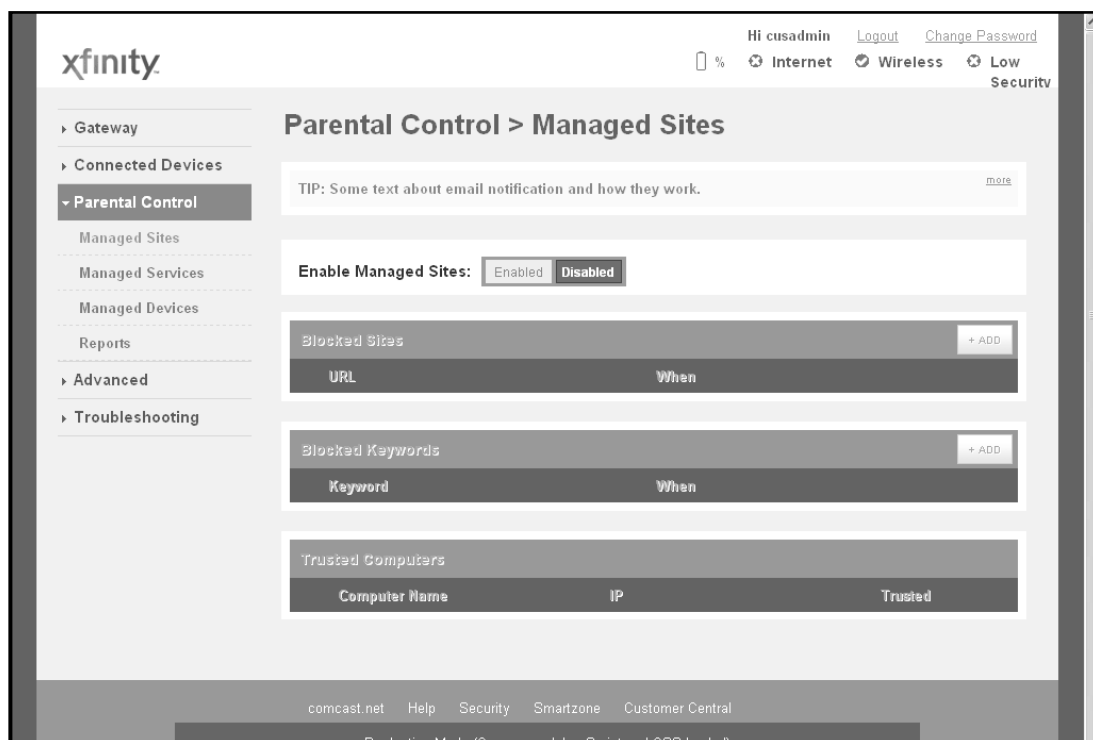


Figure 38. Example of Managed Sites Menu

Blocking Sites

To block sites:

11. If the Managed Sites menu is not displayed, click **Parental Control** in the menu bar.
12. Next to **Enabled Managed Sites**, click **Enabled**.
13. Under **Blocked Sites**, click **ADD**. The Add Blocked Domain menu appears (see Figure 39).
14. Complete the fields in the Add Blocked Domain menu (see Table 14).
15. Click **SAVE** (or click **CANCEL** to discard your settings). If you clicked **SAVE**, the blocked site appears below **Blocked Sites** on the Managed Sites menu.
16. To block additional sites, repeat steps 3 through 5.
17. To edit a blocked site, click the **EDIT** button next to the blocked site you want to modify, edit the settings on the Add Blocked Domain menu (see Table 14), and click **SAVE**.
18. To delete a blocked site, click the **X** next to the site. When the Delete URL Block Rule message appears, click **OK** to delete the blocked URL or **CANCEL** to retain it. If you clicked **OK**, the URL is removed from the **Blocked Sites** area on the Managed Sites menu.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

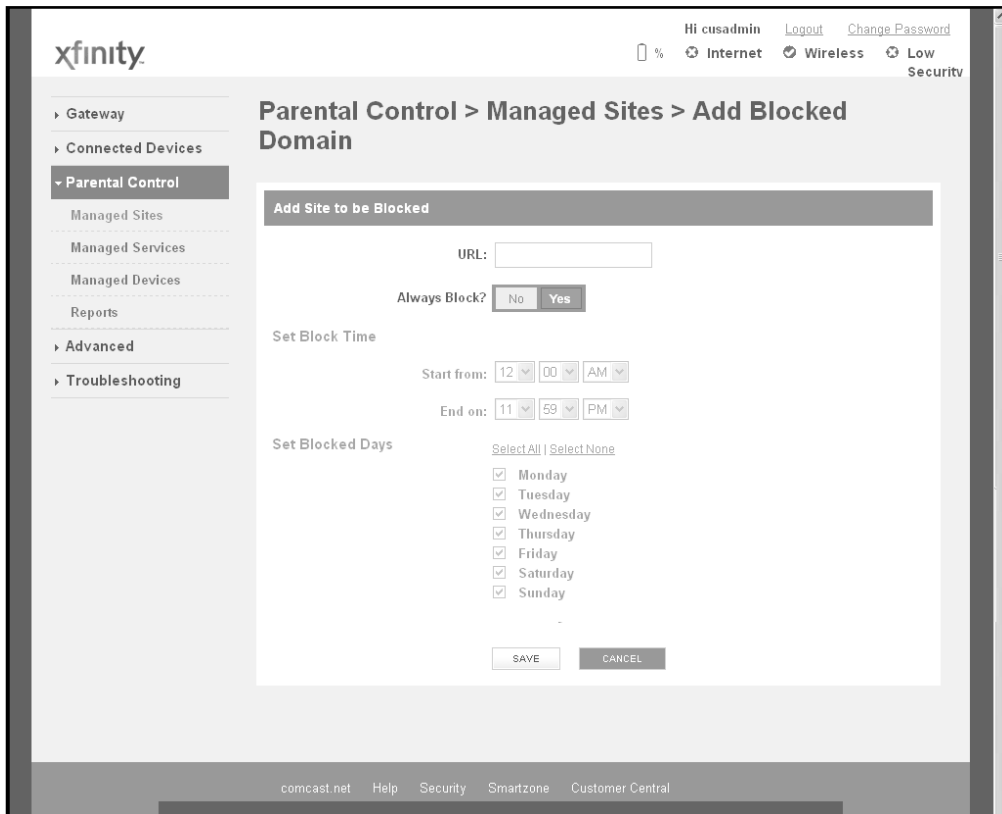


Figure 39. Add Blocked Domain Menu

Table 14. Add Blocked Domain Menu

Option	Description
URL	Enter the URL you want blocked.
Always Block?	Select whether you want the Gateway to always block this URL. Choices are <ul style="list-style-type: none"> • No = the Gateway does not always block this URL. Use the Set Block Time and Set Blocked Days to instruct the Gateway when to block this URL. • Yes = the Gateway always blocks this URL until you remove the block. (<i>default</i>)
Set Block Time	
Start from	If you selected No for Always Block? , select the time when the Gateway is to start blocking this URL.
End on	If you selected No for Always Block? , select the time when the Gateway is to stop blocking this URL.
Set Blocked Days	
Select All	Click this link to select all seven days. This link is not available if you selected Yes for Always Block?
Select None	Click this link to deselect all seven days. This link is not available if you selected Yes for Always Block?
Monday – Sunday	Check the check boxes that correspond to the days when you want the Gateway to block this URL. These checkboxes are not available if you selected Yes for Always Block?
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Add Blocked Domain menu.

Blocking Keywords

To block keywords:

19. If the Managed Sites menu is not displayed, click **Parental Control** in the menu bar.
20. Next to **Enabled Managed Sites**, click **Enabled**.
21. Under **Blocked Keywords**, click **ADD**. The Add Blocked Keyword menu appears (see Figure 40).
22. Complete the fields in the Add Blocked Keyword menu (see Table 15).
23. Click **SAVE** (or click **CANCEL** to discard your settings). If you clicked **SAVE**, the blocked keyword appears below **Blocked Keywords** on the Managed Keywords menu.
24. To block additional keywords, repeat steps 3 through 5.
25. To edit a blocked keyword, click the **EDIT** button next to the blocked keyword you want to modify, edit the settings on the Add Blocked Keyword menu (see Table 15), and click **SAVE**.
26. To delete a blocked keyword, click the **X** next to the keyword. When the Delete Keyword Block Rule message appears, click **OK** to delete the blocked keyword or **CANCEL** to retain it. If you clicked **OK**, the keyword is removed from the **Blocked Keywords** area on the Managed Keywords menu.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

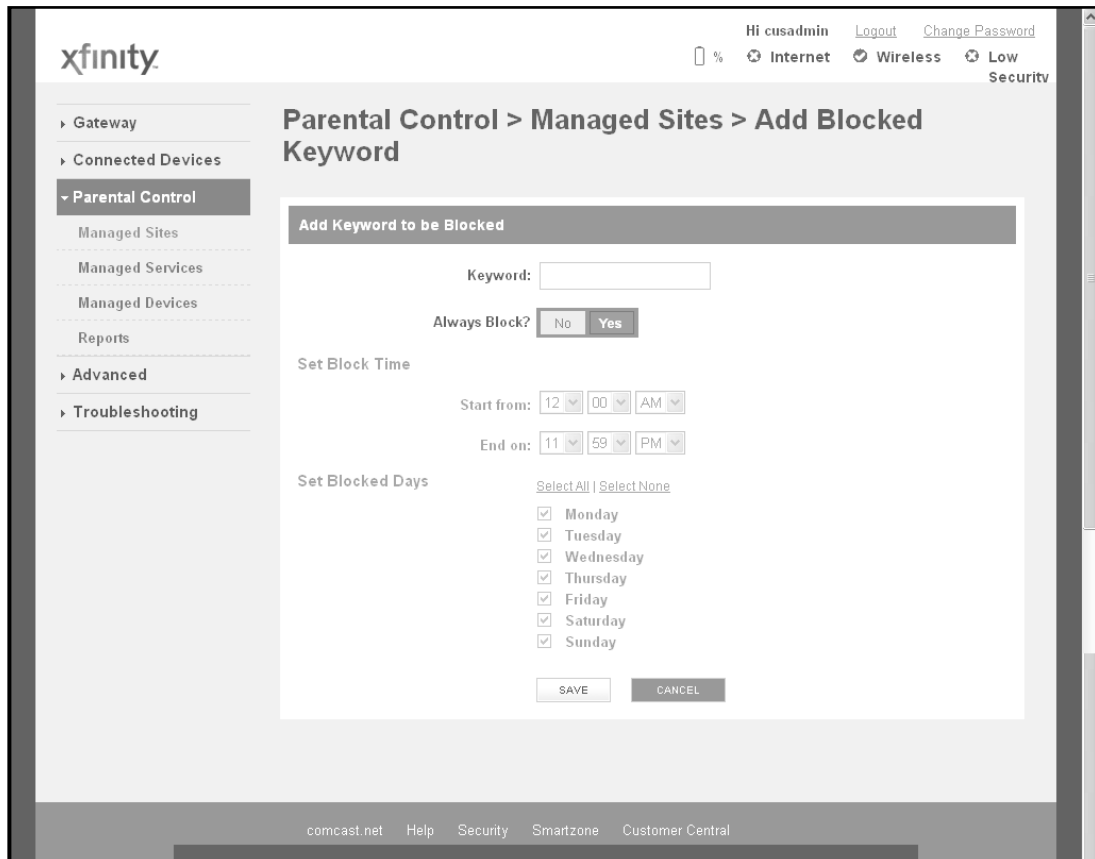


Figure 40. Add Blocked Keyword Menu

Table 15. Add Blocked Keyword Menu

Option	Description
Keyword	Enter the keyword you want blocked.
Always Block?	Select whether you want the Gateway to always block this keyword. Choices are <ul style="list-style-type: none"> • No = the Gateway does not always block this keyword. Use the Set Block Time and Set Blocked Days to instruct the Gateway when to block this Keyword. • Yes = the Gateway always blocks this keyword until you remove the block. (<i>default</i>)
Set Block Time	
Start from	If you selected No for Always Block? , select the time when the Gateway is to start blocking this keyword.
End on	If you selected No for Always Block? , select the time when the Gateway is to stop blocking this keyword.
Set Blocked Days	
Select All	Click this link to select all seven days. This link is not available if you selected Yes for Always Block?
Select None	Click this link to deselect all seven days. This link is not available if you selected Yes for Always Block?
Monday – Sunday	Check the check boxes that correspond to the days when you want the Gateway to block this keyword. These checkboxes are not available if you selected Yes for Always Block?
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Add Blocked Keyword menu.

Blocking Services

Using the Managed Services menu, you can block access to certain services from local computers. This feature can be used to protect children from accessing inappropriate services.

To display the Managed Services menu, click **Parental Control** in the menu bar, and then click the **Managed Services** submenu. Figure 41 shows an example of the menu.

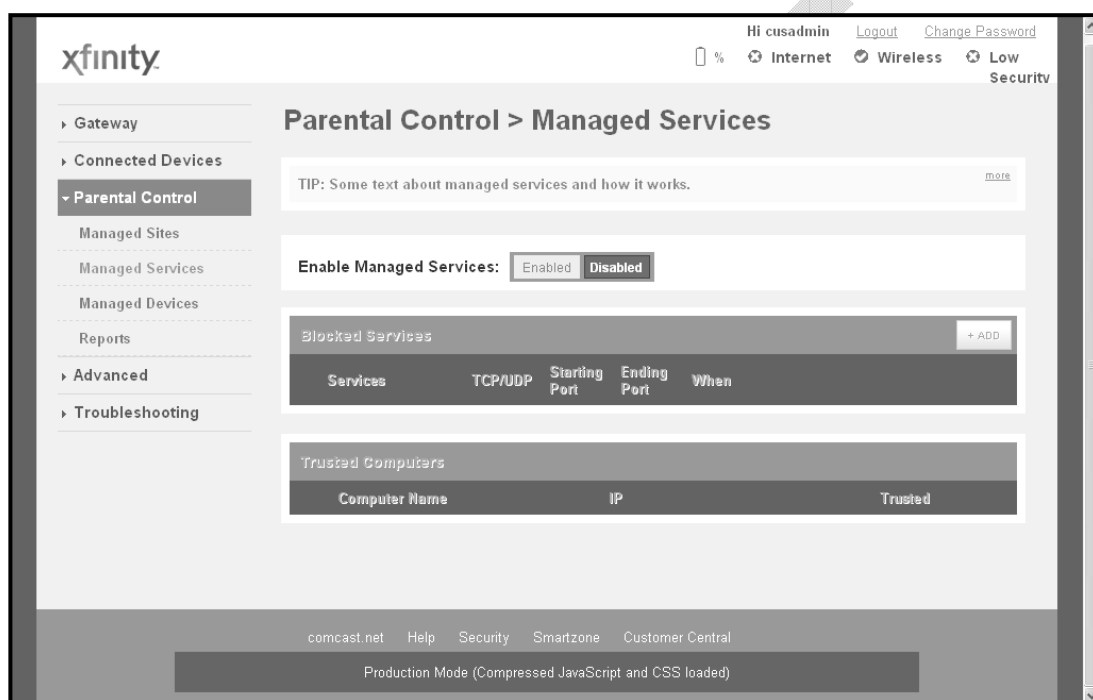


Figure 41. Example of Managed Services Menu

To block services:

27. If the Managed Services menu is not displayed, click **Parental Control** in the menu bar, and then click the **Managed Services** submenu.
28. Next to **Enabled Managed Services**, click **Enabled**.
29. Under **Blocked Services**, click **ADD**. The Add Blocked Service menu appears (see Figure 42).
30. Complete the fields in the Add Blocked Service menu (see Table 16).
31. Click **SAVE** (or click **CANCEL** to discard your settings). If you clicked **SAVE**, the blocked service appears below **Blocked Services** on the Managed Services menu.
32. To block additional services, repeat steps 3 through 5.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

33. To edit a blocked service, click the **EDIT** button next to the blocked service you want to modify, edit the settings on the Add Blocked Service menu (see Table 16), and click **SAVE**.
34. To delete a blocked service, click the **X** next to the service. When the Delete Service Block Rule message appears, click **OK** to delete the blocked URL or **CANCEL** to retain it. If you clicked **OK**, the service is removed from the **Blocked Services** area on the Managed Services menu.

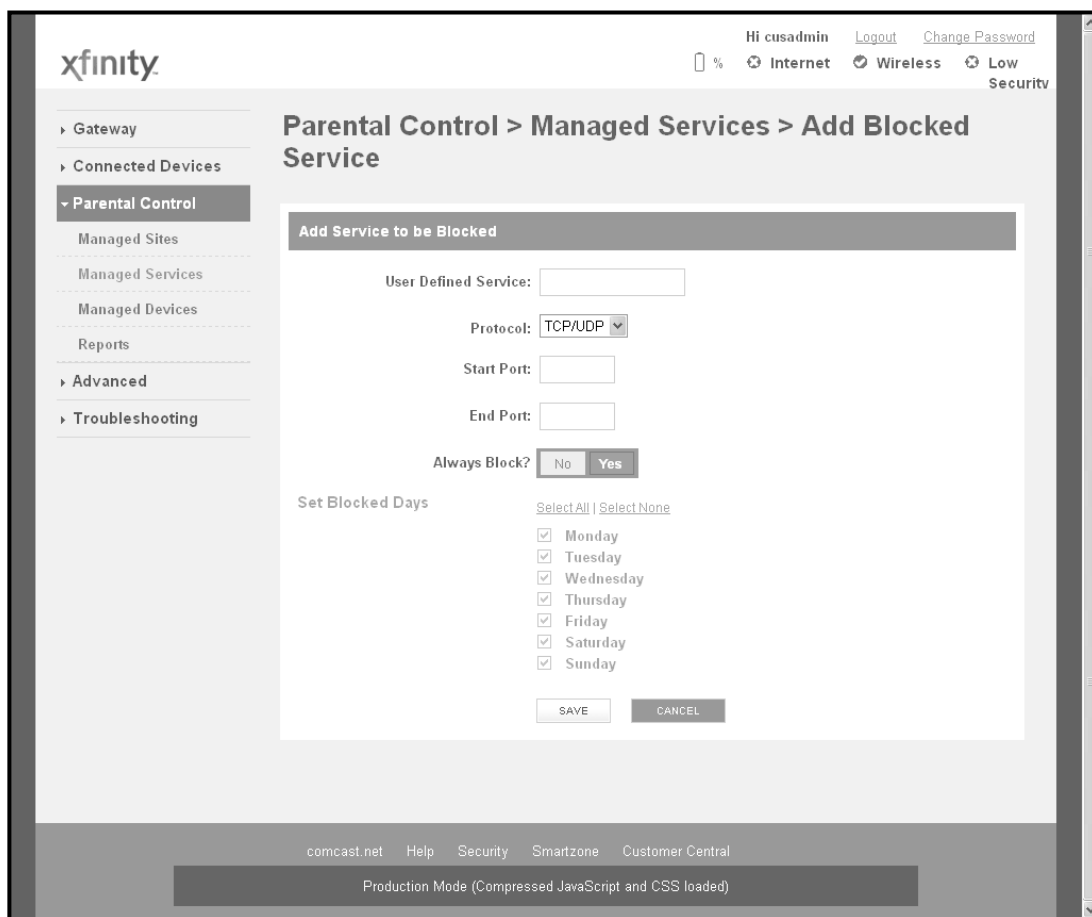


Figure 42. Add Blocked Service Menu

Table 16. Add Blocked Service Menu

Option	Description
User Defined Service	Enter the service you want blocked.
Protocol	The type of protocol associated with the service to be blocked. Choices are: <ul style="list-style-type: none"> • TCP (<i>default</i>) • UDP • TCP/UDP
StartPort	Starting port number on which the block will be applied. If necessary, contact the application vendor for this information.
End Port	Ending port number on which the block will be applied. If necessary, contact the application vendor for this information.
Always Block?	Select whether you want the Gateway to always block this service. Choices are <ul style="list-style-type: none"> • No = the Gateway does not always block this service. Use the Set Block Time and Set Blocked Days to instruct the Gateway when to block this service. • Yes = the Gateway always blocks this service until you remove the block. (<i>default</i>)
Set Block Time	
Start from	If you selected No for Always Block? , select the time when the Gateway is to start blocking this service.
End on	If you selected No for Always Block? , select the time when the Gateway is to stop blocking this service.
Set Blocked Days	
Select All	Click this link to select all seven days. This link is not available if you selected Yes for Always Block?
Select None	Click this link to deselect all seven days. This link is not available if you selected Yes for Always Block?
Monday – Sunday	Check the check boxes that correspond to the days when you want the Gateway to block this service. These checkboxes are not available if you selected Yes for Always Block?
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Add Blocked Domain menu.

Managing Devices and Access Types

Using the Managed Devices menu, you can enable or disable managed devices and allow or block all access types. You can also add devices you want to block.

To display the Managed Devices menu, click **Parental Control** in the menu bar, and then click the **Managed Devices** submenu. Figure 43 shows an example of the menu.

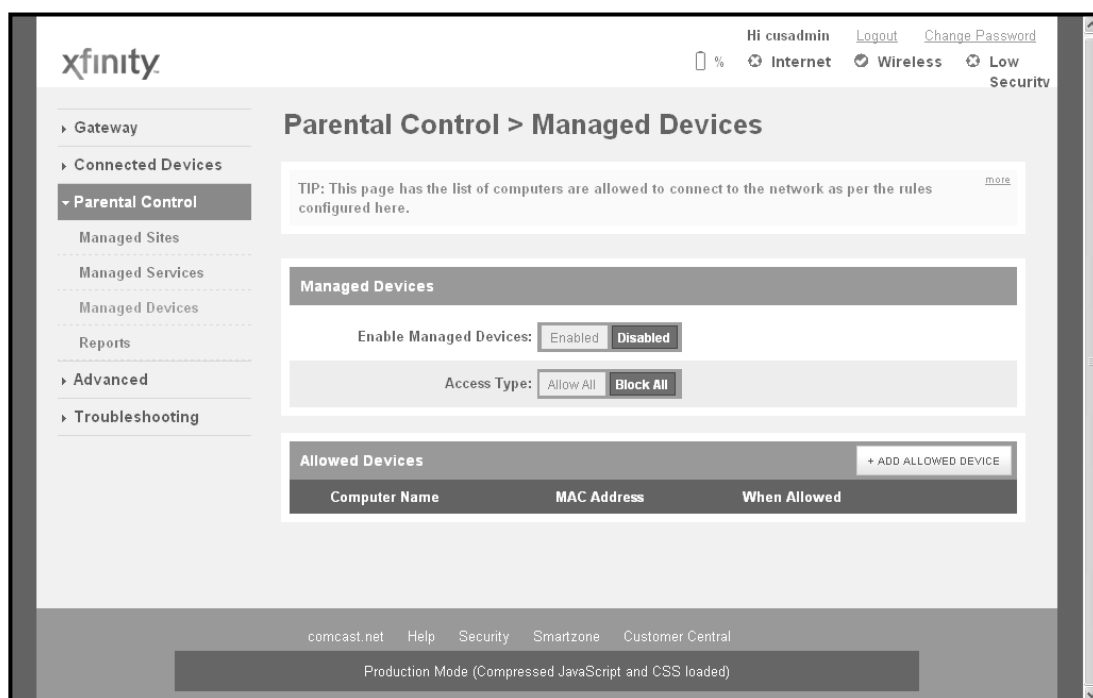


Figure 43. Example of Managed Devices Menu

Enabling or Disabling Managed Devices

By default, all managed devices are disabled. To enable them, click **Enabled** next to **Enable Managed Devices**.

Enabling or Disabling Access Types

By default, all access types are blocked. To unblock them, click **Allow All** next to **Access Type**.

Adding Blocked Devices

To add devices you want to block:

35. If the **Managed Devices** menu is not displayed, click **Parental Control** in the menu bar, and then click the **Managed Devices** submenu.
36. Next to **Blocked Devices**, click **ADD BLOCKED DEVICE**. The Add Blocked Device menu appears (see Figure 44).
37. Completed the fields in the Add Block Device menu (see Table 17).
38. Click **SAVE** (or click **CANCEL** to discard your settings). If you clicked **SAVE**, the blocked device appears below **Blocked Devices** on the Managed Devices menu.
39. To block additional devices, repeat steps 3 through 5.
40. To edit a blocked device, click the **EDIT** button next to the blocked device you want to modify, edit the settings on the Add Blocked Device menu (see Table 17), and click **SAVE**.
41. To delete a blocked device, click the **X** next to the service. When the Delete Blocked MAC Rule message appears, click **OK** to delete the blocked device or **CANCEL** to retain it. If you clicked **OK**, the device is removed from the **Blocked Devices** area on the Managed Devices menu.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

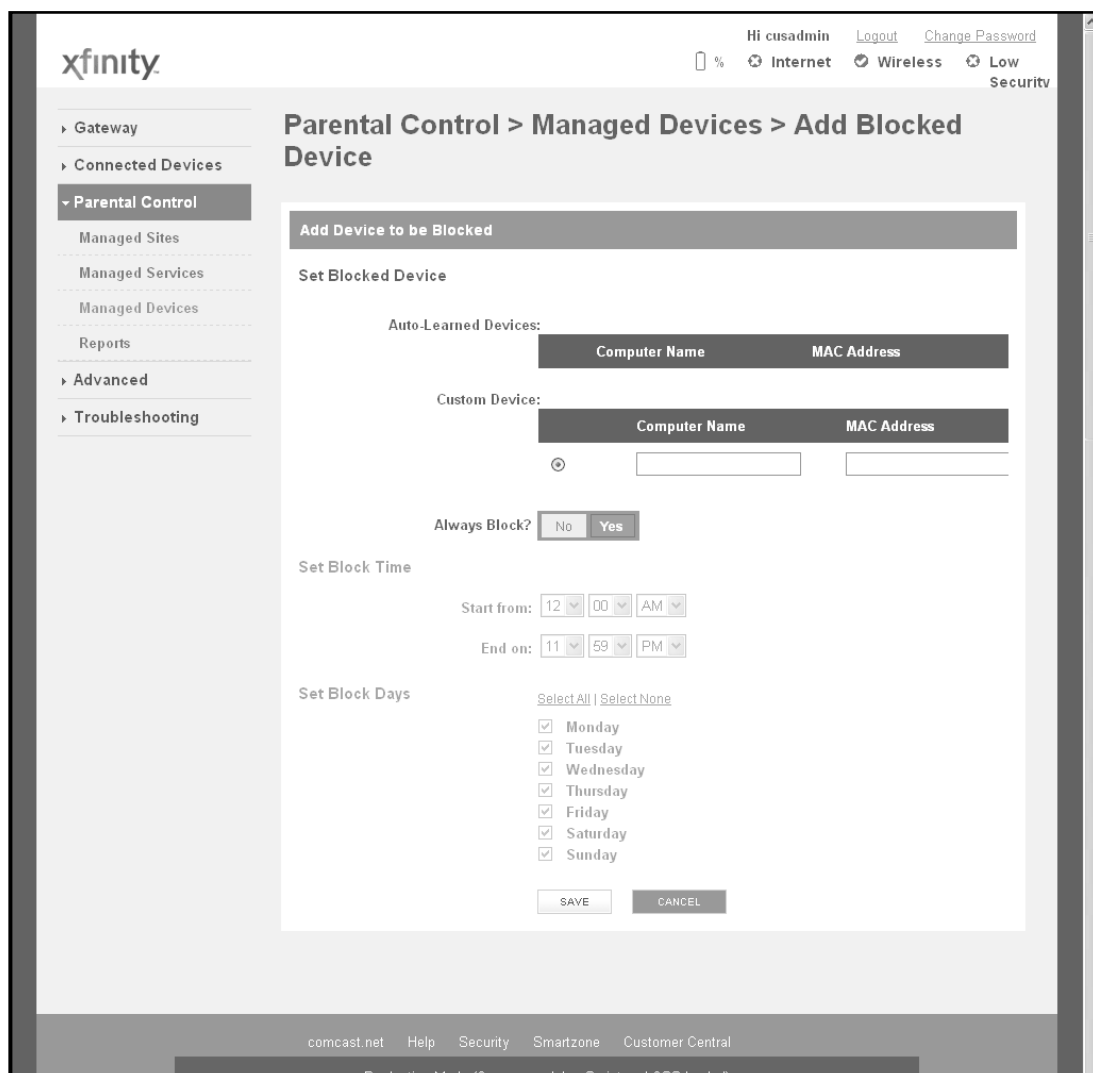


Figure 44. Add Blocked Device Menu

Table 17. Add Blocked Device Menu

Option	Description
Auto-Learned Devices	To select a device that the Gateway automatically learned, select the device under Auto-Learned Devices .
Custom Device	To select a custom device, enter the name and MAC address of the device in the Computer Name and MAC Address fields below Custom Device .
Always Block?	Select whether you want the Gateway to always block this device. Choices are <ul style="list-style-type: none"> • No = the Gateway does not always block this device. Use the Set Block Time and Set Blocked Days to instruct the Gateway when to block this device. • Yes = the Gateway always blocks this device until you remove the block. (<i>default</i>)
Set Block Time	
Start from	If you selected No for Always Block? , select the time when the Gateway is to start blocking this device.
End on	If you selected No for Always Block? , select the time when the Gateway is to stop blocking this device.
Set Blocked Days	
Select All	Click this link to select all seven days. This link is not available if you selected Yes for Always Block?
Select None	Click this link to deselect all seven days. This link is not available if you selected Yes for Always Block?
Monday – Sunday	Check the check boxes that correspond to the days when you want the Gateway to block this device. These checkboxes are not available if you selected Yes for Always Block?
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Add Blocked Device menu.

Generating Reports

The Gateway provides a reporting feature for generating reports containing selected log messages. Using the Reports menu, you can define filters for reports and print or download reports.

To display the Reports menu, click **Parental Control** in the menu bar, and then click the **Reports** submenu. Figure 45 shows an example of the menu.



Note: You can use the Logs menu to apply log filters to reports. For more information. See page 94.

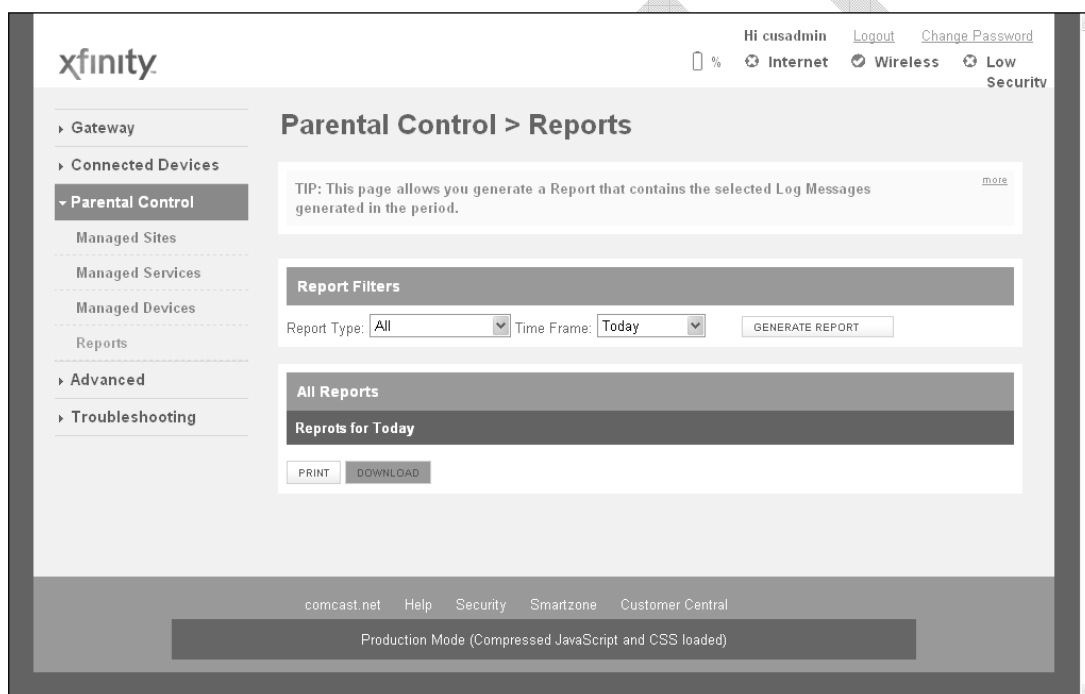


Figure 45. Example of Reports Menu

Defining Report Filters

The **Report Filters** area on the Reports menu lets you select the type of Reports you want to generate and the timeframe that the report is to cover.

To define a report filter:

42. If the Reports menu is not displayed, click **Parental Control** in the menu bar, and then click the **Reports** submenu.
43. Perform the following steps under **Report Filters**:
 - a. Using the **Report Type** drop-down list, select the report to which you want to apply a filter, Choices are:
 - All
 - Managed Sites
 - Managed Services
 - Managed Devices
 - b. By default, the report is generated for today. To change this timeframe, select a different timeframe from the **Time Frame** drop-down list.
 - c. Click **GENERATE REPORT** to apply the filter.

Printing or Downloading the Report

After defining a report filter, use the following steps under **All Reports** to print or download the report:

44. To print the report with the filter applied, click **PRINT**.
45. To download the report with the filter applied, click **DOWNLOAD**.

Using Advanced Features

Using the **Advanced Features** menu, you can:

- Enable or disable port forwarding. See page 84.
- Enable or disable port triggering. See page 87.
- Enable or disable port blocking. See page 91.
- Use the Gateway's UPnP feature to auto-discover devices. See page 92.

Enabling or Disabling Port Forwarding

Using the Firewall menu (described on page 53), you can configure the Gateway to create a firewall between your internal network and the Internet. A firewall keeps unwanted traffic from the Internet away from your networked computers. There may be times, however, when you want a "tunnel" to be created through your firewall, so computers on the Internet can communicate to one of the computers on your LAN using a single port. This is handy for running Web servers, game servers, FTP servers, or even video conferencing.

Port forwarding allows outside users access to the computers on your LAN using a given port or range of ports. Using port forwarding, for example, one of your computers could run a Web server (port 80) while another computer could run an FTP server (port 23) - both using the same IP address.

You configure the Gateway's port forwarding feature using the Port Forwarding menu. To display this menu, click **Advanced** in the menu bar, and then click the **Port Forwarding** submenu in the menu bar. Figure 46 shows an example of the menu.

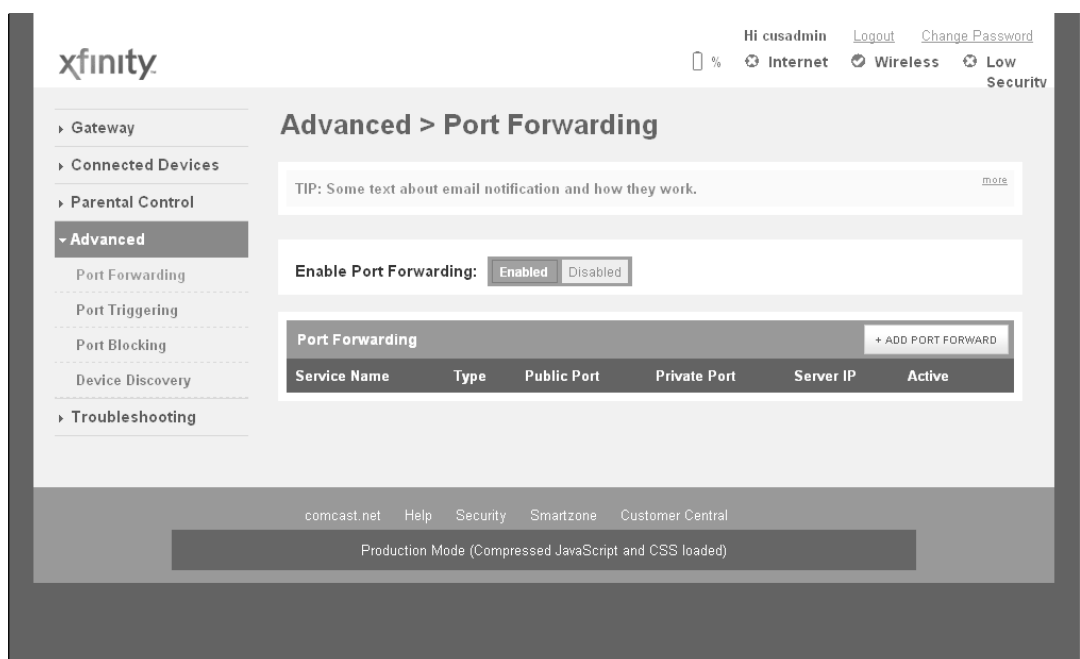


Figure 46. Example of Port Forwarding Menu

Adding a Port Forwarding Rule

To add a port forwarding rule:

46. If the Port Forwarding menu is not displayed, click **Advanced** in the menu bar, and then click the **Port Forwarding** submenu.
47. Confirm that **Enabled** is selected (green) next to **Enable Port Forwarding**. If it isn't click **Enabled**.
48. Click the **ADD PORT FORWARD** button. The Add Service menu appears (see Figure 47).
49. Complete the fields in the Add Service menu (see Table 18).
50. Click **SAVE** to save your settings (or click **CANCEL** to discard them). If you click **SAVE**, the port forwarding rule appears below **Port Forwarding** on the Port Forwarding menu.
51. To add more port forwarding rules, repeat steps 3 through 5.
52. To edit a port forwarding rule, click the **EDIT** button next to the rule you want to modify, edit the settings on the Add Service menu (see Table 17), and click **SAVE**.
53. To delete a port forwarding rule, click the **X** next to the rule. When the Delete Port Forwarding Rule message appears, click **OK** to delete the port forwarding rule or **CANCEL** to retain it. If you clicked **OK**, the rule is removed from the **Port Forwarding** area on the Port Forwarding menu.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

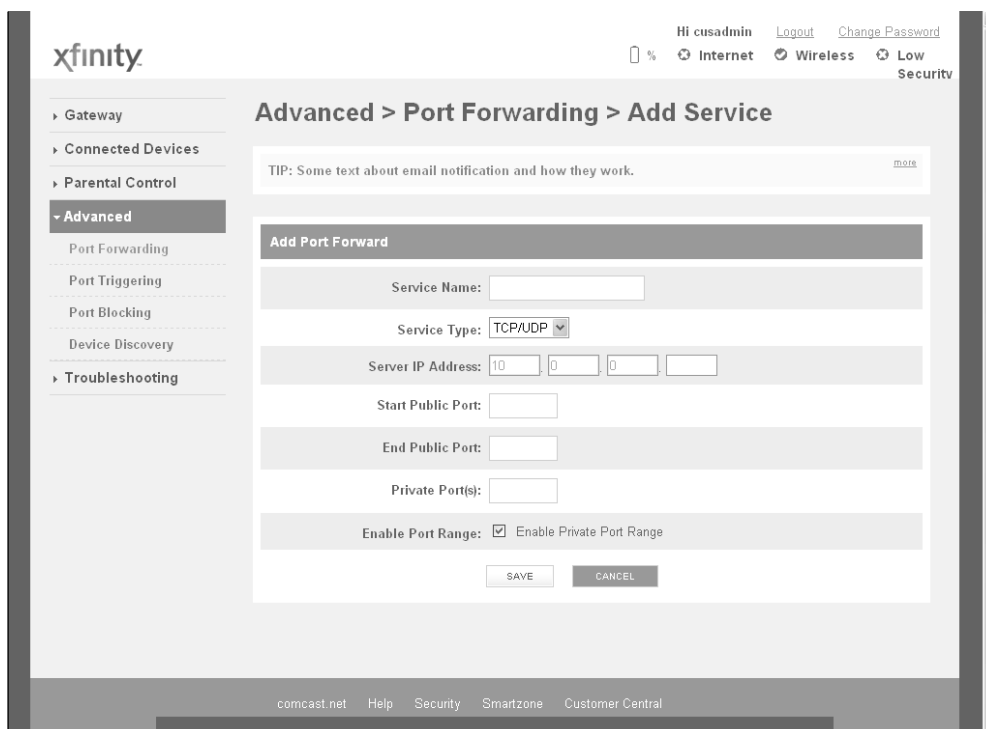


Figure 47. Add Service Menu

Table 18. Add Service Menu

Option	Description
Service Name	Name for identifying the service. The name is for reference purposes only.
Service Type	The protocol you want to use with the service. Choices are: <ul style="list-style-type: none"> • TCP • UDP • TCP/UDP (default)
Service IP Address	IP address of the LAN computer or server that is running the service.
Start Public Port	Starting number of the port on which the service is provided.
End Public Port	Ending number of the port on which the service is provided. This field is unavailable if the Gateway is configured for a single public IP port.
Private Port(s)	Numbers of the ports whose traffic the Gateway forwards to the LAN. If there is a range of ports, enter the starting private port here and check Enable Port Range . The Gateway automatically calculates the end private port. The LAN computer server listens for traffic/data on this port (or these ports).
Enable Port Range	Check this box to enable the private port range specified in Private Port(s) .
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Add Blocked Device menu.

