



HitronTechnologies

USER'S GUIDE



CGN RESIDENTIAL CABLE MODEM

VERSION 2.0 - FEBRUARY 2012

ABOUT THIS USER'S GUIDE

INTENDED AUDIENCE

This manual is intended for people who want to configure the CGN's features via its Graphical User Interface (GUI).

HOW TO USE THIS USER'S GUIDE

This manual contains information on each the CGN's GUI screens, and describes how to use its various features.

- ▶ Use the [Introduction](#) (page 12) to see an overview of the topics covered in this manual.
- ▶ Use the [Table of Contents](#) (page 7), [List of Figures](#) (page 10) and [List of Tables](#) (page 11) to quickly find information about a particular GUI screen or topic.
- ▶ Use the [Index](#) (page 112) to find information on a specific keyword.
- ▶ Use the rest of this User's Guide to see in-depth descriptions of the CGN's features.

RELATED DOCUMENTATION

- ▶ **Quick Installation Guide:** see this for information on getting your CGN up and running right away. It includes information on system requirements, package contents, the installation procedure, and basic troubleshooting tips.
- ▶ **Online Help:** each screen in the CGN's Graphical User Interface (GUI) contains a **Help** button. Click this button to see additional information about configuring the screen.

DOCUMENT CONVENTIONS

This User's Guide uses various typographic conventions and styles to indicate content type:

- ▶ Bulleted paragraphs are used to list items, and to indicate options.
- 1 Numbered paragraphs indicate procedural steps.

NOTE: Notes provide additional information on a subject.

 **Warnings provide information about actions that could harm you or your device.**

Product labels, field labels, field choices, etc. are in **bold** type. For example:

Select **UDP** to use the User Datagram Protocol.

A mouse click in the Graphical User Interface (GUI) is denoted by a right angle bracket (>). For example:

Click **Settings > Advanced Settings**.

means that you should click **Settings** in the GUI, then **Advanced settings**.

A key stroke is denoted by square brackets and uppercase text. For example:

Press [ENTER] to continue.

CUSTOMER SUPPORT

For technical assistance or other customer support issues, please consult your Hitron representative.

DEFAULT CREDENTIALS

The CGN's default login credentials are as follows. For more information, see [Logging into the CGN](#) on page 22.

Table 1: [Default Credentials](#)

Username	cusadmin
Password	password

Copyright © 2012 Hitron Technologies. All rights reserved. All trademarks and registered trademarks used are the properties of their respective owners.

DISCLAIMER: The information in this User's Guide is accurate at the time of writing. This User's Guide is provided "as is" without express or implied warranty of any kind. Neither Hitron Technologies nor its agents assume any liability for inaccuracies in this User's Guide, or losses incurred by use or misuse of the information in this User's Guide.

COMPLIANCES

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 - The cable distribution system should be grounded (earthed) in accordance with ANSI/NFPA 70, the National Electrical Code (NEC), in particular Section 820.93, Grounding of Outer Conductive Shield of a Coaxial Cable. 107 SMCD3G3-CCR 4-Port Gateway Administrator Manual

TABLE OF CONTENTS

About This User's Guide	2
Compliances	5
Table of Contents	7
List of Figures	10
List of Tables	11
Introduction	12
1.1 CGN Overview	12
1.1.1 Key Features	13
1.2 Hardware Connections	14
1.3 LEDs	17
1.4 IP Address Setup	20
1.4.1 Manual IP Address Setup	21
1.5 Logging into the CGN	22
1.6 GUI Overview	23
1.7 Resetting the CGN	24
Status	26
2.1 Cable Overview	26
2.1.1 DOCSIS	26
2.1.2 IP Addresses and Subnets	27
2.1.2.1 IP Address Format	27
2.1.2.2 IP Address Assignment	27
2.1.2.3 Subnets	28
2.1.3 DHCP	29
2.1.4 DHCP Lease	30
2.1.5 MAC Addresses	30

2.1.6 Routing Mode	31
2.1.7 Configuration Files	31
2.1.8 Downstream and Upstream Transmissions	31
2.1.9 Cable Frequencies	31
2.1.10 Modulation	32
2.1.11 TDMA, FDMA and SCDMA	32
2.2 The System Info Screen	33
2.3 The Initialization Screen	37
2.4 The CM Status Screen	38
2.5 The Password Screen	41
2.6 The Capability Screen	42
WAN/LAN	45
3.1 WAN/LAN Overview	45
3.1.1 WAN and LAN	45
3.1.2 LAN IP Addresses and Subnets	46
3.1.3 DNS and Domain Suffix	46
3.1.4 Debugging (Ping and Traceroute)	46
3.2 The IP Screen	47
3.3 The Shared Media Screen	50
3.4 The Debug Screen	51
3.5 The Backup Screen	52
Firewall	54
4.1 Firewall Overview	54
4.1.1 Firewall	54
4.1.2 Intrusion detection system	55
4.1.3 Ping	55
4.1.4 MAC Filtering	55
4.1.5 IP Filtering	55
4.1.6 Port Forwarding	56
4.1.7 Port Triggering	56
4.1.8 DMZ	56
4.2 The Firewall Options Screen	56
4.3 The Filter Setting Screen	57

4.3.1 Adding or Editing an IP Filtering Rule	63
4.4 The Forwarding Screen	65
4.4.1 Adding or Editing a Port Forwarding Rule	67
4.5 The Port Triggering Screen	69
4.5.1 Adding or Editing a Port Triggering Rule	71
4.6 The DMZ Screen	72
Parental Control	74
5.1 Parental Control Overview	74
5.1.1 Website Blocking	74
5.2 The Website Blocking Screen	75
5.3 The Scheduling Screen	77
5.4 The Email / Syslog Alert Screen	79
Wireless	83
6.1 Wireless Overview	83
6.1.1 Wireless Networking Basics	83
6.1.2 Architecture	83
6.1.3 Wireless Standards	84
6.1.4 Service Sets and SSIDs	84
6.1.5 Wireless Security	85
6.1.5.1 WPS	85
6.1.6 WMM	86
6.2 The Setup Screen	86
6.3 The Access Control Screen	93
6.4 The Advanced Screen	95
6.4.1 Configuring WMM Parameters	103
Troubleshooting	107
.....	109
FCC STATEMENT	110
Index	112

LIST OF FIGURES

Figure 1: Application Overview	13
Figure 2: Hardware Connections	15
Figure 3: LEDs	18
Figure 4: Login	23
Figure 5: GUI Overview	24
Figure 6: The Status > System Info Screen	34
Figure 7: The Status > Initialization Screen	37
Figure 8: The Status > CM Status Screen	39
Figure 9: The Status > Password Screen	42
Figure 10: The Status > Capability Screen	43
Figure 11: The WAN/LAN > IP Screen	48
Figure 12: The WAN/LAN > Shared Media Screen	51
Figure 13: The WAN/LAN > Debug Screen	52
Figure 14: The WAN/LAN > Backup Screen	53
Figure 15: The Firewall > Firewall Options Screen	57
Figure 16: The Firewall > Filter Setting Screen	59
Figure 17: The Firewall > Filter Settings > Add/Edit Screen	63
Figure 18: The Firewall > Forwarding Screen	65
Figure 19: The Firewall > Forwarding > Add/Edit Screen	67
Figure 20: The Firewall > Port Triggering Screen	69
Figure 21: The Firewall > Port Triggering > Add/Edit Screen	71
Figure 22: The Firewall > DMZ Screen	73
Figure 23: The Parental Control > Web Site Blocking Screen	75
Figure 24: The Parental Control > Scheduling Screen	78
Figure 25: The Parental Control > Email / Syslog Alert Screen	79
Figure 26: Add Target Email Address	81
Figure 27: The Wireless > Setup Screen	87
Figure 28: WPS PIN	89
Figure 29: The Wireless > Access Control Screen	93
Figure 30: The Wireless > Advanced Screen	96
Figure 31: The Wireless > Advanced > WMM Configuration Screen	103

LIST OF TABLES

Table 1: Default Credentials	4
Table 2: Hardware Connections	16
Table 3: LEDs	18
Table 4: GUI Overview	24
Table 5: Private IP Address Ranges	28
Table 6: IP Address: Decimal and Binary	28
Table 7: Subnet Mask: Decimal and Binary	29
Table 8: The Status > System Info Screen	35
Table 9: The Status > CM Status Screen	39
Table 10: The Status > Password Screen	42
Table 11: The Status > Capability Screen	43
Table 12: The WAN/LAN > IP Screen	48
Table 13: The WAN/LAN > Shared Media Screen	51
Table 14: The WAN/LAN > Debug Screen	52
Table 15: The LAN > Backup Screen	53
Table 16: The Firewall > Firewall Options Screen	57
Table 17: The Firewall > Filter Setting Screen	60
Table 18: The Firewall > Filter Settings > Add/Edit Screen	64
Table 19: The Firewall > Forwarding Screen	65
Table 20: The Firewall > Forwarding > Add/Edit Screen	68
Table 21: The Firewall > Port Triggering Screen	69
Table 22: The Firewall > Port Triggering > Add/Edit Screen	71
Table 23: The Firewall > DMZ Screen	73
Table 24: The Parental Control > Web Site Blocking Screen	76
Table 25: The Parental Control > Scheduling Screen	78
Table 26: The Parental Control > Email / Syslog Alert Screen	80
Table 27: The Wireless > Setup Screen	87
Table 28: The Wireless > Access Control Screen	94
Table 29: The Wireless > Advanced Screen	97
Table 30: The Wireless > Advanced > WMM Configuration Screen	103

1

INTRODUCTION

This chapter introduces the CGN and its GUI (Graphical User Interface). It contains the following sections:

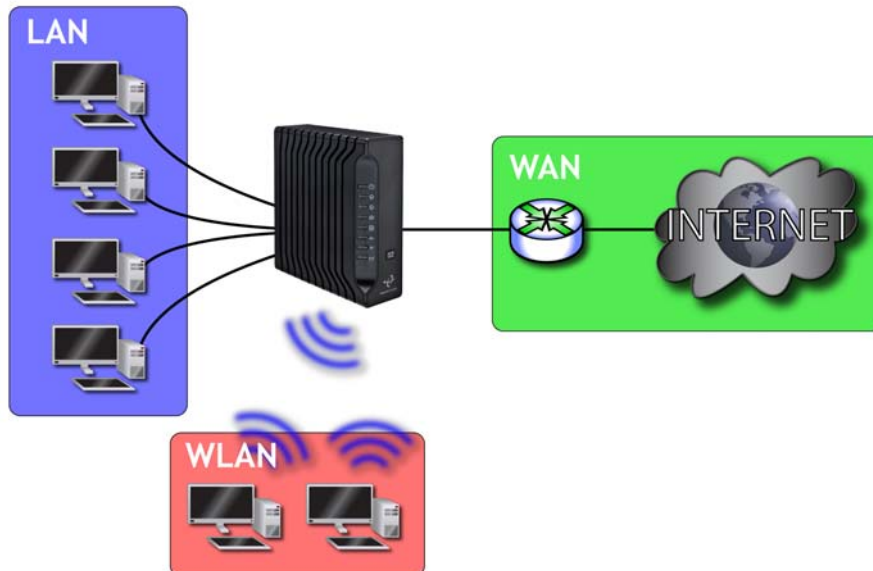
- ▶ [CGN Overview](#) on page 12
- ▶ [Hardware Connections](#) on page 14
- ▶ [LEDs](#) on page 17
- ▶ [IP Address Setup](#) on page 20
- ▶ [Logging into the CGN](#) on page 22
- ▶ [GUI Overview](#) on page 23
- ▶ [Resetting the CGN](#) on page 24

1.1 CGN OVERVIEW

Your CGN is a NAT-capable cable modem and wireless access point that allows you to connect your computers, wireless devices, and other network devices to one another, and to the Internet via the cable connection.