Disabling Port Forwarding

To disable port forwarding:

54. If the Port Forwarding menu is not displayed, click **Advanced** in the menu bar, and then click the **Port Forwarding** submenu.
55. Next to **Enable Port Forwarding**, click **Disabled**. The **ADD PORT FORWARD** button becomes unavailable and all port forwarding rules that have been defined turn gray to show they are disabled.

Enabling Port Forwarding

To enable port forwarding:

1. If the Port Forwarding menu is not displayed, click **Advanced** in the menu bar, and then click the **Port Forwarding** submenu.
2. Next to **Enable Port Forwarding**, click **Enabled**. The **ADD PORT FORWARD** button turns green, and all port forwarding rules that have been defined become available, along with the **EDIT** and delete buttons.

Enabling or Disabling Port Triggering

Using the Port Triggering menu, you can configure the Gateway to detect port triggers for detect multiple-session applications and allow them to pass the firewall. For special applications, besides the initial communication session, there are multiple related sessions created during the protocol communications. Normally, a normal treats the triggered sessions as independent sessions and blocks them. However, the Gateway can co-relate the triggered sessions with the initial session and group them together in the NAT session table. As a result, you need only specify which protocol type and port number you want to track, as well as some other related parameters. In this way, the Gateway can pass the special applications according to the supplied information.

Assume, for example, that to use H.323 in a Net Meeting application, a local client starts a session A to a remote host. The remote host uses session A to communicate with the local host, but it also could initiate another session B back to the local host. Since there is only session A recorded in the NAT session table when the local host starts the communication, session B is treated as an illegal access from the outside and is blocked. Using the Special Application menu, you can configure the Gateway to co-relate sessions A and B and automatically open the port for the incoming session B.

To display the Port Triggering menu, click **Advanced** in the menu bar, and then click the **Port Triggering** submenu in the menu bar. Figure 48 shows an example of the menu.

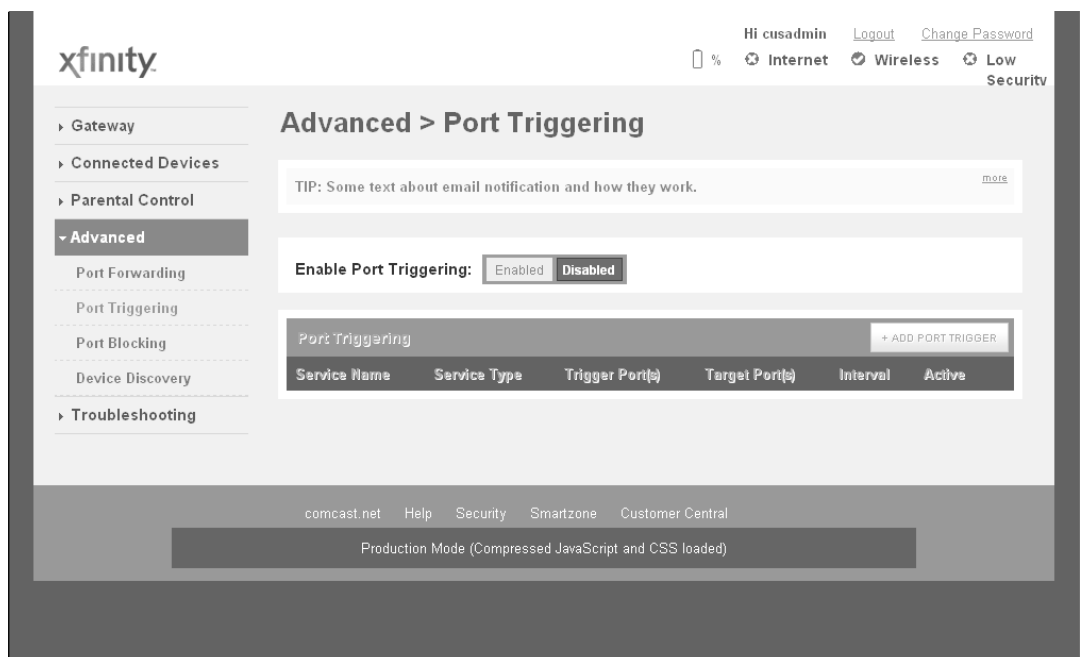


Figure 48. Example of Port Triggering Menu

Adding a Port Triggering Rule

To add a port triggering rule:

3. If the Port Triggering menu is not displayed, click **Advanced** in the menu bar, and then click the **Port Triggering** submenu.
4. Next to **Enable Port Triggering**, click **Enabled**.
5. Click the **ADD PORT FORWARD** button. The Port Triggering Add menu appears (see Figure 49).
6. Complete the fields in the Port Triggering Add menu (see Table 19).
7. Click **SAVE** to save your settings (or click **CANCEL** to discard them). If you click **SAVE**, the port triggering rule appears below **Port Triggering** on the Port Triggering menu.
8. To add more port triggering rules, repeat steps 3 through 5.
9. To edit a port triggering rule, click the **EDIT** button next to the rule you want to modify, edit the settings on the Port Triggering Add menu (see Table 19), and click **SAVE**.
10. To delete a port triggering rule, click the **X** next to the rule. When the Delete Port Triggering Rule message appears, click **OK** to delete the port triggering rule or **CANCEL** to retain it. If you clicked **OK**, the rule is removed from the **Port Triggering** area on the Port Triggering menu.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

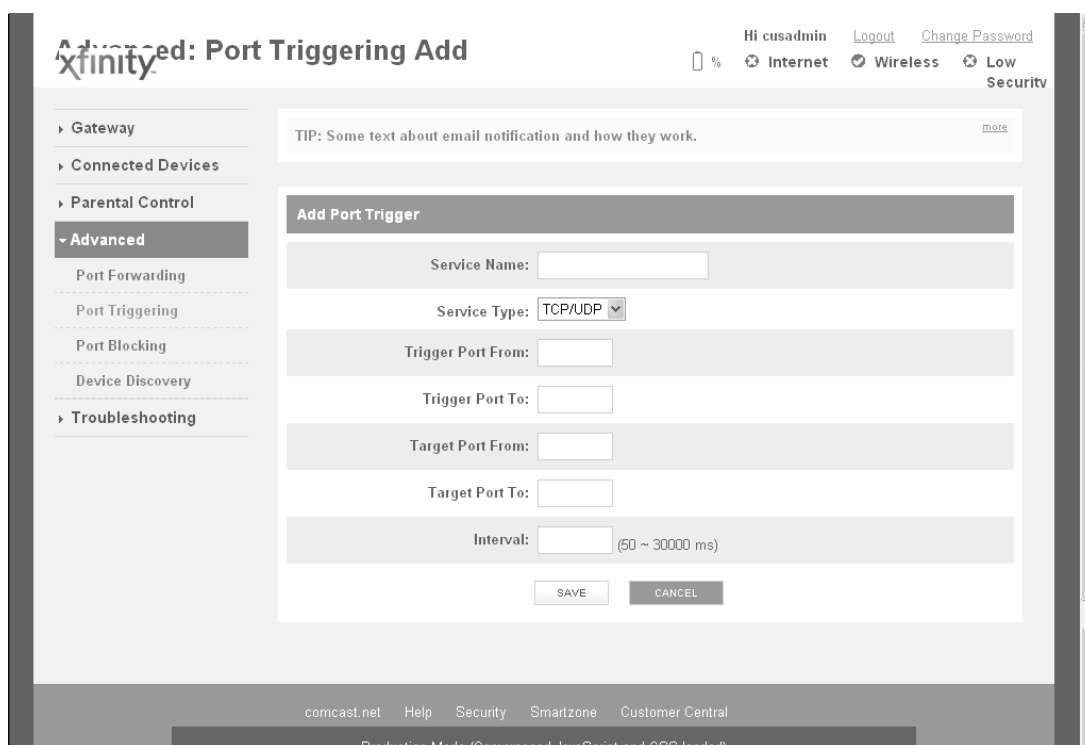


Figure 49. Port Triggering Add Menu

Table 19. Port Triggering Add Menu

Option	Description
Service Name	Name for identifying the trigger. The name is for reference purposes only.
Service Type	The type of protocol you want to use with the trigger. Choices are: <ul style="list-style-type: none"> • TCP • UDP • TCP/UDP (<i>default</i>) For example, to track the H.323 protocol, the protocol type should be TCP.
Trigger Port From	From port ranges of the special application. For example, to track H.323 protocol, the From port should be 1720.
Trigger Port To	To port ranges of the special application. For example, to track H.323 protocol, the To port should be 1720.
Target Port From	Starting port range for the target port listening for the special application.
Target Port To	Ending port range for the target port listening for the special application.
Interval	Specify the interval between 50 and 30000 between two continuous sessions. If the interval exceeds this time interval setting, the sessions are considered to be unrelated.
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Add Blocked Device menu.

Disabling Port Triggering

To disable port triggering:

1. If the Port Triggering menu is not displayed, click **Advanced** in the menu bar, and then click the **Port Triggering** submenu.
2. Next to **Enable Port Triggering**, click **Disabled**. The **ADD PORT TRIGGER** button becomes unavailable and all port triggering rules that have been defined turn gray to show they are disabled.

Enabling Port Triggering

To enable port triggering:

1. If the Port Triggering menu is not displayed, click **Advanced** in the menu bar, and then click the **Port Triggering** submenu.
2. Next to **Enable Port Triggering**, click **Enabled**. The **ADD PORT TRIGGER** button turns green, and all port triggering rules that have been defined become available, along with the **EDIT** and delete buttons.

DRAFT

Enabling or Disabling Port Blocking

By default, all four Ethernet ports on the Gateway are enabled and configured to auto-negotiate the highest speed and duplex settings. If these settings prevent the Gateway from connecting with other devices, you can use the Port Blocking menu to configure the Gateway's Ethernet ports to use specific speed and duplex settings. The Port Blocking menu also let you disable the Ethernet ports. Each port can be configured or disabled independently of the other Ethernet ports on the Gateway.

To display the Port Blocking menu, click **Advanced** in the menu bar, and then click the **Port Blocking** submenu in the menu bar. Figure 50 shows an example of the menu.

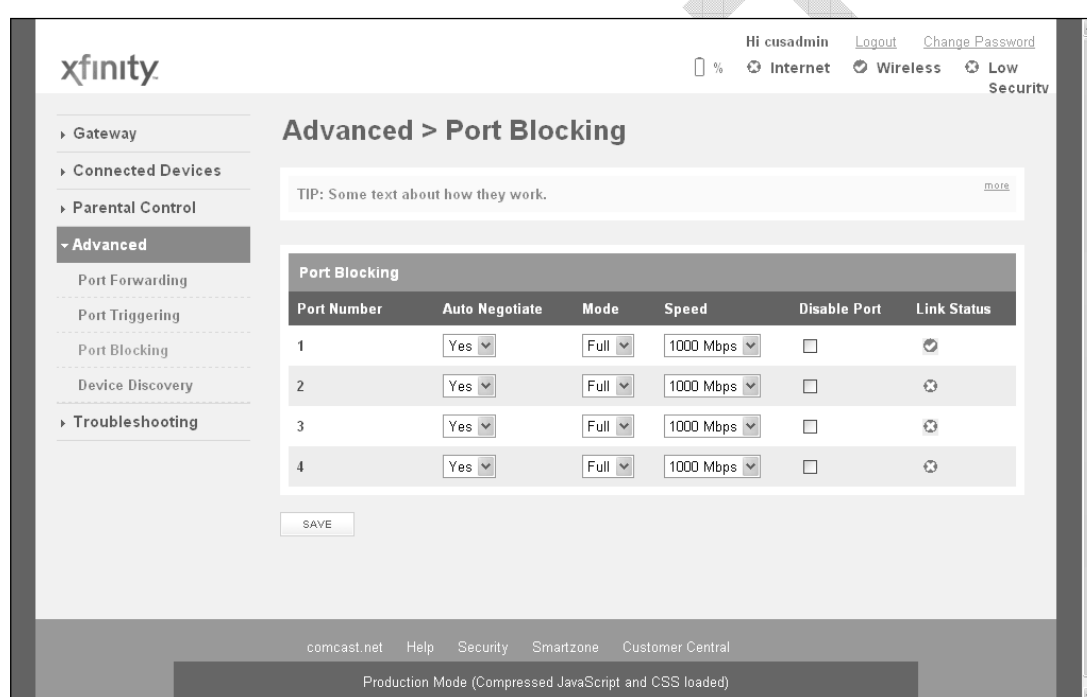


Figure 50. Example of Port Blocking Menu

To change a port from its default settings, perform the following procedure on the row that corresponds to the Ethernet port you want to configure.

3. Under the **Auto Negotiate** column, select **No**.
4. Under the **Mode** column, select **Full** for full-duplex or **Half** for half-duplex to force the selected port to use the duplex setting you select.
5. Under **Speed**, select the fixed speed that the port will use.
6. To disable the port, check the checkbox in the **Disable Port** column.
7. Click the **SAVE** button.



Note: If you disable the port through which you are accessing the Gateway's Web interface, you are disconnected and your session ends. You can reconnect to the Gateway using one of the other enabled LAN ports.

Discovering Devices

Using the Device Discovery menu, the Gateway can obtain protocol addresses of neighboring devices and discover the platform of those devices.

To display the Device Discovery menu, click **Advanced** in the menu bar, and then click the **Device Discovery** submenu in the menu bar. Figure 51 shows an example of the menu and Table 20 describes it.

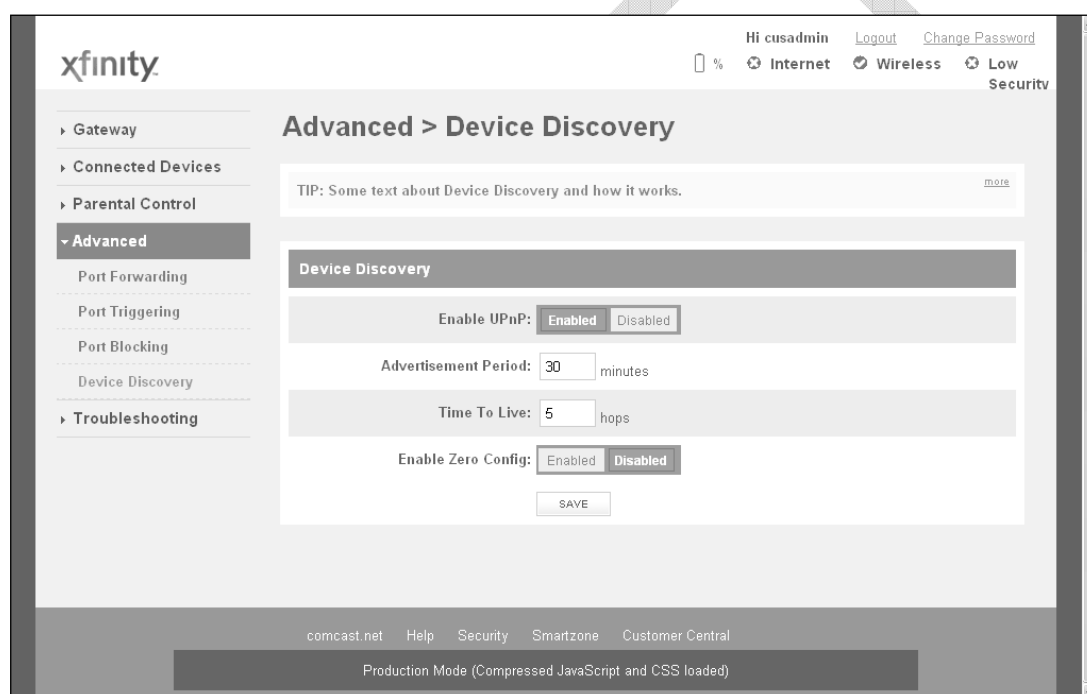


Figure 51. Example of Device Discovery Menu

Table 20. Device Discovery Menu

Option	Description
Enable UPnP	<p>Determines whether the Gateway uses its UPnP feature to communicate with other devices or your operating system.</p> <ul style="list-style-type: none">• Enabled = allows the Gateway to use its UPnP feature to communicate with other devices or your operating system. (<i>default</i>)• Disabled = prevents the Gateway from using its UPnP feature to communicate with other devices or your operating system. Also, may be disabled if your operating system does not support UPnP.
Advertisement Period	<p>How often the Gateway broadcasts its UPnP information (if UPnP is enabled). This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations can compromise the freshness of the device status, but can significantly reduce network traffic.</p>
Time To Live	<p>A counting mechanism to determine how long a packet is valid before it reaches its destination. Each time a TCP/IP packet passes through a router, it decrements its Time To Live count. When the count reaches zero, the packet is dropped by the router. This ensures that errant routing and looping aimless packets will not flood the network. The number of hops can range from 1 to 255. The default value is 5 hops, which should be fine for most networks. If you notice that some devices are not being updated or reached correctly, you might want to increase this value slightly.</p>
Enable Zero Config	<p>Determines whether zero configuration is enabled or disabled. Zero configuration networking automatically creates a usable IP network, without manual operator intervention or special configuration servers. It allows nonexpert users to connect computers, networked printers, and other network devices and expect a functioning network to be established automatically.</p> <ul style="list-style-type: none">• Enabled = enables support for zero configuration.• Disabled = disables support for zero-configuration (<i>default</i>)
SAVE button	<p>Click this button to save your settings.</p>

Troubleshooting the Gateway

Using the **Troubleshooting** menu, you can:

- Define log filters. See page 94.
- Test connectivity to a destination or IP address. See page 96.
- Reset the Gateway, reset your Wi-Fi router, or restore the Gateway to its factory default settings. See page 98.
- Change the password used to log in to the Gateway's Web interface. See page 99.



Note: For additional troubleshooting procedures, see Chapter 6.

Defining Log Filters

Using the Logs menu, you can define the filters applied to the Gateway's system, event, and firewall logs. You can also specify the timeframe to be covered by the logs, as well as download and print the logs.

To display the Logs menu, click **Troubleshooting** in the menu bar, and then click the **Logs** submenu in the menu bar. Figure 52 shows an example of the menu.

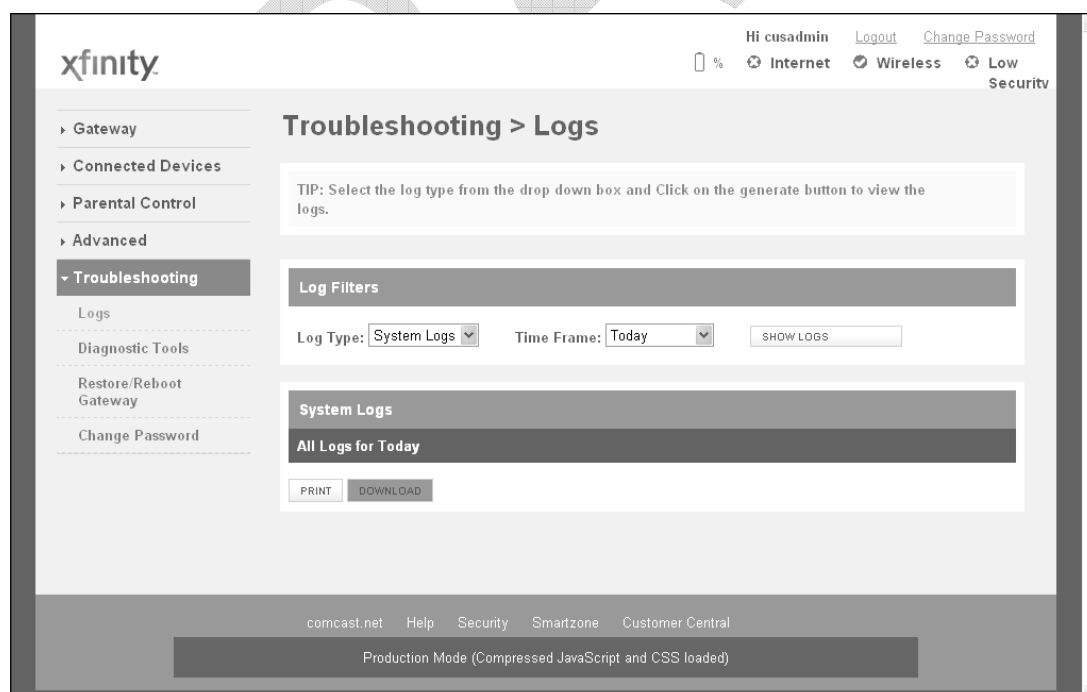


Figure 52. Example of the Logs Menu

Defining Log Filters

The **Log Filters** area on the Logs menu lets you select the type of logs you want to generate and the timeframe that the log is to cover.

To define a log filter:

1. If the Logs menu is not displayed, click **Troubleshooting** in the menu bar, and then click the **Logs** submenu.
2. Perform the following steps under **Log Filters**:
 - a. Using the **Log Type** drop-down list, select the log to which you want to apply a filter, Choices are:
 - System Logs
 - Event Logs
 - Firewall Logs
 - b. By default, the log is generated for today. To change this timeframe, select a different timeframe from the **Time Frame** drop-down list.
 - c. Click **SHOW LOGS** to apply the filter.

Printing or Downloading Log

After defining a log filter, use the following steps under **System Logs** to print or download the log:

1. To print the log with the filter applied, click **PRINT**.
2. To download the log with the filter applied, click **DOWNLOAD**.

Testing Connectivity to Destination and IP Addresses

There may be times when you encounter a problem trying to reach a certain destination. If you examine the Gateway's configuration and operation and everything looks fine, the problem might be with a router up the line from the Gateway or with the line itself.

To help you identify such issues, the Network Diagnostic Tools menu lets you test connectivity to a destination or IP address. To display the Network Diagnostic Tools menu, click **Troubleshooting** in the menu bar, and then click the **Diagnostic Tools** submenu in the menu bar. Figure 53 shows an example of the menu.

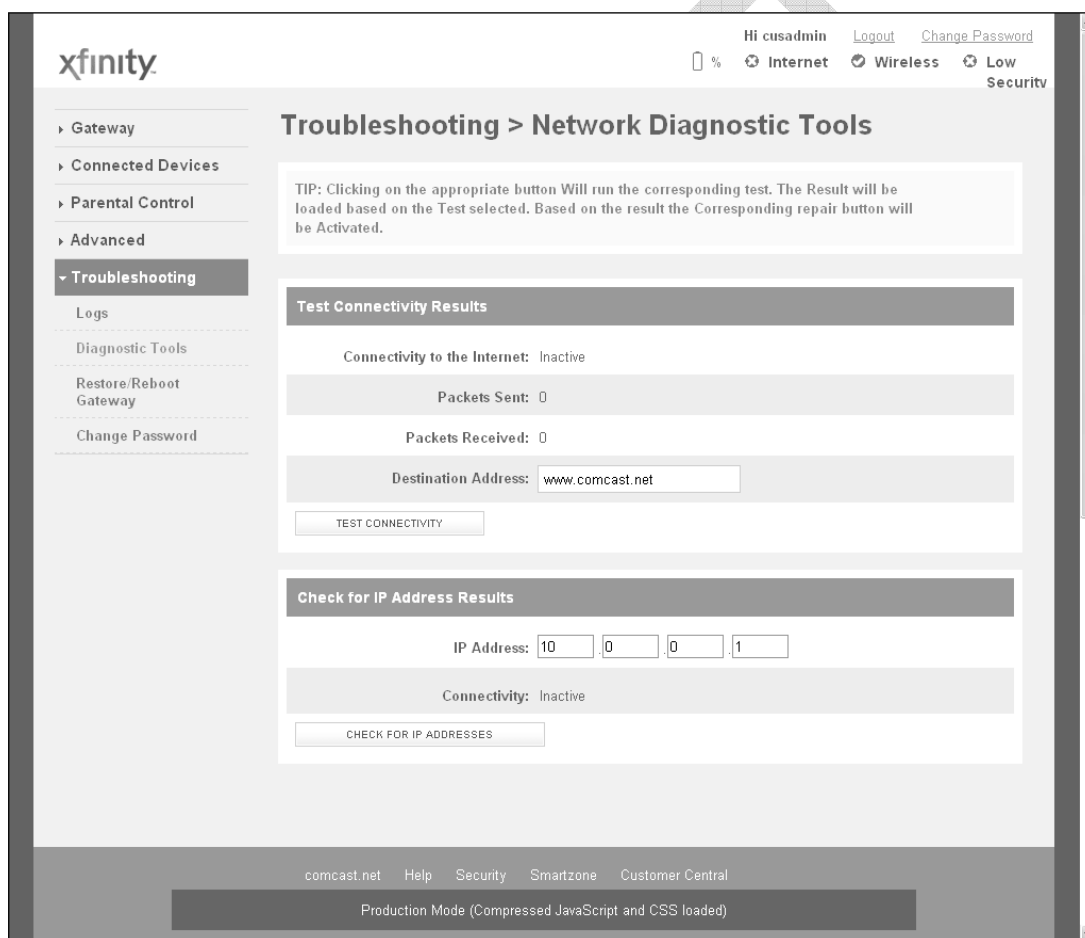


Figure 53. Example of the Network Diagnostic Tools Menu

Testing Connectivity to a Destination Address

To test the Gateway's connectivity to a destination address:

3. If the Network Diagnostic Tools menu is not displayed, click **Troubleshooting** in the menu bar, and then click the **Diagnostic Tools** submenu.
4. Under **Test Connectivity Results**, enter a destination address in the **Destination Address** field.



Note: This procedure assumes that the destination address you enter is valid and operational.

5. Click the **TEST CONNECTIVITY** button. The **Packets Sent** and **Packets Received** counters show whether packets the number of packets sent and received during the test.
6. To stop the test, click the **STOP** button.

If the test is successful, you know that the destination you are having difficulty reaching is alive and physically reachable. If there are routers between the Gateway and the destination you are having difficulty reaching, the problem might be at one of the routers.

Testing Connectivity to an IP Address

To test the Gateway's connectivity to an IP address:

7. If the Network Diagnostic Tools menu is not displayed, click **Troubleshooting** in the menu bar, and then click the **Diagnostic Tools** submenu.
8. Under **Check for IP Address Results**, enter an IP address in the **IP Address** field.



Note: This procedure assumes that the IP address you enter is valid and operational.

9. Click the **CHECK FOR IP ADDRESSES** button. The **Connectivity** indicator shows the results of the test.
10. To stop the test, click the **STOP** button.

If the test is successful, you know that the IP address you are having difficulty reaching is alive and physically reachable. If there are routers between the Gateway and the IP address you are having difficulty reaching, the problem might be at one of the routers.

Restoring or Rebooting the Gateway

The Restore / Reboot Gateway menu provides buttons for performing the following activities:

- **RESET** - restarts the Gateway while keeping any overrides you made to the Gateway's factory default settings.
- **RESET WI-FI Router** - resets the Wi-Fi router without affecting the Gateway.
- **RESTORE FACTORY SETTINGS** - returns the Gateway to its factory default settings. Any overrides you made to the default settings will be removed. This button is functionally equivalent to using the reset button to reset the Gateway (see “Using the Reset Button” on page 17).

To display the Network Diagnostic Tools menu, click **Troubleshooting** in the menu bar, and then click the **Restore Reboot Gateway** submenu in the menu bar. Figure 54 shows an example of the menu.

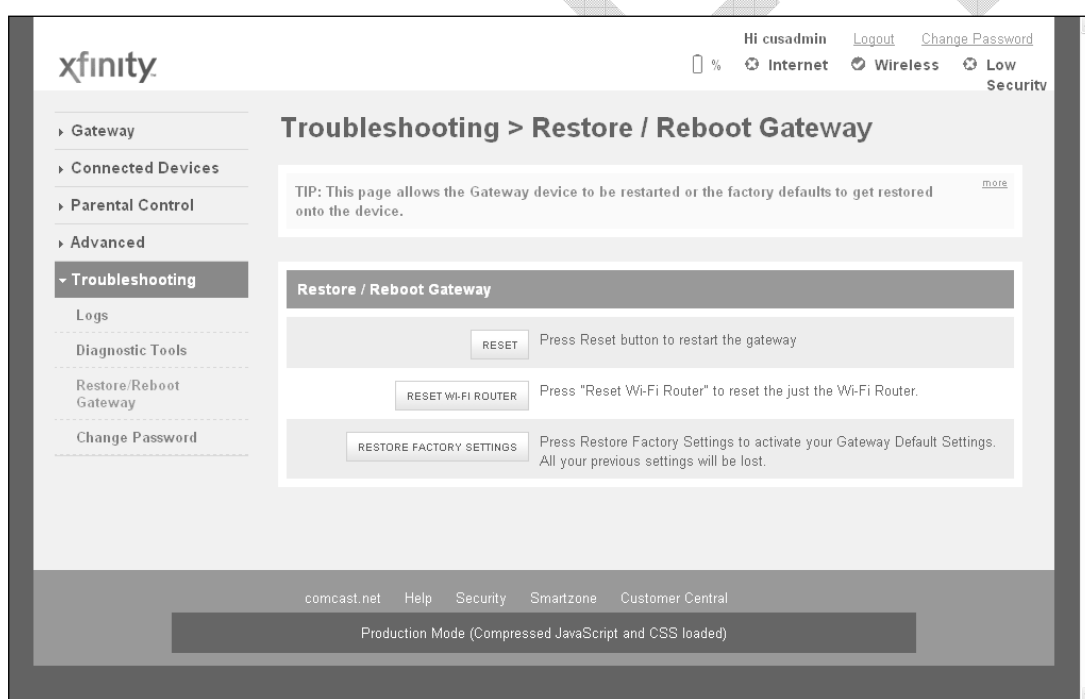


Figure 54. Example of the Restore / Reboot Gateway Menu

Changing the Login Password

The Change Password menu lets you change the password used to log in to the Gateway's Web interface. For security, we recommend you change the default log in password the first time you log in to the Web management interface to protect the Gateway from being tampered with.

To display the Change Password, click **Troubleshooting** in the menu bar, and then click the **Change Password** submenu in the menu bar. Figure 55 shows an example of the menu and Table 21 describes the menu.

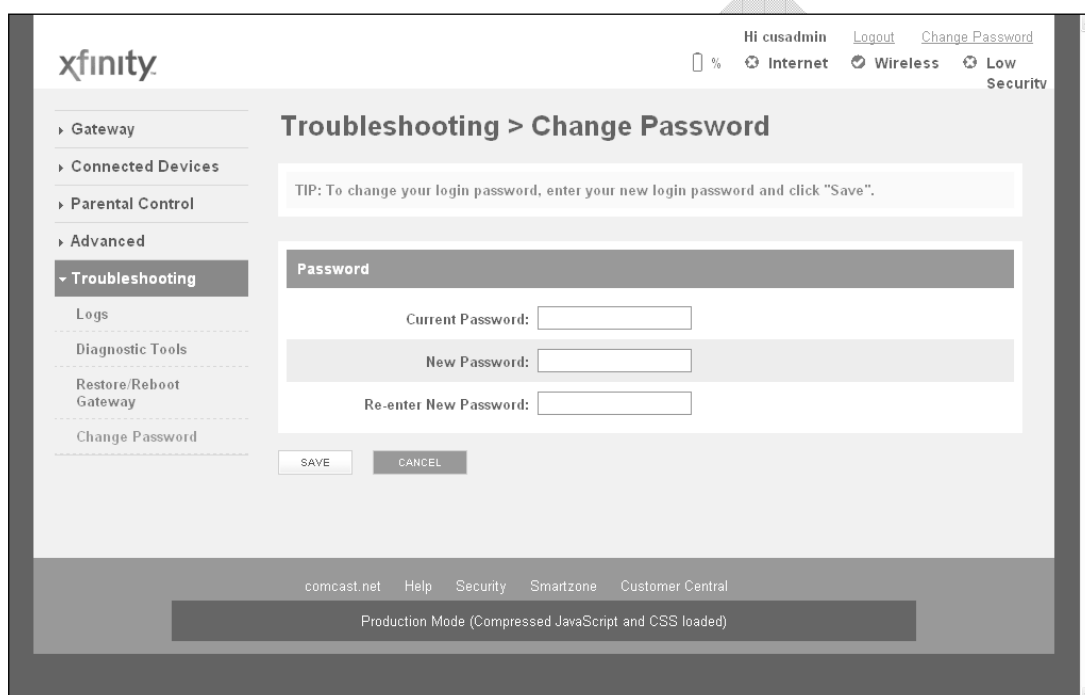


Figure 55. Example of the Change Password Menu

Table 21. Change Password Menu

Option	Description
Current Password	Enter the current case-sensitive administrator password. For security purposes, every typed character appears as a dot (*). The default password is not shown for security purposes.
New Password	Enter the new case-sensitive administrator password you want to use. A password can contain alphanumeric characters and spaces. For security purposes, every typed character appears as a dot (*).
Re-enter New Password	Enter the same case-sensitive administrator password you typed in the New Password field. For security purposes, every typed character appears as a dot (*).
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Change Password menu.

5 Configuring the Gateway's mso Interface

After configuring your computer for TCP/IP and following the preconfiguration guidelines in Chapter 3, use that computer's Web browser to configure your SMCD3GNV3 Gateway using the Gateway's mso interface. This chapter describes how to use your computer's Web browser to configure the Gateway.

The topics covered in this chapter are:

- Accessing the Gateway's Web Management (page 37)
- Understanding the Web Management Interface Menus (page 38)
- Web Management Interface Menus (page 40)

Accessing the Gateway's Web Management

After configuring your computer for TCP/IP and reviewing the guidelines on the previous page, configure the Gateway using its Web-based management interface. From your Web browser, log in to the interface to define system parameters, change password settings, view status windows to monitor network conditions, and control the Gateway and its ports.

To display the SMCD3GNV3 Wireless Cable Modem Gateway's Web-based management screens, use the following procedure.

11. Launch a Web browser.



Note: Your computer does not have to be online to configure the Gateway.

12. In the browser address bar, type <http://10.0.0.1> and press the Enter key. The Login screen appears (see Figure 18).

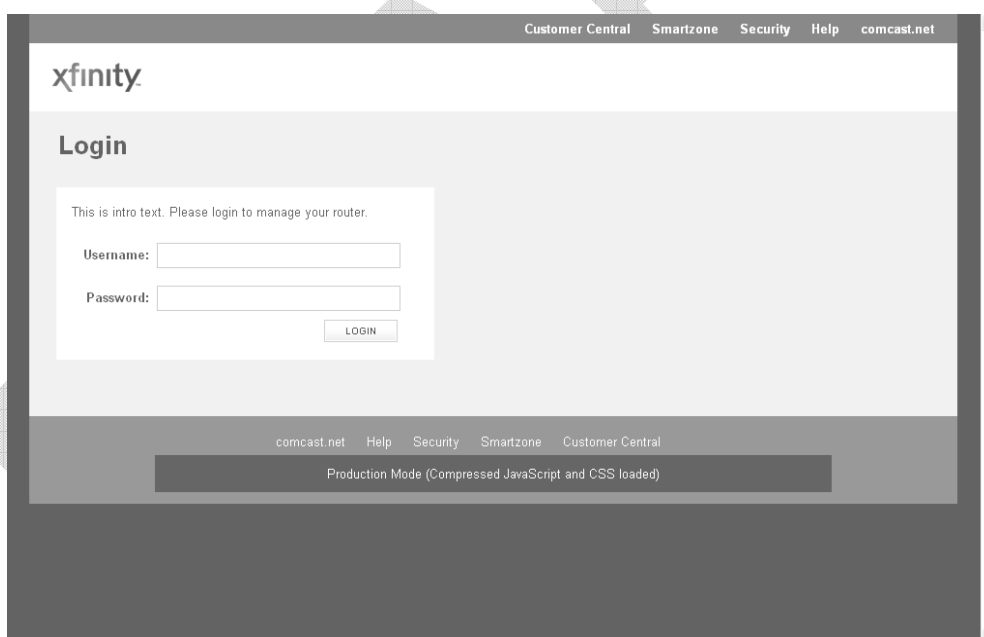


Figure 56. Login Screen

13. In the Login User Password screen, enter the default username and x default password furnished by SMC Networks. Both are case sensitive. For security, each password character appears as a dot (•). After you log in, we recommend you change the default password on the Change Password menu (see “Changing the Login Password” on page 99).



Note: Your cable modem operator may customize the login password, so please check with your operator for the correct password to use.

14. Click the **LOGIN** button to access the Gateway's Web interface. The At a Glance menu appears, showing connection status information about the Gateway. You can also display this menu any time by clicking **At a Glance** in the menu bar.

Understanding the Web Management Interface Menus

The left side of the management interface contains a menu bar for selecting menus to configure the Gateway. When you click a menu, information and any configuration settings associated with the menu appear in the main area (see Figure 19). If the displayed information exceeds the main area, scroll bars appear to the right of the main area so you can scroll up and down through the information.

The top of the main area shows the path (or “breadcrumb”) associated with the information displayed in the main area. For example, if you click the **Status** submenu in the **Connection** menu, **Connection > Status** appears at the top of the main area.

The top-right area shows the username used to log in to the Web interface, along with links for changing the login password and logging out of your current session.

Below the login user name and links are status icons that show the:

- Percentage of battery power remaining
- Gateway's Internet access
- Status of the Gateway's wireless connection
- Firewall security level

A control panel at the bottom of the menu provides links for accessing comcast.net, help, security, smartzone, and customer central.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

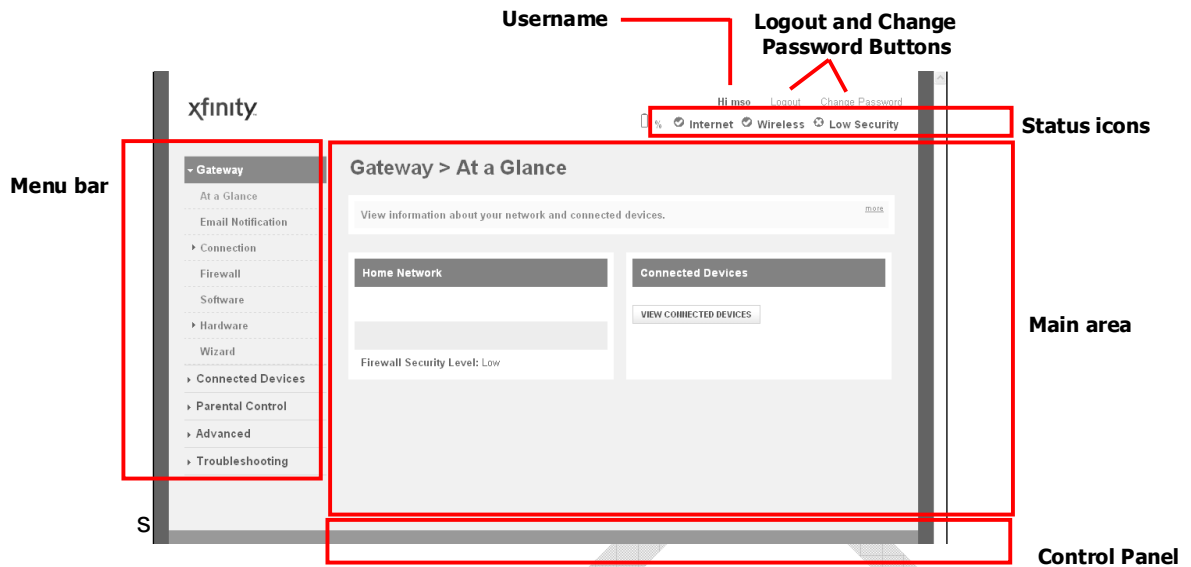


Figure 57. Main Areas on the Web Management Interface

Some menus in the menu bar have submenus associated with them. If you click a menu that has submenus, the submenus appear below the menu. For example, if you click the **Connection** menu, the submenus in Figure 58 appear.



Figure 58. Example of Connection Submenus

Web Management Interface Menus

Table 3 describes the menus in the Web management interface.

In Table 3 and the sections in this chapter, angle brackets show the path of menus and submenus. For example, **Gateway > Connection > XFINITY Network** means you click the **Gateway** menu in the menu bar, and then click the **Connection** and **XFINITY Network** submenus below **Gateway**. The same convention is used in the breadcrumbs displayed in the Gateway configuration menus, so you can keep track of your location within the Gateway's Web management interface.

Table 22. Web Management Interface Menus and Submenus

Menus and Submenus	Description	See Page
Gateway > At a Glance	View information about your home network and connected devices.	107
Gateway > Email Notification	Configure the Gateway to send email notifications when there is a firewall and/or parental control breach.	108
Gateway > Connection > Status	View and edit the settings for your local IP network, and view the status of the Wi-Fi network and XFINITY network.	111
Gateway > Connection > Local IP Network	View and change the Gateway's IPv4 and IPv6 settings.	112
Gateway > Connection > WiFi	View and edit the Gateway's basic and advanced wireless settings.	114
Gateway > Connection > XFINITY Network	View XFINITY network settings and initialization procedure information, including cable modem and downstream channel bonding values.	121
Gateway > Firewall	View and edit the security level of the Gateway's internal firewall.	123
Gateway > Software	View the software version and packet cable version for the Gateway.	125
Gateway > Hardware > System Hardware	View information about the Gateway system hardware.	127
Gateway > Hardware > Battery	View information about the Gateway's internal battery.	128
Gateway > Hardware > LAN	View the link status and Media Access Control (MAC) address for the Gateway's four Ethernet ports.	129
Gateway > Hardware > WiFi	View the status and MAC address of the Gateway's Wi-Fi port.	130
Gateway > Wizard	Use a wizard to set up your home network.	131
Connected Devices > Computers	View computers connected to the Gateway's LAN, add computer's with static IP addresses to the Gateway's LAN, and add WiFi-protected clients to the Gateway's LAN.	135

Table 22. Web Management Interface Menus and Submenus

Menus and Submenus	Description	See Page
Parental Control > Managed Sites	Restrict access to Web sites for non-trusted computers on the network.	142
Parental Control > Managed Services	Restrict access to certain services and applications for non-trusted computers on the network	148
Parental Control > Managed Devices	Enable or disable managed devices, allow or block all access types, and add devices you want to block.	152
Parental Control > Reports	Define a default report filter and generate reports.	156
Advanced > Port Forwarding	Enable the Gateway's port forwarding feature to create a "tunnel" through the Gateway firewall.	157
Advanced > Port Triggering	Configure the Gateway to detect port triggers for multiple-session applications and allow them to pass through the firewall.	160
Advanced > Remote Management	Configure the Gateway for remote management using HTTP, Hypertext Transfer Protocol Secure (HTTPS), Telnet, Secure Shell (SSH), Simple Network Management Protocol (SNMP), and/or H NAP.	163
Advanced > DMZ	Configure the Gateway to provide a local computer with unrestricted two-way Internet access by defining it as a Virtual Demilitarized Zone (DMZ) host.	165
Advanced > Routing	Configure how the Gateway adjusts to physical changes in the network's layout and exchanges routing tables with other routers.	167
Advanced > Dynamic DNS	Allows the Gateway to notify a domain name server to change, in real time, the active DNS configuration of its configured hostnames, addresses, or other information stored in DNS.	169
Advanced > Device Discovery	Configure the Gateway to obtain protocol addresses of neighboring devices and discover the platform of those devices.	171
Troubleshooting > Logs	Define a default log filter and generate logs.	174
Troubleshooting > Diagnostic Tools	Test the Gateway's connectivity to a destination or IP address.	175
Troubleshooting > Restore/Reboot Gateway	Reset the Gateway, reset the Wi-Fi router only, restore the Gateway's wireless settings only, or restore the Gateway's factory settings.	177
Troubleshooting > Change Password	Change the password used to log in to the Gateway's Web management interface.	178

Configuring the Gateway Settings

Using the submenus below **Gateway**, you can:

- View at-a-glance settings for your network and connected devices. See page 107.
- Set up email notifications. See page 108.

DRAFT

Viewing At-a-Glance Configuration Settings

The At a Glance menu appears when you log in to the Gateway's Web interface. You can also display this menu by clicking **Gateway > At a Glance** in the menu bar. Figure 59 shows an example of the At a Glance menu and Table 23 describes the menu.

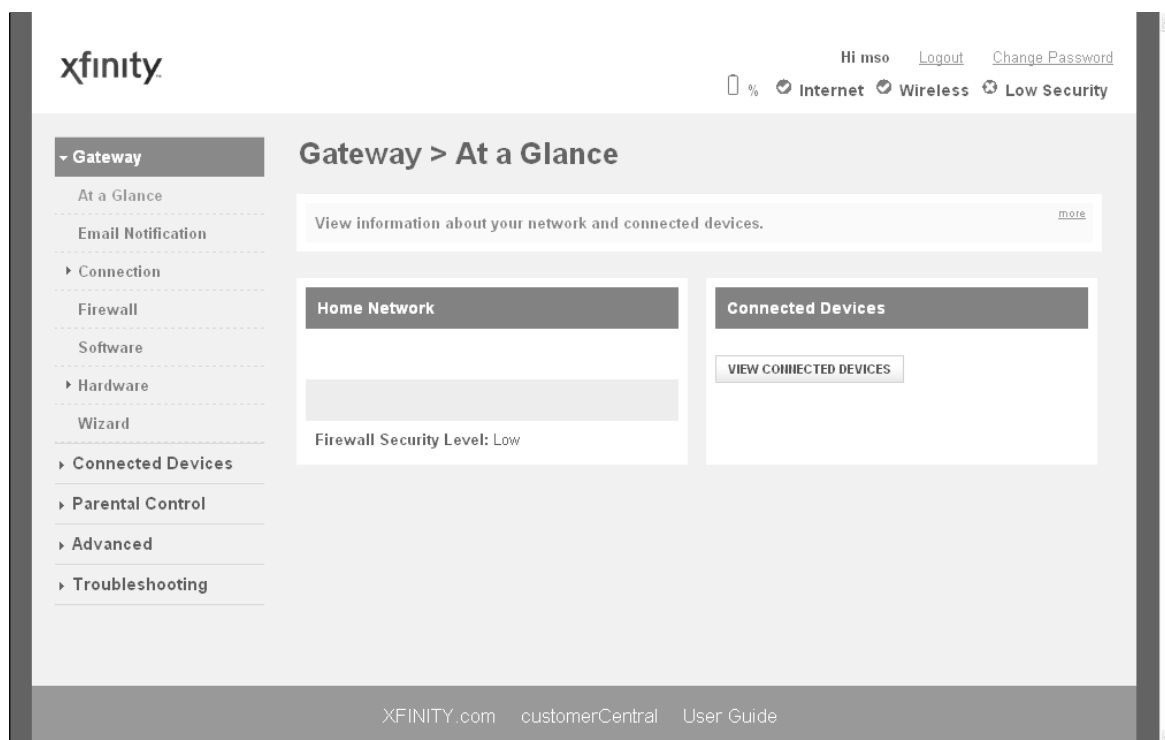


Figure 59. Example of the At a Glance Menu<<screen missing items??>>

Table 23. At a Glance Menu

Option	Description
Home Network	Shows the status of your home network's Ethernet and Wi-Fi home status. A green check mark indicates normal operation. This area also shows the Gateway's firewall security level. To change this level, see "Configuring Firewall Settings" on page 123.
Connected Devices	Shows the names of the devices connected to the Gateway. A View Connected Devices button opens the Computers menu for viewing devices that the Gateway automatically detects using DHCP (see page 135).

Configuring Email Notifications

Using the Email Notification menu, you can configure the Gateway to send email notifications when there is:

- A firewall and/or parental control breach
- An alert or warning <true??>>

If desired, you can configure the Gateway to send the logs with the email.

To display this menu, click **Gateway > Email Notification** in the menu bar. Figure 60 shows an example of the Email Notification menu and Table 24 describes the menu.

The screenshot shows the Xfinity Gateway configuration interface. The top navigation bar includes the Xfinity logo, user information (Hi mso), and links for Logout and Change Password. The main navigation sidebar on the left lists various settings categories: Gateway (selected), At a Glance, Email Notification, Connection, Firewall, Software, Hardware, Wizard, Connected Devices, Parental Control, Advanced, and Troubleshooting. The main content area is titled 'Gateway > Email Notification' and contains the following configuration options:

- Email Notification** (Section Header)
- Recipient Email:
- Notification Types** (Section Header)
- Firewall Breach: No Yes
- Parental Control Breach: No Yes
- Alerts or Warnings: No Yes
- Send Logs: No Yes
- Mail Server Configuration** (Section Header)
- SMTP Server Address:
- Sender's Email Address:
- Sender's Username:
- Sender's Password:
- SAVE CANCEL

At the bottom of the page, there is a footer with the text: XFINITY.com customerCentral User Guide

Figure 60. Email Notification Menu

Table 24. Email Notification Menu

Option	Description
Recipient Email	Email address of the recipient who will receive email notifications. <can you enter ore than one address??>
Notification Types	
Firewall Breach	Determines whether an email notification is sent when the Gateway detects a firewall breach. <ul style="list-style-type: none"> • Yes = Gateway sends a notification when it detects a firewall breach. • No = Gateway does not send a notification when it detects a firewall breach. (<i>default</i>)
Parental Control Breach	Determines whether an email notification is sent when the Gateway detects a parental control breach. <ul style="list-style-type: none"> • Yes = Gateway sends a notification when it detects a parental control breach. • No = Gateway does not send a notification when it detects a parental control breach. (<i>default</i>)
Alerts or Warnings	Determines whether an email notification is sent when a Gateway alert or warning occurs. <ul style="list-style-type: none"> • Yes = email notification is enabled. • No = email notification is disabled. (<i>default</i>)
Send Logs	Determines whether the Gateway sends logs with the email notification. <ul style="list-style-type: none"> • Yes = logs are sent with the email notification. • No = logs are not sent with the email notification. (<i>default</i>)
Mail Server Configuration	
SMTP Server Address	The address of the SMTP server through which the Gateway will send email notifications. For this configuration to succeed, this procedure assumes that your SMTP server is operational and configured properly.
Sender's Email Address	The email address that will appear as the sender of the email notification.
Sender's Username	The name that will appear as the sender of the email notification.
Sender's Password	The password used by the sender to send email.
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Email Notification menu.

Configuring Connections

Using the submenus below **Connections**, you can:

- View and edit the settings for your local IP network, and view the Gateway's Wi-Fi and XFINITY network connections. See page 111.
- Configure the Gateway's IPv4 or IPv6 settings. See page 112.
- View and edit basic and advanced wireless settings. See page 114.
- View XFINITY network information. See page 121.

DRAFT

Viewing the Gateway's Connection Status

The Status menu lets you view and edit the settings for your local IP network. You can also use this menu to view the status of the Wi-Fi network and XFINITY network.

To display the Status menu, click **Gateway > Connection > Status** in the menu bar. Figure 61 shows an example of the Status menu and Table 25 describes the menu.



Figure 61. Example of the Status Menu

Table 25. Status Menu

Option	Description
Local IP Network	Displays information about the local network. The EDIT button opens the Local IP Configuration menu for viewing and changing IPv4 or IPv6 settings (see "Viewing and Editing Your Local IP Configuration" on page 112).
WiFi Network	Lets you view information about your Wi-Fi network. A VIEW button opens the WiFi menu for viewing the link status and MAC address of the Gateway's WiFi LAN port (see "Viewing Wi-Fi Settings" on page 130).
XFINITY Network	Lets you view information about the XFINITY network. A VIEW button opens the Comcast Network menu for viewing the initialization procedures, including cable modem, downstream, and upstream information (see "Viewing XFINITY Network Information" on page 121).

Viewing and Editing Your Local IP Configuration

The Local IP Configuration menu lets you view and change the Internet Protocol (IP) settings used by the Gateway. Fields are provided for configuring IP version 4 (IPv4) and the newer IP version 6 (IPv6).

To display the Local IP Configuration menu, click **Gateway > Connection > Local IP Network** in the menu bar. Figure 62 shows an example of the Local IP Configuration menu and Table 26 describes the menu.

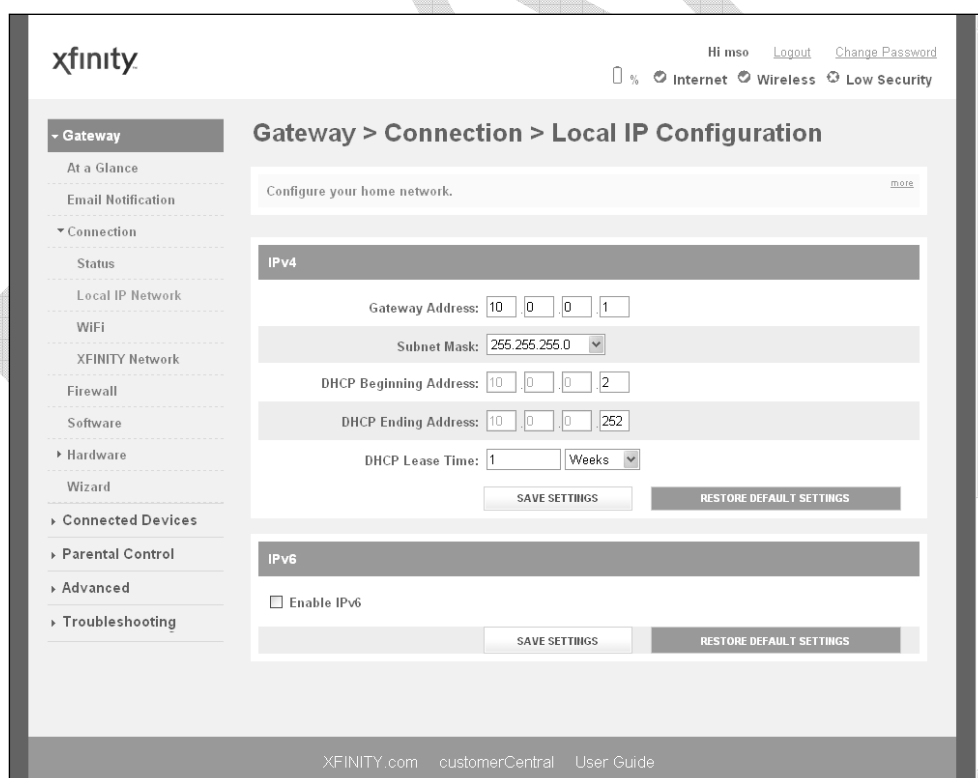


Figure 62. Example of Local IP Configuration Menu

Table 26. Local IP Configuration Menu

Option	Description
IPv4 (for computers that use IP v4 Messaging)	
Gateway Address	IPv4 IP address that the Gateway is to use.
Subnet Mask	IPv4 subnet mask that the Gateway is to use.
DHCP Beginning Address	Starting IP address range for the pool of allocated for DHCP IP addresses. The first two fields match the first two octets in the Gateway's IP address and cannot be changed. The last two fields let you enter the final two octets in the starting IP address range.
DHCP Ending Address	Ending IP address range for the pool of allocated for DHCP IP addresses. The first two fields match the first two octets in the Gateway's IP address and cannot be changed. The last two fields let you enter the final two octets in the ending IP address range.
DHCP Lease Time	Amount of time a DHCP network user is allowed connection to the Gateway with their current dynamic IP address. Default is One Week.
SAVE SETTINGS button	After configuring your IPv4 settings, click this button to save them.
RESTORE DEFAULT SETTINGS FOR IPV4 button	Resets the Gateway to the factory default IPv4 settings.
IPv6 (for computers that use IP v6 Messaging)	
Enable IPv6	Check this box to configure the Gateway to use IPv6 settings.
Gateway Address	IPv6 IP address that the Gateway is to use.
Prefix Length	A read-only value that shows the IPv6 prefix length, which is always 64.
SAVE SETTINGS button	After enabling or disabling IPv6, click this button to apply.
RESTORE DEFAULT SETTINGS FOR IPV6 button	Resets the Gateway to the factory default IPv6 settings.

Viewing and Editing Wireless Configuration

The Wireless menu lets you view and change the Gateway's basic and advanced wireless settings. To display the Wireless menu, click **Gateway > Connection > WiFi** in the menu bar .

The Wireless menu is organized into the following areas:

- Private WiFi and Public WiFi networks – see page 115
- Private wireless basic settings – see page 116
- Private advanced basic settings – see page 117
- MAC filter settings – see page 119
- WiFi client setup configuration (WPS) - see page 120
- Connect to your WPS-supported device – see page 121

DRAFT

Private and Public WiFi Networks

Figure 63 shows the Private and Public WiFi Network areas on the WiFi menu, and Table 27 describes the fields shown.

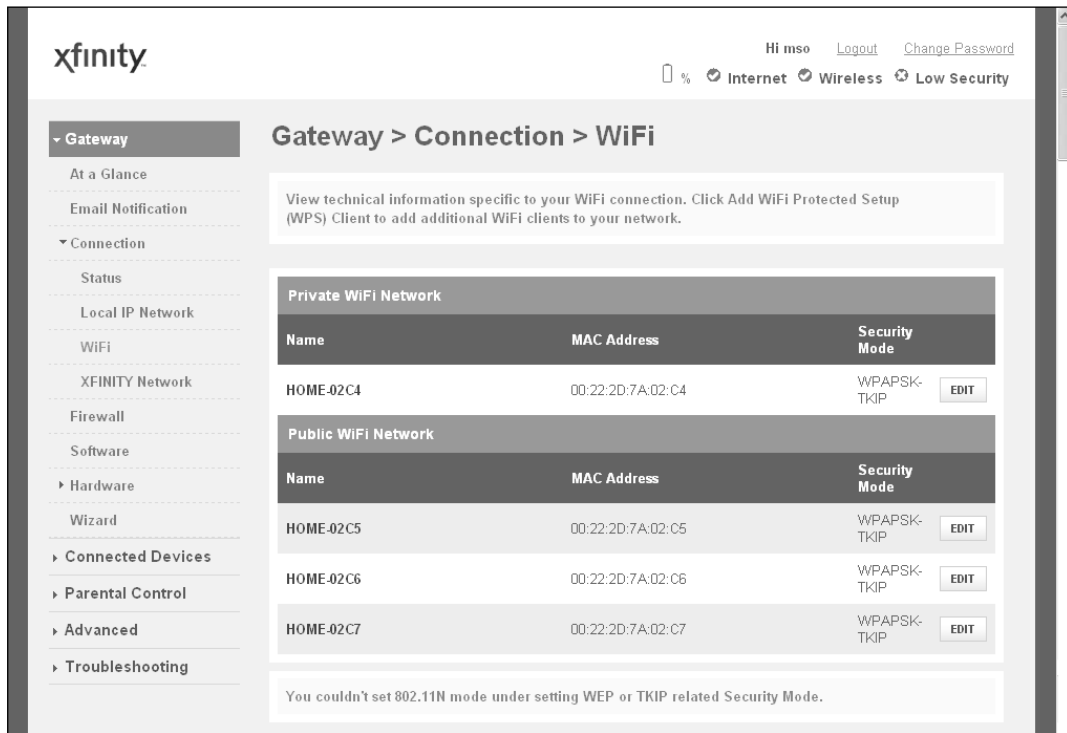


Figure 63. Wireless Menu - Private and Public WiFi Networks Areas

Table 27. Wireless Menu - Private and Public WiFi Networks Areas

Option	Description
Private WiFi Network	
Name MAC Address Security Mode	Shows the name MAC address, and security setting, if any, for each private wireless network detected. An EDIT button is provided to change these settings.
Public WiFi Network	
Name MAC Address Security Mode	Shows the name MAC address, and security setting, if any, for each public wireless network detected. An EDIT button is provided to change these settings.

Private Wireless Basic Settings

Figure 64 shows the private wireless basic settings on the WiFi menu, and Table 28 describes the fields shown.

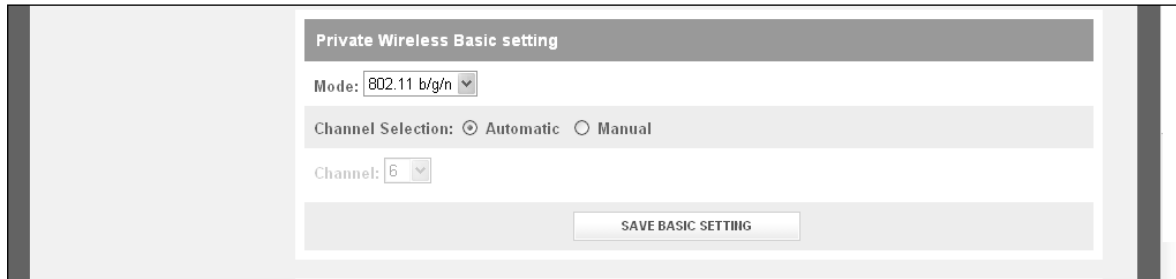


Figure 64. Wireless Menu - Private Wireless Basic Settings

Table 28. Wireless Menu - Private Wireless Basic Settings

Option	Description
Mode	<p>If wireless operation is enabled for the Gateway, this option selects the wireless mode used by the Gateway. Choices are:</p> <ul style="list-style-type: none"> • 802.11 b/g = use this setting if you have a combination of IEEE 802.11b and IEEE 802.11g devices on your network. • 802.11g/n = use this setting if you have IEEE 802.11g and IEEE 802.11n devices on your network. • 802.11 b/g/n = use this setting if you have a combination of IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n devices on your network. <i>(default)</i>
Channel Selection	<p>Select how the Gateway will select a channel for communicating over the wireless network. Choices are:</p> <ul style="list-style-type: none"> • Automatic = the Gateway selects the channel automatically. <i>(default)</i> • Manual = the Gateway uses the channel specified in the Channel option.
Channel	<p>If the Channel Selection option is Manual, specify the appropriate channel from the list provided to correspond with your network settings. Choices are 1, 6, and 11. The default setting is 6, which refers to radio frequency ranges within the 2.4 GHz range. You can change this setting if necessary; however, all devices in your wireless network must use the same channel to work properly.</p>
SAVE BASIC SETTING button	<p>Click this button to save your changes to the private wireless basic settings.</p>

Private Wireless Advanced Settings

Figure 65 shows the private wireless basic settings on the WiFi menu, and Table 29 describes the fields shown.

Figure 65. Wireless Menu - Private Wireless Advanced Settings

Table 29. Wireless Menu - Private Wireless Advanced Settings

Option	Description
BG Protection Mode	This mode is a protection mechanism that prevents collisions among 802.11b/g modes. Choices are: <ul style="list-style-type: none"> • Auto = BG protection mode goes on or off automatically as needed. • Always-On = BG protection mode is always on. • Always-Off = BG protection mode is always off. (<i>default</i>)
IGMP Snooping	Enables or disables the Gateway from forwarding multicast traffic intelligently. <ul style="list-style-type: none"> • Enable = Gateway listens to IGMP membership reports, queries, and leave messages to identify the Gateway ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups. • Disable = Gateway does not analyze all IGMP packets. (<i>default</i>)

錯誤! 使用 [常用] 索引標籤將 **Heading 1** 套用到您想要在此處顯示的文字。

Option	Description
Operation Mode	Lets you select between Mixed Mode and Green Field. <ul style="list-style-type: none"> Mixed Mode = provides backward compatibility with IEEE 802.11n/a/g/b devices. (<i>default</i>) Green Field = used for pure network of 802.11n access points and clients, taking full advantage of the high-throughput capabilities of the 11n multiple-input multiple-output (MIMO) architecture.
Channel Bandwidth	Select a channel bandwidth of 20 or 20/40. <ul style="list-style-type: none"> 20 = allows only single-channel operation (e.g., 20 MHz). 20/40 = allows both single channel operation (20 MHz) and the wider bandwidth operation (40 MHz) by using two or more adjacent (contiguous) channels. A 20/40 BSS is a wireless network that allows a wider bandwidth operation mode. (<i>default</i>)
Guard Interval	The guard interval is the period in nanoseconds that the Gateway listens between packets. Choices are: <ul style="list-style-type: none"> Long = 800 ns guard interval. Short = 400 ns guard interval. (<i>default</i>)
Reverse Direction Grant (RDG)	Speeds up data transmission between the Gateway and 802.11n access points and clients by allowing wireless workstations to send/receive data simultaneously, without contending for shared medium. Default is enable.
Extension Channel	Defines a second 20-MHz channel. 40-MHz stations can use this channel in addition to using the control channel simultaneously.
Aggregation MSDUA (A-MSDU)	Enables or disables aggregation of multiple MSDUs in one MPDU. Default is disable.
Auto-Block Ack	Enables or disables Auto Block ACL function. Default is enable.
Decline BA Request	Enables or disables the BA request function. Default is disable.
HT Tx Stream	Select 1 or 2 from the pull-down menu. Default is 2.
HT Rx Stream	Select 1 or 2 from the pull-down menu. Default is 2.
WMM Power Save	When checked, enables the Gateway's power-management features for optimizing battery life. Default is checked.
STBC	Space Time Block Coding (STBC) is an 802.11n technique intended to improve the reliability of data transmissions. With STBC, the data stream is transmitted on multiple antennas, so the receiving system has a better chance of detecting at least one of the data streams. Choices are: <ul style="list-style-type: none"> Disable = Gateway does not transmit the same data on multiple antennas. (<i>default</i>) Enable = Gateway transmits the same data stream on multiple antennas at the same time.
SAVE ADVANCED SETTING button	Click this button to save your changes to the private wireless advanced settings.

MAC Filter Settings

Figure 66 shows the MAC filter settings on the WiFi menu, and Table 30 describes the fields shown.

The screenshot displays the 'Mac Filter Setting' interface. At the top, it states: 'The SMC-D3GNV can allow the wireless client stations to connect to your SMC-D3GNV in any of these ways:'. Below this, the SSID is set to 'HOME-02C4' and the MAC Filtering Mode is set to 'Allow-All'. There are three main sections: 'Wireless Control List (up to 16 items)' with a table header for '#', 'Device Name', and 'MAC Address', and a 'DELETE' button; 'Auto-Learned Wireless Devices' with a table header for 'Device Name' and 'MAC Address'; and 'Manually-Added Wireless Devices' with input fields for 'Device Name' and 'MAC Address' and an 'ADD' button. A 'SAVE FILTER SETTING' button is located at the bottom of the page.

Figure 66. Wireless Menu – MAC Filter Settings

Table 30. Wireless Menu – MAC Filter Settings

Option	Description
SSID	Network name of the of the primary wireless carrier.
MAC Filtering Mode	Use MAC Filtering Mode to allow or deny all or certain wireless devices within the LAN from accessing the Internet. You can either manually add a MAC address or select the MAC address from the list of auto-learned wireless devices. The choices are: <ul style="list-style-type: none"> • Allow- All = all wireless client stations can connect to the Internet. (<i>default</i>) • Allow = allow only the wireless client stations in the Wireless Control List to connect to the Internet. • Deny = deny the wireless client stations in the Wireless Control List from connecting to the Internet.
Wireless Control List	Shows up to 16 wireless devices whose MAC addresses you have added.
Aut-Learned Wireless Devices	Shows the wireless devices whose presence the Gateway has automatically learned.
Manually-Added Wireless Devices	Enter a unique name and MAC address of the wireless devices that you want to manually add to the Wireless Control List, then click Add to add the device.
SAVE FILTER SETTING button	Click this button to save your changes to the MAC filter settings.

WiFi Client Setup Configuration (WPS)

Figure 67 shows the WiFi client setup configuration settings on the WiFi menu, and Table 31 describes the fields shown.

Figure 67. Wireless Menu – WiFi Client Setup Configuration (WPS) Settings

Table 31. Wireless Menu – WiFi Client Setup Configuration (WPS) Settings

Option	Description
SSID	Network name of the of the primary wireless carrier.
MAC Filtering Mode	Use MAC Filtering Mode to allow or deny all or certain wireless devices within the LAN from accessing the Internet. You can either manually add a MAC address or select the MAC address from the list of auto-learned wireless devices. The choices are: <ul style="list-style-type: none"> • Allow- All = all wireless client stations can connect to the Internet. (<i>default</i>) • Allow = allow only the wireless client stations in the Wireless Control List to connect to the Internet. • Deny = deny the wireless client stations in the Wireless Control List from connecting to the Internet.
Wireless Control List	Shows up to 16 wireless devices whose MAC addresses you have added.
Aut-Learned Wireless Devices	Shows the wireless devices whose presence the Gateway has automatically learned.
Manually-Added Wireless Devices	Enter a unique name and MAC address of the wireless devices that you want to manually add to the Wireless Control List, then click Add to add the device.
SAVE FILTER SETTING button	Click this button to save your changes to the MAC filter settings.

Connect to Your WPS-Supported Device

Figure 68 shows the WiFi client setup configuration settings on the WiFi menu, and Table 32 describes the fields shown.

Figure 68. Wireless Menu – Connect to Your WPS-Supported Device Settings

Table 32. Wireless Menu – Connect to Your WPS-Supported Device Settings

Option	Description
Push Button	Click this option to use the WPS button on the top panel of the Gateway to configure WPS (see Figure 3).
PIN Number	Click this option if you need to enter a PIN to configure WPS.
Enter Wireless Client's PIN	If you clicked PIN Number , enter the PIN in this field.
PAIR WITH MY WIFI CLIENT button	Click this button to pair (connect) the Gateway's Wi-Fi settings with your Wi-Fi client.

Viewing XFINITY Network Information

The XFINITY Network menu is a read-only screen that displays:

- XFINITY network settings
- Initialization procedure information, including cable modem and downstream channel bonding values

The information shown on this menu automatically updates (refreshes) every 10 seconds.

To display the XFINITY Network menu, click **Gateway > Connection > XFINITY Network** in the menu bar. Figure 69 shows an example of the XFINITY Network menu.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

The screenshot displays the XFINITY Network menu within a gateway user interface. The page is titled "Gateway > Connection > XFINITY Network". On the left, there is a navigation sidebar with options like Gateway, At a Glance, Email Notification, Connection, Status, Local IP Network, WIFI, XFINITY Network, Firewall, Software, Hardware, Wizard, Connected Devices, Parental Control, Advanced, and Troubleshooting. The main content area shows the XFINITY Network status, including Internet: Active, System Uptime: 002 days 03h:42m:07s, WAN IP Address: 10.30.20.176, DHCP Client: Enable, and various MAC addresses. Below this is the Initialization Procedure section, which lists several steps as complete, such as Initialize Hardware, Acquire Downstream Channel, Upstream Ranging, DHCP Bound, Set Time of Day, Configuration File Download, and Registration. The Cable Modem section provides detailed specifications like HW Version (1A), Vendor (SMC Networks), BOOT Version (PSPU-Boot(EBU) 1.0.9.15-H2.5), Core Version (2.1.2.5), Model (SMC-D3GNV), Product Type (SMC-D3GNV), Flash Part (32 MB), Download Version (2.1.2.5), and Serial Num (H2A040A884). Finally, there are two tables: Downstream Channel Bonding Value and Upstream Channel Bonding Value, both showing lock status, frequency, SNR, power, and modulation for different channels.

Figure 69. Example of XFINITY Network Menu

Configuring Firewall Settings

The Firewall menu lets you view and edit the settings for the Gateway's internal firewall. The setting you select here is displayed at the top-right area of the Gateway's Web interface.

To display the Firewall menu, click **Gateway > Firewall** in the menu bar. Figure 70 shows an example of the Firewall menu and Table 33 describes the menu.