Computers with a wired connection to the CGN are on the Local Area Network (LAN), computers with a wireless connection to the CGN are on the Wireless Local Area Network (WLAN) and the CGN connects to the service provider over the Wide Area Network (WAN).

Figure 1: Application Overview



1.1.1 KEY FEATURES

The CGN provides:

- ▶ Internet connection to cable modem service via **CABLE** port (F-type RF connector)
- ▶ Local Area Network connection via four 10/100/1000 Mbps (megabits per second) Ethernet ports
- ▶ Dynamic Host Configuration Protocol (DHCP) for devices on the LAN
- ▶ LAN troubleshooting tools (Ping and Traceroute)
- ▶ IEEE 802.11b/g/n wireless MIMO (Multiple-In, Multiple-Out) networking, allowing speeds of up to 300Mbps
- ▶ Wireless security: WEP, WPA-PSK and WPA2-PSK encryption, Wifi Protected Setup (WPS) push-button and PIN configuration, MAC filtering,
- ▶ Wired security: stateful inspection firewall with intrusion detection system, IP and MAC filtering, port forwarding and port triggering, De-Militarized Zone (DMZ) and event logging
- ▶ Parental control: scheduled website blocking and access logs

- ▶ Settings backup and restore
- ▶ Secure configuration interface, accessible by Web browser

1.2 HARDWARE CONNECTIONS

This section describes the CGN's physical ports and buttons.

Figure 2: Hardware Connections

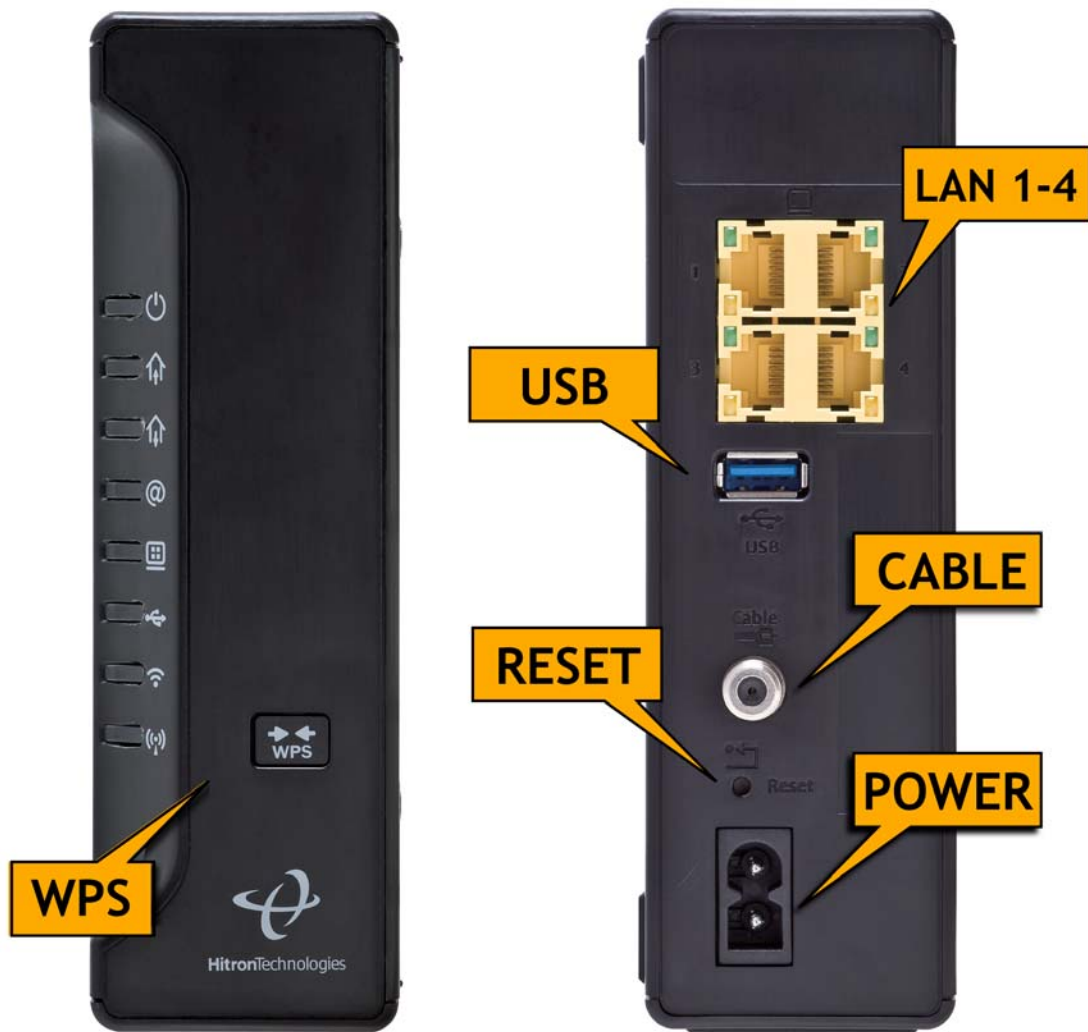


Table 2: Hardware Connections


WPS PBC	<p>Press this button to begin the WiFi Protected Setup (WPS) Push-Button Configuration (PBC) procedure.</p> <p>Press the PBC button on your wireless clients in the coverage area within two minutes to enable them to join the wireless network.</p> <p>See WPS on page 85 for more information.</p>
Reset	<p>Use this button to reboot or reset your CGN.</p> <ul style="list-style-type: none"> ▶ Press the button and hold it for less than five seconds to reboot the CGN. The CGN restarts, using your existing settings. ▶ Press the button and hold it for more than five seconds to delete all user-configured settings and restart the CGN using its factory default settings. See Resetting the CGN on page 24 for more information on resetting the CGN. <p>NOTE: Unless you previously backed-up the CGN's configuration settings prior to resetting the CGN, the settings cannot be recovered.</p>
USB	<p>The CGN provides one USB 2.0 host port, allowing you to plug in a USB flash disk for mounting and sharing through the LAN interfaces via the Samba protocol (network neighborhood).</p> <p>The CGN supports the following Windows file systems:</p> <ul style="list-style-type: none"> ▶ FAT16 ▶ FAT32 ▶ NTFS <p> USB devices must not drain more than 500mA from the USB port. USB devices requiring more than 500mA should be provided with their own power source(s).</p>
LAN1	<p>Use these ports to connect your computers and other network devices, using Category 5 or 6 Ethernet cables with RJ45 connectors.</p>
LAN2	
LAN3	
LAN4	

Table 2: [Hardware Connections](#)

CABLE	Use this to connect to the Internet via an F-type RF cable.
POWER	Cable modem is plugged in to an electrical outlet and is and receiving power.

1.3 LEDS

This section describes the CGN's LEDs (lights).

Figure 3: LEDs



Table 3: LEDs


LED	STATUS	DESCRIPTION
WPS	Off	The WPS is not enabled.
	Green, steady	The WPS is enabled.
	Red, blinking	Error: Some error occurred which was not related to security, such as failed to find any partner or protocol prematurely aborted. Session Overlap Detected: Protocol detected overlapping operation could be a security risk.
	Orange, blinking	The protocol is searching for a partner, connecting, or exchanging network parameters
WIRELESS 	Off	The wireless network is not enabled.
	Green, steady	The wireless network is enabled, and no data is being transmitted or received over the wireless network.
	Green, blinking	The wireless network is enabled, and data is being transmitted or received over the wireless network.

Table 3: **LEDs**







USB 	Off	The CGN is not linked up USB.
	Green, steady	The CGN has successfully linked up USB.
LAN/ Front 	Off	No device is connected to the LAN port.
	Green, blinking	A device is connected to the LAN port via a Ethernet link, and is transmitting or receiving data.
	Green, steady	A device has successfully connected to the LAN port via a Ethernet link.
LAN/ Back	Off	No device is connected to the relevant LAN port.
	Green, blinking	A device is connected to the relevant LAN port via a Fast Ethernet (10/100Mbps) link, and is transmitting or receiving data.
	Green, steady	A device is connected to the relevant LAN port via a Fast Ethernet (10/100Mbps) link, but is not transmitting or receiving data.
	Blue, blinking	A device is connected to the relevant LAN port via a Gigabit Ethernet (1000Mbps) link, and is transmitting or receiving data.
	Blue, steady	A device is connected to the relevant LAN port via a Gigabit Ethernet (1000Mbps) link, but is not transmitting or receiving data.
Status 	Green, Blinking	The CGN's cable modem is registering with the service provider's CMTS.
	Green	The CGN's cable modem has successfully registered with the service provider and is ready for data transfer.
US 	Green, blinking	The CGN is searching for an upstream frequency on the CABLE connection.
	Green, steady	The CGN has successfully located and locked onto an upstream frequency on the CABLE connection.
	Blue, steady	The CGN is engaged in channel bonding on the upstream connection.
	Off	There is no upstream activity on the CABLE connection.

Table 3: **LEDs**

DS 	Green, blinking	The CGN is searching for a downstream frequency on the CABLE connection.
	Green, steady	The CGN has successfully located and locked onto a downstream frequency on the CABLE connection.
	Blue, steady	The CGN is engaged in channel bonding on the downstream connection.
	Off	There is no downstream activity on the CABLE connection.
Power 	Green	Cable modem is plugged in to an electrical outlet and is and receiving power
	Off	The CGN is not receiving power.

When you turn on the CGN, the LEDs light up in the following order:

- ▶ **Power**
- ▶ **US**
- ▶ **DS**
- ▶ **Status**
- ▶ The **ETH 1~4** LEDs light up as soon as there is activity on the relevant port, and the **WIRELESS** LED lights up once the wireless network is ready.
- ▶ **USB**
- ▶ **WIRELESS**

1.4 IP ADDRESS SETUP

Before you log into the CGN's GUI, your computer's IP address must be in the same subnet as the CGN. This allows your computer to communicate with the CGN.

NOTE: [See IP Addresses and Subnets on page 27 for background information.](#)

The CGN has a built-in DHCP server that, when active, assigns IP addresses to computers on the LAN. When the DHCP server is active, you can get an IP address automatically. The DHCP server is active by default.

If your computer is configured to get an IP address automatically, or if you are not sure, try to log in to the CGN (see [Logging into the CGN](#) on page 22).

- ▶ If the login screen displays, your computer is already configured correctly.
- ▶ If the login screen does not display, either the CGN's DHCP server is not active or your computer is not configured correctly. Follow the procedure in [Manual IP Address Setup](#) on page 21 and set your computer to get an IP address automatically. Try to log in again. If you cannot log in, follow the manual IP address setup procedure again, and set a specific IP address as shown. Try to log in again.

NOTE: [If you still cannot see the login screen, your CGN's IP settings may have been changed from their defaults. If you do not know the CGN's new address, you should return it to its factory defaults. See \[Resetting the CGN\]\(#\) on page 24. Bear in mind that ALL user-configured settings are lost.](#)

1.4.1 MANUAL IP ADDRESS SETUP

By default, your CGN's local IP address is **192.168.0.1**. If your CGN is using the default IP address, you should set your computer's IP address to be between **192.168.0.2** and **192.168.0.254**.

NOTE: [If your CGN DHCP server is active, set your computer to get an IP address automatically in step 5. The CGN assigns an IP address to your computer. The DHCP server is active by default.](#)

Take the following steps to manually set up your computer's IP address to connect to the CGN:

NOTE: [This example uses Windows XP; the procedure for your operating system may be different.](#)

- 1** Click **Start**, then click **Control Panel**.
- 2** In the window that displays, double-click **Network Connections**.
- 3** Right-click your network connection (usually **Local Area Connection**) and click **Properties**.
- 4** In the **General** tab's **This connection uses the following items** list, scroll down and select **Internet Protocol (TCP/IP)**. Click **Properties**.