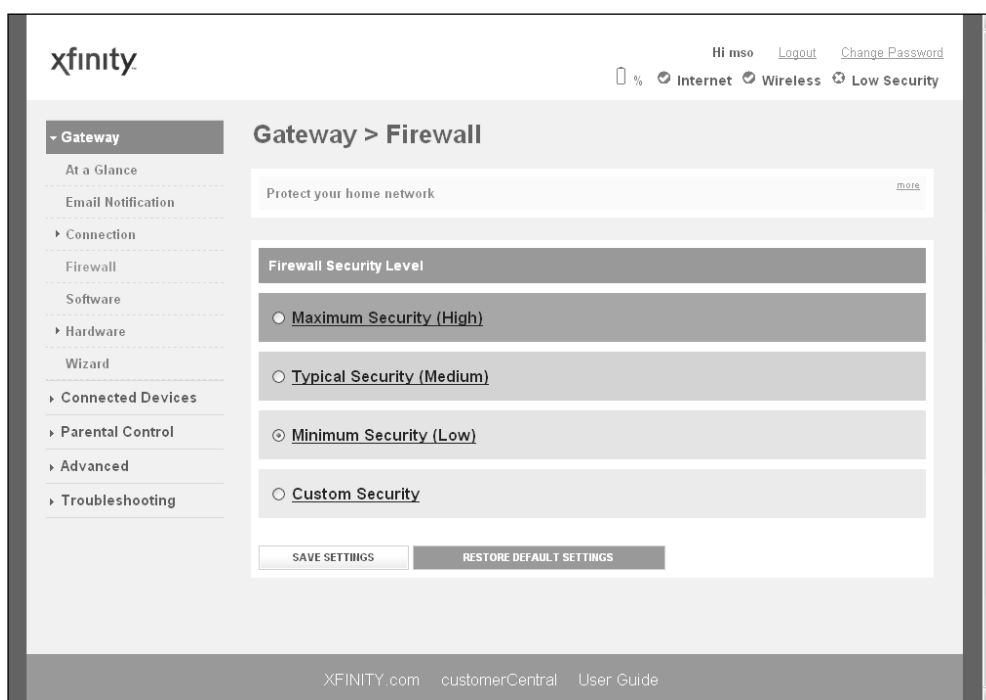


Figure 70. Example of the Firewall Menu

Table 33. Firewall Menu

Option	Description
Maximum Security (High)	Configures the Gateway's firewall to the highest setting. Select this setting for environments where security is critical.
Typical Security (Medium)	Configures the Gateway's firewall for typical (medium) security. Select this setting for environments where security is important.
Minimum Security (Low)	Configures the Gateway's firewall for minimum (low) security. Select this setting for environments where security is not important.
Custom Security	Clicking this option displays the custom security settings in Figure 71. For more information, see Table 34s.
SAVE SETTINGS button	After configuring your firewall settings, click this button to save them.
RESTORE DEFAULT SETTINGS button	Resets the Gateway to the factory default firewall settings.

Custom Security

Blocked: No access to local network from Internet.

Limited: Commonly used services as given below can be blocked by selecting the check box, all other services will be enabled by default. For blocking a specific port, please use port blocking.

Block http (TCP port 80, 443)

Block ICMP

Block Multicast

Block Peer-to-peer applications

Block IDENT (port 113)

Disable entire firewall

Figure 71. Custom Firewall Security Settings

Table 34. Custom Security Settings

Option	Description
Block http	Blocks HTTP downloads on ports 80 and 443.
Block ICMP	Blocks Internet Control Message Protocol (ICMP) traffic at the outer perimeter of the Gateway to protect against attacks such as cascading ping floods.
Block Multicast	Blocks unsolicited multicast packets.
Block Peer-to-peer application	Blocks peer-to-peer applications
Block IDENT	Blocks identification (Ident) requests from Ident servers on port 113. Note: Port 113 is associated with Ident. If a client program on a computer connected to the Gateway contacts a remote server for services such as POP, IMAP, SMTP, or IRC, the remote server returns a query to the "Ident" server running in many systems listening for these queries on port 113. Essentially, the remote server is asking your system to identify itself and you. This means that port 113 is often probed by attackers as a source of your personal information.
Disable entire firewall	Disables all of the Gateway's firewall settings.

Viewing System Software Settings

The Software menu is a read-only screen that shows the software version and packet cable version associated with the Gateway.

To display the Software menu, click **Gateway > Software** in the menu bar. Figure 72 shows an example of the Software menu.

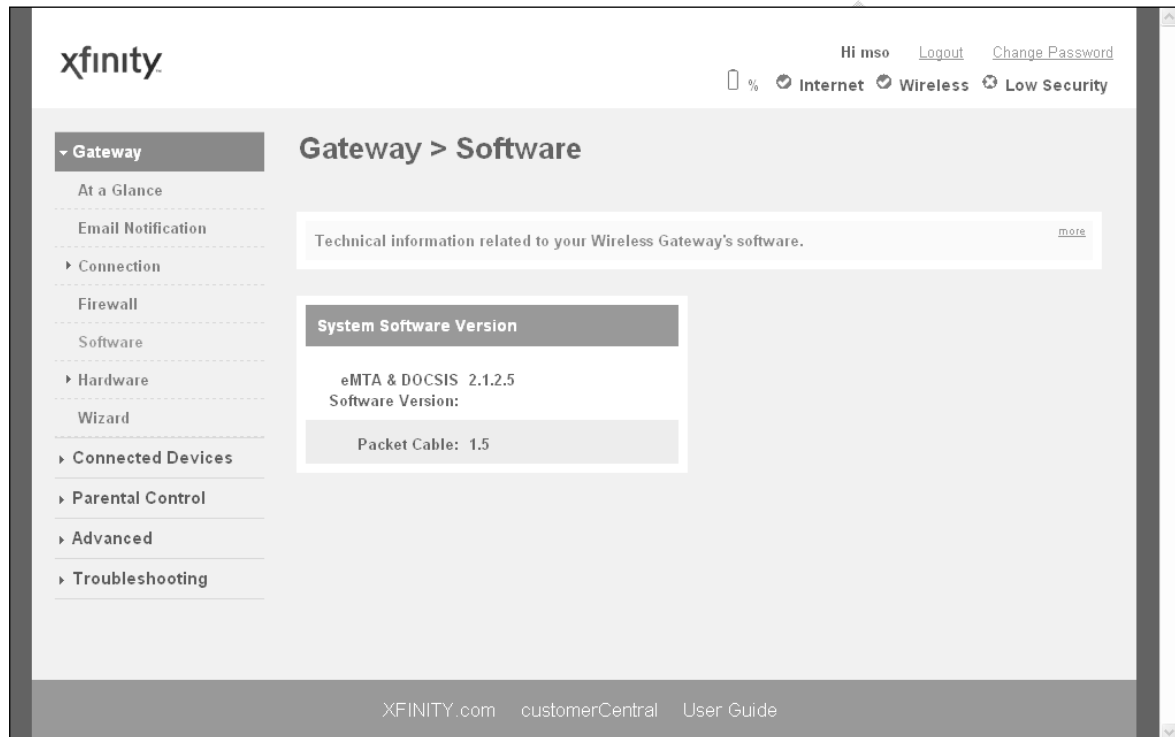


Figure 72. Example of the Software Menu

Configuring Hardware

Using the submenus below **Hardware**, you can view information about the:

- Gateway system hardware, such as model, serial number, and processor speed. See page 127.
- Gateway's battery status. See page 128.
- Link status and MAC address of the Gateway's four Ethernet ports. See page 129.
- Wi-Fi link status and MAC address of the Gateway's WiFi port . See page 130.

DRAFT

Viewing System Hardware Settings

The System Hardware menu is a read-only screen that shows the Gateway's system hardware.

To display the System Hardware menu, click **Gateway > Hardware > System Hardware** in the menu bar. Figure 73 shows an example of the System Hardware menu.

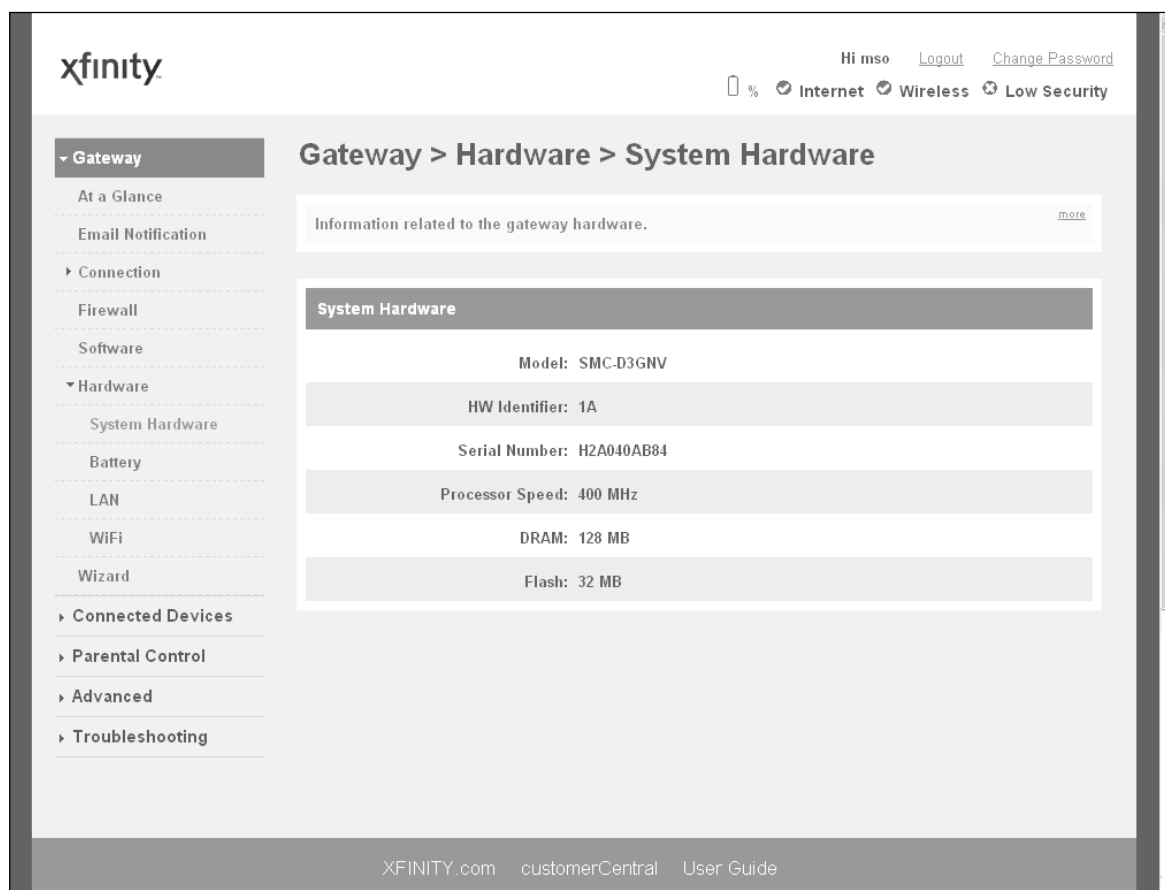


Figure 73. Example of the System Hardware Menu

Viewing Battery Settings

The Battery menu is a read-only screen that shows information about the Gateway's internal battery.

To display the Battery menu, click **Gateway > Hardware > Battery** in the menu bar. Figure 74 shows an example of the Battery menu.

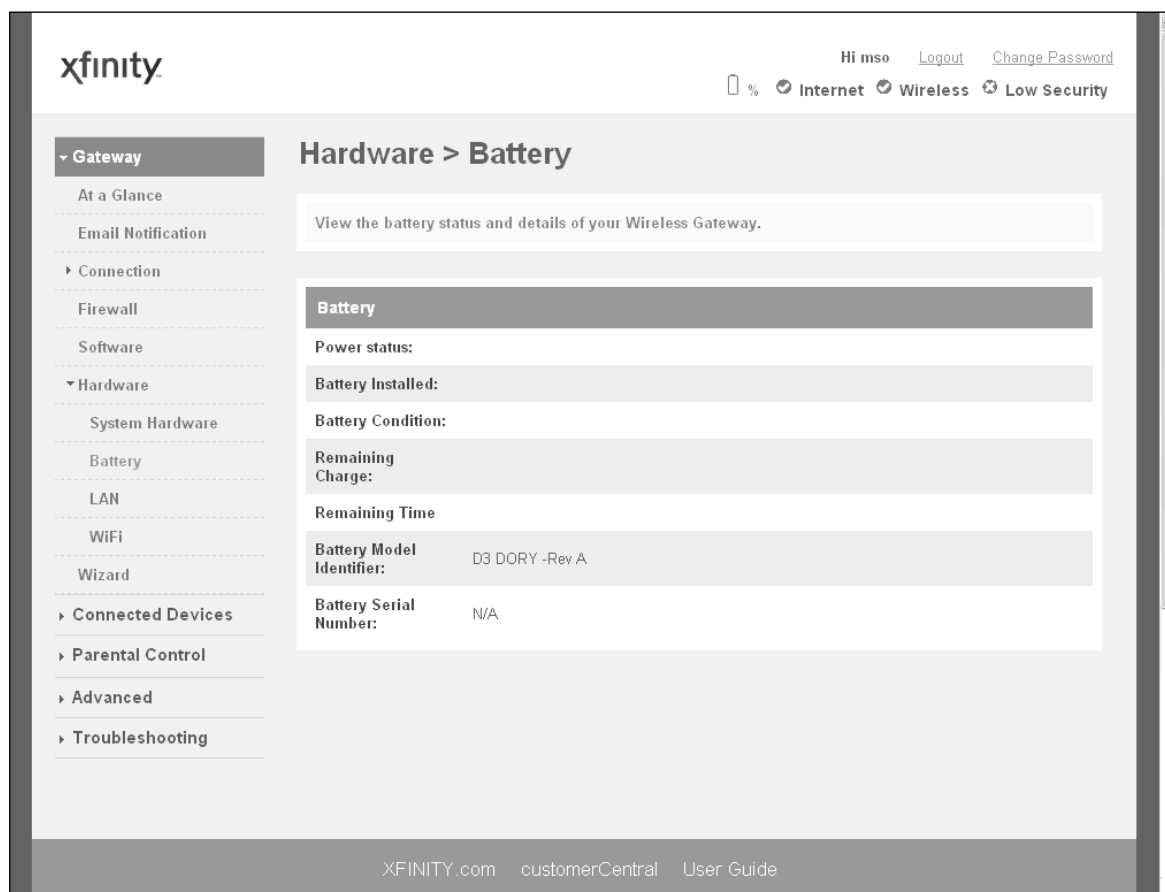


Figure 74. Example of the Battery Menu

Viewing LAN Ethernet Settings

The LAN Ethernet menu is a read-only screen that shows the link status and MAC address of the Gateway's four Ethernet ports.

To display the LAN Ethernet menu, click **Gateway > Hardware > LAN** in the menu bar. Figure 75 shows an example of the LAN Ethernet menu.

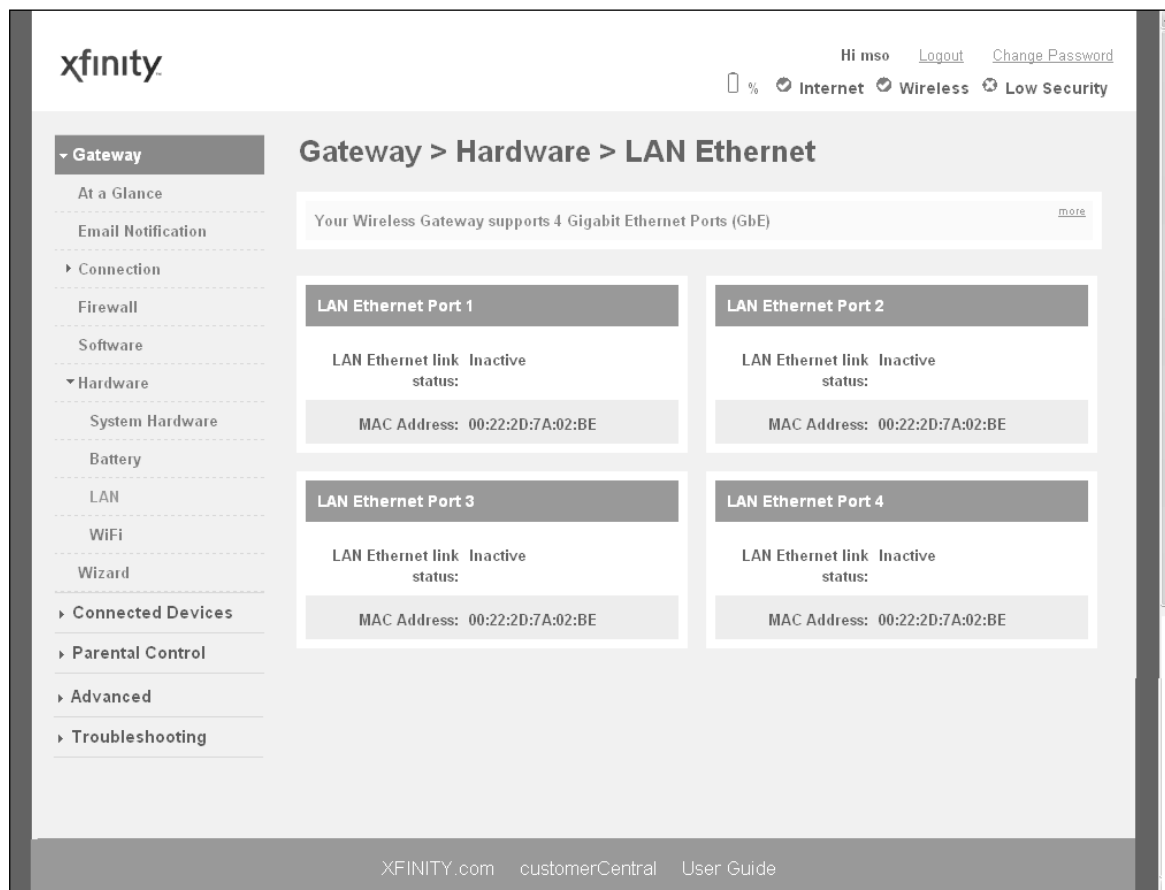


Figure 75. Example of the LAN Ethernet Menu

Viewing Wi-Fi Settings

The WiFi menu is a read-only screen that shows the Wi-Fi link status and MAC address of the Gateway's Wi-Fi port.

To display the WiFi menu, click **Gateway > Hardware > WiFi** in the menu bar. Figure 76 shows an example of the WiFi menu.

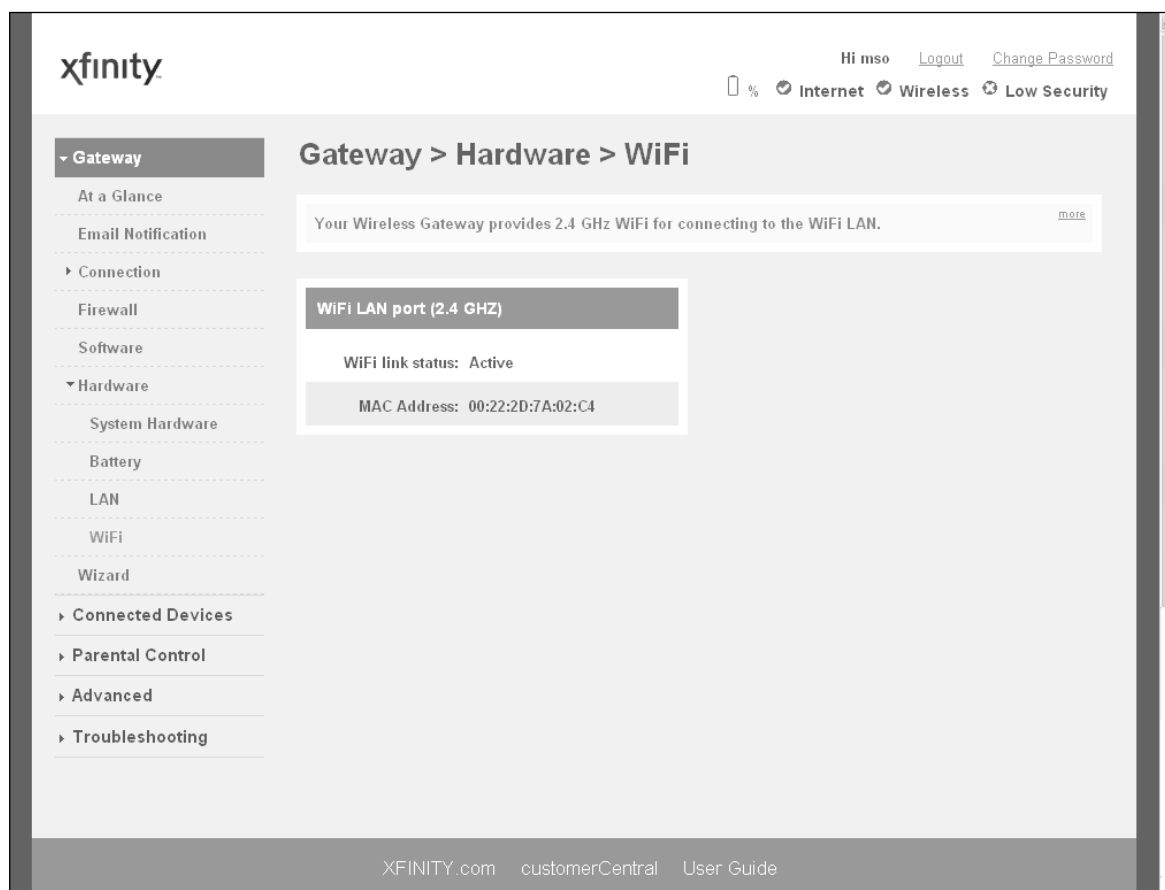


Figure 76. Example of the WiFi Menu

Configuring Your Home Network

The Home Network Wizard menu is part of a 2-page wizard you can use to configure your home network.

To display the first page of the Home Network Wizard, click **Gateway > Wizard** in the menu bar. Figure 77 shows an example of the first page of the Home Network Wizard and Table 35 describes the page.

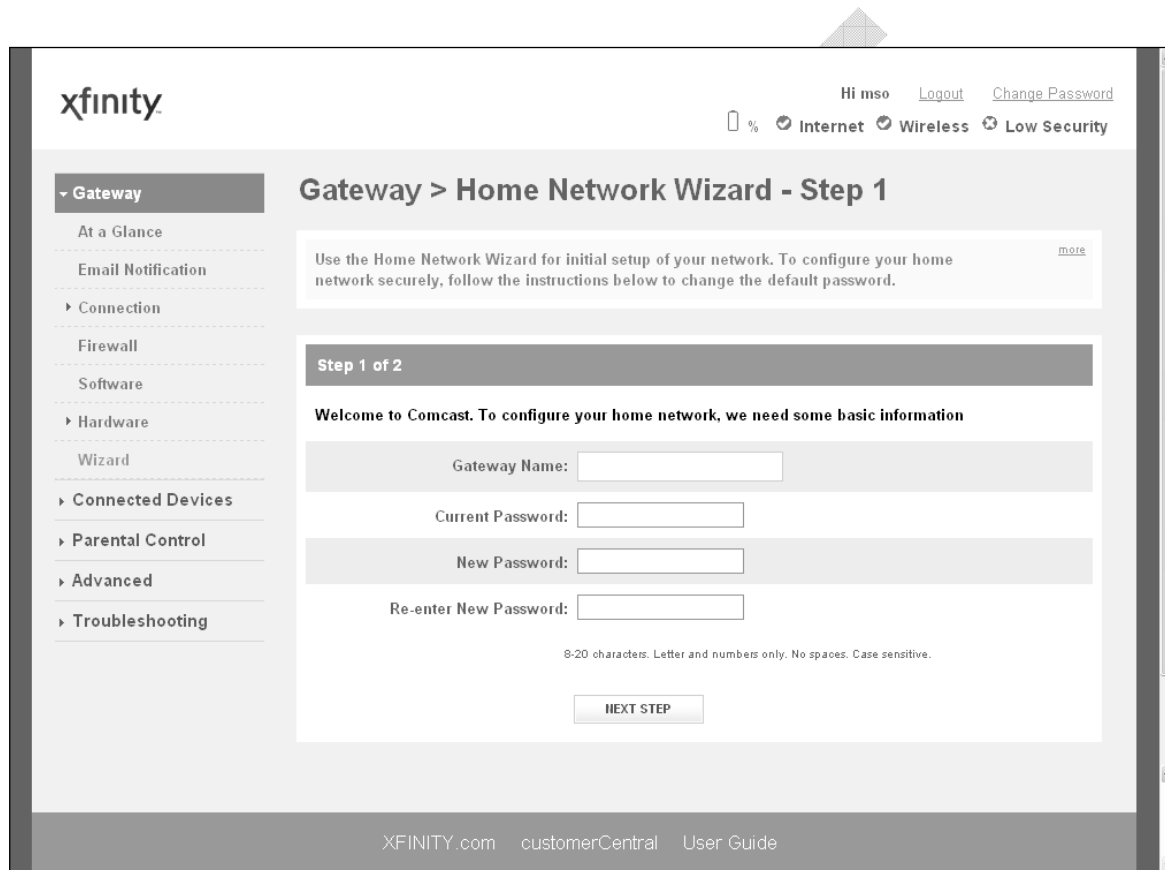


Figure 77. Example of the First Page of the Home Network Wizard

Table 35. Home Network Wizard – Step 1

Option	Description
Gateway Name	The name you want to assign to the Gateway. Assign a name so that this device will not be confused with other devices on your wireless network. We recommend you use a name that is meaningful to you so you can identify the Gateway easily. The Gateway name is case sensitive and can contain from 8 to 20 alphanumeric characters, but no spaces.
Current Password	Enter the current case-sensitive password. For security purposes, every typed character appears as a dot (•). The default password is not shown for security purposes. The password is case sensitive and can contain from 8 to 20 alphanumeric characters, but no spaces.
New Password	Enter the new password you want to use to protect your network. The password is case sensitive and can contain from 8 to 20 alphanumeric characters, but no spaces. Spaces count as password characters. For security purposes, every typed character appears as a dot (•).
Re-enter New Password	Enter the same case-sensitive password you typed in the New Password field. For security purposes, every typed character appears as a dot (•).
NEXT STEP button	Click this button to display the second page of the Home Network Wizard (see Figure 78 and Table 36).

DRAFT

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

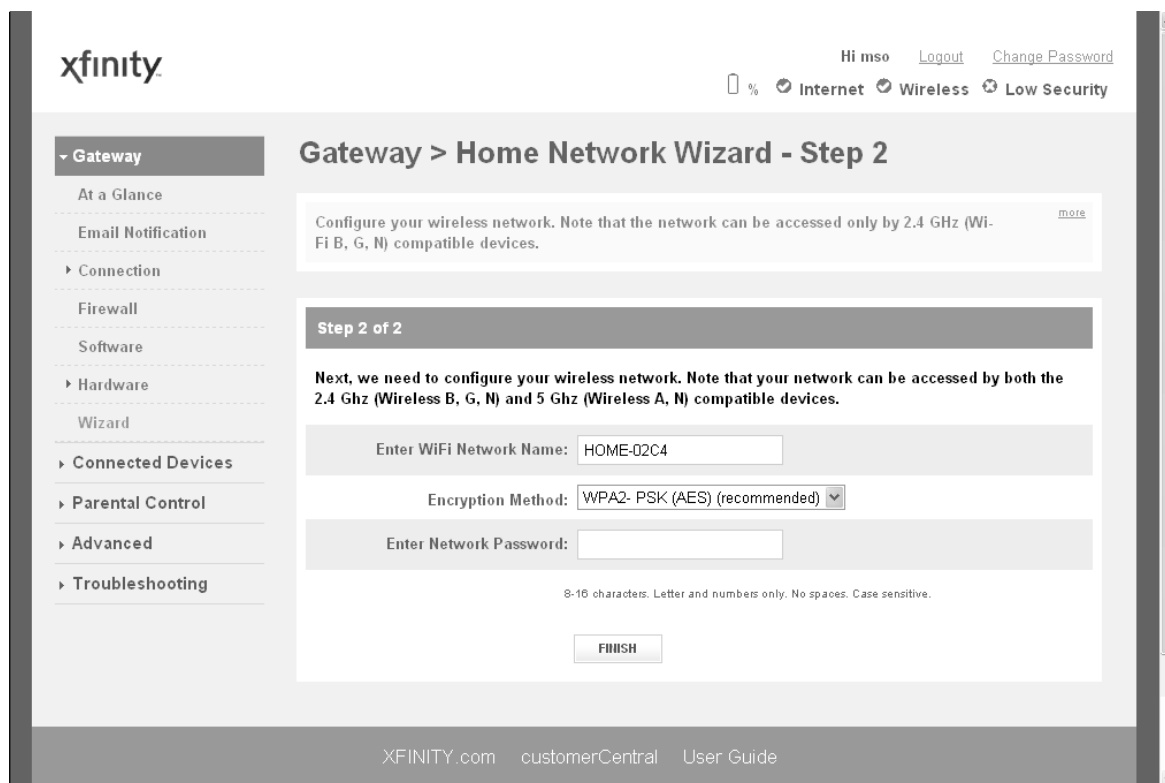


Figure 78. Example of the Second Page of the Home Network Wizard

Table 36. Home Network Wizard – Step 2

Option	Description
Enter WiFi Network Name	Enter the name of your wireless network (typically, the SSID). The Wi-Fi name will make it more obvious for others to know which network they are connecting to.
Encryption Method	<p>To prevent other computers in the area from using your Internet connection, secure your wireless network by selecting an encryption method from this drop-down list. There are several selections available, including the following. (Risky appears next to selections that provide little or no protection).</p> <ul style="list-style-type: none">• Open = wireless transmissions are not protected.• WEP = basic encryption and therefore least secure (i.e., it can be easily cracked, but is compatible with a wide range of devices including older hardware). WEP 64- and 128-bit selections are provided.• WPA-PSK = designed for home and small-office networks. Each wireless network device encrypts the network traffic using a 256-bit key. Select this option if your wireless adapters support WiFi Protected Access Pre-shared Key (WPA-PSK) mode.• WPA2 = second generation of WPA that adds CCMP encryption with mathematically proven security. Select this option if your wireless adapters support WPA2.• WPA-Enterprise = provides extremely strong wireless security and adds authentication to WEP's basic encryption. This option is mainly suited for enterprise users, not home users, and can be selected if your wireless adapters support WPA-Enterprise.• WPA2-Enterprise = second generation of WPA2-Enterprise. This option is mainly suited for enterprise users, not home users, and can be selected if your wireless adapters support WPA2-Enterprise.
Enter Network Password	If you select one of the WEP or WPA encryption settings, enter the password used for encryption and decryption.
FINISH button	Click this button to complete the Home Network Wizard.

Working with Connected Devices

Using the submenus under **Connected Devices**, you can:

- View computers connected to the Gateway's LAN
- Add computer's with static IP addresses to the Gateway's LAN
- Add WiFi-protected clients to the Gateway's LAN

All of these activities are performed from the Computers menu. To display the Computers menu, click **Connected Devices** in the menu bar. Figure 79 shows an example of the Computers menu.

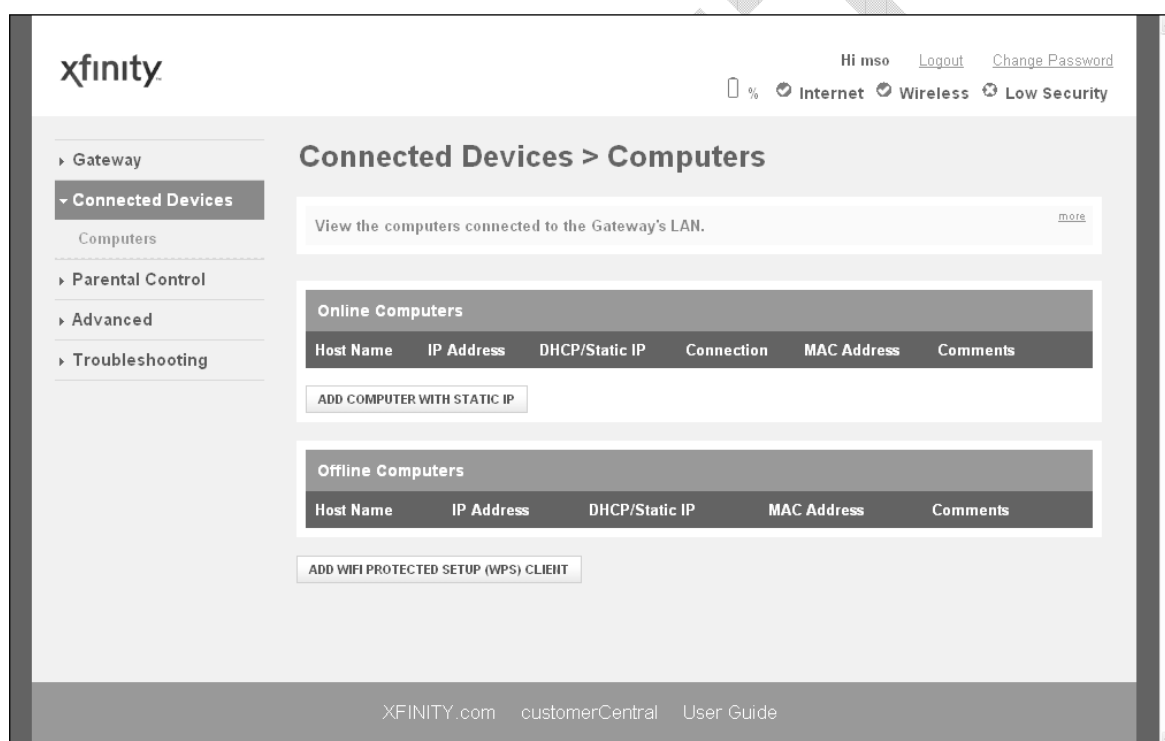


Figure 79. Example of the Computers Menu

Manually Adding Computers with Static IP Addresses

To manually add a computer with a static IP address to the Gateway's LAN, perform the following procedure from the Computers menu.

1. Under **Online Computers**, click the **ADD COMPUTER WITH STATIC IP** button. The Add Computer menu appears (see Figure 80).
2. Complete the fields in the Add Computer menu (see Table 37).
3. Click **SAVE** to save your settings (or click **CANCEL** to discard them). If you click **SAVE**, the Computer menu reappears, with the computer you added displayed under **Offline Computers**.
4. To add more computers with static IP addresses, repeat steps 1 through 3.
5. To edit an online computer, click the **EDIT** button next to the computer you want to modify, edit the settings on the Edit Computer menu (see Figure 81 and Table 38), and click **SAVE**.<l did not see this button??>
6. To delete an online or offline computer, click the **X** next to the computer. When the Delete Computer message appears, click **OK** to delete the computer or **CANCEL** to retain it. If you clicked **OK**, the computer is removed from the Computers menu.

The screenshot displays the Xfinity Gateway web interface. At the top left is the 'xfinity' logo. On the top right, there is a user profile 'Hi mso' with links for 'Logout' and 'Change Password'. Below this, there are status indicators for 'Internet', 'Wireless', and 'Low Security'. A left-hand navigation menu includes 'Gateway', 'Connected Devices' (selected), 'Range Extenders', 'Parental Control', 'Advanced', and 'Troubleshooting'. The main content area is titled 'Connected Devices > Computers > Add Computer'. It contains a placeholder for help text and a form titled 'Add Computer with Static IP Address'. The form fields are: 'Host Name' (text input), 'Connection' (set to 'Ethernet'), 'MAC Address' (text input), 'Static IP Address' (text input), and 'Comments' (text area with up/down arrows). At the bottom of the form are 'SAVE' and 'CANCEL' buttons. The footer of the page includes 'XFINITY.com', 'customerCentral', and 'User Guide'.

Figure 80. Example of the Add Computer Menu

Table 37. Add Computer Menu

Option	Description
HostName	Host name of the computer you want to add.
Connection	Read-only field that displays shows the network connection of Ethernet .
MAC Address	MAC address of the computer you want to add. Add a colon between each 2-character ID in the MAC address. For information about obtaining the MAC address of a computer, see "Determining a Computer's MAC Address" on page 196.
Static IP Address	Static IP address of the computer you want to add. Add a period between each octet in the IP address.
Comments	Optional comments about the computer.
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Add Computer menu.

DRAFT

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

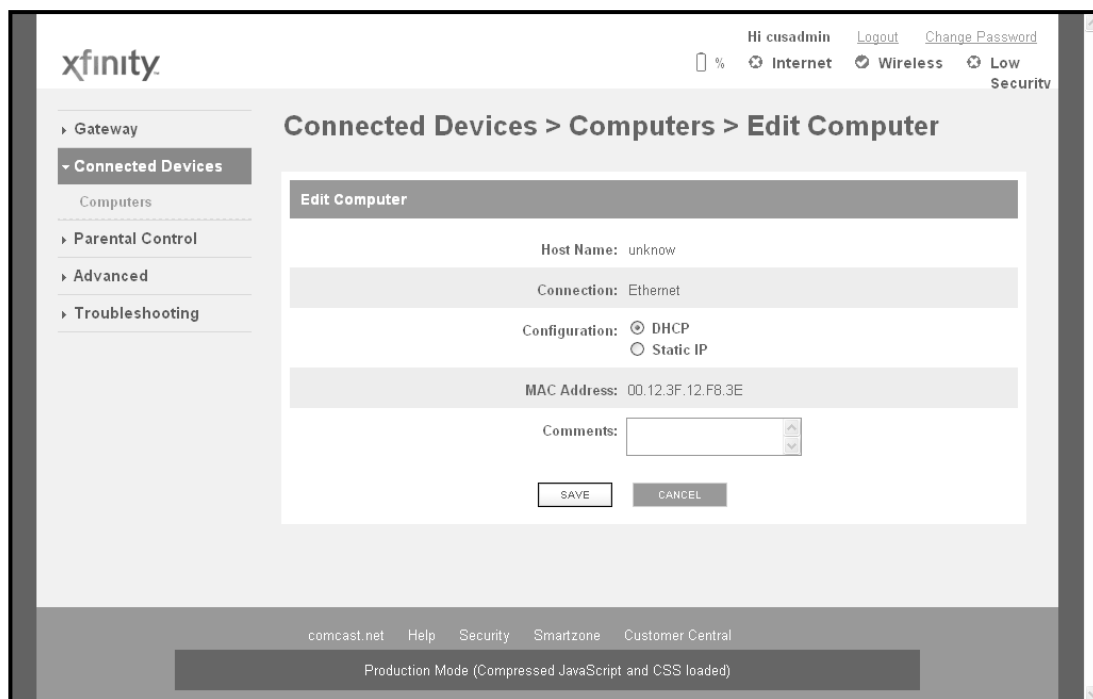


Figure 81. Example of the Edit Computer Menu

Table 38. Edit Computer Menu

Option	Description
Host Name	Read-only field that shows the host name of the computer you selected.
Connection	Read-only field that displays shows the network connection of Ethernet .
Configuration	Select whether the selected computer should be discovered by the Gateway using DHCP or a static IP address. If you select Static IP , enter the static IP address in the Static IP Address field.
MAC Address	Edit the MAC address of the selected computer. Add a colon between each 2-character ID in the MAC address.
Static IP Address	If you selected Static IP for Configuration , enter the computer's static IP address. Add a period between each octet in the IP address.
Comments	Optional comments about the computer.
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Edit Computer menu.

Manually Adding Wireless Clients

You can manually add a wireless client to the Gateway's LAN using Wireless Protected Setup (WPS). While not a security feature, WPS is a standard for easy and secure wireless network set up and connections.



Note: WPS is optional for Wi-Fi Certified products. Check for the Wi-Fi Protected Setup logo or terms on products to see whether the product is WPS compatible.

A few of the key advantages associated with WPS are:

- WPS automatically configures the network name (SSID) and WPA security key for the Gateway or access point and for wireless devices that join the network.
- You do not have to know the network name and security keys or passphrases to use WPS to join a wireless network.
- Security keys or passphrase because are generated randomly generated, making them nearly impossible to guess.
- WPS uses the Extensible Authentication Protocol (EAP), a strong authentication protocol used in WPA2.

To manually add a wireless client to the Gateway's LAN, perform the following procedure from the Computers menu.

1. Under **Offline Computers**, click the **ADD WIFI PROTECTED SETUP (WPS) CLIENT** button. The Add Wireless Client menu appears (see Figure 82).
2. Complete the fields in the Add Wireless Client menu (see Table 39).
3. Click **PAIR** to pair the wireless device with the Gateway's LAN (pairing can take up to 2 minutes). Alternatively, if your wireless device has a Pair button, you can press this button to pair the device with the Gateway's LAN.
4. If you click **PAIR**, the Private Wireless Advanced Setting options in the WiFi menu appear. For information about completing these settings see page 50.
5. To add more wireless devices, repeat steps 1 through 4.
6. To edit an online wireless device, click the **EDIT** button next to the computer you want to modify, edit the settings on the Edit Computer menu (see Figure 82 and Table 39), and click **SAVE**.<<l did not see this button??>>
7. To delete an online or offline wireless device, click the **X** next to the device. When the Delete Computer message appears, click **OK** to delete the device or **CANCEL** to retain it. If you clicked **OK**, the device is removed from the Computers menu. <<true??>>

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

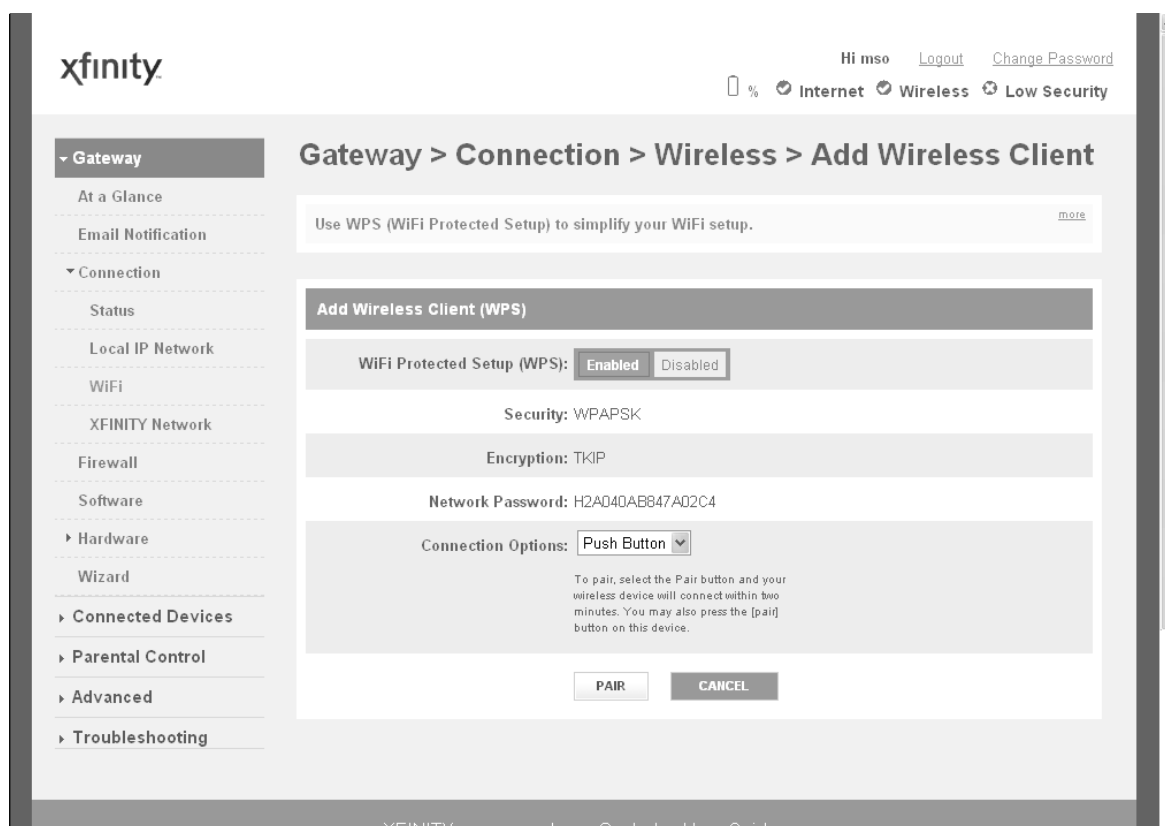


Figure 82. Example of the Add Wireless Client Menu

Table 39. Edit Wireless Client Menu

Option	Description
WiFi Protected Setup (WPS)	Enables or disables the Gateway's WPS setup. <ul style="list-style-type: none"> Enabled = Gateway's WPS setup is activated. (<i>default</i>) Disabled = Gateway's WPS setup is not activated.
Security	Read-only screen that shows the security, if any, used on the Gateway's wireless LAN. To change the security used, see the Encryption Method option in the Home Network Wizard – Step 2 menu (see “Configuring Your Home Network” on page 131).
Encryption	Read-only screen that shows the encryption method, if any, used on the Gateway's wireless LAN. To change the encryption method used, see the Encryption Method option in the Home Network Wizard – Step 2 menu (see “Configuring Your Home Network” on page 131).
Network Password	Read-only screen that shows the network password you entered in the Enter Network Password option in the Home Network Wizard – Step 2 menu (see “Configuring Your Home Network” on page 131).

Option	Description
Connection Options	<p>Determines whether WPS can be configured using a PIN or the WPS button on the front panel of the Gateway.</p> <ul style="list-style-type: none"> • PIN = requires you to enter a PIN in the WPS Setup menu to configure WPS. The PIN can be viewed in the AP PIN option in the WiFi Client Setup Configuration (WP5) section of the Wireless Menu (see page 120). • PBC = Push Button Configuration. Lets you use the WPS button on the front panel of the Gateway to configure WPS.
PAIR button	Click this button to pair the wireless device settings with the Gateway's LAN (can take up to 2 minutes). If your wireless device has a Pair button, you can press this button instead to pair the device with the Gateway's LAN.
CANCEL button	Click this button to discard your settings on the Add Wireless Client menu.

<<need this screen??>>

Figure 83. Example of the Edit Device Menu

Table 40. Edit Device Menu<<true??>>

Option	Description
HostName	Read-only field that shows the host name of the computer you selected.
Connection	Read-only field that displays shows the network connection of Ethernet .
Configuration	Select whether the selected computer should be discovered by the Gateway using DHCP or a static IP address. If you select Static IP , enter the static IP address in the Static IP Address field.
MAC Address	Edit the MAC address of the selected computer. Add a colon between each 2-character ID in the MAC address.
Static IP Address	If you selected Static IP for Configuration , enter the computer's static IP address. Add a period between each octet in the IP address.
Comments	Optional comments about the computer.
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Edit Computer menu.

Configuring Parental Controls

Regulating Web browsing can prevent children and workers from accessing dangerous content on the Internet, or having to make judgment calls over suitable relationships in chat-rooms. The fact is, Web sites, chat-room users, and downloaded programs may not have the best interests of you, your family, or your workers at heart. The unscrupulous may try to manipulate the people you care about or try to gain trust, which may result in unacceptable access to your family, your coworkers, your computer, or personal information.

Using the **Parental Controls** menu, you can prevent access to unwanted Web content by:

- Blocking sites and keywords. See page 142.
- Blocking services. See page 148.
- Blocking devices and access types. See page 152.

You can also define report filters and generate reports. See page 156.

Blocking Sites and Keywords, and Selecting Trusted Computers

Using the Managed Sites menu, you can restrict access to Web sites for non-trusted computers on the network. This procedure involves the following steps:

1. Specify the sites to be blocked. See “Specifying Sites to be Blocked” on page 143.
2. Specify the keywords to be blocked. See “Specifying Keywords to be Blocked” on page 145.
3. Identify the trusted computers that are allowed to access the blocked Web sites and keywords. See “Defining Trusted Computers” on page 147.

To display the Managed Sites menu, click **Parental Control** in the menu bar. Figure 84 shows an example of the Managed Sites menu.

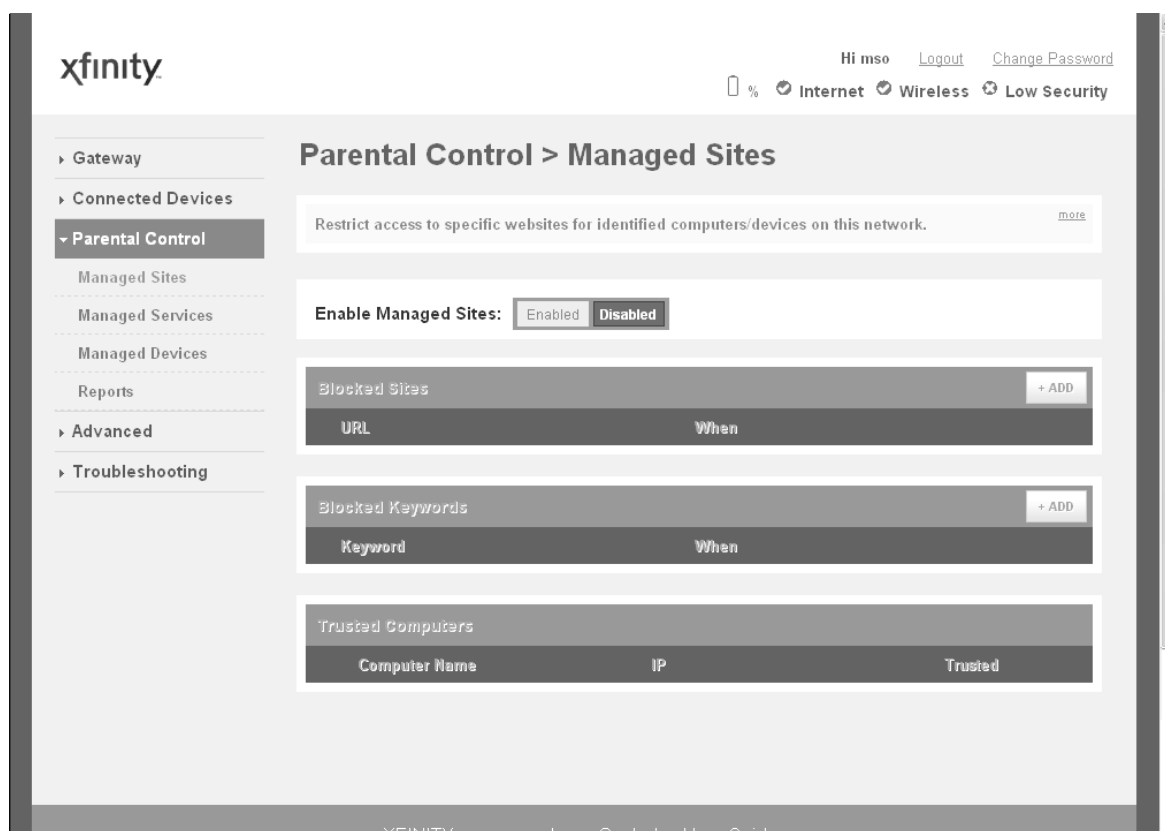


Figure 84. Example of Managed Sites Menu

Specifying Sites to be Blocked

To block sites for non-trusted computers, perform the following procedure from the Managed Sites menu.

1. Next to **Enable Managed Sites**, click **Enabled**.
2. Under **Blocked Sites**, click **ADD**. The Add Blocked Domain menu appears (see Figure 85).
3. Complete the fields in the Add Blocked Domain menu (see Table 41).
4. Click **SAVE** (or click **CANCEL** to discard your settings). If you clicked **SAVE**, the blocked site appears below **Blocked Sites** on the Managed Sites menu.
5. To block additional sites, repeat steps 2 through 4.
6. To edit a blocked site, click the **EDIT** button next to the blocked site you want to modify, edit the settings on the Add Blocked Domain menu (see Table 41), and click **SAVE**.
7. To delete a blocked site, click the **X** next to the site. When the Delete URL Block Rule message appears, click **OK** to delete the blocked URL or **CANCEL** to retain it. If you clicked **OK**, the URL is removed from **Blocked Sites** on the Managed Sites menu.

錯誤! 使用 [常用] 索引標籤將 **Heading 1** 套用到您想要在此處顯示的文字。

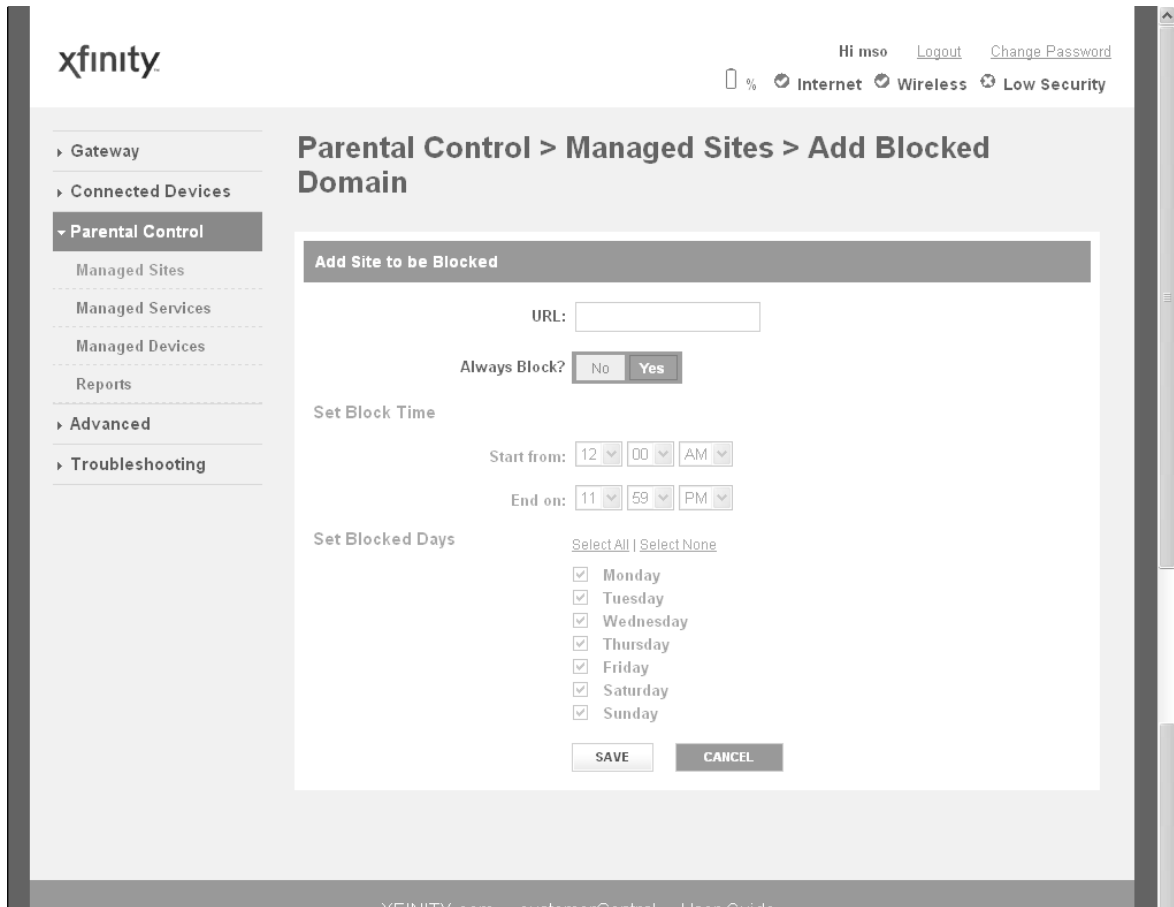


Figure 85. Add Blocked Domain Menu

Table 41. Add Blocked Domain Menu

Option	Description
URL	Enter the URL you want blocked.
Always Block?	Select whether you want the Gateway to always block this URL. Choices are <ul style="list-style-type: none"> No = the Gateway does not always block this URL. Use the Set Block Time and Set Blocked Days to instruct the Gateway when to block this URL. Yes = the Gateway always blocks this URL until you remove the block. (<i>default</i>)
Set Block Time	
Start from	If you selected No for Always Block? , select the time when the Gateway is to start blocking this URL.
End on	If you selected No for Always Block? , select the time when the Gateway is to stop blocking this URL.
Set Blocked Days	

Option	Description
Set Blocked Days	If you selected No for Always Block? , use any of the following methods to specify when the Gateway is to block this URL: <ul style="list-style-type: none">• Select All = blocks the URL for seven days.• Select None = deselect blocking of the URL for seven days.• Monday – Sunday = check the check boxes that correspond to the days when you want the Gateway to block this URL.
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Add Blocked Domain menu.

Specifying Keywords to be Blocked

To block keywords for non-trusted computers, perform the following procedure from the Managed Sites menu.

1. Next to **Enable Managed Sites**, click **Enabled**.
2. Under **Blocked Keywords**, click **ADD**. The Add Blocked Keyword menu appears (see Figure 86).
3. Complete the fields in the Add Blocked Keyword menu (see Table 42).
4. Click **SAVE** (or click **CANCEL** to discard your settings). If you clicked **SAVE**, the blocked keyword appears below **Blocked Keywords** on the Managed Keywords menu.
5. To block additional keywords, repeat steps 2 through 4.
6. To edit a blocked keyword, click the **EDIT** button next to the blocked keyword you want to modify, edit the settings on the Add Blocked Keyword menu (see Table 42), and click **SAVE**.
7. To delete a blocked keyword, click the **X** next to the keyword. When the Delete Keyword Block Rule message appears, click **OK** to delete the blocked keyword or **CANCEL** to retain it. If you clicked **OK**, the keyword is removed from **Blocked Keywords** on the Managed Keywords menu.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

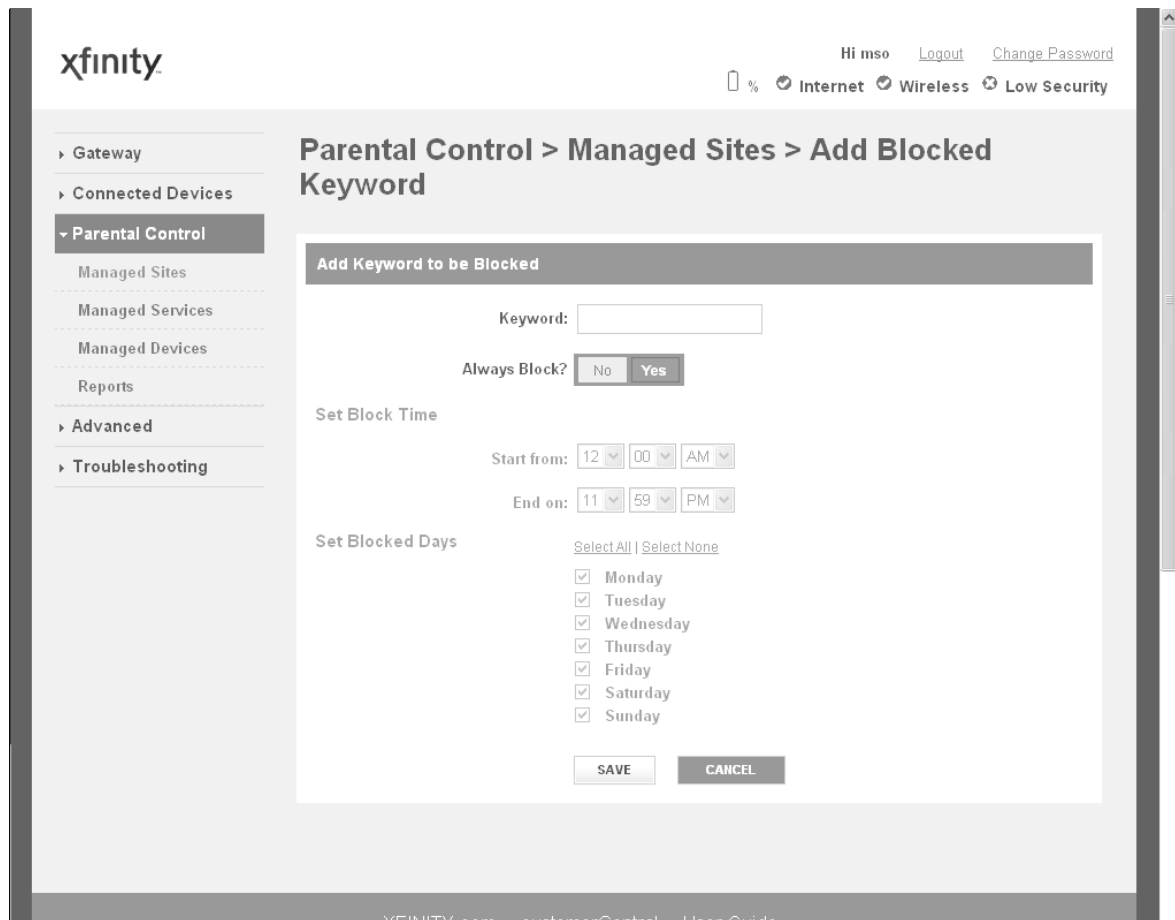


Figure 86. Add Blocked Keyword Menu

Table 42. Add Blocked Keyword Menu

Option	Description
Keyword	Enter the keyword you want blocked.
Always Block?	Select whether you want the Gateway to always block this keyword. Choices are <ul style="list-style-type: none"> • No = the Gateway does not always block this keyword. Use the Set Block Time and Set Blocked Days to instruct the Gateway when to block this Keyword. • Yes = the Gateway always blocks this keyword until you remove the block. (<i>default</i>)
Set Block Time	
Start from	If you selected No for Always Block? , select the time when the Gateway is to start blocking this keyword.
End on	If you selected No for Always Block? , select the time when the Gateway is to stop blocking this keyword.
Set Blocked Days	
Set Blocked Days	If you selected No for Always Block? , use any of the following methods to specify when the Gateway is to block this keyword: <ul style="list-style-type: none"> • Select All = blocks the keyword for seven days. • Select None = deselect blocking of the keyword for seven days. • Monday – Sunday = check the check boxes that correspond to the days when you want the Gateway to block this keyword.
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Add Blocked Keyword menu.

Defining Trusted Computers

Trusted computers let you exempt connected computers from the blocked site and blocked keyword rules you defined in the previous sections. To build a list of trusted computers, perform the following procedure from the Managed Sites menu.

<<need to verify??>>

Blocking Services and Selecting Trusted Computers

Using the Managed Services menu, you can restrict access to certain services and applications for non-trusted computers on the network.

This procedure involves the following steps:

1. Specify the services to be blocked. See “Specifying Services” on page 149.
2. Identify the trusted computers that are allowed to access the blocked services. See “Defining Trusted Computers” on page 151.

To display the Managed Services menu, click **Parental Control > Managed Services** in the menu bar. Figure 87 shows an example of the menu.

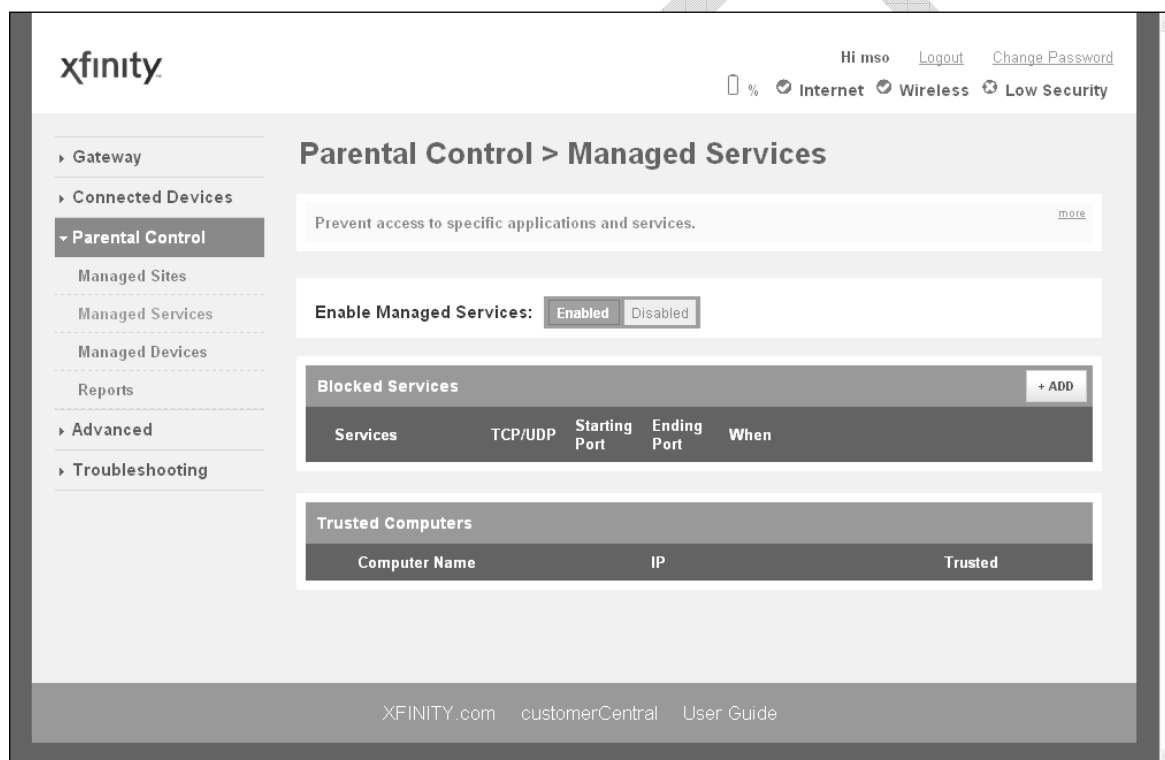


Figure 87. Example of Managed Services Menu

Specifying Services to be Blocked

To block services for non-trusted computers, perform the following procedure from the Managed Services menu.

1. Next to **Enable Managed Services**, click **Enabled**.
2. Under **Blocked Services**, click **ADD**. The Add Blocked Service menu appears (see Figure 88).
3. Complete the fields in the Add Blocked Service menu (see Table 43).
4. Click **SAVE** (or click **CANCEL** to discard your settings). If you clicked **SAVE**, the blocked service appears below **Blocked Services** on the Managed Services menu.
5. To block additional services, repeat steps 2 through 4.
6. To edit a blocked service, click the **EDIT** button next to the blocked service you want to modify, edit the settings on the Add Blocked Service menu (see Table 43), and click **SAVE**.
7. To delete a blocked service, click the **X** next to the service. When the Delete Service Block Rule message appears, click **OK** to delete the blocked URL or **CANCEL** to retain it. If you clicked **OK**, the service is removed from **Blocked Services** on the Managed Services menu.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

xfinity

Hi mso [Logout](#) [Change Password](#)

% Internet Wireless Low Security

Parental Control > Managed Services > Add Blocked Service

Add Service to be Blocked

User Defined Service:

Protocol: TCP/UDP

Start Port:

End Port:

Always Block? No Yes

Set Block Time

Start from: 12 00 AM

End on: 11 59 PM

Set Blocked Days

Select All | Select None

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday

SAVE CANCEL

Figure 88. Add Blocked Service Menu

Table 43. Add Blocked Service Menu

Option	Description
User Defined Service	Enter the service you want blocked.
Protocol	The type of protocol associated with the service to be blocked. Choices are: <ul style="list-style-type: none"> • TCP • UDP • TCP/UDP (<i>default</i>)
StartPort	Starting port number on which the block will be applied. If necessary, contact the application vendor for this information.
End Port	Ending port number on which the block will be applied. If necessary, contact the application vendor for this information.
Always Block?	Select whether you want the Gateway to always block this service. Choices are <ul style="list-style-type: none"> • No = the Gateway does not always block this service. Use the Set Block Time and Set Blocked Days to instruct the Gateway when to block this service. • Yes = the Gateway always blocks this service until you remove the block. (<i>default</i>)
Set Block Time	
Start from	If you selected No for Always Block? , select the time when the Gateway is to start blocking this service.
End on	If you selected No for Always Block? , select the time when the Gateway is to stop blocking this service.
Set Blocked Days	
Set Blocked Days	If you selected No for Always Block? , use one of the following methods to specify when the Gateway is to block this service: <ul style="list-style-type: none"> • Select All = blocks the service for seven days. • Select None = deselect blocking of the service for seven days. • Monday – Sunday = check the check boxes that correspond to the days when you want the Gateway to block this service.
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Add Blocked Domain menu.

Defining Trusted Computers

Trusted computers let you exempt connected computers from the blocked services rules you defined in the previous section. To build a list of trusted computers, perform the following procedure from the Managed Sites menu.

<<need to verify??>>

Managing Devices and Access Types

Using the Managed Devices menu, you can enable or disable managed devices and allow or block all access types. You can also add devices you want to block.

To display the Managed Devices menu, click **Parental Control > Managed Devices** in the menu bar. Figure 89 shows an example of the menu.

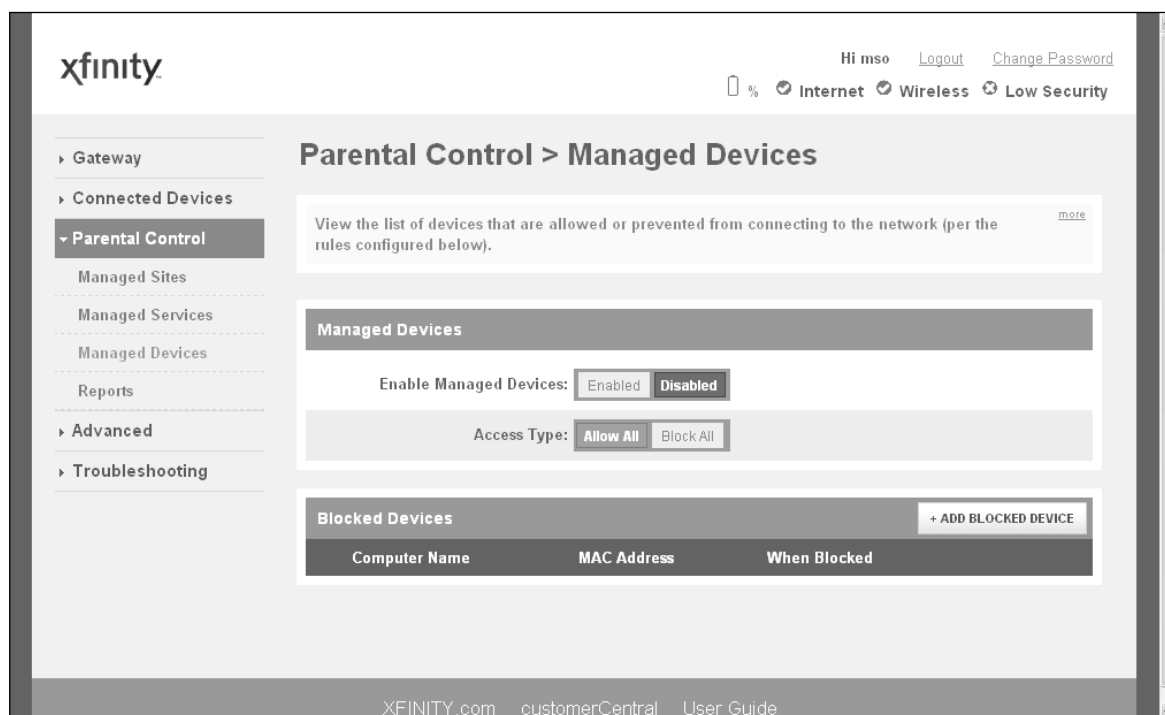


Figure 89. Example of Managed Devices Menu

Enabling or Disabling Managed Devices

By default, all managed devices are disabled. To enable them, display the Managed Devices menu and click **Enabled** next to **Enable Managed Devices**.

Enabling or Disabling Access Types

By default, all access types are allowed. To block them, display the Managed Devices menu and click **Block All** next to **Access Type**.

Adding Blocked Devices

To add devices you want to block, perform the following procedure from the Managed Devices menu.

1. Next to **Blocked Devices**, click **ADD BLOCKED DEVICE**. The Add Blocked Device menu appears (see Figure 90).
2. Completed the fields in the Add Block Device menu (see Table 44).
3. Click **SAVE** (or click **CANCEL** to discard your settings). If you clicked **SAVE**, the blocked device appears below **Blocked Devices** on the Managed Devices menu.
4. To block additional devices, repeat steps 1 through 3.
5. To edit a blocked device, click the **EDIT** button next to the blocked device you want to modify, edit the settings on the Add Blocked Device menu (see Table 44), and click **SAVE**.
6. To delete a blocked device, click the **X** next to the service. When the Delete Blocked MAC Rule message appears, click **OK** to delete the blocked device or **CANCEL** to retain it. If you clicked **OK**, the device is removed from **Blocked Devices** on the Managed Devices menu.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

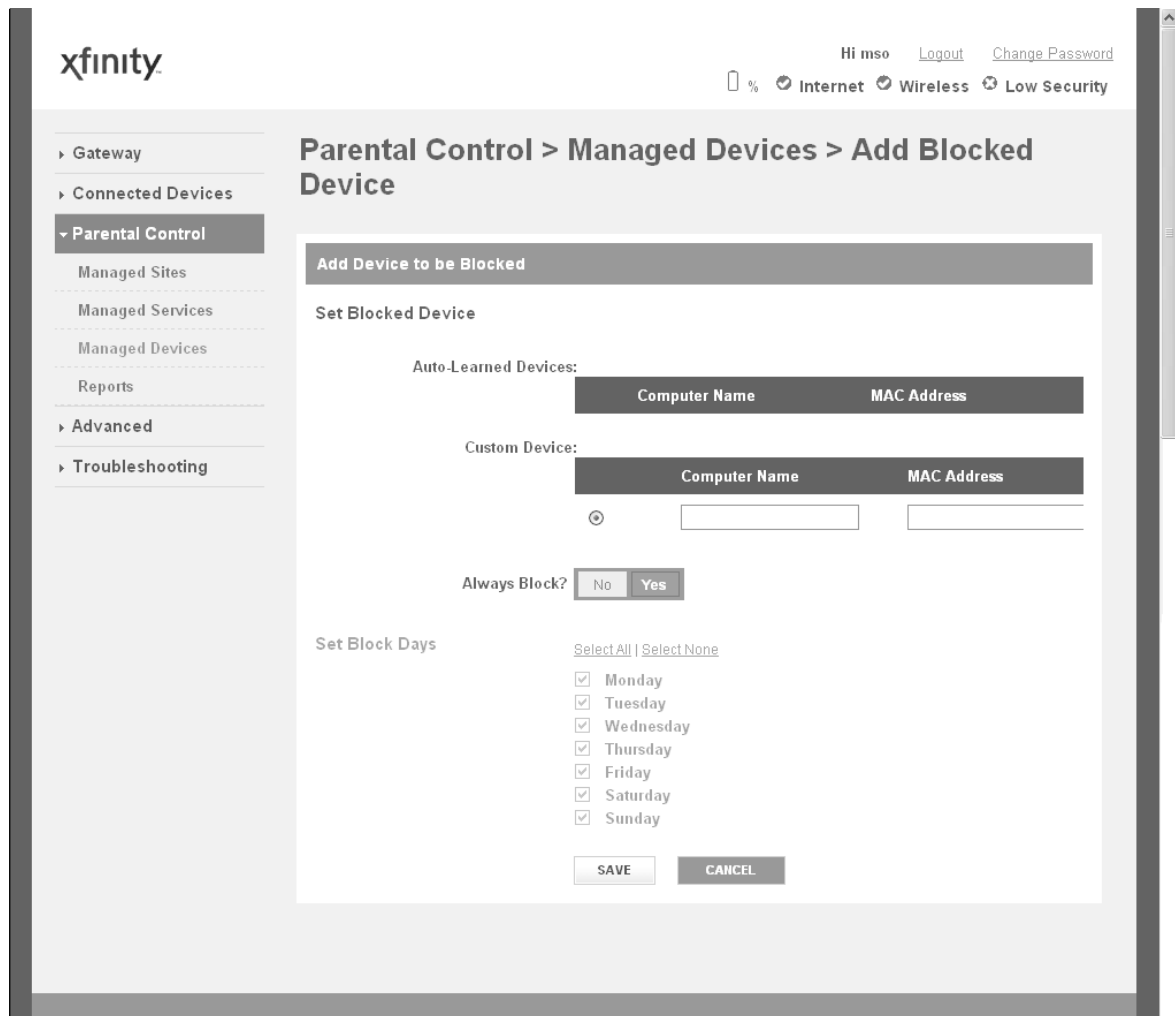


Figure 90. Add Blocked Device Menu

Table 44. Add Blocked Device Menu

Option	Description
Auto-Learned Devices	To select a device that the Gateway automatically learned, select the device under Auto-Learned Devices .
Custom Device	To select a custom device, enter the name and MAC address of the device in the Computer Name and MAC Address fields below Custom Device .
Always Block?	Select whether you want the Gateway to always block this device. Choices are <ul style="list-style-type: none"> • No = the Gateway does not always block this device. Use the Set Block Time and Set Blocked Days to instruct the Gateway when to block this device. • Yes = the Gateway always blocks this device until you remove the block. (<i>default</i>)
Set Block Time	
Start from	If you selected No for Always Block? , select the time when the Gateway is to start blocking this device.
End on	If you selected No for Always Block? , select the time when the Gateway is to stop blocking this device.
Set Blocked Days	
Set Blocked Days	If you selected No for Always Block? , use one of the following methods to specify when the Gateway is to block this device: <ul style="list-style-type: none"> • Select All = blocks the device for seven days. • Select None = deselect blocking of the device for seven days. • Monday – Sunday = check the check boxes that correspond to the days when you want the Gateway to block this device.
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Add Blocked Device menu.