5 You can get an IP address automatically, or specify one manually:

- ▶ If your CGN's DHCP server is active, select **Get an IP address automatically**.
- ▶ If your CGN's DHCP server is active, select **Use the following IP address**. In the **IP address** field, enter a value between **192.168.0.2** and **192.168.0.254** (default). In the **Subnet mask** field, enter **255.255.255.0** (default).

NOTE: If your CGN is not using the default IP address, enter an IP address and subnet mask that places your computer in the same subnet as the CGN.

6 Click **OK**. The **Internet Protocol (TCP/IP)** window closes. In the **Local Area Connection Properties** window, click **OK**.

Your computer now obtains an IP address from the CGN, or uses the IP address that you specified, and can communicate with the CGN.

1.5 LOGGING INTO THE CGN

Take the following steps to log into the CGN's GUI.

NOTE: You can log into the CGN's GUI via the wireless interface. However, it is strongly recommended that you configure the CGN via a wired connection on the LAN.

- 1** Open a browser window.
- 2** Enter the CGN's IP address (default **192.168.0.1**) in the URL bar. The **Login** screen displays.

Figure 4: Login

The image shows a login form for Hitron Technologies. At the top left is the Hitron Technologies logo, which consists of three curved lines in blue, green, and orange. To the right of the logo is the text "HitronTechnologies". Below the logo and text are two input fields: "Username:" followed by a white rectangular box, and "Password:" followed by a white rectangular box. At the bottom center of the form is a blue circular button with the word "Login" written in white.

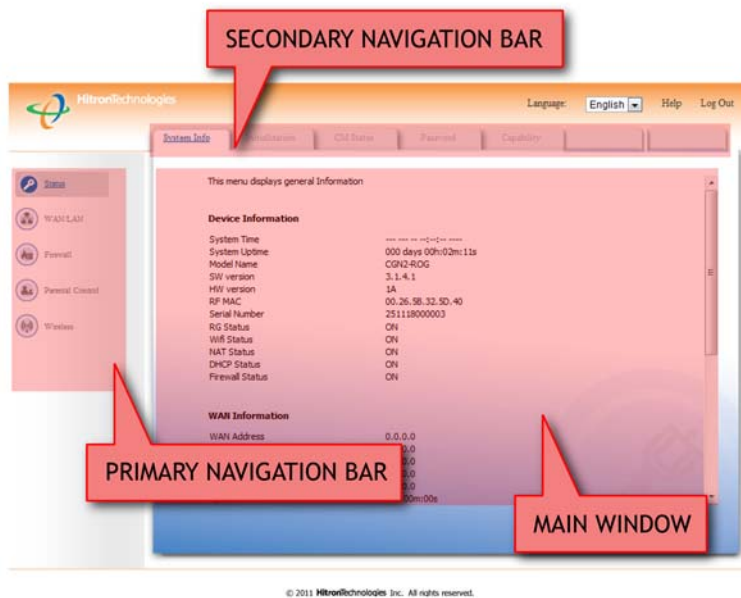
- 3 Enter the **Username** and **Password**. The default login username is **cusadmin**, and the default password is **password**.

NOTE: The Username and Password are case-sensitive; "password" is not the same as "Password".

- 4 Click **Login**. The **System Info** screen displays (see [The System Info Screen](#) on page 33).

1.6 GUI OVERVIEW

This section describes the CGN's GUI.

Figure 5: GUI Overview

Table 4: GUI Overview

Primary Navigation Bar	Use this section to move from one part of the GUI to another.
Secondary Navigation Bar	Use this section to move from one related screen to another.
Main Window	Use this section to read information about your CGN's configuration, and make configuration changes.

Each item in the **Primary Navigation Bar** has its own chapter in this User's Guide; items in the **Secondary Navigation Bar** have their own section within a chapter.

1.7 RESETTING THE CGN

When you reset the CGN to its factory defaults, all user-configured settings are lost, and the CGN is returned to its initial configuration state.

There are two ways to reset the CGN:

- ▶ Press the **RESET** button on the CGN, and hold it in for ten seconds or longer.

- ▶ Click **WAN/LAN > Backup**. In the screen that displays, click the **Factory Reset** button.

The CGN turns off and on again, using its factory default settings.

NOTE: Depending on your CGN's previous configuration, you may need to re-configure your computer's IP settings; see [IP Address Setup](#) on page 20.

2

STATUS

This chapter describes the screens that display when you click **Status** in the toolbar. It contains the following sections:

- ▶ [Cable Overview](#) on page 26
- ▶ [The System Info Screen](#) on page 33
- ▶ [The Initialization Screen](#) on page 37
- ▶ [The CM Status Screen](#) on page 38
- ▶ [The Password Screen](#) on page 41
- ▶ [The Capability Screen](#) on page 42

2.1 CABLE OVERVIEW

This section describes some of the concepts related to the **Cable** screens.

2.1.1 DOCSIS

The Data Over Cable Service Interface Specification (DOCSIS) is a telecommunications standard that defines the provision of data services (Internet access) over a traditional cable TV (CATV) network.

Your CGN supports DOCSIS version 3.0.

2.1.2 IP ADDRESSES AND SUBNETS

Every computer on the Internet must have a unique Internet Protocol (IP) address. The IP address works much like a street address, in that it identifies a specific location to which information is transmitted. No two computers on a network can have the same IP address.

2.1.2.1 IP ADDRESS FORMAT

IP addresses consist of four octets (8-bit numerical values) and are usually represented in decimal notation, for example **192.168.1.1**. In decimal notation, this means that each octet has a minimum value of 0 and a maximum value of 255.

An IP address carries two basic pieces of information: the “network number” (the address of the network as a whole, analogous to a street name) and the “host ID” (analogous to a house number) which identifies the specific computer (or other network device).

2.1.2.2 IP ADDRESS ASSIGNMENT

IP addresses can come from three places:

- ▶ The Internet Assigned Numbers Agency (IANA)
- ▶ Your Internet Service Provider
- ▶ You (or your network devices)

IANA is responsible for IP address allocation on a global scale, and your ISP assigns IP addresses to its customers. You should never attempt to define your own IP addresses on a public network, but you are free to do so on a private network.

In the case of the CGN:

- ▶ The public network (Wide Area Network or WAN) is the link between the cable connector and your Internet Service Provider. Your CGN's IP address on this network is assigned by your service provider.

- ▶ The private network (in routing mode - see [Routing Mode](#) on page 31) is your Local Area Network (LAN) and Wireless Local Area Network (WLAN), if enabled. You are free to assign IP addresses to computers on the LAN and WLAN manually, or to allow the CGN to assign them automatically via DHCP (Dynamic Host Configuration Protocol). IANA has reserved the following blocks of IP addresses to be used for private networks only:

Table 5: [Private IP Address Ranges](#)

FROM...	...TO
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

If you assign addresses manually, they must be within the CGN's LAN subnet.

2.1.2.3 SUBNETS

A subnet (short for sub-network) is, as the name suggests, a separate section of a network, distinct from the main network of which it is a part. A subnet may contain all of the computers at one corporate local office, for example, while the main network includes several offices.

In order to define the extent of a subnet, and to differentiate it from the main network, a subnet mask is used. This "masks" the part of the IP address that refers to the main network, leaving the part of the IP address that refers to the sub-network.

Each subnet mask has 32 bits (binary digits), as does each IP address:

- ▶ A binary value of **1** in the subnet mask indicates that the corresponding bit in the IP address is part of the main network.
- ▶ A binary value of **0** in the subnet mask indicates that the corresponding bit in the IP address is part of the sub-network.

For example, the following table shows the IP address of a computer (**192.168.1.1**) expressed in decimal and binary (each cell in the table indicates one octet):

Table 6: [IP Address: Decimal and Binary](#)

192	168	0	1
11000000	10101000	00000000	00000001

The following table shows a subnet mask that “masks” the first twenty-four bits of the IP address, in both its decimal and binary notation.

Table 7: [Subnet Mask: Decimal and Binary](#)

255	255	255	0
11111111	11111111	11111111	00000000

This shows that in this subnet, the first three octets (**192.168.1**, in the example IP address) define the main network, and the final octet (**1**, in the example IP address) defines the computer's address on the subnet.

The decimal and binary notations give us the two common ways to write a subnet mask:

- ▶ **Decimal:** the subnet mask is written in the same fashion as the IP address: **255.255.255.0**, for example.
- ▶ **Binary:** the subnet mask is indicated after the IP address (preceded by a forward slash), specifying the number of binary digits that it masks. The subnet mask **255.255.255.0** masks the first twenty-four bits of the IP address, so it would be written as follows: **192.168.1.1/24**.

2.1.3 DHCP

The Dynamic Host Configuration Protocol, or DHCP, defines the process by which IP addresses can be assigned to computers and other networking devices automatically, from another device on the network. This device is known as a DHCP server, and provides addresses to all the DHCP client devices.

In order to receive an IP address via DHCP, a computer must first request one from the DHCP server (this is a broadcast request, meaning that it is sent out to the whole network, rather than just one IP address). The DHCP server hears the requests, and responds by assigning an IP address to the computer that requested it.

If a computer is not configured to request an IP address via DHCP, you must configure an IP address manually if you want to access other computers and devices on the network. See [IP Address Setup](#) on page 20 for more information.

By default, the CGN is a DHCP client on the WAN (the CATV connection). It broadcasts an IP address over the cable network, and receives one from the service provider. By default, the CGN is a DHCP server on the LAN; it provides IP addresses to computers on the LAN which request them.

2.1.4 DHCP LEASE

“DHCP lease” refers to the length of time for which a DHCP server allows a DHCP client to use an IP address. Usually, a DHCP client will request a DHCP lease renewal before the lease time is up, and can continue to use the IP address for an additional period. However, if the client does not request a renewal, the DHCP server stops allowing the client to use the IP address.

This is done to prevent IP addresses from being used up by computers that no longer require them, since the pool of available IP addresses is finite.

2.1.5 MAC ADDRESSES

Every network device possesses a Media Access Control (MAC) address. This is a unique alphanumeric code, given to the device at the factory, which in most cases cannot be changed (although some devices are capable of “MAC spoofing”, where they impersonate another device’s MAC address).

MAC addresses are the most reliable way of identifying network devices, since IP addresses tend to change over time (whether manually altered, or updated via DHCP).

Each MAC address displays as six groups of two hexadecimal digits separated by colons (or, occasionally, dashes) for example **00:AA:FF:1A:B5:74**.

NOTE: Each group of two hexadecimal digits is known as an “octet”, since it represents eight bits.

Bear in mind that a MAC address does not precisely represent a computer on your network (or elsewhere), it represents a network device, which may be part of a computer (or other device). For example, if a single computer has an Ethernet card (to connect to your CGN via one of the **LAN** ports) and also has a wireless card (to connect to your CGN over the wireless interface) the MAC addresses of the two cards will be different. In the case of the CGN, each internal module (cable modem module, Ethernet module, wireless module, etc.) possesses its own MAC address.

2.1.6 ROUTING MODE

When your CGN is in routing mode, it acts as a gateway for computers on the LAN to access the Internet. The service provider assigns an IP address to the CGN on the WAN, and all traffic for LAN computers is sent to that IP address. The CGN assigns private IP addresses to LAN computers (when DHCP is active), and transmits the relevant traffic to each private IP address.

NOTE: When DHCP is not active on the CGN in routing mode, each computer on the LAN must be assigned an IP address in the CGN's subnet manually.

When the CGN is not in routing mode, the service provider assigns an IP address to each computer connected to the CGN directly. The CGN does not perform any routing operations, and traffic flows between the computers and the service provider.

Routing mode is not user-configurable; it is specified by the service provider in the CGN's configuration file.

2.1.7 CONFIGURATION FILES

The CGN's configuration (or config) file is a document that the CGN obtains automatically over the Internet from the service provider's server, which specifies the settings that the CGN should use. It contains a variety of settings that are not present in the user-configurable Graphical User Interface (GUI) and can be specified only by the service provider.