Generating Reports

Using the Reports menu, you can define filters for managed sites, services, and devices, and then show, print or download the reports. To display the Reports menu, click **Parental Control > Reports** in the menu bar. Figure 91 shows an example of the menu.

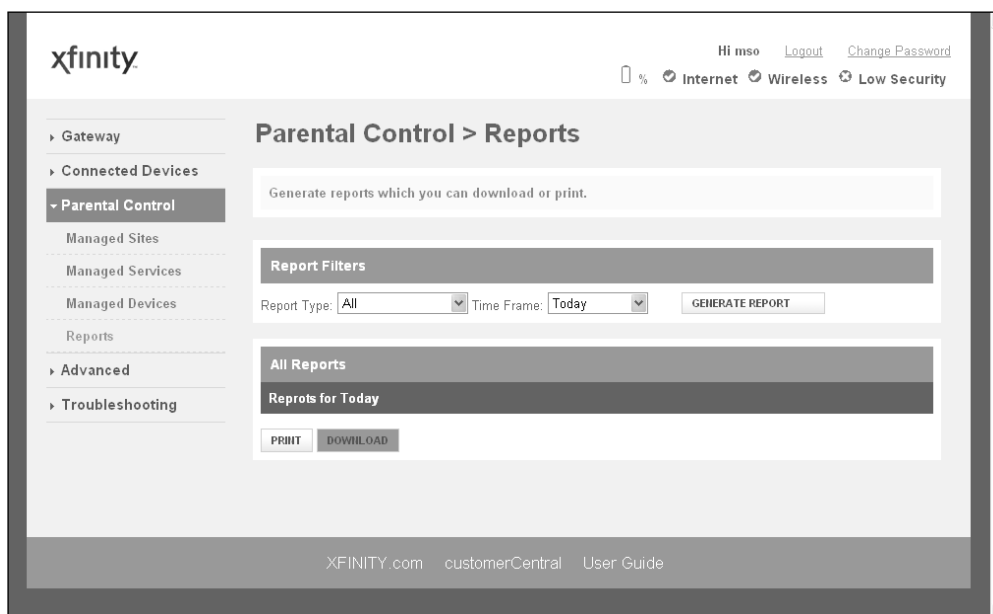


Figure 91. Example of Reports Menu

Under **Reports Filters**, you can set a report filter for the type of reports you want to generate and the time frame they are to cover. If you do not set a report filter, the default filter is automatically set to all report types for the current day (today). After you define the filter, you can show, print, or download the report.

1. Using the **Report Type** drop-down list, select the report to which you want to apply a filter, Choices are:
 - All
 - Managed Sites
 - Managed Services
 - Managed Devices
2. Using the **Time Frame** drop-down list, select a time frame that the report is to cover.
3. To show the report, click the **GENERATE REPORT** button.
4. To print the report with the filter applied, click **PRINT**.
5. To download the report with the filter applied, click **DOWNLOAD**

Using Advanced Features

Using the **Advanced Features** menu, you can:

- Enable or disable port forwarding. See page 157.
- Enable or disable port triggering. See page 160.
- Enable or disable remote management. See page 163.
- Configuring DMZ settings. See page 165.
- Configure routing. See page 167.
- Configure Dynamic DNS. See page 169.
- Use the Gateway's UPnP feature to discover UPnP-enabled devices. See page 171.

Enabling or Disabling Port Forwarding

Using the Firewall menu (described on page 53), you can configure the Gateway to create a firewall between your internal network and the Internet. A firewall keeps unwanted traffic from the Internet away from your networked computers. There may be times, however, when you want a "tunnel" to be created through the Gateway firewall, so computers on the Internet can communicate to one of the computers on your LAN using a single port. This is handy for running Web servers, game servers, FTP servers, or even video conferencing.

Port forwarding allows outside users access to the computers on your LAN using a given port or range of ports. Using port forwarding, for example, one of your computers can run a Web server (port 80) while another computer runs an FTP server (port 23) - both using the same IP address.

You configure the Gateway's port forwarding feature using the Port Forwarding menu. To display this menu, click **Advanced** in the menu bar. Figure 92 shows an example of the menu.

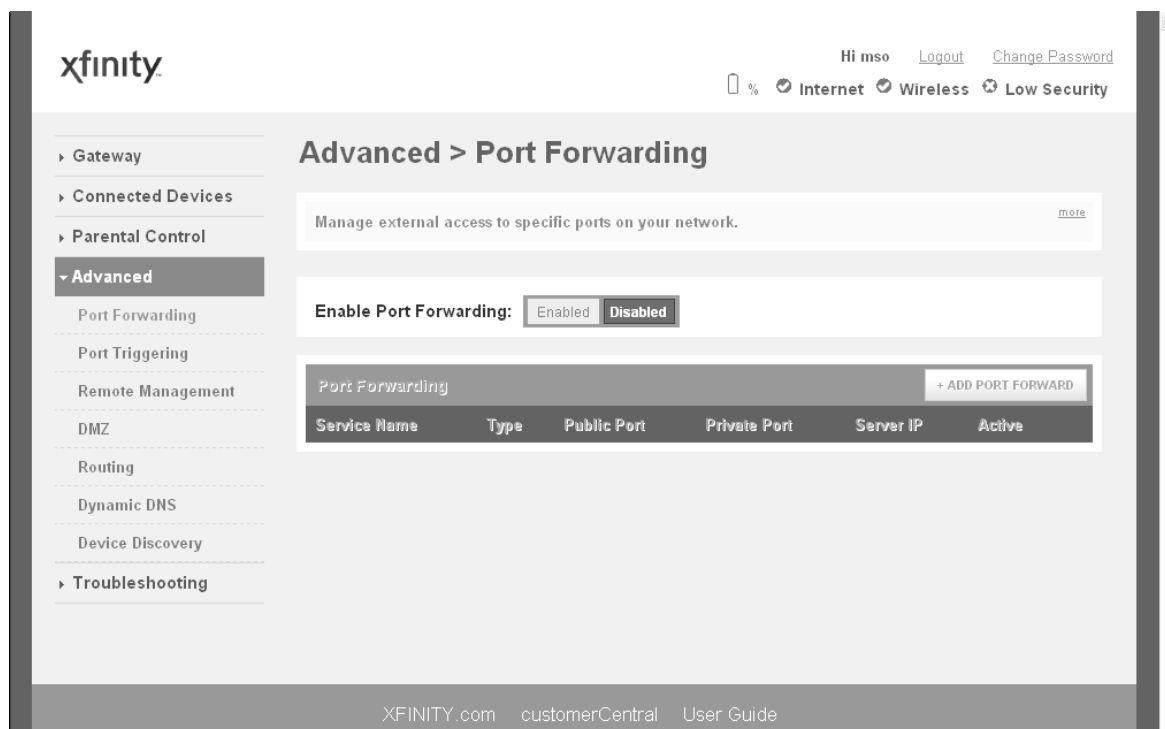


Figure 92. Example of Port Forwarding Menu

Adding a Port Forwarding Rule

To add a port forwarding rule, perform the following procedure from the Port Forwarding menu.

1. Next to **Enable Port Forwarding**, click **Enabled**.
2. Click the **ADD PORT FORWARD** button. The Add Service menu appears (see Figure 93).
3. Complete the fields in the Add Service menu (see Table 45).
4. Click **SAVE** to save your settings (or click **CANCEL** to discard them). If you click **SAVE**, the port forwarding rule appears below **Port Forwarding** on the Port Forwarding menu.
5. To add more port forwarding rules, repeat steps 2 through 4.
6. To edit a port forwarding rule, click the **EDIT** button next to the rule you want to modify, edit the settings on the Add Service menu (see Table 45), and click **SAVE**.
7. To delete a port forwarding rule, click the **X** next to the rule. When the Delete Port Forwarding Rule message appears, click **OK** to delete the port forwarding rule or **CANCEL** to retain it. If you clicked **OK**, the rule is removed from the **Port Forwarding** area on the Port Forwarding menu.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

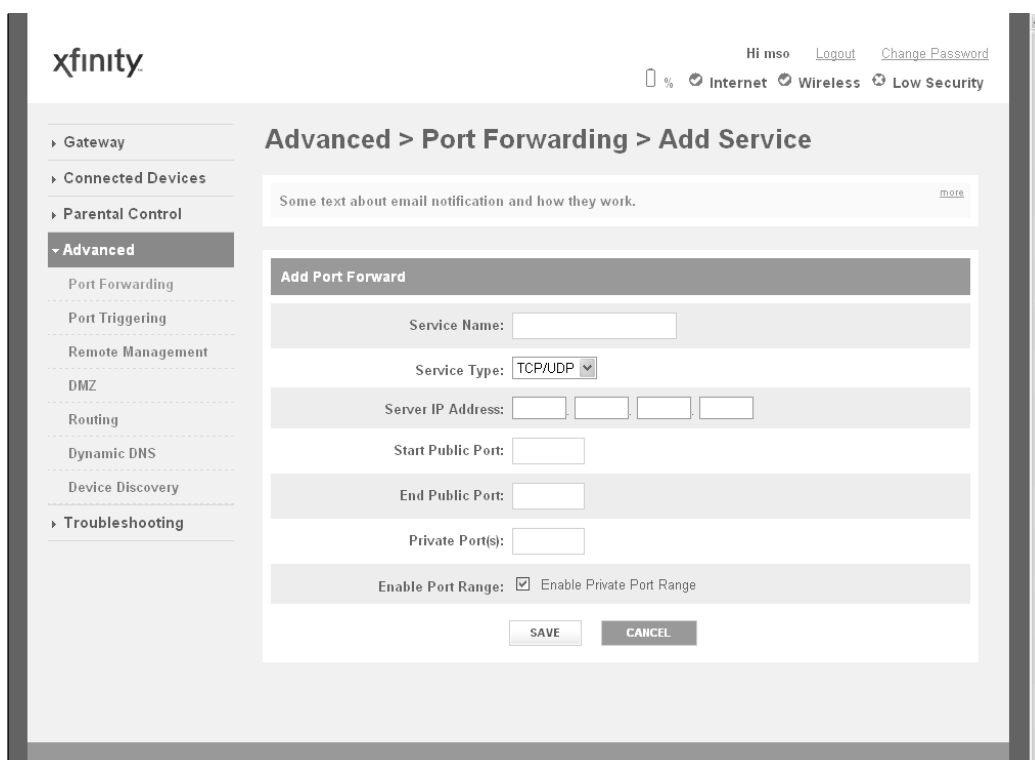


Figure 93. Add Service Menu

Table 45. Add Service Menu

Option	Description
Service Name	Name for identifying the service. The name is for reference purposes only.
Service Type	The protocol you want to use with the service. Choices are: <ul style="list-style-type: none"> • TCP • UDP • TCP/UDP (default)
Service IP Address	IP address of the LAN computer or server that is running the service.
Start Public Port	Starting number of the port on which the service is provided.
End Public Port	Ending number of the port on which the service is provided. This field is unavailable if the Gateway is configured for a single public IP port.
Private Port(s)	Numbers of the ports whose traffic the Gateway forwards to the LAN. If there is a range of ports, enter the starting private port here and check Enable Port Range . The Gateway automatically calculates the end private port. The LAN computer server listens for traffic/data on this port (or these ports).
Enable Port Range	Check this box to enable the private port range specified in Private Port(s) .
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Add Service menu.

Disabling Port Forwarding

You can disable individual or all port-forwarding rules from the Port Forwarding menu.

- To disable an individual port-forwarding rule, uncheck the rule in the **Active** column. Although disabled, you can still use the buttons to the right of the checkbox to edit or delete the rule. To enable the rule, check the checkbox in the **Active** column.
- To disable all port-forwarding rules, click **Disabled** next to **Enable Port Forwarding**. The **ADD PORT FORWARD** button becomes unavailable and all port forwarding rules turn gray to show they are disabled. In addition, the buttons to the right of the checkboxes become gray, preventing you from editing or deleting port-forwarding rules. To enable all port-forwarding rules, click **Enabled** next to **Enable Port Forwarding**.

Enabling or Disabling Port Triggering

Using the Port Triggering menu, you can configure the Gateway to detect port triggers for multiple-session applications and allow them to pass through the firewall. For special applications, besides the initial communication session, there are multiple related sessions created during the protocol communications. Normally, a normal treats the triggered sessions as independent sessions and blocks them. However, the Gateway can co-relate the triggered sessions with the initial session and group them together in the NAT session table. As a result, you need only specify which protocol type and port number you want to track, as well as some other related parameters. In this way, the Gateway can pass the special applications according to the supplied information.

Assume, for example, that to use H.323 in a Net Meeting application, a local client starts a session A to a remote host. The remote host uses session A to communicate with the local host, but it also could initiate another session B back to the local host. Since there is only session A recorded in the NAT session table when the local host starts the communication, session B is treated as an illegal access from the outside and is blocked. Using the Special Application menu, you can configure the Gateway to co-relate sessions A and B and automatically open the port for the incoming session B.

To display the Port Triggering menu, click **Advanced > Port Triggering** in the menu bar. Figure 94 shows an example of the menu.

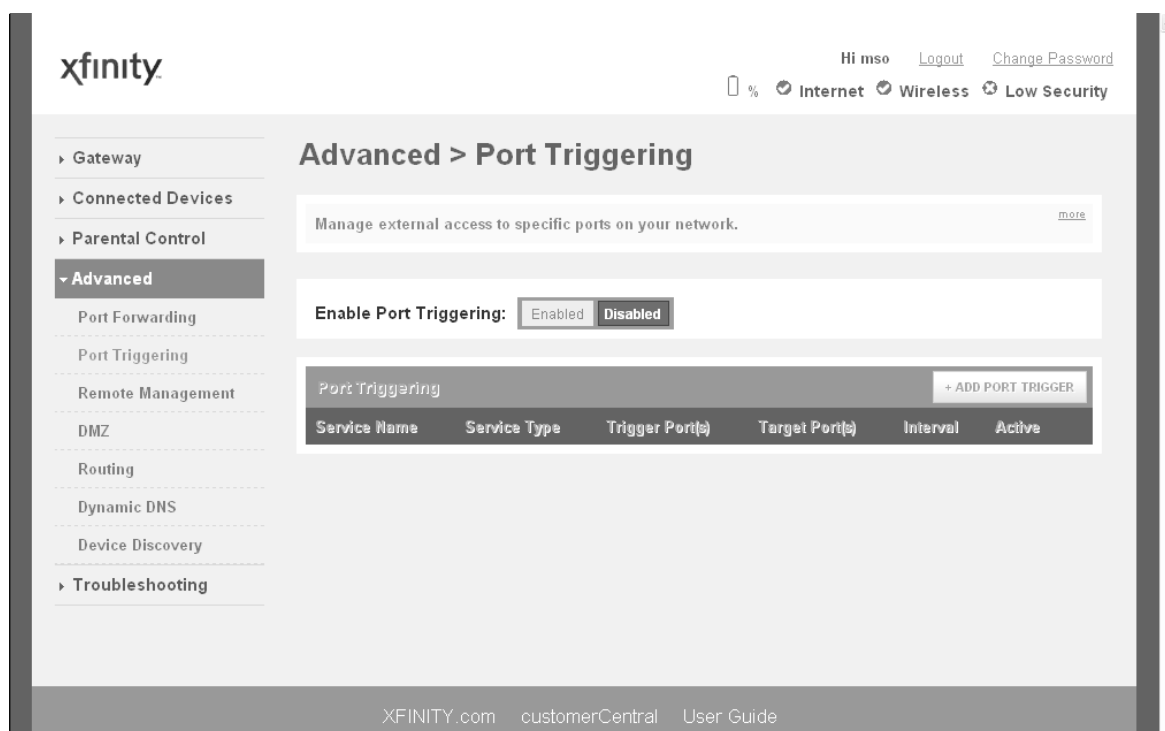


Figure 94. Example of Port Triggering Menu

Adding a Port Triggering Rule

To add a port triggering rule, perform the following procedure from the Port Triggering menu.

1. Next to **Enable Port Triggering**, click **Enabled**.
2. Click the **ADD PORT FORWARD** button. The Port Triggering Add menu appears (see Figure 95).
3. Complete the fields in the Port Triggering Add menu (see Table 46).
4. Click **SAVE** to save your settings (or click **CANCEL** to discard them). If you click **SAVE**, the port triggering rule appears below **Port Triggering** on the Port Triggering menu.
5. To add more port triggering rules, repeat steps 2 through 4.
6. To edit a port triggering rule, click the **EDIT** button next to the rule you want to modify, edit the settings on the Port Triggering Add menu (see Table 46), and click **SAVE**.
7. To delete a port triggering rule, click the **X** next to the rule. When the Delete Port Triggering Rule message appears, click **OK** to delete the port triggering rule or **CANCEL** to retain it. If you clicked **OK**, the rule is removed from the **Port Triggering** area on the Port Triggering menu.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

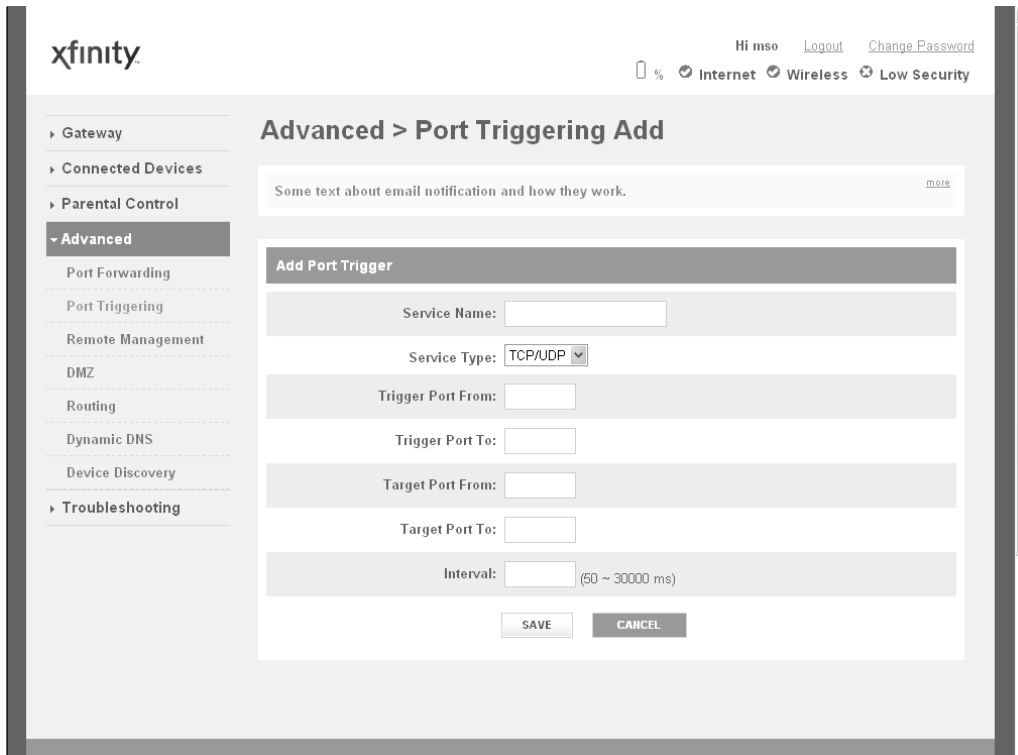


Figure 95. Port Triggering Add Menu

Table 46. Port Triggering Add Menu

Option	Description
Service Name	Name for identifying the trigger. The name is for reference purposes only.
Service Type	The type of protocol you want to use with the trigger. Choices are: <ul style="list-style-type: none"> • TCP • UDP • TCP/UDP (<i>default</i>) For example, to track the H.323 protocol, the protocol type should be TCP.
Trigger Port From	From port ranges of the special application. For example, to track H.323 protocol, the From port should be 1720.
Trigger Port To	To port ranges of the special application. For example, to track H.323 protocol, the To port should be 1720.
Target Port From	Starting port range for the target port listening for the special application.
Target Port To	Ending port range for the target port listening for the special application.
Interval	Specify the interval between 50 and 30000 between two continuous sessions. If the interval exceeds this time interval setting, the sessions are considered to be unrelated.
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Port Triggering Add menu.

Disabling Port Triggering

You can disable individual or all port-triggering rules from the Port Triggering menu.

- To disable an individual port-triggering rule, uncheck the rule in the **Active** column. Although disabled, you can still use the buttons to the right of the checkbox to edit or delete the rule. To enable the rule, check the checkbox in the **Active** column.
- To disable all port-triggering rules, click **Disabled** next to **Enable Port Triggering**. The **ADD PORT TRIGGER** button becomes unavailable and all port triggering rules turn gray to show they are disabled. In addition, the buttons to the right of the checkboxes become gray, preventing you from editing or deleting port-triggering rules. To enable all port-triggering rules, click **Enabled** next to **Enable Port Triggering**.

Remote Management

The Gateway supports centralized administration and management via the following methods:

- HTTP
- HTTPS
- Telnet
- SSH
- SNMP
- HNAP

Using the Remote Management menu, you can independently enable or disable these remote management methods. The Remote Management menu also lets you provide remote access to a single computer, a group of computers that fall within a particular range of IP addresses, or any computer.

To display the Remote Management menu, click **Advanced > Remote Management** in the menu bar. Figure 96 shows an example of this menu and Table 47 describes the settings.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

The screenshot shows the xfinity web interface for configuring Remote Management. The page title is "Advanced > Remote Management". On the left, a navigation menu includes Gateway, Connected Devices, Parental Control, Advanced (selected), Port Forwarding, Port Triggering, Remote Management, DMZ, Routing, Dynamic DNS, Device Discovery, and Troubleshooting. The main content area has a sub-header "Advanced > Remote Management" and a text box with "Some text about Remote Management and how it works." Below this is a "Remote Management" section with several rows of configuration options, each with a text input field and "Enabled" or "Disabled" buttons:

HTTP:	8080	Enabled	Disabled
HTTPs:	8181	Enabled	Disabled
Telnet:	2323	Enabled	Disabled
SSH:	22	Enabled	Disabled
SNMP:	161	Enabled	Disabled
HNAP:	8081	Enabled	Disabled

Below the table, it says "Remote Management Address: 10.30.20.176".

The next section is "Remote Access Allowed From" with three radio button options:

- Single Computer
IP Address: 0 0 0 0
- Range of IPs
Start IP Address: [] [] [] []
End IP Address: [] [] [] []
- Any Computer
Note: This option will allow any computer on the Internet access to your network and may cause a security risk.

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

Figure 96. Example of Remote Management Menu

Table 47. Remote Management Menu

Option	Description
Remote Management	
Remote Management	<p>You can remotely manage the Gateway using HTTP, HTTPS, Telnet, SSH, SNMP, and HNAP. Each method has Enabled and Disabled buttons for enabling or disabling that remote management method. If you enable a remote management method, specify the port number to be used with that method in the field to the left of Enabled.</p> <p>Note: The Gateway's remote management address appears below HNAP.</p>
Remote Access Allowed From	
Remote Access Allowed From	<p>Lets you provide remote access to Gateway for one computer, all computers on the Internet, or computers that fall within a specified range of IP addresses. Choices are:</p> <ul style="list-style-type: none">• Single Computer = to allow a single computer to remotely manage the Gateway, check this option and enter the IP address of the computer next to IP Address.• Range of IPs = to allow a group of computers to remotely manage the Gateway, check this option. Then enter the starting range of IP addresses next to Start IP Address boxes and the ending range of IP addresses next to End IP Address.• Any Computer = allows any computer on the Internet to access your network. This setting can cause a security risk.

Configuring DMZ Settings

If you have a local client computer that cannot run an Internet application properly behind the NAT firewall, you can configure it for unrestricted two-way Internet access by defining it as a Virtual DMZ host.

A DMZ allows a single computer on your LAN to expose all of its ports to the Internet. When doing this, the exposed computer is no longer “behind” the firewall. Therefore, placing a computer in the DMZ should be considered temporary because your firewall is no longer able to provide any security to it..

You configure the Gateway's DMZ settings using the DMZ menu. To display this menu, click **Advanced > DMZ** in the menu bar. Figure 97 shows an example of this menu and Table 48 describes the settings.

錯誤! 使用 [常用] 索引標籤將 Heading 1 套用到您想要在此處顯示的文字。

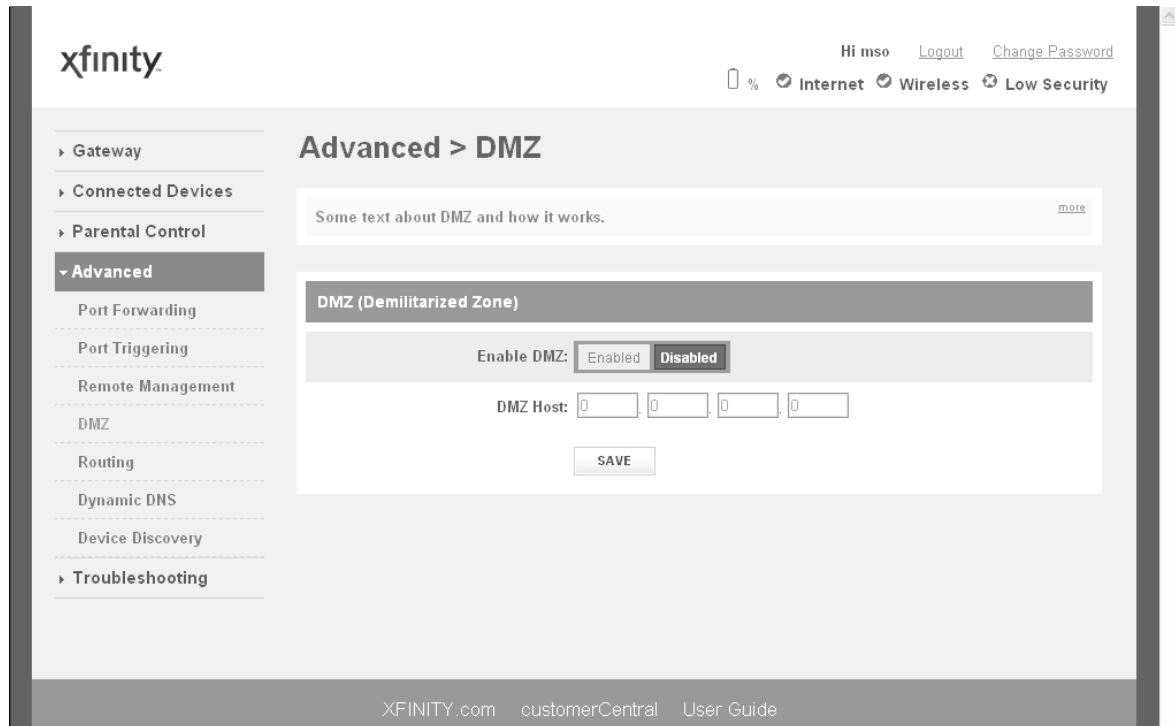


Figure 97. Example of DMZ Menu

Table 48. DMZ Menu

Option	Description
Enable DMZ	Enables or disables the Gateway's DMZ setting. <ul style="list-style-type: none">• Enabled = Gateway's DMZ feature is enabled.• Disabled = Gateway's DMZ feature is disabled.
DMZ Host	IP addresses of the computer to be used as the DMZ server.
SAVE button	Click this button to save your settings.

Configuring Routing Settings

Using the Routing menu, you can configure how the Gateway adjusts to physical changes in the network's layout and exchanges routing tables with other routers. To access the Routing menu, click **Advanced > Routing** in the menu bar. Figure 98 shows an example of the menu and Table 49 describes the settings.

The screenshot displays the Xfinity web interface for configuring routing settings. The page title is "Advanced > Routing". A sidebar on the left lists navigation options: Gateway, Connected Devices, Parental Control, Advanced, and Troubleshooting. The main content area features a "RIP (Routing information Protocol)" section with the following fields:

- Interface Name: Cable
- RIP Send Version: Do Not Send
- RIP Receive Version: Do Not Receive
- Update Interval: [] sec
- Default Metric: 1
- Authentication Type: No Authentication
- Authentication Key & ID: Key: [] ID: []
- Neighbor: [] [] [] []

A "SAVE" button is located below the settings. The footer of the page includes "XFFINITY.com", "customerCentral", and "User Guide".

Figure 98. Example of Routing Menu

Table 49. Routing Menu

Option	Description
Interface Name	Select the Gateway interface on which routing will be performed.
RIP Send Version	<p>Select the format and the broadcasting method of the RIP packets that the Gateway sends. Choices are:</p> <ul style="list-style-type: none"> • Do Not Send (<i>default</i>) • RIP1 • RIP2 • RIP1/2 <p>Your selection should match the version supported by other routers on your network.</p>
RIP Receive Version	<p>Select the format and the broadcasting method of the RIP packets that the Gateway receives. Choices are:</p> <ul style="list-style-type: none"> • Do Not Receive (<i>default</i>) • RIP1 • RIP2 • RIP1/2 <p>Your selection should match the version supported by other routers on your network.</p>
Update Interval	How often, in seconds, the Gateway sends routing-update messages. Default is 30 seconds.
Default Metric	Number by which the metric value for the path increases when the Gateway receives a routing update that includes changes to an entry. Choices are 1 – 15. Default is 1.
Authentication Type	<p>The authentication mechanism used, if any. Choices are:</p> <ul style="list-style-type: none"> • No Authentication = no authentication is used. If you keep this default setting, the Authentication Key & ID fields are gray and unavailable. (<i>default</i>) • Simple Password = an authentication method where a clear text password is sent to participating neighbors on the network. This selection sends the authenticating password over the network, possibly making it available to individuals who can access packets off the network. Do not use this option as part of your security strategy. Rather, use it to avoid accidental changes to the routing infrastructure. If you select this setting, the first field in the Authentication Key & ID option becomes available for entering the password. • MD5 = an authentication method that works much like Simple Password authentication, except that MD5 does not send the key over the network. Instead, a router uses the MD5 algorithm to produce a message digest of the key (also called a hash). The router sends the message digest instead of the key itself, which ensures that no one can eavesdrop on the network and learn keys during transmission. If you select this setting, the first field in the Authentication Key & ID option becomes available for entering the key and the second field becomes available for entering the ID.
Authentication Key & ID	<p>Specify the appropriate information based on the Authentication Type selected:</p> <ul style="list-style-type: none"> • No Authentication – no entry required; fields are gray and unavailable. (<i>default</i>) • Simple Password = in the first field, enter the clear-text password to be used for authentication. The second field requires no entry, and is gray and unavailable. • MD5 = in the first field, enter the MD5-hash password. In the second field, enter the Key Identifier that identifies the key used to create the authentication data for this message.
Neighbor	Enter the IP address of the Gateway's RIP neighbor router.
SAVE button	Click this button to save your settings.

Configuring Dynamic DNS Settings

The Gateway provides a dynamic DNS feature that can notify a domain name server to change, in real time, the active DNS configuration of its configured hostnames, addresses, or other information stored in DNS.

If you have already set up a dynamic domain service with a service provider, use the following procedure to set up the Gateway to update your DDNS automatically whenever your Internet connection's IP address changes.

1. Click **Advanced > Dynamic DNS**. The Dynamic DNS menu appears (see Figure 99).
2. Complete the fields in the Dynamic DNS menu (see Table 50).
3. Click **SAVE** to save your settings (or click **CANCEL** to discard them)

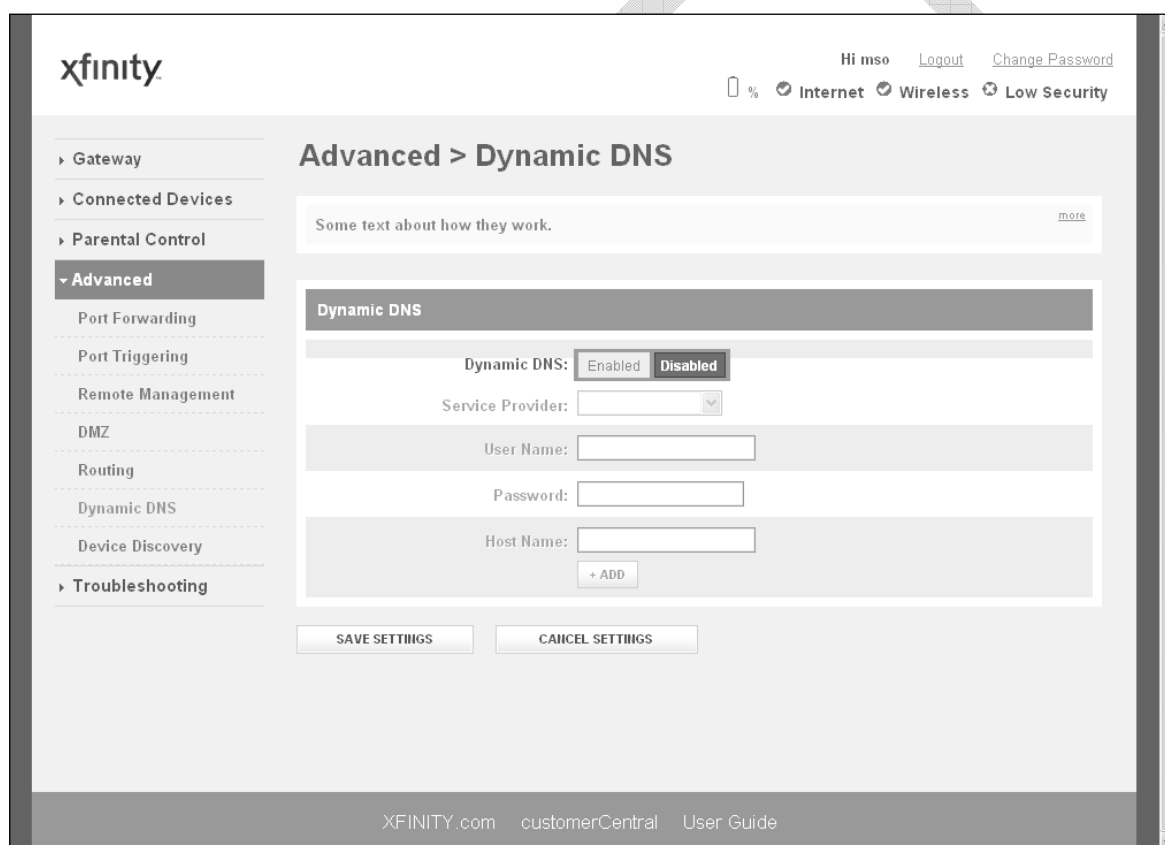


Figure 99. Example of Dynamic DNS Menu

Table 50. Dynamic DNS Menu

Option	Description
Enable Dynamic DNS	Enables or disables the Gateway's Dynamic DNS setting. <ul style="list-style-type: none">• Enabled = Gateway's Dynamic DNS feature is enabled.• Disabled = Gateway's Dynamic DNS feature is disabled.
Server Provider	Select a service provider.
User Name	Enter your service provider user name that you set up.
Password	Enter your service provider password that you set up. The password must be at least 6 characters long. For security, each password character appears as a dot (•).
Host Name	Enter the complete Host Name that you setup with service provider. To specify more than one host name, click the +ADD button and enter the next host name in the box that appears. To remove a host name, click Remove next to the host name you want to remove.
SAVE button	Click this button to save your settings.
CANCEL SETTINGS button	Click this button to discard your settings on the Dynamic DNS menu.

Discovering Devices

Using the Device Discovery menu, the Gateway can obtain protocol addresses of neighboring devices and discover the platform of those devices.

To display the Device Discovery menu, click **Advanced > Device Discovery** in the menu bar. Figure 100 shows an example of the menu and Table 51 describes it.

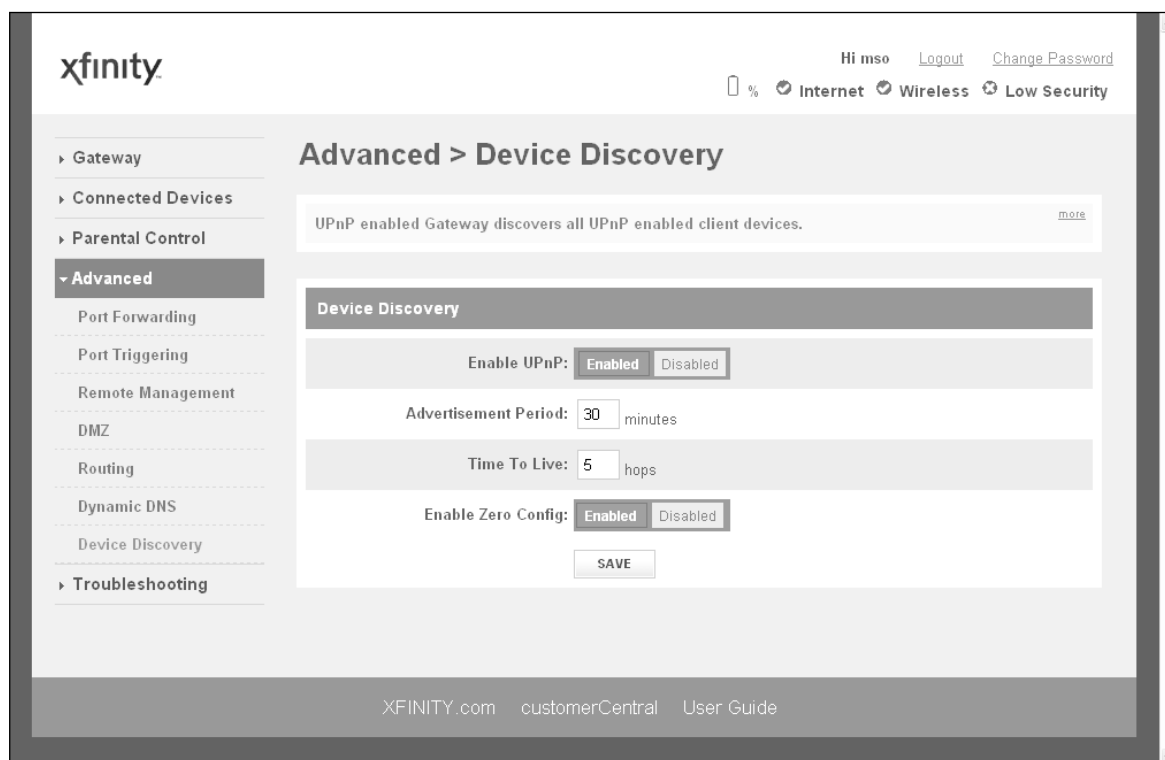


Figure 100. Example of Device Discovery Menu

Table 51. Device Discovery Menu

Option	Description
Enable UPnP	<p>Determines whether the Gateway uses its UPnP feature to communicate with other devices or your operating system.</p> <ul style="list-style-type: none">• Enabled = allows the Gateway to use its UPnP feature to communicate with other devices or your operating system. (<i>default</i>)• Disabled = prevents the Gateway from using its UPnP feature to communicate with other devices or your operating system. Also, may be disabled if your operating system does not support UPnP.
Advertisement Period	<p>How often the Gateway broadcasts its UPnP information (if UPnP is enabled). This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations can compromise the freshness of the device status, but can significantly reduce network traffic.</p>
Time To Live	<p>A counting mechanism to determine how long a packet is valid before it reaches its destination. Each time a TCP/IP packet passes through a router, it decrements its Time To Live count. When the count reaches zero, the packet is dropped by the router. This ensures that errant routing and looping aimless packets will not flood the network. The number of hops can range from 1 to 255. The default value is 5 hops, which should be fine for most networks. If you notice that some devices are not being updated or reached correctly, you might want to increase this value slightly.</p>
Enable Zero Config	<p>Determines whether zero configuration is enabled or disabled. Zero configuration networking automatically creates a usable Internet Protocol (IP) network, without manual operator intervention or special configuration servers. It allows nonexpert users to connect computers, networked printers, and other network devices and expect a functioning network to be established automatically.</p> <ul style="list-style-type: none">• Enabled = enables support for zero configuration.• Disabled = disables support for zero-configuration (<i>default</i>)
SAVE button	<p>Click this button to save your settings.</p>

Troubleshooting the Gateway

Using the **Troubleshooting** menu, you can:

- Define log filters and generate logs. See page 174.
- Test connectivity to a destination or IP address. See page 175.
- Reset the Gateway, reset your Wi-Fi router, or restore the Gateway's WiFi and factory default settings. See page 177.
- Change the password used to log in to the Gateway's Web interface. See page 178.



Note: For additional troubleshooting procedures, see Chapter 6.

DRAFT

Generating Logs

Using the Logs menu, you can define filters for system, event, and firewall logs, and then show, print or download the logs. To display the Logs menu, click **Troubleshooting > Logs** in the menu bar. Figure 101 shows an example of the menu.

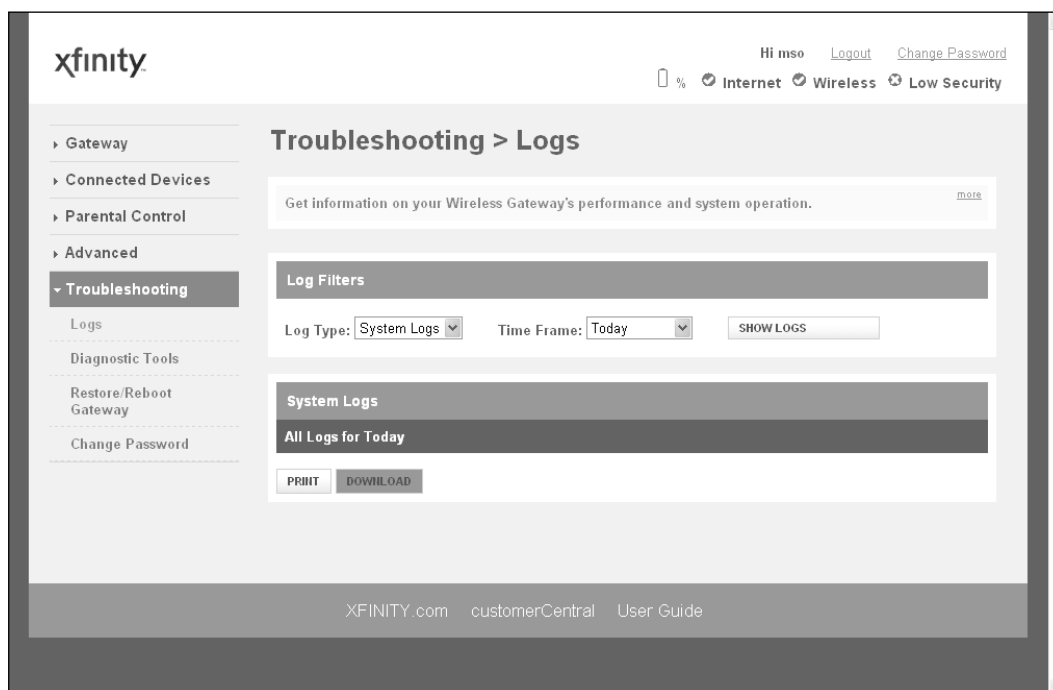


Figure 101. Example of Logs Menu

Under **Logs Filters**, you can set a log filter for the type of logs you want to generate and the time frame they are to cover. If you do not set a log filter, the default filter is automatically set to system log types for the current day (today). After you define the filter, you can show, print, or download the log.

4. Using the **Log Type** drop-down list, select the log to which you want to apply a filter, Choices are:
 - System Logs
 - Event Logs
 - Firewall Logs
5. Using the **Time Frame** drop-down list, select a time frame that the log is to cover.
6. To show the log, click the **SHOW LOGS** button.
7. To print the log with the filter applied, click **PRINT**.
8. To download the log with the filter applied, click **DOWNLOAD**.

Testing Connectivity to Destination and IP Addresses

There may be times when you encounter a problem trying to reach a certain destination. If you examine the Gateway's configuration and operation and everything looks fine, the problem might be with a router up the line from the Gateway or with the line itself.

To help you identify such issues, the Network Diagnostic Tools menu lets you test connectivity to a destination or IP address. To display the Network Diagnostic Tools menu, click **Troubleshooting > Diagnostic Tools** in the menu bar. Figure 102 shows an example of the menu.

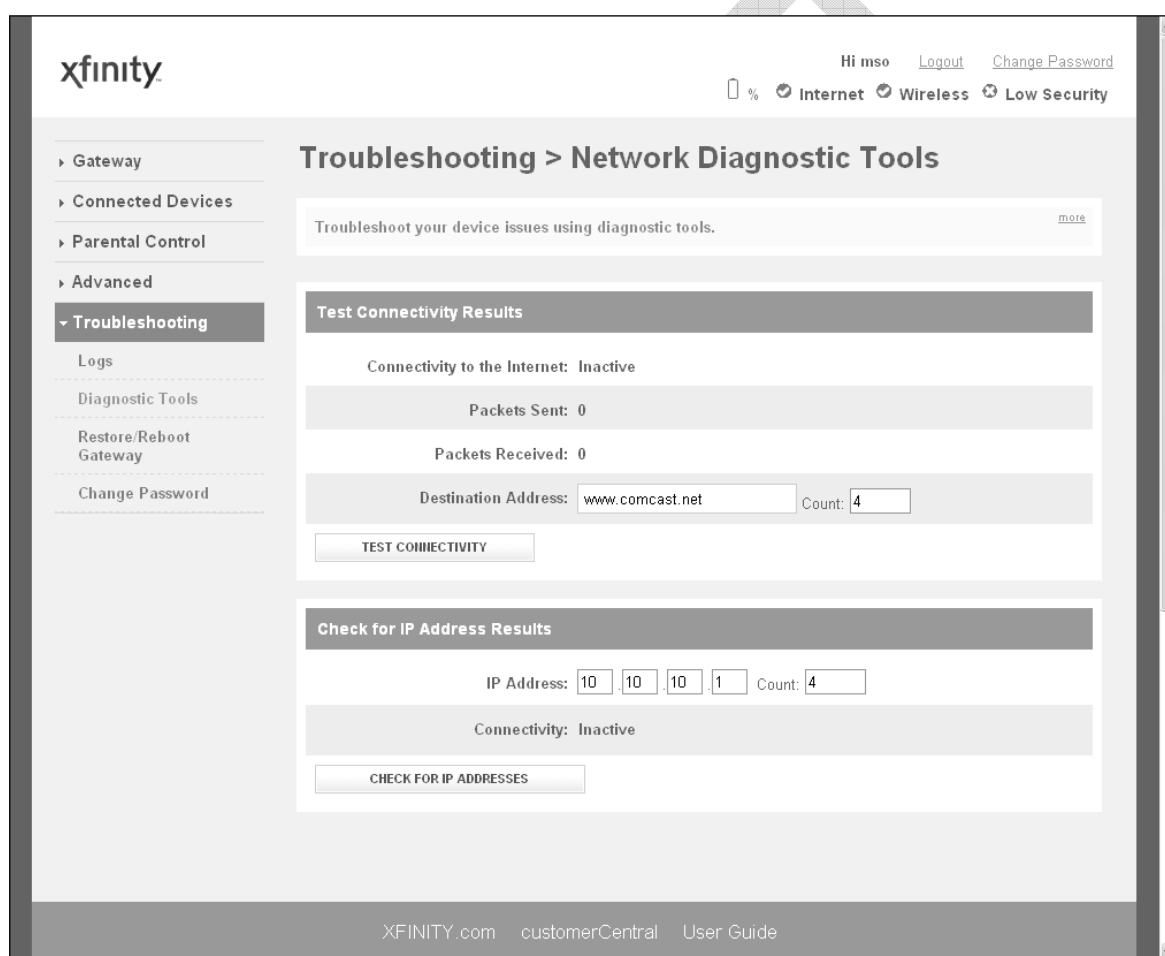


Figure 102. Example of the Network Diagnostic Tools Menu

Testing Connectivity to a Destination Address

To test the Gateway's connectivity to a destination address, perform the following procedure from the Network Diagnostic Tools menu.

1. Under **Test Connectivity Results**, enter a destination address in the **Destination Address** field.



Note: This procedure assumes that the destination address you enter is valid and operational.

2. Click the **TEST CONNECTIVITY** button. The **Packets Sent** and **Packets Received** counters show whether packets the number of packets sent and received during the test.
3. To stop the test, click the **STOP** button.

If the test is successful, you know that the destination you are having difficulty reaching is alive and physically reachable. If there are routers between the Gateway and the destination you are having difficulty reaching, the problem might be at one of the routers.

Testing Connectivity to an IP Address

To test the Gateway's connectivity to an IP address, perform the following procedure from the Network Diagnostic Tools menu.

1. Under **Check for IP Address Results**, enter an IP address in the **IP Address** field.



Note: This procedure assumes that the IP address you enter is valid and operational.

2. Click the **CHECK FOR IP ADDRESSES** button. The **Connectivity** indicator shows the results of the test.
3. To stop the test, click the **STOP** button.

If the test is successful, you know that the IP address you are having difficulty reaching is alive and physically reachable. If there are routers between the Gateway and the IP address you are having difficulty reaching, the problem might be at one of the routers.

Restoring or Rebooting the Gateway

The Restore / Reboot Gateway menu provides buttons for performing the following activities:

- **RESET** - restarts the Gateway while keeping any overrides you made to the Gateway's factory default settings.
- **RESET WI-FI Router** - resets the Wi-Fi router without affecting the Gateway.
- **RESTORE WI-FI SETTINGS** – returns the Gateway to its factory default WiFi settings. Settings that are not related to the Gateway's wireless operation are not changed.
- **RESTORE FACTORY SETTINGS** - returns the Gateway to its factory default settings. Any overrides you made to the default settings will be removed. This button is functionally equivalent to using the reset button to reset the Gateway (see “Using the Reset Button” on page 17).

To display the Network Diagnostic Tools menu, click **Troubleshooting > Restore/Reboot Gateway** in the menu bar. Figure 103 shows an example of the menu.

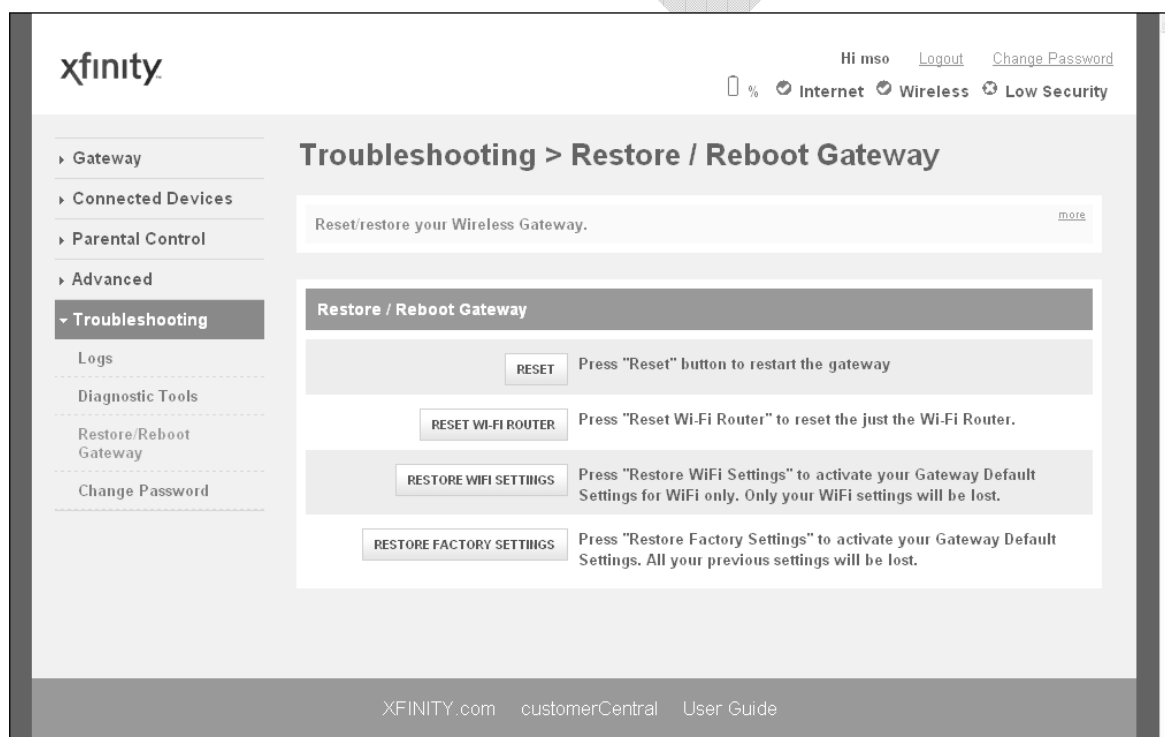


Figure 103. Example of the Restore / Reboot Gateway Menu

Changing the Login Password

The Change Password menu lets you change the password used to log in to the Gateway's Web interface. For security, we recommend you change the default log in password the first time you log in to the Web management interface to protect the Gateway from being tampered with.

To display the Change Password, click **Troubleshooting > Change Password** in the menu bar, or click the **Change Password** link at the top-right area of the Web management interface. Figure 104 shows an example of the menu and Table 52 describes the menu.

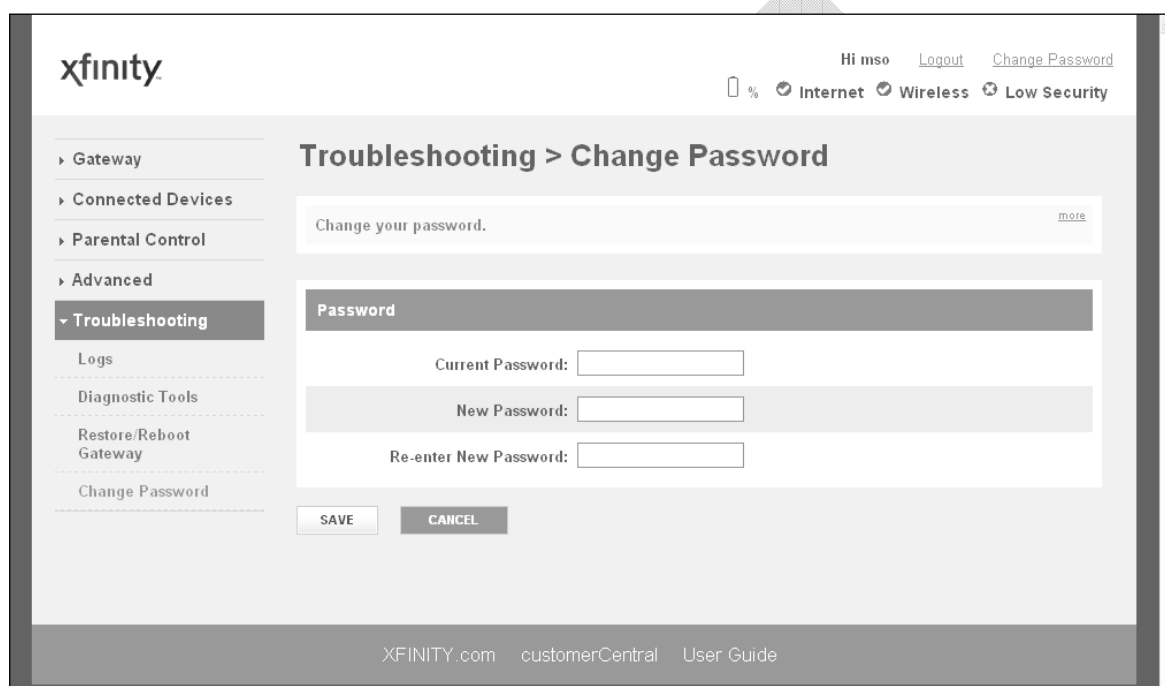


Figure 104. Example of the Change Password Menu

Table 52. Change Password Menu

Option	Description
Current Password	Enter the current case-sensitive administrator password. For security purposes, every typed character appears as a dot (•). The default password is not shown for security purposes.
New Password	Enter the new case-sensitive administrator password you want to use. A password can contain alphanumeric characters and spaces. For security purposes, every typed character appears as a dot (•).
Re-enter New Password	Enter the same case-sensitive administrator password you typed in the New Password field. For security purposes, every typed character appears as a dot (•).
SAVE button	Click this button to save your settings.
CANCEL button	Click this button to discard your settings on the Change Password menu.

6 Troubleshooting Procedures

Successful troubleshooting requires a logical, consistent approach that narrows down the source of a problem by ascertaining what is and isn't working until a single cause is identified. This chapter provides suggestions for identifying and resolving problems in the unlikely event you encounter a problem using the Gateway. It also provides tips for tuning your configuration to optimize your wired and wireless networking experience.

The topics covered in this chapter are:

Topic	Subtopics
Basic Troubleshooting Procedures	See page 180
Advanced Troubleshooting Procedures	<ul style="list-style-type: none"> • Troubleshooting Physical Network Problems (page 182) • Troubleshooting Configuration Problems (page 183) • Determining Your IP Address (page 183) • Troubleshooting Software-Interaction Problems (page 187)
Specific Troubleshooting Procedures	<ul style="list-style-type: none"> • Unable to Log In to Gateway (page 188) • Local Networked Devices Unable to Access the Gateway (page 188) • Unable to Access the Internet (page 189) • Unable to Access Networked Devices (page 191) • Using the Ping Utility to Troubleshoot (page 191) • Gateway Disconnects from the Internet (page 194) • Slow Web Browsing (page 195) • Unable to Configure Port Forwarding (page 195) • Unable to Use Pass-thru VPN (page 195) • Gateway is Not Passing DHCP Address to a computer (page 195) • Determining a Computer's MAC Address (page 196)
Wireless Troubleshooting	See page 198
Application and Gaming Troubleshooting	See page 204

Basic Troubleshooting Procedures

The following procedures cover basic troubleshooting procedures. Carefully review the sections to make sure you follow the recommended procedures.

Always start your network using the following sequence

1. Unplug the Gateway and any other routers or switches.
2. Shut down connected computers.
3. Plug in the Gateway first and wait for the lights to cycle through the startup routine. This prevents another device from taking the DHCP lease.
4. Plug in any other routers and switches.
5. Lastly, start up your computer.

Check basic Gateway functions

After you turn on power to the Gateway, check that the following LED sequences have occurred (and see “Front Panel” on page 13):

1. When power is first applied, verify that the **Power** LED is ON.
2. After about a minute, verify the statuses of the following LEDs on the front panel of the Gateway (see Figure 1 on page 13):
 - **Online** = ON (Gateway is operational)
 - **DS** = ON (Gateway is connected to the Internet)
 - **US** = ON (Gateway is connected to the Internet)
 - **WiFi** = ON (Gateway is ready for wireless operation)

If this behavior does not occur, see Table 53. If the incorrect behavior persists, use the Reset button to return the Gateway to its factory default configuration settings (see “Using the Reset Button” on page 17).

Table 53. Checking Basic Gateway Functions

If...	Perform This Procedure
The Power and other LEDs are OFF.	<ol style="list-style-type: none">1. Turn off the Gateway and then turn it on again to see whether the problem is resolved.2. Check that you are using the power adapter supplied with the Gateway.3. Be sure the power cord is connected to the Gateway and to a functioning power outlet.4. Plug a working device, such as a lamp, into the power outlet to confirm that the outlet is working.5. Be sure the power outlet is not controlled by a wall switch that can inadvertently remove power from the outlet.
The DS and US LEDs are OFF.	<ol style="list-style-type: none">1. Be sure the Ethernet cable connections are secure at the Gateway and at the computer.2. Be sure that power is turned on to the computer connected to the Gateway.3. Be sure you are using the Ethernet cable supplied with the Gateway or one configured similarly to it.
The WiFi LED is OFF.	See "Checking the Gateway's Wireless Connection" on page 198.

Check the Gateway's telephone interfaces

To confirm that the Gateway's two telephone interfaces are working properly:

1. Lift the handset of the device connected to the Gateway's telephone 1 interface, Confirm that the **Tel¹** LED goes ON. Hang up the device (place the device onhook) and confirm that the **Tel¹** LED goes OFF.
2. Lift the handset of the device connected to the Gateway's telephone 2 interface, Confirm that the **Tel²** LED goes ON. Hang up the device (place the device onhook) and confirm that the **Tel²** LED goes OFF.

Advanced Troubleshooting Procedures

Most advanced troubleshooting procedures fall into one of the following categories:

- Physical - an underlying problem with cables, a bad Gateway, or similar hardware problem. See page 182.
- Configuration - a problem with the configuration of one or more of network components. See page 183.
- Software - a failure of one or more software applications, an undesired interaction between two or more applications, or an undesired application that has been introduced into the network. See page 187.

Troubleshooting Physical Network Problems

When you experience network troubles, start by checking the physical network devices and connections. These problems are the most easily fixed and include:

- Performing a thorough physical inspection of your network.
- Checking that all hardware devices, including the Gateway, are plugged in and physically connected to the network.
- Making sure you are using the proper network cables (for example, not using a crossover cable with a NIC that requires a straight-through cable).
- Making sure all network cables are in good condition and well seated. Often, reseating the cable into a connector is all that is required to ensure a firm connection.

In addition, some operating systems, such as Microsoft Windows XP, show errors, such as when a network cable is unplugged. Figure 2, for instance, shows examples of how Microsoft Windows XP shows connection statuses in the Network Connections window. For information about other operating systems, refer to the documentation for those operating systems.

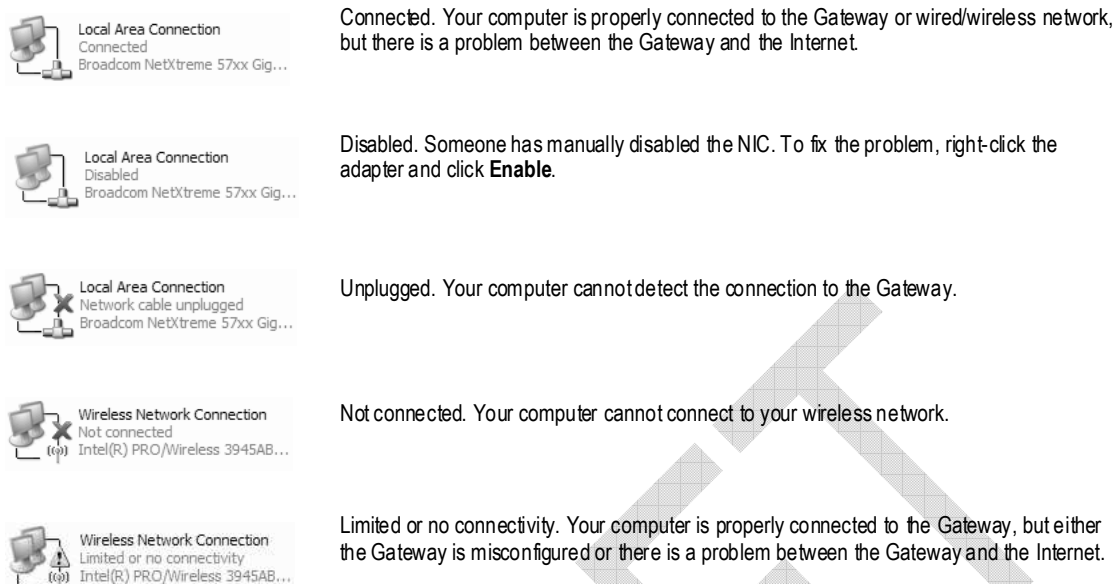


Figure 105. Examples of Connectivity Statuses for Microsoft Windows XP

Troubleshooting Configuration Problems

After confirming that your hardware is working properly, examine your networking configuration to determine whether there is a misconfiguration of IP addresses, subnet masks, gateways, or broadcast addresses. Common configuration problems can be caused by misconfiguring newly connected or configured devices.

Determining Your IP Address

An IP address uniquely identifies computers and computing devices, such as the Gateway, on a TCP/IP network. IP addresses are normally expressed in dotted-decimal format, with four numbers (or “octets”) separated by periods, such as 10 . 1 . 10 . 1.

For troubleshooting purposes, all the numbers in the IP addresses of your networked devices must be consistent across the network. This means:

- The first nine numbers (i.e., the first three octets) in the IP addresses are the same for all the devices on the network.
- The last three numbers (i.e., the last octet) in the IP addresses are different and not in use by other devices on the network (assuming your subnet mask is 255 . 255 . 255 . 000).

For example, if the IP address for the Gateway is 10 . 1 . 10 . 1, the other devices on the network must have an IP address whose:

- First three octets are 10 . 1 . 10.

- Last octet is any unique number from 0 to 255 (there are restrictions on using 0 and 255, so avoid using them). You would not use 1 as the last number, since that number is the last octet in the Gateway IP address in our example.

Figure 106 shows an example of IP addresses assigned to devices on the network.

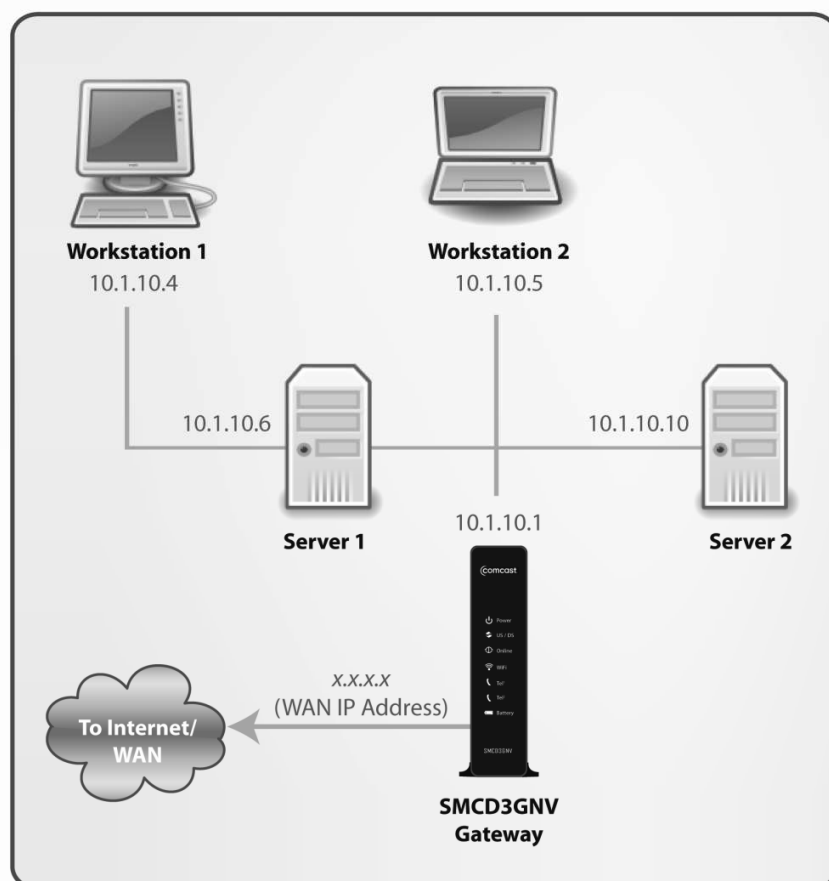


Figure 106. Example of IP Addresses for Networked Devices

You define the computer's IP address using the procedure appropriate for your operating system, as described in Chapter 3.



Tip: The following Windows sections describe how to use the command-line program Windows IP Configuration (ipconfig) to see the IP address of a computer running a Windows operating system. However, if you want even more information, such as IP routing and DHCP information, type **ipconfig /all** instead of **ipconfig** in the Windows sections that follow.

The most common problem associated when viewing IP addresses is that either:

- A computer's IP address is not on the same subnet as the other networked devices. In other words, the first nine numbers (three octets) in the device's IP address are not identical to those of the other networked devices.
- A computer shows an IP address that starts with the digits **169.254**. When this happens, it often means the computer could not retrieve a network address from a DHCP server and therefore automatically assigned itself an address from the base network address **169.254**. This would be fine if all the computers on your network used IP addresses from the **169.254** base network address. If one of them isn't, however, that computer will have problems connecting to the other network computers.

Possible causes for an IP address not being assigned are:

- Defective cables Replace the cable if it is worn or defective.
- An Ethernet cable may not be firmly connected at both ends. Secure the cable at both ends. Often, just reseating the cable into a connector is all that is required.
- The NIC may be bad or the network cable connected to it may be the wrong kind (for example, it might be a straight-through cable when a crossover cable is required). If you have another NIC and cable available, try using them instead.
- The Gateway port may be bad. Plug the network cable into a different port on the Gateway.
- The DHCP server that would automatically assign IP addresses is not configured for DHCP.
- Wrong WEP or WPA settings are configured on the Gateway or access point for wireless connections.

The sections that follow describe how to identify the IP addresses on devices running Windows and Macintosh operating systems.

Microsoft Windows 2000

To find the IP address of a computer running Microsoft Windows 2000:

1. From the Windows task bar, click **Start** and select **Run**.
2. In the **Open** field, type **cmd** and click **OK**. A DOS command window appears.
3. In the DOS command window, type **ipconfig** and then press Enter. Your IP address will be listed (see Figure 107).
4. When you finish, type **exit** at the command prompt and press Enter to close the window

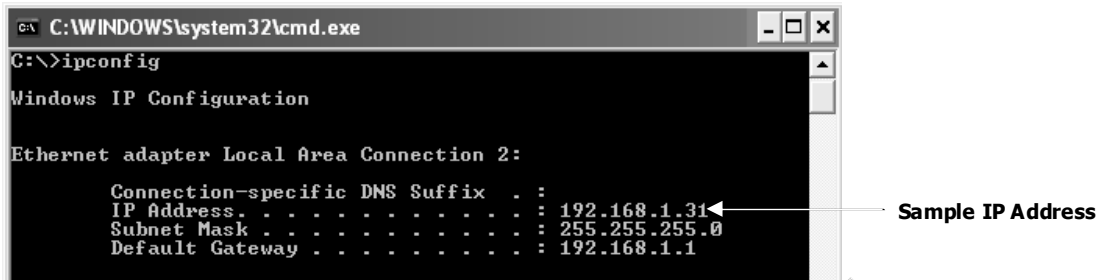


Figure 107. Example of an IP Address

Microsoft Windows XP, Vista, and 7

To find the IP address of a computer running Microsoft Windows XP, Vista, or 7:

1. Click on **Start** and in the Start Search box type **cmd**.
2. Press Enter on your keyboard or click **cmd.exe** in your search list (see Figure 108).



Figure 108. Example of md.exe in the Search List

3. In the DOS command window, type **ipconfig** and then press Enter. Your IP address will be listed (see Figure 107).
4. When you finish, type **exit** at the command prompt and press Enter to close the window.

Apple Macintosh OS X

To find the IP address of a Mac OS X OS X 10.6 or 10.5 computer:

1. From the Apple menu, select **System Preferences...**
2. In **System Preferences**, from the **View** menu, select **Network**.
3. In the Network preference window, click a network port (for example, **Ethernet**, **AirPort**, **modem**). If you are connected, the IP address appears below **Status**.
4. Close the window when finished.

To find the IP address of a Mac OS X 10.4 or 10.3 computer:

1. From the Apple menu, select **Location**, and then **Network Preferences...**
2. In the Network Preference window, next to **Show:**, select **Network Status**. Your network status and IP address appear.
3. Close the window when finished.

Via the Web

There are various Web sites, such as <http://whatismyipaddress.com/>, that display your IP address and other information about your system. If the page does not display, you may not have a working Internet connection and should try one of the methods described above to find your IP address.

Troubleshooting Software-Interaction Problems

If the physical network and basic configuration procedures in the preceding sections do not resolve your problem, focus on software problems. The most common software problems are related to firewalls.

Many third-party antivirus programs include built-in firewalls. You may not realize that you installed the firewall component when you installed the antivirus software, and now the firewall may be interfering with your network connectivity.

To troubleshoot software problems:

1. Disconnect your network from the Internet so that you can safely disable any firewalls or antivirus software while you troubleshoot.
2. Disconnect the Gateway from the Internet and unplug the Gateway.
3. After you are off the Internet, disable any antivirus or firewall programs you have, including Internet Connection Firewall or Windows Firewall, on all the computers that have problems. If this step solves the problem, the problem exists with one of these Windows features or products. Enable one at a time and see when things break again. When they do, you know where the problem is and you can either replace that product with one that does not cause problems or change the program's configuration to resolve the problem.

4. When you have everything working, reconnect your devices to the Internet.
5. Restart all your computers.

Specific Troubleshooting Procedures

The following sections cover specific troubleshooting suggestions you may find helpful if the basic and advanced troubleshooting procedures in the previous sections did not resolve your problem.

Unable to Log In to Gateway

If you are unable to log in to the Gateway's Web management interface:

1. Confirm that the Ethernet cable connecting the computer and Gateway is connected securely at both ends. Often, just reseating the cable into a connector is all that is required.
2. If you have more than one network port available on the Gateway, plug the cable into a different port. If the network connection works, the original port on the Gateway is faulty. However, you can continue to use the other ports.
3. The NIC in your computer might have failed. If possible, connect a different computer to the same network cable. If the connection works, the problem is with the NIC. Contact the NIC manufacturer for support or install a new NIC. If the new computer also fails to connect, replace the Ethernet cable with a new cable, as you might have a faulty cable. If the problem persists, contact technical support for the Gateway.
4. Be sure you are using the correct login information. The factory default login name is **cusadmin** and the password is **highspeed**. Be sure Caps Lock is off when entering this information.
5. Run the Home Network Wizard (see "Configuring Your Home Network" on page 60).
6. Change the login password (see "Changing the Login Password" on page 99).

Local Networked Devices Unable to Access the Gateway

If devices on the local network cannot access the Gateway:

1. Go to **Connection > Status** (see "Viewing the Gateway's Connection Status" on page 44).
2. Under **Local IP Network**, check that the following statuses are shown:
 - **Local Network = Connected**
 - **No of Clients connected** = a number greater than zero

If your statuses show no local network connection and/or no clients connected, proceed to the next step.

3. Be sure the computer connected to the Gateway is configured to use the same subnet mask and gateway settings as the Gateway (see “Viewing and Editing Your Local IP Configuration” on page 47).
4. Ping the Gateway from a computer on the same subnet as the Gateway (see “Testing the Path from a Computer to the ” on page 191). If the ping fails and there is no firewall software installed, your network configuration, NIC, or cabling is probably at fault.
5. Release and renew the NIC’s IP address:
 - a. From the Windows task bar, click **Start** and select **Run**.
 - b. In the **Open** field, type **cmd** and click **OK**.
 - c. At the first command prompt, type **ipconfig/release** and press Enter.
 - d. At the next command prompt, type **ipconfig/renew** and press Enter.
 - e. Check whether your computer obtained an IP address other than **169.254.x.x** or **0.0.0.0**.
6. If the problem continues, power cycle the Gateway and computer:
 - a. Turn off the computer and turn off Gateway.
 - b. Turn on the Gateway and turn on computer.
7. For secured wireless connections, be sure you entered the correct security key when connecting to a secured wireless network.