2.1.8 DOWNSTREAM AND UPSTREAM TRANSMISSIONS

The terms "downstream" and "upstream" refer to data traffic flows, and indicate the direction in which the traffic is traveling. "Downstream" refers to traffic from the service provider to the CGN, and "upstream" refers to traffic from the CGN to the service provider.

2.1.9 CABLE FREQUENCIES

Just like radio transmissions, data transmissions over the cable network must exist on different frequencies in order to avoid interference between signals.

The data traffic band is separate from the TV band, and each data channel is separate from other data channels.

2.1.10 MODULATION

Transmissions over the cable network are based on a strong, high frequency periodic waveform known as the “carrier wave.” This carrier wave is so called because it “carries” the data signal. The data signal itself is defined by variations in the carrier wave. The process of varying the carrier wave (in order to carry data signal information) is known as “modulation.” The data signal is thus known as the “modulating signal.”

Cable transmissions use a variety of methods to perform modulation (and the “decoding” of the received signal, or “demodulation”). The modulation methods defined in DOCSIS 3 are as follows:

- ▶ **QPSK:** Quadrature Phase-Shift Keying
- ▶ **QAM:** Quadrature Amplitude Modulation
- ▶ **QAM TCM:** Trellis modulated Quadrature Amplitude Modulation

In many cases, a number precedes the modulation type (for example **16 QAM**). This number refers to the complexity of modulation. The higher the number, the more data can be encoded in each symbol.

NOTE: In modulated signals, each distinct modulated character (for example, each audible tone produced by a modem for transmission over telephone lines) is known as a symbol.

Since more information can be represented by a single character, a higher number indicates a higher data transfer rate.

2.1.11 TDMA, FDMA AND SCDMA

Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA) and Synchronous Code Division Multiple Access (SCDMA) are channel access methods that allow multiple users to share the same frequency channel.

- ▶ TDMA allows multiple users to share the same frequency channel by splitting transmissions by time. Each user is allocated a number of time slots, and transmits during those time slots.
- ▶ FDMA allows multiple users to share the same frequency channel by assigning a frequency band within the existing channel to each user.

- ▶ SCDMA allows multiple users to share the same frequency channel by assigning a unique orthogonal code to each user.

2.2 THE SYSTEM INFO SCREEN

Use this screen to see general information about your CGN's hardware, its software, and its connection to the Internet.

NOTE: Most of the information that displays in this screen is for troubleshooting purposes only. However, you may need to use the MAC Address information when setting up your network.

Click **Status** > **System Info**. The following screen displays.

Figure 6: The Status > System Info Screen

This menu displays general Information

Device Information

System Time	-----:--:-----
System Uptime	000 days 01h:24m:49s
Model Name	██████████
SW version	3.1.4.1
HW version	1A
RF MAC	00.26.5B.32.5D.40
Serial Number	251118000003
RG Status	ON
Wifi Status	ON
NAT Status	ON
DHCP Status	ON
Firewall Status	ON

WAN Information

WAN Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway Address	0.0.0.0
DNS Server	0.0.0.0
	0.0.0.0
Uptime	00h:00m:00s
Traffic Count	Receiving: 0 bytes Sending: 0 bytes

Wireless Information

SSID	██████████
Wireless Mode	802.11b/g/n Mixed
Channel	Auto
Security Type	None
Cipher type	None
SSID MAC	00:26:5B:32:5D:48

LAN Status

MAC Address	00.26.5B.32.5D.42
Private LAN IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Uptime	01h:24m:49s
Traffic Count	Receiving:218838 bytes , Sending 1813440bytes

The following table describes the labels in this screen.

Table 8: [The Status > System Info Screen](#)

Device Information	
System Time	This displays the current date and time.
System Uptime	This displays the number of days, hours, minutes and seconds since the CGN was last switched on or rebooted.
Model Name	This displays the device's model name.
SW Version	This displays the version number of the software that controls the CGN.
HW Version	This displays the version number of the CGN's physical hardware.
RF MAC	This displays the Media Access Control (MAC) address of the CGN's RF module. This is the module that connects to the Internet through the CATV connection.
Serial Number	This displays a number that uniquely identifies the device.
RG Status	This displays whether or not the CGN is in Residential Gateway (RG) mode. When the CGN is in Residential Gateway mode, ON displays. When the CGN is not in Residential Gateway mode, OFF displays.
Wifi Status	This displays whether or not the CGN's wireless network is active. When the CGN's wireless network is active, ON displays. When the CGN's wireless network is not active, OFF displays.
NAT Status	This displays whether or not the CGN's Network Address Translation (NAT) feature is active. When NAT is active, ON displays. When NAT is not active, OFF displays.
DHCP Status	This displays whether or not the CGN's DHCP server is active. When the DHCP server is active, ON displays. When the DHCP server is not active, OFF displays.
Firewall Status	This displays whether or not the CGN's firewall is active. When the firewall is active, ON displays. When the firewall is not active, OFF displays.

Table 8: [The Status > System Info Screen \(continued\)](#)

WAN Information	
WAN Address	This field displays the CGN's IP address on the WAN (Wide Area Network) interface.
Subnet Mask	This field displays the CGN's WAN subnet mask.
Gateway Address	This field displays the address of the device on the WAN to which the CGN is connected.
DNS Server	This field displays the Domain Name Servers that the CGN uses to resolve domain names into IP addresses.
Uptime	This displays the number of hours, minutes and seconds that the CGN has been connected to another device over the WAN interface.
Traffic Count	This displays the number of bytes received and sent on the WAN interface.
Wireless Information	
SSID	This displays the wireless network's Service Set Identifier. This is the name of the wireless network, to which wireless clients connect.
Wireless Mode	This displays the type of wireless network that the CGN is using.
Channel	This displays the wireless channel on which the CGN is transmitting and receiving.
Security Type	This displays the type of security the CGN's wireless network is currently using.
Cipher type	This displays the type of encryption that the wireless network's security is using: <ul style="list-style-type: none"> ▶ TKIP displays if it is using the Temporal Key Integrity Protocol. ▶ AES displays if it is using the Advanced Encryption Standard. ▶ TKIP and AES displays if it allows clients using either encryption type to connect to the CGN.
SSID MAC	This displays the Media Access Control (MAC) address of the wireless module, to which wireless clients connect.
LAN Status	
MAC Address	This displays the Media Access Control (MAC) address of the CGN's Ethernet module. This is the module to which you connect through the LAN ports.

Table 8: [The Status > System Info Screen \(continued\)](#)

Private LAN IP Address	This displays the IP address of the CGN's Ethernet module. This is the IP address you use to connect with the CGN's admin interface via the LAN ports.
Subnet Mask	This displays the CGN's LAN subnet mask.
Uptime	This displays the number of hours, minutes and seconds that the CGN has been connected to another device over the LAN interface.
Traffic Count	This displays the number of bytes received and sent on the LAN interface.

2.3 THE INITIALIZATION SCREEN

This screen displays the steps successfully taken to connect to the Internet over the **CABLE** connection.

Use this screen for troubleshooting purposes to ensure that the CGN has successfully connected to the Internet; if an error has occurred you can identify the stage at which the failure occurred.

NOTE: [This screen displays when you first log in to the CGN.](#)

Click **Status > Initialization**. The following screen displays.

Figure 7: [The Status > Initialization Screen](#)

This menu displays the connectivity status of the modem and its boot state	
Modem Status	
HW init	Success
Find Downstream	Success
Ranging	Success
DHCP	Success
Time of Day	Success
Download CM Config File	Success
Registration	Success
EAE status	Disable
BPI status	AUTH:start, TEK:start
Network Access	Permitted
Traffic Enable!	

For each step:

- ▶ **Process** displays when the CGN is attempting to complete a connection step.
- ▶ **Success** displays when the CGN has completed a connection step.

2.4 THE CM STATUS SCREEN

Use this screen to discover information about:

- ▶ The nature of the upstream and downstream connection between the CGN and the device to which it is connected through the **CABLE** interface.
- ▶ IP details of the CGN's WAN connection.

You can also configure the CGN's downstream center frequency.

Click **Status** > **CM Status**. The following screen displays.

Figure 8: The Status > CM Status Screen

This menu displays both upstream and downstream signal parameters and Attached Devices

CM Configuration file name ArrisC4_IPv4_default.cfg
 Network Access Permitted

Tune Channel

Downstream Frequency (MHz) Upstream ID

Downstream

Port	1	2	3	4	5	6	7	8
Frequency (MHz)	117.000	123.000	129.000	135.000				
Modulation	256 QAM	256 QAM	256 QAM	256 QAM				
Signal power (dBmV)	7.66	7.45	7.297	6.924				
Signal noise ratio (dB)	37.935	37.092	37.636	37.092				
Channel ID	5	6	7	8				

Upstream

Port	1	2	3	4
Frequency (Hz)	31799454			23199583
Bandwidth (KSym/sec)	1280			1280
SCDMA mode	0			0
Signal power (dBmV)	28.0000			26.5000
Channel ID	9			10

Cable Modem IP Information

IP Address 192.168.52.55
 Subnet Mask 255.255.255.0
 Gateway IP 192.168.52.254
 DHCP Lease Time D: 00 H: 02 M: 00 S: 00

The following table describes the labels in this screen.

Table 9: The Status > CM Status Screen

CM Configuration File Name	This displays the name of the configuration file that the CGN downloaded from your service provider. This file provides the CGN with the service parameter data that it needs to perform its functions correctly.
Network Access	This displays whether or not your service provider allows you to access the Internet over the CABLE connection. <ul style="list-style-type: none"> ▶ Permitted displays if you can access the Internet. ▶ Denied displays if you cannot access the Internet.
Tune Channel	

Table 9: The Status > CM Status Screen (continued)

Downstream Frequency	<p>This displays the center frequency in Megahertz (MHz) at which the CGN connects over the CABLE interface.</p> <p>If you want the CGN to use a different center frequency, enter it in the field and click Apply.</p> <p>NOTE: Do not change the frequency unless you have a good reason to do so.</p>
Upstream ID	<p>This displays the ID number of the channel on which the upstream signal is to be transmitted. When an upstream connection cannot be made on the specified channel, the CGN attempts to connect on the next channel.</p> <p>If you want the CGN to attempt to connect on a different channel, enter it in the field and click Apply.</p> <p>NOTE: Do not change the channel unless you have a good reason to do so.</p>
Downstream	
NOTE: The downstream signal is the signal transmitted to the CGN.	
Frequency (MHz)	This displays the actual frequency in Megahertz (MHz) of each downstream data channel to which the CGN is connected.
Modulation	This displays the type of modulation that each downstream channel uses.
Signal Power (dBmV)	This displays the power of the signal of each downstream data channel to which the CGN is connected, in dBmV (decibels above/below 1 millivolt).
Signal Noise Ratio (dB)	This displays the Signal to Noise Ratio (SNR) of each downstream data channel to which the CGN is connected, in dB (decibels).
Upstream	
NOTE: The upstream signal is the signal transmitted from the CGN.	
Frequency (Hz)	This displays the frequency in Herz (Hz) of each upstream data channel to which the CGN is connected.
Bandwidth (KSym/sec)	This displays the bandwidth of each upstream data channel to which the CGN is connected (in thousands of symbols per second).

Table 9: [The Status > CM Status Screen \(continued\)](#)

SCDMA Mode	This displays the Synchronous Code Division Multiple Access (SCDMA) mode of each channel on which the upstream signal is transmitted.
Signal Power (dBmV)	This displays the transmitted power of the signal of each upstream data channel to which the CGN is connected, in dBmV (decibels above/below 1 millivolt).
Channel ID	This displays the ID number of each channel on which the upstream signal is transmitted.
Cable Modem IP Information	
IP Address	This displays the CGN's WAN IP address. This IP address is automatically assigned to the CGN
Subnet Mask	This displays the CGN's WAN subnet mask.
Gateway IP	This displays the IP address of the device to which the CGN is connected over the CABLE interface.
DHCP Lease Time	This displays the time that elapses before your device's IP address lease expires, and a new IP address is assigned to it by the DHCP server.