Unable to Access the Internet

If the Gateway cannot access the Internet, it could be due to several reasons, such as a failed Internet connection, a misconfigured Gateway, or a misconfigured NIC.

1. Unplug the Gateway.



Note: If the Gateway is located where you cannot easily unplug it, you can restart it using the Restore / Reboot Gateway menu (“Restoring or Rebooting the Gateway” on page 98).

2. Turn off the Gateway for three minutes.
3. Turn off all computers attached to your network.
4. Plug in the Gateway first, turn it on, and let it boot.
5. After the Gateway completes its connection to the ISP, restart your computer.
6. Check that the Gateway’s **Online** LED is ON. If it is OFF, replace the coaxial cable connecting the Gateway to the cable service. If the **Online** LED does not go ON after the Gateway has been powered up for several minutes, contact your cable provider to confirm that the service is active.

7. If the **Online** LED is ON, go to **Connection > Status** (see “Viewing the Gateway’s Connection Status” on page 44). Then, under **Comcast Network**, confirm that **Internet = Active**. If it isn’t, contact your cable provider to confirm that the service is active.
8. If you have more than one network port available on the Gateway, plug the cable into a different port. If the network connection works, the original port on the Gateway is faulty. However, you can continue to use the other ports.
9. Close any network applications that you might have opened, especially file-sharing and peer-to-peer applications. These applications can consume large amounts of bandwidth that can prevent you from being able to browse the Web.
10. Ping a location on the Internet (see “Testing the Path from a Computer to the Internet” on page 192). For example, ping `www.yahoo.com`. If the ping succeeds, proceed to the next step. If the ping fails:
 - Your Web browser may be misconfigured. Be sure you do not have an incorrect proxy server setting in your Web browser.
 - If your computer is running a Microsoft Windows operating system, check whether the computer has a corrupt winsock registry entry (refer to your Windows documentation).
 - The site might be down. Try to ping another site.
 - If your additional pings fail, please contact technical support.
11. Check your computer’s operating system to see whether the computer has connectivity (for example, see Figure 105 and refer to the documentation for your operating system). If it doesn’t, try using another computer and NIC attached to the Gateway to connect to the Internet.
12. Try accessing the Internet with a different browser. If you succeed, the problem exists with the previous browser you used.

Unable to Access Networked Devices

If you are on a network, but cannot connect to any resources on the network:

1. The Ethernet cable may be worn. Replace the cable if it is worn.
2. The Ethernet cable may not be firmly connected at both ends. Secure the cable at both ends. Often, just reseating the cable into a connector is all that is required.
3. The port on the Gateway may be bad. Plug the network cable into a different port on the Gateway.
4. The NIC may be bad or the cable connected to the NIC may be the wrong kind of network cable (for example, you may be using a straight-through cable when a crossover cable is required). If you have another NIC available, try using it instead of the one currently used.
5. Ping the IP address of other computers and devices on your network.
6. For Windows operating systems:
 - Try connecting to a computer on the network using **Start \ Run** and enter **\\PCname**, where **PCname** is the name of the computer you want to connect to.
 - Add the computer and its IP address to the LMHOSTS file. This is a text file that resides in the `Windows\System32\drivers\etc` directory (for Windows2000 or XP) and has the format `IP_Address Computer_Name`.



Tip: Browsing is fairly complicated issue and has a lot of places for failure. If you need to have resources available, create shortcuts on your desktop instead.

Using the Ping Utility to Troubleshoot

You can use your computer's ping utility to test the path from the computer to the Gateway and from your computer to the Internet.

Testing the Path from a Computer to the Gateway

You can ping the Gateway to verify that the LAN path from your computer to the Gateway is set up correctly. To ping the Gateway from a Windows computer:

1. From the Windows task bar, click **Start** and select Run.
2. In the **Open** field, type **ping** followed by the IP address of the Gateway.
3. Click **OK**. A message similar to the following appears (in this example, 192.168.0.1 is the IP address entered as part of the **ping** command):

```
Pinging 192.168.0.1 with 32 bytes of data
```

If the destination IP address was contacted successfully, a message similar to the following appears:

```
Reply from 192.168.0.1: bytes=32 time=NN ms TTL=xxx
```

If the path was not contacted successfully, a message similar to the following appears:

```
Request timed out
```

If the path is not working properly:

- The physical connections may be wrong. Be sure the Gateway's **Online** LED is ON. If is OFF, review "Basic" on page 180.
- Check that the corresponding LEDs on the NIC installed in your computer are ON (refer to the documentation for your NIC). If they are OFF, verify that the Ethernet card driver software and TCP/IP software are both installed and configured properly on your computer.
- Verify that the IP addresses for the Gateway and your computer are correct and that both addresses are on the same subnet (for example, 192.168.1.x/255.255.255.0).

Testing the Path from a Computer to the Internet

After verifying that the path between your computer and Gateway is working properly, use the following procedure to test the path from your computer to the Internet.

To test the path using ping from a Windows PC:

1. From the Windows task bar, click **Start** and select **Run**.
2. In the **Open** field, type **cmd** and click **OK**. A DOS command window appears.
3. At the **>** prompt, type **ping -n 10 IPaddress** where **IPaddress** is the IP address of a remote device (such as your ISP's server) or Web site (such as www.yahoo.com).
4. Press Enter. If the path is working, a reply similar to the one in the previous section appears. If you do not receive replies:
 - Confirm that your computer has the IP address of the Gateway listed as the default gateway. If your computer's IP address is obtained automatically through DHCP, this information will not be visible in your computer's Control Panel. Verify that the Gateway's IP address is shown as the TCP/IP default gateway.
 - Check whether your computer's network address (the portion of the IP address specified by the netmask) is different than the network address of the remote device.
 - If your ISP assigned a host name to your computer, enter the name in the **Host Name** field in the Add Computer Menu (see "Manually Adding Computers with Static IP Addresses to the Wireless Network" on page 65).
5. When you finish, type **exit** at the command prompt and press Enter to close the window

Using Ping on a Macintosh

To ping on a Macintosh:

1. Click on **Go > Applications > Utilities**.
2. Click on **Network Utility**, and then click the **Ping** tab. A page similar to the one in Figure 109 appears.
3. In the first field, enter the IP address you want to ping.
4. Using the options below the field, select an unlimited number of pings or send a specific number of pings.
5. Click the **Ping** button.

If you receive **reply from...**, the destination IP address was contacted successfully.

If you receive **request timed out**, the destination IP address was not contacted successfully.

If you receive **destination host unreachable**, you are not on the same subnet as the destination address. Change your IP address to communicate with the destination address.

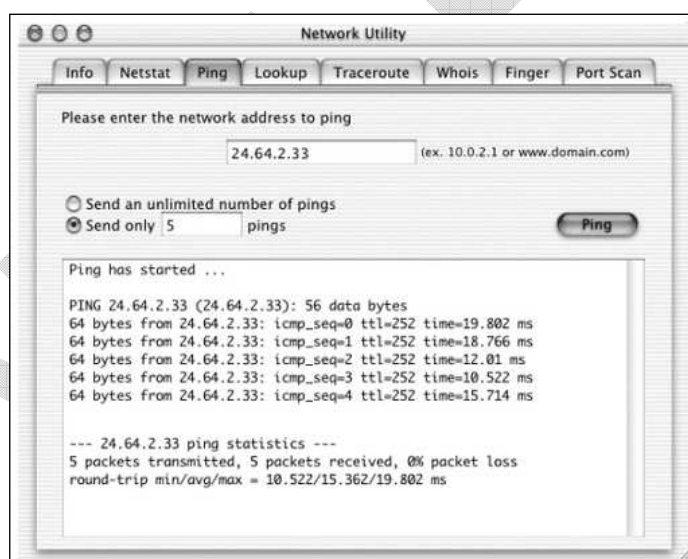


Figure 109. Ping Tab on the Network Utility Page

Gateway Disconnects from the Internet

If the Gateway has been connected to the Internet for an extended period and holds an IP address (DHCP lease) for a longer period of time than your ISP allows, it is not uncommon for the Gateway to disconnect from the Internet. This is normal and does not indicate any issue with the Gateway.

1. Unplug the power to the Gateway, then reconnect power.



Note: If the Gateway is located where you cannot easily unplug it, you can restart it using the Restore / Reboot Gateway menu (“Restoring or Rebooting the Gateway” on page 98). If your DHCP lease time seems to be extremely short, contact your ISP to see if there are other issues on the network. You can reconfigure the Gateway’s lease time using the Local IP Configuration menu (see “Viewing and Editing Your Local IP Configuration” on page 47).

2. Connect a computer to one of the Gateway’s LAN ports.
3. Restart your computer.
4. Reset the Gateway to its factory default settings using either the Reset button (see “Using the Reset Button” on page 17) or the Restore / Reboot Gateway menu (see “Restoring or Rebooting the Gateway” on page 98).



Note: This step removes all overrides made to the Gateway’s default settings and returns the Gateway to its original factory default settings.

In certain network scenarios, it may be helpful to turn off all the equipment on your network, and then turn the equipment all back on. Leaving some devices unplugged for up to five minutes can also help.

If the disconnections are limited to wired clients only

Check your NIC settings and all cable routing, connections, and power supplies.

If the disconnections are limited to wireless clients only

Focus on factors that affect wireless clients, such as:

- Network selection and security
- Hardware access control
- Client TCP/IP settings
- Signal strength
- Sources of interference

Can you connect to the Internet directly?

5. Set up a computer to connect to the Internet directly, without using the Gateway.
6. If you cannot connect to the Internet without the Gateway, contact your ISP for assistance.

Slow Web Browsing

If you experience slow Web browsing with the Gateway:

1. Check for possible intrusion by spyware and viruses.
2. Clear browser settings and cache (refer to the documentation for your Web browser).
3. Stop other programs running in the background that are consuming bandwidth.
4. A specific site may be suffering from server issues, try another site.
5. Update the Gateway firmware.

Unable to Configure Port Forwarding

If you are not able to configure port forwarding for software applications, external servers or gaming:

- Ascertain the port(s) that the application or game calls for.
- Some ISPs block ports, such as ports 20, 21, and 80. Check with ISP to confirm whether it is blocking ports.
- Reserve IP addresses for the computers to ensure they receive the appropriate IP address(es) for the service created (see “Working with Connected Devices” on page 64).
- Disable firewalls and stateful packet inspection (SPI) applications.
- Create a dynamic DNS (DynDNS) account for dynamic IP addresses from the ISP.
- Update the Gateway firmware.

Unable to Use Pass-thru VPN

If VPN pass-through is not working:

- You may have to forward ports (see “Adding a Port Forwarding Rule” on page 85). Ports 50, 51, 500, 1701 and 1723 are standard VPN ports.
- Update the Gateway firmware.

Gateway is Not Passing DHCP Address to a computer

If the Gateway is not passing DHCP addresses to a computer over a wired or wireless connection:

1. Be sure computer IP is not statically set already.

2. Release and renew the NIC's IP address:
 - a. From the Windows task bar, click **Start** and select **Run**.
 - b. In the **Open** field, type **cmd** and click **OK**.
 - c. At the first command prompt, type **ipconfig/release** and press Enter.
 - d. At the next command prompt, type **ipconfig/renew** and press Enter.
3. For wired connections, be sure the physical cable connections are correct.
4. For wireless operation, verify that the Gateway's SSID and security settings are correct (see "Configuring Your Home Network" on page 60).

Determining a Computer's MAC Address

The following sections describe how to obtain a computer's MAC address.

Microsoft Windows

To determine the MAC address on a Windows computer:

1. From the Windows task bar, click **Start** and select **Run**.
2. In the **Open** field, type **cmd** and click **OK**. A DOS command window appears.
3. In the DOS command window, type **ipconfig/all** and press Enter.
4. This window displays your networking information. The MAC address appears as a **Physical Address** below **Ethernet adapter Local Area Connection**. In the example in Figure 110, the MAC address is **00-1E-8C-94-09-EA**, which is the physical address of the NIC card.
5. When you finish, type **exit** at the command prompt and press Enter to close the window.

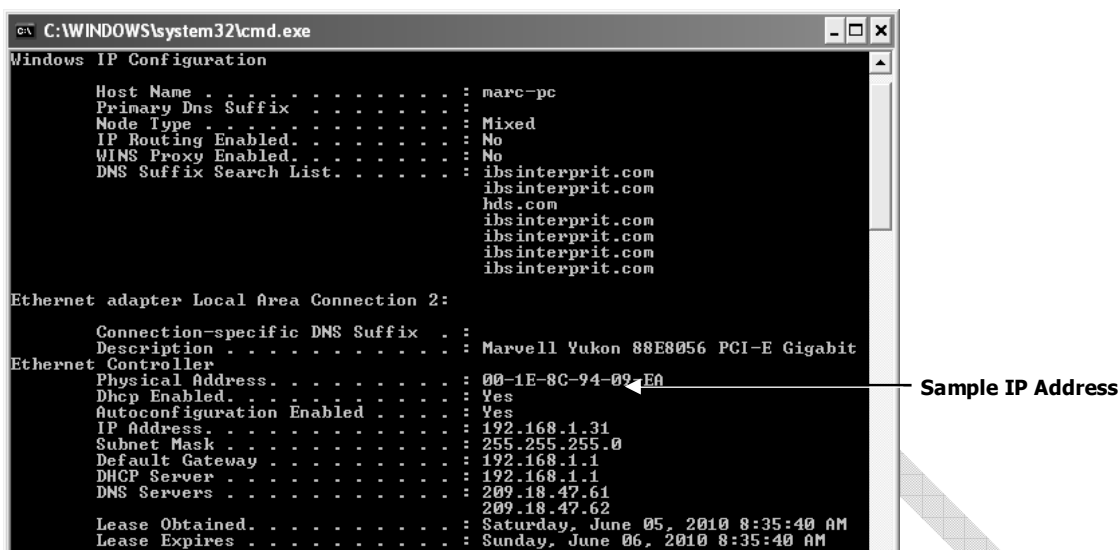


Figure 110. Example of MAC Address

Apple Macintosh Windows OS X

To determine the MAC address on a Mac running OS X, perform the following procedure. The MAC address appears in the form of 00 0D 93 13 51 1A.

1. From the dock, select **System Preferences**.
2. Select **Network**, **Select Location**, **Select Interface**.
3. Perform one of the following steps:
 - For a wired Mac running Mac OS 10.2 or earlier, select the **TCP/IP** tab. The number next to the **Ethernet Address** is your MAC address.
 - For a wired MAX running OS 10.3 and later), select the **Ethernet** tab. The number next to the **Ethernet ID** is your MAC address.
 - For a wireless connection (AirPort), select **AirPort** tab . The number next to the **AirPort ID** is your MAC address.

Wireless Troubleshooting

The following sections cover troubleshooting procedures for wireless networking.

Checking the Gateway's Wireless Connection

If you experience a problem with the Gateway's wireless operation, log in to the Gateway's Web management interface and verify the wireless settings. In particular, the Gateway's Wireless Network Name (SSID) and security settings must match the wireless computer settings exactly.

1. Use an Ethernet cable to connect a computer to the Gateway.
2. Open a Web browser on the computer and log in to the Gateway's Web management interface.
3. Go to **Connection > Status** (see "Viewing the Gateway's Connection Status" on page 44). Then, under **Local IP Network**, check that an IP address is shown for the **Internet Port**. If 0.0.0.0 is shown, the Gateway has not obtained an IP address from your ISP.
4. Click **Gateway** in the menu bar, and then click the **Wizard** submenu.
5. Verify that the Gateway's wireless configuration settings match those of the other wireless devices in your wireless network. In the Home Network Wizard Page 2, confirm that the case-sensitive **Enter WiFi Network Name** exactly matches the SSID of the other wireless devices in your wireless network. For example, **hOME** is not the same as **home** or **Home**.
6. Access the Wireless menu by clicking **Gateway** in the menu bar and then clicking the **Connection** and **WiFi** submenus. In **Operation Mode**, confirm that the correct setting is used for your wireless network (see page 50).

Wireless Range is Low

If your wireless range is very low, or if your wireless computer cannot connect to your wireless network, use the following procedure to improve the wireless range of the Gateway.

1. Review the guidelines under "Guidelines for Improving Your Wireless Network" on page 201.
2. Change the wireless channel of the Gateway. Just like one radio station may be clear while another suffers from interference, sometimes one wireless channel is clearer than others. To change channels:
 - a. Open a Web browser on the computer.
 - b. Log in to the Gateway's Web management interface.

- c. Use the **Channel Selection** and **Channel** settings in the Wireless menu to select the Gateway's channel settings (see "Viewing and Editing Wireless Configuration" on page 49).



Note: You do not have to change your computer's configuration, because it automatically detects the new channel.

Unable to Connect to a Wireless Network Using Windows XP and Vista

If you encounter the following when connecting to a wireless network using a Microsoft Windows XP or Vista computer and the Gateway:

- A message appears after entering the appropriate network or passphrase for a wireless connection where `validating identity` replaces the name of the wireless network,
- A pop-up window asks for login credentials for the wireless connection, and
- The following error message appears: `windows was unable to find a certificate to log you on to the network.`

Use the following procedure to create or add a wireless network profile manually on the computer.

To add a wireless network on a Windows Vista computer manually

1. From the Windows task bar, click **Start** and select **Network**.
2. Select **Network and Sharing Center**.
3. Click **Manage wireless networks**.
4. Click **Add** and select **Manually create a network profile**.
5. Enter the SSID, select the type of security, and enter the wireless password in the **Security Key/Passphrase** field.
6. Check the **Start this connection Automatically** and **Connect even if the network is not broadcasting** checkboxes.
7. Click **Next** and close the window.
8. Go to the **Network and Sharing Center** and select **Manage network connections**.
9. Right-click **Wireless network connection** and select **Status**.
10. Click **details** and check the IPv4 address.
11. If there is a valid IPv4 address, check whether the computer can access the Internet wireless.

To add a wireless network on a Windows XP computer manually



Note: The following steps are for a wireless network that has WEP security.

1. From the Windows task bar, click **Start** and double-click **Control Panel**.
2. In the left pane, select Switch to Classic view.
3. Click Network Connections.
4. Right click Wireless Network Connections and select Properties.
5. Click on the Wireless Networks tab.
6. Click the Add button.
7. Enter the name of the wireless network (SSID).
8. Set the encryption type to WEP.
9. Clear the key is provided for me automatically check box.
10. Enter the network key and confirm it. Be sure **This is a computer-to-computer (ad-hoc) network** is not selected.
11. Click **OK** and then click **OK** again.
12. Right-click **Wireless Network Connections** and select **Status**.
13. Click the **Support** tab and check for a valid IP address.
14. Check whether the computer can access the Internet wirelessly.

If you receive the same error message, ensure that IEEE 802.1x authentication of the wireless adapter is disabled.

To disable IEEE 802.1x authentication

1. From the Windows task bar, click **Start** and select **Run**.
2. In the **Open** field, type **ncpa.cpl** and click **OK**.
3. Right-click the **Wireless network connections** icon, and select **Properties**.
4. Click the **Wireless network** tab.
5. Click the **Properties** button next to **Remove**.
6. Click the **Authentication** tab and uncheck the **Enable IEEE 802.1x authentication for this network** checkbox.
7. Click **OK** to update the settings.

Achieving Optimal Wireless Performance

To achieve optimal wireless performance with the Gateway, perform the following procedure.

1. Right-click **My Computer** and select **Properties**.
2. Click the **Hardware** tab and click **Device Manager**.
3. Under **Network adapters list**, double-click your wireless NIC.
4. Click the **Advanced** tab. Under the **Property** field, select **Wireless mode**.
5. Select the highest value your NIC is capable of performing.
6. Click **OK** and try the new settings.

Guidelines for Improving Your Wireless Network

The following guidelines describe how to improve and secure your wireless network.

- **Position the Gateway and wireless access point(s)** in a central location. If the Gateway and access point(s) are located against an outside wall of your home or office, the signal will be weak on the other side of your home or office.
- **Move the Gateway away from the floor, walls, and metal objects** such as metal file cabinets. Floors, walls, and metal interfere with the Gateway's wireless signals. The closer the Gateway is to these obstructions, the more severe the interference, and the weaker your connection will be.
- **The Gateway supports STBC**, which is a technique used to transfer multiple copies of data by multiple antennas to improve data transfer. Using multiple antennas improves data transfers and wireless stability. By default STBC is disabled on the Gateway. To enable it, use the **STBC** option in the Wireless menu (see "Viewing and Editing Wireless Configuration" on page 51).
- **Wireless repeaters** extend your wireless network range, without requiring you to add wiring. Place the wireless repeater halfway between your wireless access point and your computer to boost to your wireless signal strength.
- **Wireless devices can broadcast on several different channels**, similar to the way radio stations use different channels. In the United States and Canada, these channels are 1, 6, and 11. Just like you'll sometimes hear interference on one radio station while another is perfectly clear, sometimes one wireless channel is clearer than others. If you encounter interference, change the Gateway's channel using the **Channel Selection** and **Channel** options in the Wireless menu (see "Viewing and Editing Wireless Configuration" on page 49) to see whether your signal strength improves. You do not need to change your computer's configuration, because it'll automatically detect the new channel.
- **If you have cordless phones or other wireless electronics** in your home or office, your computer might not be able to "hear" the Gateway over the noise from the other

wireless devices. To quiet the noise, avoid wireless electronics that use the 2.4 GHz frequency. Instead, look for cordless phones that use the 5.8 GHz or 900 MHz frequencies.

- **Update firmware and drivers for your wireless networking devices.** Device manufacturers, including SMC, regularly make free improvements to their devices that improve performance. To obtain the latest firmware and driver updates for your devices, visit the vendor's Web site.
- **To improve the security of your wireless network,** change the SSID to a different name than the default. You can access the Gateway's SSID setting using the **Enter WiFi Network Name** option in Step 2 of the Home Network Wizard (see "Configuring Your Home Network" on page 60). An SSID can be changed at any time, as long as the change is also made on all wireless clients.
- **By default, most wireless access points broadcast the SSID** to all wireless devices. While this feature of WiFi network protocols is intended to allow clients to dynamically discover and roam between WLANs, it also allows anyone with a wireless NIC to detect the SSID you use to gain access to your wireless network. Therefore, you may want to consider disabling this feature. For more information, refer to the documentation for your wireless access points.
- **MAC filtering** is the process of configuring a wireless access point with a list of MAC addresses that will be allowed or not allowed to gain access to the rest of the network via that access point. Only MAC addresses that are registered with the wireless access point can gain access to the wireless network. The Gateway provides a similar feature with its **Private Wireless Network** option in the Wireless to limit connections to certain MAC addresses (see "Viewing and Editing Wireless Configuration" on page 49).
- **Guessing default user names and passwords** for wireless access points is a common practice hackers use to access wireless networks. Therefore, change the default user name and password for your wireless access point and the configuration settings of your devices. For information about changing the default username and password for the Gateway, see "Changing the Login Password" on page 99.

Wireless IEEE 802.11n Guidelines

The wireless IEEE 802.11n standard is an extension to 802.11 specification developed by the IEEE for wireless LAN (WLAN) technology. 802.11n builds upon previous 802.11 standards by adding multiple-input multiple-output (MIMO). The additional transmitter and receiver antennas allow for increased data throughput, at speeds up to 100 Mbps, which is 4-to-5 times faster than 802.11g. 802.11n also offers a better operating distance than current networks.

If you use or are considering using 802.11n in your wireless network, observe the following guidelines:

- **If your maximum data rate is 54 Mbps or lower**, confirm your NIC is an 802.11n adapter and not an older 802.11g adapter. Although 802.11g NICs can connect to the newer 802.11n devices, high speeds and performance are possible only on connections between a wireless N device (such as the Gateway) or access point (AP) and a wireless N adapter. Therefore, you may need to upgrade your older wireless equipment to achieve faster speed and performance.
- **While devices certified by the Wi-Fi Alliance** are designed to work together regardless of manufacturer, some proprietary features require compatible equipment to work. Additionally, there may be interoperability issues with wireless 802.11n devices because the official standard is not complete. Therefore, manufacturers are releasing “draft” products. To prevent potential problems, use devices from the same manufacturer for your wireless network.
- **Because the wireless 802.11n standard does not support WEP encryption**, 802.11n connections using WEP are limited to maximum wireless 802.11g speeds of 54 Mbps, even on mixed 802.11/GN networks. Moreover, the first WPA version does not provide maximum wireless performance on 802.11n networks. For these reasons, either:
 - Upgrade your 802.11g equipment for 802.11n devices, or
 - Configure the devices on your wireless network to use WPA2 (on the Gateway, this setting is configured in the Encryption Method field in step 2 of the Home Network Wizard – see page 63). For old 802.11g devices that support WEP encryption only, check the vendor's Web site for updated drivers.
- **Wireless 802.11 N is backward compatible** with older 802.11g wireless devices and even older 802.11b devices. However, traffic on a wireless network is managed differently when older devices connect to an 802.11n network that can adversely affect speed and performance. Therefore, if you are not realizing optimum data and throughput rates, you may want to configure the Gateway so it only offers connections to wireless 802.11n clients. To limit the types of clients allowed to connect, configure the **Operation Mode** setting in the Wireless menu to allow only wireless 802.11n connections (see page 50).
- **To exceed 130 Mbps on wireless 802.11n connections**, the channel width must double from 20 to 40 MHz. By default, the Gateway is configured for 20/40 MHz operation. However, if this default setting has a negative impact on clients with low signals, you might want to select 20 MHz operation in the Gateway's **Channel Bandwidth** setting in the Wireless menu (see page 51) to limit connections to 20 MHz only.

Application and Gaming Troubleshooting

Connecting to Messenger Services Behind the Gateway

If you experience intermittent errors, cannot connect to servers, or find some features not working when using MSN or AIM Messenger with the Gateway:

- You may have to open the following ports:
 - For MSN Messenger, open port 443.
 - For AIM, open port 5190.

Connecting to America Online Behind the Gateway

If you cannot connect to AOL servers on a computer after connecting to AOL using the Gateway:

- Create an account for the Gateway.
- Create a password that is 8 alphanumeric characters long.
- Append **@aol.com** to the end of the username.
- Some AOL packages only allow for one internet connection.

Connecting to XBox Live, PSP, and Nintendo WFC

If you cannot connect to servers or experience server timeouts:

- Disable firewall and SPI applications.
- Reserve IP addresses for clients.
- Putting the XBox or Nintendo DS in the DMZ.
- Upgrade the latest firmware for your applications and Gateway.
- Enable the Gateway's UPnP feature (see "Discovering Devices" on page 92).
- Open specific ports for the game server.
- Enable wireless on PSP.

Nintendo DS does not support WPA or passphrase.

Appendix A - Compliance

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IEEE 802.11b or 802.11g operation of this product in the U.S.A is firmware-limited to channels 1 through 11.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Note to CATV System Installer - This reminder is provided to call the CATV systems installer's attention to Section 820-93 of the National Electric Code which provide guideline for proper grounding and, in particular,

specify that the Coaxial cable shield shall be connected to the grounding system of the building, as close to the point of cable entry as practical.

FCC Part 68 Statement

This equipment complies with Part 68 of the FCC Rules. A label is attached to the equipment that contains, among other information, its FCC registration number and ringer equivalence number. If requested, this information must be provided to the telephone company.

This equipment uses the following USOC Jack: RJ-11.

An FCC-compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack, which is FCC Part 68 compliant. Connection to the telephone network should be made by using the standard modular telephone jack.

The REN is useful to determine the quantity of devices that may be connected to the telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of RENs should not exceed 5. To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum REN for the calling area.

If this equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

In the event this equipment should fail to operate properly, disconnect the unit from the telephone line. Try using another FCC approved device in the same telephone jack. If the trouble persists, call the telephone company repair service bureau. If the trouble does not persist and appears to be with this unit, disconnect the unit from the telephone line and discontinue use of the unit until it is repaired. Please note that the telephone company may ask that you disconnect the equipment from the telephone network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

The user must use the accessories and cables supplied by the manufacturer to get optimum performance from the product.

No repairs may be done by the customer. If trouble is experienced with this equipment, please contact your authorized support provider for repair and warranty information. If the trouble is causing harm to the telephone network, the telephone company may request you remove the equipment from the network until the problem is resolved. This equipment cannot be used on telephone company provided coin service. Connection to Party Line Service is subject to state tariffs.

Index

A

- Access types
 - disabling, 78, 152
 - enabling, 78, 152
- Adding
 - blocked devices, 79, 153
 - computers with static IP address, 65, 136, 139
 - port forwarding rule, 85, 158
 - port triggering rule, 88, 161
- Advanced Features menu, 84, 157
- Apple Macintosh
 - IP address, 187
 - MAC address, 197
 - Ping utility, 193
 - TCP/IP configuration, 33
- At a Glance menu, 42, 107

B

- Basic setup procedures, 180
- Battery
 - menu, 57, 128
- Blocking
 - devices, 79, 153
 - keywords, 72, 145
 - services, 75
 - sites, 69, 143
- Bottom panel, 16
- Browsing on Web is slow, 195

C

- Change Password menu, 99, 178
- Comcast Network menu, 46
- Comcast network status, 44, 111
- Computers
 - adding, 65, 136, 139
 - editing, 66, 138, 141

- Configuration, 36, 100
 - TCP/IP, 24
- Configuring
 - PC for TCP/IP, 183
- Configuring login password, 99, 178
- Connected Devices menu, 64, 135
- Connecting
 - LAN, 21
 - public telephone network, 22
 - WAN, 22
- Conventions in this document, ix

D

- Destination address, testing connection to, 97, 176
- Determining
 - IP address, 183
 - MAC address, 196
- Device Discovery menu, 92, 171
- DHCP
 - address is not passed to computers, 195
 - beginning address, 48, 113
 - configuring computers to use, 24
 - ending address, 48, 113
 - lease time, 48, 113
- Disabling
 - access types, 78, 152
 - managed devices, 78, 152
 - port blocking, 91
 - port forwarding, 87, 160, 163
 - port triggering, 87, 90, 160
- Disabling firewall, 35
- Disabling proxy settings
 - Firefox, 34
 - Internet Explorer, 34
 - Safari, 35
- Disabling security software, 35
- DMZ (Demilitarized Zone) menu, 165

Document
conventions, ix
organization, ix

Downloading
logs, 95
reports, 83

E

Editing computers with static IP address, 66, 138, 141

Enabling
access types, 78, 152
managed devices, 78, 152
port blocking, 91
port forwarding, 87
port triggering, 87, 90, 160

F

Factory defaults
resetting and keeping, 98, 177
restoring, 17, 98, 177

Filters
logs, 94, 174
reports, 82

Firefox, disabling proxy settings, 34

Firewall menu, 53, 123

Firewall, disabling, 35

Front panel, 13

G

Gateway
bottom panel, 16
configuring, 36, 100
connecting to the LAN, 21
connecting to the public telephone network, 22
connecting to the WAN, 22
connectivity to destination address, 97, 176
connectivity to IP address, 97, 176
disconnects from the Internet, 194
front panel, 13
installing, 18

key features, viii
locating, 19
package contents, 12
powering on, 23
rear panel, 15
rebooting and restoring custom settings, 17
resetting, 98, 177
restoring factory defaults, 17, 98, 177
specifications, 205
system requirements, 12
top panel, 16
troubleshooting, 94, 173
Web management, 37, 101
Gateway menu, 43, 106
Gateway port status
Ethernet, 58, 129
wireless, 59, 130

H

Home Network Wizard menu, 60, 131

I

Installing
Gateway, 18
Internet
Gateway disconnects, 194
testing path from a computer, 192
unable to access, 189
Internet Explorer, disabling proxy settings, 34
IP address
determining, 183
IPv4, 47, 112
IPv6, 47, 112
testing connection to, 97, 176
IPv4 addressing, 47, 112
IPv6 addressing, 47, 112

K

Key features, viii
Keywords, blocking, 72, 145

L

- LAN connection, 21
- LAN Ethernet menu, 58, 129
- Local IP
 - Configuration menu, 47, 112
 - network status, 44, 111
- Locating the Gateway, 19
- Log filters, 94, 174
 - defining, 95
- Logging in to Web management, 37, 101
- Login password
 - changing, 99, 178
 - entering, 37, 101
- Logs
 - downloading, 95
 - printing, 95
- Logs menu, 94, 174

M

- MAC address
 - determining, 196
 - viewing, 59, 130
- Managed devices
 - disabling, 78, 152
 - enabling, 78, 152
- Managed Devices menu, 78, 152
- Managed Services menu, 75
- Managed Sites menu, 68, 142
- Menus
 - DMZ (Demilitarized Zone), 165
- Menus in Web management, 38, 40, 102, 104
- Microsoft
 - TCP/IP configuration for Windows 2000, 25, 26
 - TCP/IP configuration for Windows 7, 30
 - TCP/IP configuration for Windows Vista, 27

N

- Network Diagnostic Tools menu, 96, 175

P

- Package contents, 12

- Parental Control menu, 68, 142
- Pass-thru VPN troubleshooting, 195
- Password Settings menu, 99, 178
- Ping
 - testing the path from
 - a computer to the Gateway, 191
 - a computer to the Internet, 192
- Ping utility, 191
 - on a Macintosh, 193
- Port Blocking menu, 91
- Port forwarding
 - disabling, 87, 160, 163
 - enabling, 87
 - enabling or disabling, 84, 157
 - rule, 85, 158
 - unable to configure, 195
- Port status
 - Ethernet, 58, 129
 - wireless, 59, 130
- Port trigger rule, 88, 161
- Port triggering
 - disabling, 90
 - enabling, 90
- Port Triggering menu, 87, 160
- Powering-on the Gateway, 23
- Printing
 - logs, 95
 - reports, 83
- Proxy settings, 34
- Public telephone network connection, 22

R

- Rear panel, 15
- Rebooting
 - restoring custom settings, 17
- Report filters, 82
 - defining, 83
- Reports
 - downloading, 83
 - printing, 83
- Reports menu, 82
- Requirements, 12

Resetting
 Gateway, 98, 177
 Wi-Fi router, 98, 177
Restore / Reboot Gateway menu, 98, 177
Restoring factory defaults, 17, 98, 177

S

Safari, disabling proxy settings, 35
Security software, 35
Services, blocking, 75
Sites, blocking, 69, 143
Slow Web browsing, 195
Software menu, 55, 125
Specifications, 205
Status menu, 44, 111
System Hardware menu, 56, 127
System requirements, 12
System software, 55, 125

T

TCP/IP configuration, 24
 Apple Macintosh, 33
 Microsoft Windows 2000, 25, 26
 Microsoft Windows 7, 30
 Microsoft Windows Vista, 27
Testing connection to
 destination address, 97, 176
 IP address, 97, 176
Testing the path from a computer to
 the Gateway, 191
 the Internet, 192
Top panel, 16
Troubleshooting
 basic setup procedures, 180
 Gateway Disconnects from the Internet, 194
 Gateway is not passing DHCP to computers, 195
 Ping utility, 191
 Ping utility on Macintosh, 193
 slow Web browsing, 195
 testing the path from
 a computer to the Gateway, 191
 a computer to the Internet, 192

unable to
 use pass-thru VPN, 195
unable to access Gateway, 188
unable to access the Internet, 189
unable to configure port forwarding, 195
unable to connect to a wireless network, 199
unable to connect to networked devices, 191
unable to log In to Gateway, 188
wireless, 198
Troubleshooting menu, 94, 173

U

Unable to
 access Gateway, 188
 access the Internet, 189
 configure port forwarding, 195
 connect to a wireless network, 199
 connect to networked devices, 191
 log In to Gateway, 188
 use pass-thru VPN, 195

V

VPN troubleshooting, 195

W

WAN connection, 22
Web browsing is slow, 195
Web management
 DMZ (Demilitarized Zone) menu, 165
 logging in, 37, 101
 menus, 38, 40, 102, 104
Web management menus
 Advanced Features, 84, 157
 At a Glance, 42, 107
 Battery, 57, 128
 Change Password, 99, 178
 Comcast Network, 46
 Connected Devices, 64, 135
 Device Discovery, 92, 171
 Firewall, 53, 123
 Gateway, 43, 106

Index

- Home Network Wizard, 60, 131
- LAN Ethernet, 58, 129
- Local IP Configuration, 47, 112
- Logs, 174
- Logs menu, 94
- Managed Devices, 78, 152
- Managed Services, 75
- Managed Sites, 68, 142
- Network Diagnostic Tools menu, 96, 175
- Parental Controls, 68, 142
- Port Blocking, 91
- Port Triggering, 87, 160
- Reports, 82
- Restore / Reboot Gateway, 98, 177
- Software, 55, 125
- Status, 44, 111
- System Hardware, 56, 127
- Troubleshooting, 94, 173
- WiFi, 59, 130
- Wireless, 49, 114
 - XFINITY Network, 121
- WiFi menu, 59, 130
- Wi-Fi network status, 44, 111
- Wi-Fi router, resetting, 98, 177
- Wireless
 - improving performance, 201
 - improving performance for 802.11N, 202
 - optimizing performance, 201
 - range is low, 198
- Wireless menu, 49, 114
- Wireless troubleshooting, 198
- XFINITY Network menu, 121

X



SMC[®]
Networks

DRAFT

20 Mason
Irvine, CA. 92618
U.S.A.
<http://www.smc.com>

Document number: D3GNV311122012

DRAFT