2.5 THE PASSWORD SCREEN

Use this screen to change the password with which you log in to the CGN.

NOTE: [If you forget your password, you will need to reset the CGN to its factory defaults.](#)

Click **Status > Password**. The following screen displays.

Figure 9: [The Status > Password Screen](#)

This menu displays the Customer password settings

Modify Password

Enter Current Password

Enter New Password

Re-enter New Password

Password Idle Time minutes

The following table describes the labels in this screen.

Table 10: [The Status > Password Screen](#)

Enter Current Password	Enter the password with which you currently log into the CGN
Enter New Password	Enter and re-enter the password you want to use to log into the CGN.
Re-enter New Password	
Password Idle Time	Enter the number of minutes of inactivity after which you should be automatically logged out of the CGN. Once this period elapses, you will need to log in again.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

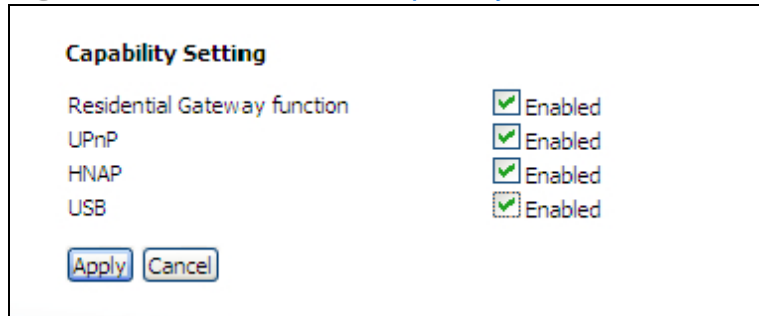
2.6 THE CAPABILITY SCREEN

Use this screen to enable or disable the CGN's residential gateway and Universal Plug n Play (UPnP) functions.

Disabling the residential gateway feature sets the unit to use bridge mode only. Use this mode when your network is already using another router.

Click **Status > Capability**. The following screen displays.

Figure 10: [The Status > Capability Screen](#)



The following table describes the labels in this screen.

Table 11: [The Status > Capability Screen](#)

Residential Gateway function	Select the checkbox to enable the CGN's residential gateway features, or deselect the checkbox to disable them.
UPnP	Select the checkbox to enable the CGN's Universal Plug n Play features, or deselect the checkbox to disable them.
HNAP	Select the checkbox to enable the CGN's Home Network Administration Protocol features, or deselect the checkbox to disable them.
USB	<p>Select the checkbox to enable the CGN's USB media sharing capability, or deselect the checkbox to disable them.</p> <p>NOTE: This option is available to logged-in MSO users only.</p> <p>When you select this checkbox and apply your changes, the CGN reboots. Once it has successfully rebooted, the WAN/LAN > Shared Media screen displays in the cusadmin user interface.</p>
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

3

WAN/LAN

This chapter describes the screens that display when you click **WAN/LAN** in the toolbar. It contains the following sections:

- ▶ [WAN/LAN Overview](#) on page 45
- ▶ [The IP Screen](#) on page 47
- ▶ [The Shared Media Screen](#) on page 50
- ▶ [The Debug Screen](#) on page 51
- ▶ [The Backup Screen](#) on page 52

3.1 WAN/LAN OVERVIEW

This section describes some of the concepts related to the **WAN/LAN** screens.

3.1.1 WAN AND LAN

A Local Area Network (LAN) is a network of computers and other devices that usually occupies a small physical area (a single building, for example). Your CGN's LAN consists of all the computers and other networking devices connected to the **LAN 1~4** ports. This is your private network (in routing mode - see [Routing Mode](#) on page 31).

The LAN is a separate network from the Wide Area Network (WAN). In the case of the CGN, the WAN refers to all computers and other devices available on the cable connection.

By default, computers on the WAN cannot identify individual computers on the LAN; they can see only the CGN. The CGN handles routing to and from individual computers on the LAN.

3.1.2 LAN IP ADDRESSES AND SUBNETS

IP addresses on the LAN are controlled either by the CGN's built-in DHCP server (see [DHCP](#) on page 29), or by you (when you manually assign IP addresses to your computers).

For more information about IP addresses and subnets in general, see [IP Addresses and Subnets](#) on page 27.

3.1.3 DNS AND DOMAIN SUFFIX

A domain is a location on a network, for instance **example.com**. On the Internet, domain names are mapped to the IP addresses to which they should refer by the Domain Name System. This allows you to enter "www.example.com" into your browser and reach the correct place on the Internet even if the IP address of the website's server has changed.

Similarly, the CGN allows you to define a **Domain Suffix** to the LAN. When you enter the domain suffix into your browser, you can reach the CGN no matter what IP address it has on the LAN.

3.1.4 DEBUGGING (PING AND TRACEROUTE)

The CGN provides a couple of tools to allow you to perform network diagnostics on the LAN:

- ▶ Ping: this tool allows you to enter an IP address and see if a computer (or other network device) responds with that address on the network. The name comes from the pulse that submarine SONAR emits when scanning for underwater objects, since the process is rather similar. You can use this tool to see if an IP address is in use, or to discover if a device (whose IP address you know) is working properly.
- ▶ Traceroute: this tool allows you to see the route taken by data packets to get from the CGN to the destination you specify. You can use this tool to solve routing problems, or identify firewalls that may be blocking your access to a computer or service.

3.2 THE IP SCREEN

Use this screen to:

- ▶ View information about the CGN's connection to the WAN
- ▶ Enable or disable manual DNS assignment
- ▶ Define DNS servers for manual DNS assignment
- ▶ Configure the CGN's LAN IP address, subnet mask and domain suffix
- ▶ Configure the CGN's internal DHCP server
- ▶ Define how the CGN assigns IP addresses on the LAN
- ▶ See information about the network devices connected to the CGN on the LAN.

Click **WAN/LAN > IP**. The following screen displays.

Figure 11: [The WAN/LAN > IP Screen](#)

WAN Information

WAN Address 0.0.0.0
 Subnet Mask 0.0.0.0
 Gateway Address 0.0.0.0
 Assign DNS Manually Enabled
 DNS Server

Private LAN IP Setting

Private LAN IP Address
 Subnet Mask
 Domain Suffix

Private LAN DHCP Setting

Enable LAN DHCP Enabled
 Lease Time ▾
 DHCP Start IP
 DHCP End IP

Connected Computers

Host Name	IP Address	MAC Address	Type	Interface
unknown	192.168.0.10	██████████	Self-assigned	Ethernet

The following table describes the labels in this screen.

 Table 12: [The WAN/LAN > IP Screen](#)

WAN Information	
WAN Address	This field displays the CGN's IP address on the WAN (Wide Area Network) interface.
Subnet Mask	This field displays the CGN's WAN subnet mask.
Gateway Address	This field displays the address of the device on the WAN to which the CGN is connected.

Table 12: [The WAN/LAN > IP Screen \(continued\)](#)

Assign DNS Manually	<ul style="list-style-type: none"> ▶ Select the checkbox to enable manual DNS server assignment, and enter the DNS servers that you want to use in the DNS Server fields below. ▶ Deselect the checkbox to disable manual DNS server assignment. The CGN uses the DNS servers assigned automatically when it receives an IP address over the WAN. <p>It is strongly recommended that you do not enable manual DNS server assignment unless you have good reason to do so.</p>
DNS Server	<p>These fields display the Domain Name Servers that the CGN uses to resolve domain names into IP addresses.</p> <p>If you selected the Assign DNS Manually checkbox, enter the DNS servers that you want to use in these fields.</p>
Private LAN IP Setting	
IP Address	Use this field to define the IP address of the CGN on the LAN.
Subnet Mask	Use this field to define the LAN subnet. Use dotted decimal notation (for example, 255.255.255.0).
Domain Suffix	Use this field to define the domain that you can enter into a Web browser (instead of an IP address) to reach the CGN on the LAN. <p><i>It is suggested that you make a note of your device's Domain Suffix in case you ever need to access the CGN's GUI without knowledge of its IP address.</i></p>
Private LAN DHCP Setting	
Enable LAN DHCP	Select this if you want the CGN to provide IP addresses to network devices on the LAN automatically. <p>Deselect this if you already have a DHCP server on your LAN, or if you wish to assign IP addresses to your computers and other network devices manually.</p>
Lease Time	Use this field to define the time after which the CGN renews the IP addresses of all the network devices connected to the CGN on the LAN (when DHCP is enabled).
DHCP Start IP	Use this field to specify the IP address at which the CGN begins assigning IP addresses to devices on the LAN (when DHCP is enabled).

Table 12: [The WAN/LAN > IP Screen \(continued\)](#)

DHCP End IP	Use this field to specify the IP address at which the CGN stops assigning IP addresses to devices on the LAN (when DHCP is enabled). NOTE: Devices requesting IP addresses once the DHCP pool is exhausted are not assigned an IP address.
Connected Computers	
Host Name	This displays the name of each network device connected on the LAN.
IP Address	This displays the IP address of each network device connected on the LAN.
MAC Address	This displays the Media Access Control (MAC) address of each network device connected on the LAN.
Type	This displays whether the device's IP address was assigned by DHCP (DHCP-IP), or self-assigned .
Interface	This displays whether the device is connected on the LAN (Ethernet) or the WLAN (Wireless(x)), where x denotes the wireless mode; b , g or n .
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

3.3 THE SHARED MEDIA SCREEN

Use this screen to manage and share data stored on devices connected to the CGN's **USB** port. The CGN provides one USB 2.0 host port, allowing you to plug in a USB flash disk for mounting and sharing through the LAN interfaces via the Samba protocol (network neighborhood).

NOTE: [This screen is not available unless a logged-in MSO admin user previously enabled the **USB** option in the **Status > Capability** screen; see \[The Capability Screen on page 42\]\(#\) for more information.](#)

Click **WAN/LAN > Shared Media**. The following screen displays.

Figure 12: [The WAN/LAN > Shared Media Screen](#)


The following table describes the labels in this screen.

 Table 13: [The WAN/LAN > Shared Media Screen](#)

Group ID	Specify the name of the Network Neighborhood workgroup whose users may access the shared media on the USB device.
No.	This field displays the index number of the connected USB device. When no USB device is connected, no number displays in this column.
Name	This field displays the identifying name of the connected USB device. <ul style="list-style-type: none"> ▶ When no USB device is connected, no name displays in this column. ▶ When a USB device is connected, click its Name to view the files on the device. These files are shared with the relevant user group (defined in the Group ID field).
Apply	Click this to save your changes to the fields in this screen.
Refresh	Click this to reload the information in this screen. Do this if you connect or disconnect a device from the USB port and the information in this screen does not update automatically.
Help	Click this to see information about the fields in this screen.

3.4 THE DEBUG SCREEN

Use this screen to perform ping and traceroute tests on IP addresses or URLs.

Click **WAN/LAN > Debug**. The following screen displays.

Figure 13: [The WAN/LAN > Debug Screen](#)

Debug Tools, ping and tracerout, can aid troubleshooting for the network connectivity.

Debug Tools

IP/URL

Method

The following table describes the labels in this screen.

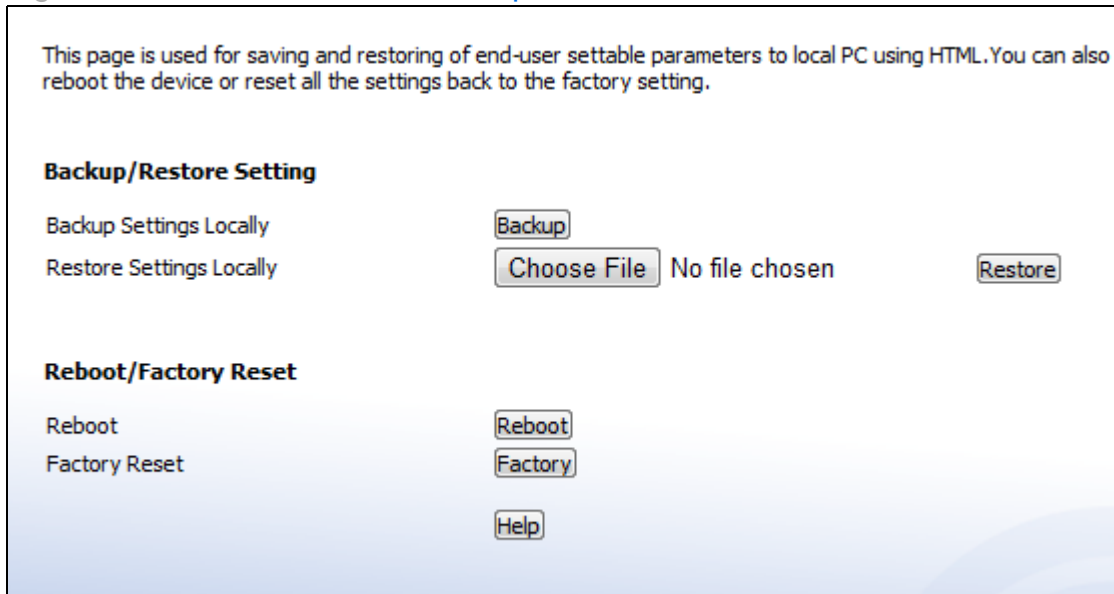
Table 14: [The WAN/LAN > Debug Screen](#)

IP/URL	Enter the IP address or URL that you want to test.
Method	Select the type of test that you want to run on the IP/URL that you specified.
Run	Click this to perform the test.
Help	Click this to see information about the fields in this screen.

3.5 THE BACKUP SCREEN

Use this screen to back up your CGN's settings to your computer, to load settings from a backup you created earlier, to reboot your CGN, or to return it to its factory default settings.

Click **WAN/LAN > Backup**. The following screen displays.

Figure 14: [The WAN/LAN > Backup Screen](#)


The following table describes the labels in this screen.

 Table 15: [The LAN > Backup Screen](#)

Backup/Restore Setting	
Backup Settings Locally	Click this to create a backup of all your CGN's settings on your computer.
Restore Settings Locally	Use these fields to return your CGN's settings to those specified in a backup that you created earlier. Click Choose File to select a backup, then click Restore to return your CGN's settings to those specified in the backup.
Reboot/Factory Reset	
Reboot	Click Reboot to restart your CGN.
Factory Reset	Click Factory to return your CGN to its factory default settings. NOTE: When you do this, all your user-configured settings are lost, and cannot be retrieved.
Help	Click this to see information about the fields in this screen.

4

FIREWALL

This chapter describes the screens that display when you click **Firewall** in the toolbar. It contains the following sections:

- ▶ [Firewall Overview](#) on page 54
- ▶ [The Firewall Options Screen](#) on page 56
- ▶ [The Filter Setting Screen](#) on page 57
- ▶ [The Forwarding Screen](#) on page 65
- ▶ [The Port Triggering Screen](#) on page 69
- ▶ [The DMZ Screen](#) on page 72

4.1 FIREWALL OVERVIEW

This section describes some of the concepts related to the **Firewall** screens.

4.1.1 FIREWALL

The term “firewall” comes from a construction technique designed to prevent the spread of fire from one room to another. Similarly, your CGN’s firewall prevents intrusion attempts and other undesirable activity originating from the WAN, keeping the computers on your LAN safe. You can also use filtering techniques to specify the computers and other devices you want to allow on the LAN, and prevent certain traffic from going from the LAN to the WAN.

4.1.2 INTRUSION DETECTION SYSTEM

An intrusion detection system monitors network activity, looking for policy violations, and malicious or suspicious activity. The CGN's intrusion detection system logs all such activity to the **Firewall > Local Logs** screen.

4.1.3 PING

The CGN allows you to use the ping utility on the LAN (in the **WAN/LAN > Debug** screen) and also on the WAN (in the **Firewall > Firewall Options** screen). For more information, see [Debugging \(Ping and Traceroute\)](#) on page 46.

4.1.4 MAC FILTERING

Every networking device has a unique Media Access Control (MAC) address that identifies it on the network. When you enable MAC address filtering on the CGN's firewall, you can set up a list of MAC addresses, and then specify whether you want to:

- ▶ Deny the devices on the list access to the CGN and the network (in which case all other devices can access the network)

or

- ▶ Allow the devices on the list to access the network (in which case no other devices can access the network)

4.1.5 IP FILTERING

IP filtering allows you to prevent computers on the LAN from sending certain types of data to the WAN. You can use this to prevent unwanted outgoing communications. Specify the IP address of the computer on the LAN from which you want to prevent communications, and specify the port range of the communications you want to prevent. The CGN discards outgoing data packets that match the criteria you specified.

4.1.6 PORT FORWARDING

Port forwarding allows a computer on your LAN to receive specific communications from the WAN. Typically, this is used to allow certain applications (such as gaming) through the firewall, for a specific computer on the LAN. Port forwarding is also commonly used for running a public HTTP server from a private network.

You can set up a port forwarding rule for each application for which you want to open ports in the firewall. When the CGN receives incoming traffic from the WAN with a destination port that matches a port forwarding rule, it forwards the traffic to the LAN IP address and port number specified in the port forwarding rule.

NOTE: [For information on the ports you need to open for a particular application, consult that application's documentation.](#)

4.1.7 PORT TRIGGERING

Port triggering is a means of automating port forwarding. The CGN scans outgoing traffic (from the LAN to the WAN) to see if any of the traffic's destination ports match those specified in the port triggering rules you configure. If any of the ports match, the CGN automatically opens the incoming ports specified in the rule, in anticipation of incoming traffic.

4.1.8 DMZ

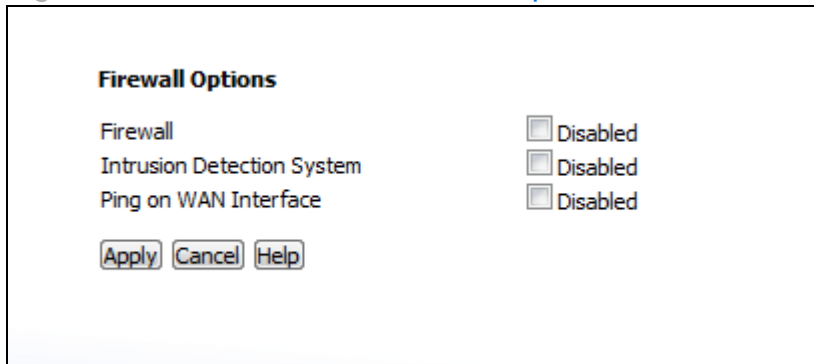
In networking, the De-Militarized Zone (DMZ) is a part of your LAN that has been isolated from the rest of the LAN, and opened up to the WAN. The term comes from the military designation for a piece of territory, usually located between two opposing forces, that is isolated from both and occupied by neither.

4.2 THE FIREWALL OPTIONS SCREEN

Use this screen to turn firewall features on or off. You can enable or disable the CGN's intrusion detection system, and allow or prevent responses to ICMP requests from the WAN.

Click **Firewall > Firewall Options**. The following screen displays.

Figure 15: [The Firewall > Firewall Options Screen](#)



The following table describes the labels in this screen.

Table 16: [The Firewall > Firewall Options Screen](#)

Firewall	<ul style="list-style-type: none"> ▶ Select this to turn the firewall on. ▶ Deselect this to turn the firewall off. <p>NOTE: It is strongly recommended that you enable the CGN's firewall unless LAN protection is provided by another device or software.</p>
Intrusion Detection System	<ul style="list-style-type: none"> ▶ Select this to turn the intrusion detection system off. ▶ Deselect this to turn the intrusion detection system on.
Ping on WAN Interface	<ul style="list-style-type: none"> ▶ Select this to prevent responses to ICMP requests originating from the WAN. ▶ Select this to allow responses to ICMP requests originating from the WAN.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.3 THE FILTER SETTING SCREEN

Use this screen to configure Media Access Control (MAC) address filtering on the LAN, and to configure IP filtering.

NOTE: To configure MAC address filtering on the wireless network, see The Access Control Screen on page 93.

You can set the CGN to allow only certain devices to access the CGN and the network, or to deny certain devices access.

NOTE: To see a list of all the computers connected to the CGN on the LAN, click the **Connected Computers** button in the **Firewall > IP Filtering, Forwarding, Port Triggering** or **Firewall Options** screens.

You can turn IP filtering on or off, and configure new and existing IP filtering rules.

Click **Firewall > Filter Setting**. The following screen displays.

Figure 16: [The Firewall > Filter Setting Screen](#)

The MAC address filter allows you to specify which devices to be blocked/allowed from accessing the Internet and your network.

Mac Filter Options Allow-All ▼

Allow Table (up to 16 items)

Select	#	Device Name	MAC Address
<input type="button" value="Delete"/>			

Deny Table (up to 16 items)

Select	#	Device Name	MAC Address
<input type="button" value="Delete"/>			

Auto-Learned Lan Devices

Select	Device Name	MAC Address	Type
<input type="radio"/>	unknown		<input type="radio"/> Allow <input type="radio"/> Deny

Manually-Added Lan Devices

Device Name	MAC Address	Type
<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	<input type="radio"/> Allow <input type="radio"/> Deny

IP Filtering Options

IP filtering is used to prevent specific computers on the LAN from transmitting outbound traffic to specific ports, or port ranges, on the WAN. Outbound traffic is blocked according to the remote destination ports and the source IP address.

All IP Filtering rules Disabled

Select	#	Application Name	Port Range	Protocol	IP Address Range	Enable
<input type="button" value="add new"/> <input type="button" value="edit"/> <input type="button" value="delete"/>						

The following table describes the labels in this screen.

Table 17: [The Firewall > Filter Setting Screen](#)

MAC Filter Options	
MAC Filter Options	<p>Use this field to control whether the CGN performs MAC filtering.</p> <ul style="list-style-type: none"> ▶ Select Allow-All to turn MAC filtering off. All devices may access the CGN and the network. ▶ Select Allow to permit only devices with the MAC addresses you set up in the Allow Table to access the CGN and the network. All other devices are denied access. ▶ Select Deny to permit all devices except those with the MAC addresses you set up in the Deny Table to access the CGN and the network. The specified devices are denied access.
Allow Table (up to 16 Items)	
#	This displays the index number assigned to the permitted device.
Device Name	This displays the name you gave to the permitted device.
MAC Address	This displays the MAC address of the permitted device.
Delete	<p>Select a permitted device's radio button (<input checked="" type="radio"/>) and click this to remove the device from the list. The device may no longer access the CGN and the network.</p> <p>NOTE: Make sure you do not delete your management computer from the list; if you do so, you will need to log back in from another computer, or reset the CGN.</p>
Deny Table (up to 16 Items)	
#	This displays the index number assigned to the denied device.
Device Name	This displays the name you gave to the denied device.
MAC Address	This displays the MAC address of the denied device.
Delete	<p>Select a denied device's radio button (<input type="radio"/>) and click this to remove the device from the list. The device may now access the CGN and the network.</p>
Auto-Learned LAN Devices	

Table 17: [The Firewall > Filter Setting Screen \(continued\)](#)

Device Name	This displays the name of each network device that has connected to the CGN on the LAN. To change the name assigned to a device, edit it in the relevant field.
MAC Address	This displays the MAC address of each network device that has connected to the CGN on the LAN.
Type	Use this field to specify the list to which you want to add the device. <ul style="list-style-type: none"> ▶ Select Allow to add the device to the Allow Table. ▶ Select Deny to add the device to the Deny Table.
Manually-Added LAN Devices	
Device Name	Enter the name to associate with a network device that you want to permit or deny access to the CGN and the network. NOTE: This name is arbitrary, and does not affect functionality in any way.
MAC Address	Specify the MAC address of the network device that you want to permit or deny access to the CGN and the network.
Type	Use this field to specify the list to which you want to add the device. <ul style="list-style-type: none"> ▶ Select Allow to add the device to the Allow Table. ▶ Select Deny to add the device to the Deny Table.
Add	Click this to add the device to the list you specified.
Cancel	Click this to clear the Manually-Added LAN Devices fields.
Apply	Click this to save your changes to the fields in the Mac Filter tables.
Cancel	Click this to return the fields in the Mac Filter tables to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.
IP Filtering Options	

Table 17: [The Firewall > Filter Setting Screen \(continued\)](#)

All IP Filtering Rules	<p>Use this to turn IP filtering on or off.</p> <ul style="list-style-type: none"> ▶ Deselect the checkbox to enable IP filtering. ▶ Select the checkbox to disable IP filtering (default). <p>NOTE: You can add, edit or delete IP filtering rules only when this checkbox is deselected.</p>
Select	Select an IP filtering rule's radio button (<input type="radio"/>) before clicking Edit or Delete .
#	This displays the arbitrary identification number assigned to the IP filtering rule.
Application Name	This displays the arbitrary name you assigned to the rule when you create it.
Port Range	This displays the start and end values of the ports to which communications from the specified IP addresses is not permitted.
Protocol	<p>This displays the type of communications that are not permitted:</p> <ul style="list-style-type: none"> ▶ TCP displays if communications via the Transmission Control Protocol are not permitted. ▶ UDP displays if communications via the User Datagram Protocol are not permitted. ▶ TCP/UDP displays if communications via the Transmission Control Protocol and the User Datagram Protocol are not permitted.
IP Address Range	This displays the start and end IP address from which communications to the specified ports are not permitted.
Enable	<p>Use this field to turn each IP filtering rule on or off.</p> <ul style="list-style-type: none"> ▶ Select this checkbox to enable the IP filtering rule. ▶ Deselect this checkbox to disable the IP filtering rule.
Add New	Click this to define a new IP filtering rule. See Adding or Editing an IP Filtering Rule on page 63 for information on the screen that displays.
Edit	Select an IP filtering rule's radio button (<input type="radio"/>) and click this to make changes to the rule. See Adding or Editing an IP Filtering Rule on page 63 for information on the screen that displays.

Table 17: [The Firewall > Filter Setting Screen \(continued\)](#)

Delete	Select an IP filtering rule's radio button (☉) and click this to remove the rule. The deleted rule's information cannot be retrieved.
Apply	Click this to save your changes to the fields in the IP Filtering Options section.
Cancel	Click this to return the fields in the IP Filtering Options section to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.3.1 ADDING OR EDITING AN IP FILTERING RULE

- ▶ To add a new IP filtering rule, click **Add** in the **Firewall > Filter Setting** screen's **IP Filtering Options** section.
- ▶ To edit an existing IP filtering rule, select the rule's radio button (☉) in the **Firewall > Filter Setting** screen's **IP Filtering Options** section and click the **Edit** button.

NOTE: Ensure that the **Disabled** checkbox is deselected in order to add or edit IP filtering rules.

The following screen displays.

 Figure 17: [The Firewall > Filter Settings > Add/Edit Screen](#)

You can add or edit your IP Filtering rules here.

IP Filtering ADD/EDIT

Application Name

Port Range ~

Protocol

IP Address Range ~

The following table describes the labels in this screen.

Table 18: [The Firewall > Filter Settings > Add/Edit Screen](#)

Application Name	<p>Enter a name for the application that you want to block.</p> <p>NOTE: This name is arbitrary, and does not affect functionality in any way.</p>
Port Range	<p>Use these fields to specify the target port range to which communication should be blocked.</p> <p>Enter the start port number in the first field, and the end port number in the second field.</p> <p>To specify only a single port, enter its number in both fields.</p>
Protocol	<p>Use this field to specify whether the CGN should block communication via:</p> <ul style="list-style-type: none"> ▶ Transmission Control Protocol (TCP) ▶ User Datagram Protocol (UDP) ▶ Both TCP and UDP. <p>NOTE: If in doubt, leave this field at its default (Both).</p>
IP Address Range	<p>Use these fields to specify the range of local computers' IP addresses from which communications should be blocked.</p> <p>Enter the start IP address in the first field, and the end IP address in the second.</p> <p>To specify only a single IP address, enter it in both fields.</p>
Connected Computers	<p>Click this to see a list of the computers currently connected to the CGN on the LAN.</p>
Back	<p>Click this to return to the Firewall > Filter Settings screen without saving your changes to the IP filtering rule.</p>
Apply	<p>Click this to save your changes to the fields in this screen.</p>
Cancel	<p>Click this to return the fields in this screen to their last-saved values without saving your changes.</p>
Help	<p>Click this to see information about the fields in this screen.</p>

4.4 THE FORWARDING SCREEN

Use this screen to configure port forwarding between computers on the WAN and computers on the LAN. You can turn port forwarding on or off and configure new and existing port forwarding rules.

Click **Firewall > Forwarding**. The following screen displays.

Figure 18: [The Firewall > Forwarding Screen](#)

Forwarding is used to redirect the inbound traffic to the appropriate server(s) or specifically identified application(s) in the internal network. In the setting, the public ports are the target ports seen by the Internet world and the private ports are the target ports in the inside hosts to be translated by the device. The IP addresses are the hosts which host these private ports

Port Forwarding Options

All Port Forwarding rules Disabled

Select	#	Application Name	Port Range		Protocol	IP Address	Enable
			Public	Private			
<input type="button" value="add new"/> <input type="button" value="edit"/> <input type="button" value="delete"/>							
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>							

The following table describes the labels in this screen.

Table 19: [The Firewall > Forwarding Screen](#)

All Port Forwarding Rules	Use this field to turn port forwarding on or off. <ul style="list-style-type: none"> ▶ Select the checkbox to enable port forwarding. ▶ Deselect the checkbox to disable port forwarding.
Select	Select a port forwarding rule's radio button (<input type="radio"/>) before clicking Edit or Delete .
#	This displays the arbitrary identification number assigned to the port forwarding rule.
Application Name	This displays the arbitrary name you assigned to the rule when you created it.

Table 19: [The Firewall > Forwarding Screen \(continued\)](#)

Port Range	<p>These fields display the ports to which the rule applies:</p> <ul style="list-style-type: none"> ▶ The Public field displays the incoming port range. These are the ports on which the CGN received traffic from the originating host on the WAN. ▶ The Private field displays the port range to which the CGN forwards traffic to the device on the LAN.
Protocol	<p>This field displays the protocol or protocols to which this rule applies:</p> <ul style="list-style-type: none"> ▶ Transmission Control Protocol (TCP) ▶ User Datagram Protocol (UDP) ▶ Transmission Control Protocol and User Datagram Protocol (TCP/UDP) ▶ Generic Routing Encapsulation (GRE) ▶ Encapsulating Security Protocol (ESP)
IP Address	<p>This displays the IP address of the computer on the LAN to which traffic conforming to the Public Port Range and Protocol conditions is forwarded.</p>
Enable	<p>Use this field to turn each port forwarding rule on or off.</p> <ul style="list-style-type: none"> ▶ Select this checkbox to enable the port forwarding rule. ▶ Deselect this checkbox to disable the port forwarding rule.
Add New	<p>Click this to define a new port forwarding rule. See Adding or Editing a Port Forwarding Rule on page 67 for information on the screen that displays.</p>
Edit	<p>Select a port forwarding rule's radio button (<input type="radio"/>) and click this to make changes to the rule. See Adding or Editing a Port Forwarding Rule on page 67 for information on the screen that displays.</p>
Delete	<p>Select a port forwarding rule's radio button (<input type="radio"/>) and click this to remove the rule. The deleted rule's information cannot be retrieved.</p>
Apply	<p>Click this to save your changes to the fields in this screen.</p>

Table 19: [The Firewall > Forwarding Screen \(continued\)](#)

Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.4.1 ADDING OR EDITING A PORT FORWARDING RULE

- ▶ To add a new port forwarding rule, click **Add** in the **Firewall > Forwarding** screen.
- ▶ To edit an existing port forwarding rule, select the rule's radio button (☉) in the **Firewall > Forwarding** screen and click the **Edit** button.

NOTE: Ensure that the **Disabled** checkbox is disabled in order to add or edit port forwarding rules.

The following screen displays.

 Figure 19: [The Firewall > Forwarding > Add/Edit Screen](#)

You can add or edit your port forwarding rules here.

Port Forwarding rules

Common Application

Application Name

Protocol

Public Port Range ~

Private Port Range ~

IP Address

The following table describes the labels in this screen.

Table 20: [The Firewall > Forwarding > Add/Edit Screen](#)

Application Name	<p>Enter a name for the application for which you want to create the rule.</p> <p>NOTE: This name is arbitrary, and does not affect functionality in any way.</p>
Public Port Range	<p>Use these fields to specify the incoming port range. These are the ports on which the CGN received traffic from the originating host on the WAN.</p> <p>Enter the start port number in the first field, and the end port number in the second field.</p> <p>To specify only a single port, enter its number in both fields.</p>
Private Port Range	<p>Use these fields to specify the ports to which the received traffic should be forwarded.</p> <p>Enter the start port number in the first field. The number of ports must match that specified in the Public Port Range, so the CGN completes the second field automatically.</p>
Protocol	<p>Use this field to specify whether the CGN should forward traffic via:</p> <ul style="list-style-type: none"> ▶ Transmission Control Protocol (TCP) ▶ User Datagram Protocol (UDP) ▶ Transmission Control Protocol and User Datagram Protocol (TCP/UDP) ▶ Generic Routing Encapsulation (GRE) ▶ Encapsulating Security Protocol (ESP) <p>NOTE: If in doubt, leave this field at its default (TCP/UDP).</p>
IP Address	<p>Use this field to enter the IP address of the computer on the LAN to which you want to forward the traffic.</p>
Connected Computers	<p>Click this to see a list of the computers currently connected to the CGN on the LAN.</p>
Back	<p>Click this to return to the Firewall > Forwarding screen without saving your changes to the port forwarding rule.</p>

Table 20: [The Firewall > Forwarding > Add/Edit Screen](#)

Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.5 THE PORT TRIGGERING SCREEN

Use this screen to configure port triggering. You can turn port triggering on or off and configure new and existing port triggering rules.

Click **Firewall > Port Triggering**. The following screen displays.

 Figure 20: [The Firewall > Port Triggering Screen](#)

Port Triggering is used to allow computers on your local area network access specific applications on the Internet.

Port Triggering Options

All Port Triggering rules Disabled

Select	#	Application Name	Port Range		Protocol	Timeout(ms)	Enable
			Trigger	Target			
<input type="button" value="add new"/> <input type="button" value="edit"/> <input type="button" value="delete"/>							
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>							

The following table describes the labels in this screen.

 Table 21: [The Firewall > Port Triggering Screen](#)

All Port Triggering Rules	Use this field to turn port triggering on or off. <ul style="list-style-type: none"> ▶ Select the checkbox to enable port triggering. ▶ Deselect the checkbox to disable port triggering.
Select	Select a port triggering rule's radio button (<input type="radio"/>) before clicking Edit or Delete .
#	This displays the arbitrary identification number assigned to the port triggering rule.

Table 21: The Firewall > Port Triggering Screen

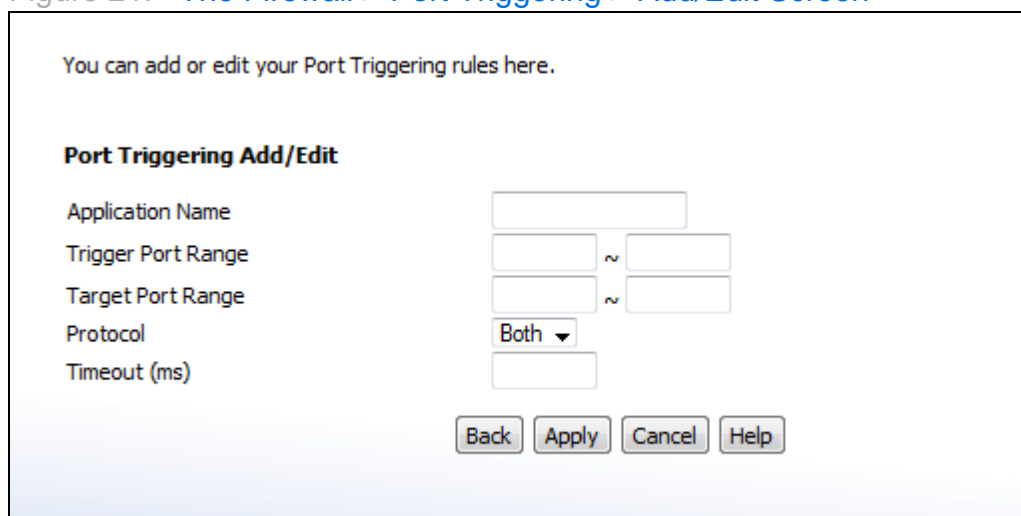
Application Name	This displays the arbitrary name you assigned to the rule when you created it.
Port Range	These fields display the ports to which the rule applies: <ul style="list-style-type: none"> ▶ The Trigger field displays the range of outgoing ports. When the CGN detects activity (outgoing traffic) on these ports from computers on the LAN, it automatically opens the Target ports. ▶ The Target field displays the range of triggered ports. These ports are opened automatically when the CGN detects activity on the Trigger ports from computers on the LAN.
Protocol	This displays the protocol of the port triggering rule.
Timeout (ms)	This displays the time (in milliseconds) after the CGN opens the Target ports that it should close them.
Enable	Use this field to turn each port triggering rule on or off. <ul style="list-style-type: none"> ▶ Select this checkbox to enable the port triggering rule. ▶ Deselect this checkbox to disable the port triggering rule.
Add New	Click this to define a new port triggering rule. See Adding or Editing a Port Triggering Rule on page 71 for information on the screen that displays.
Edit	Select a port triggering rule's radio button (<input type="radio"/>) and click this to make changes to the rule. See Adding or Editing a Port Triggering Rule on page 71 for information on the screen that displays.
Delete	Select a port triggering rule's radio button (<input type="radio"/>) and click this to remove the rule. The deleted rule's information cannot be retrieved.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.5.1 ADDING OR EDITING A PORT TRIGGERING RULE

- ▶ To add a new port triggering rule, click **Add** in the **Firewall > Port Triggering** screen.
- ▶ To edit an existing port triggering rule, select the rule's radio button (☉) in the **Firewall > Port Triggering** screen and click the **Edit** button.

The following screen displays.

Figure 21: [The Firewall > Port Triggering > Add/Edit Screen](#)



You can add or edit your Port Triggering rules here.

Port Triggering Add/Edit

Application Name

Trigger Port Range ~

Target Port Range ~

Protocol Both ▾

Timeout (ms)

The following table describes the labels in this screen.

Table 22: [The Firewall > Port Triggering > Add/Edit Screen](#)

Application Name	<p>Enter a name for the application for which you want to create the rule.</p> <p>NOTE: This name is arbitrary, and does not affect functionality in any way.</p>
Trigger Port Range	<p>Use these fields to specify the trigger ports. When the CGN detects activity on any of these ports originating from a computer on the LAN, it automatically opens the Target ports in expectation of incoming traffic.</p> <p>Enter the start port number in the first field, and the end port number in the second field.</p> <p>To specify only a single port, enter its number in both fields.</p>

Table 22: The Firewall > Port Triggering > Add/Edit Screen

Target Port Range	<p>Use these fields to specify the target ports. The CGN opens these ports in expectation of incoming traffic whenever it detects activity on any of the Trigger ports. The incoming traffic is forwarded to these ports on the computer connected to the LAN.</p> <p>Enter the start port number in the first field, and the end port number in the second field.</p> <p>To specify only a single port, enter its number in both fields.</p>
Protocol	<p>Use this field to specify whether the CGN should activate this trigger when it detects activity via:</p> <ul style="list-style-type: none"> ▶ Transmission Control Protocol (TCP) ▶ User Datagram Protocol (UDP) ▶ Transmission Control Protocol and User Datagram Protocol (Both) <p>NOTE: <i>If in doubt, leave this field at its default (Both).</i></p>
Timeout (ms)	<p>Enter the time (in milliseconds) after the CGN opens the Target ports that it should close them.</p>
Connected Computers	<p>Click this to see a list of the computers currently connected to the CGN on the LAN.</p>
Back	<p>Click this to return to the Firewall > Forwarding screen without saving your changes to the port forwarding rule.</p>
Apply	<p>Click this to save your changes to the fields in this screen.</p>
Cancel	<p>Click this to return the fields in this screen to their last-saved values without saving your changes.</p>
Help	<p>Click this to see information about the fields in this screen.</p>

4.6 THE DMZ SCREEN

Use this screen to configure your network's Demilitarized Zone (DMZ).

NOTE: *Only one device can be on the DMZ at a time.*

Click **Firewall > DMZ**. The following screen displays.

Figure 22: [The Firewall > DMZ Screen](#)

DMZ allows the selected computer to bypass the firewall features of the gateway and permits unrestricted access from the Internet to that computer.

Enable DMZ Host

[Connected Computers](#)

Please enter the IP address of the computer that you wish to add to the DMZ below.

[Apply](#) [Cancel](#) [Help](#)

The following table describes the labels in this screen.

Table 23: [The Firewall > DMZ Screen](#)

Enable DMZ Host	Use this field to turn the DMZ on or off. <ul style="list-style-type: none"> ▶ Select the checkbox to enable the DMZ. ▶ Deselect the checkbox to disable the DMZ. Computers that were previously in the DMZ are now on the LAN.
Connected Computers	Click this to see a list of the computers currently connected to the CGN on the LAN. To add a connected computer to the DMZ, click its Add button and click Apply in the screen that displays.
[...] IP Address [...]	Enter the IP address of the computer that you want to add to the DMZ.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

5

PARENTAL CONTROL

This chapter describes the screens that display when you click **Parent Control** in the toolbar. It contains the following sections:

- ▶ [Parental Control Overview](#) on page 74
- ▶ [The Website Blocking Screen](#) on page 75
- ▶ [The Scheduling Screen](#) on page 77
- ▶ [The Email / Syslog Alert Screen](#) on page 79

5.1 PARENTAL CONTROL OVERVIEW

This section describes some of the concepts related to the **Parental Control** screens.

5.1.1 WEBSITE BLOCKING

The **Parental Control** screens allow you to block access from computers on the LAN to certain websites, or websites whose URLs (website addresses) contain the keywords you specify.

You can also specify “trusted” computers, which should be exempted from website blocking, and you can schedule website blocking so that it is only in effect at certain times (evenings and weekends, for example).

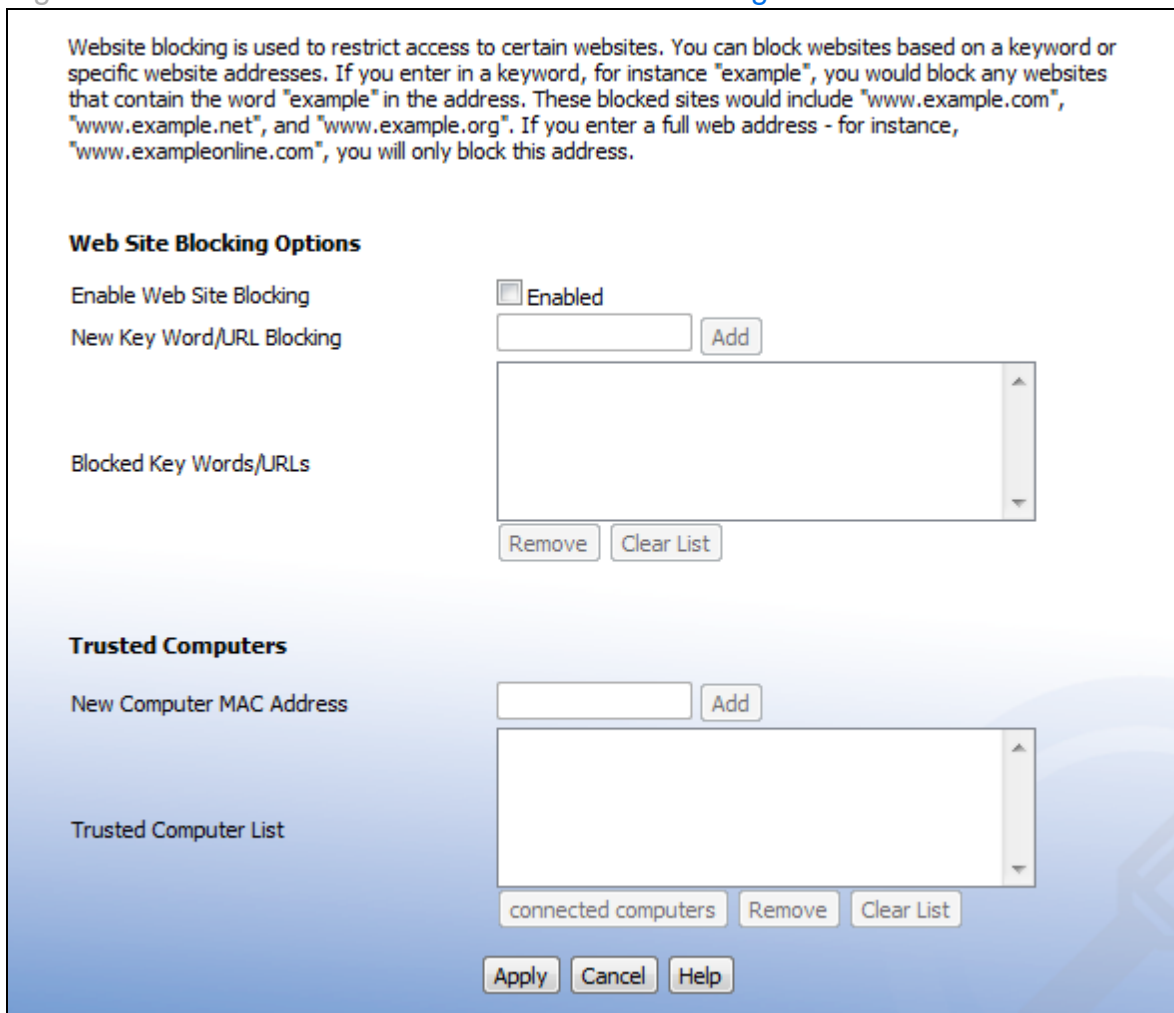
5.2 THE WEBSITE BLOCKING SCREEN

Use this screen to block access from the LAN to certain websites. You can also specify trusted computers, which are not subject to the blocking filter.

NOTE: To apply the blocking filter only at certain times, use the **Parental Control > Scheduling** screen.

Click **Parental Control > Web Site Blocking**. The following screen displays.

Figure 23: The Parental Control > Web Site Blocking Screen



Website blocking is used to restrict access to certain websites. You can block websites based on a keyword or specific website addresses. If you enter in a keyword, for instance "example", you would block any websites that contain the word "example" in the address. These blocked sites would include "www.example.com", "www.example.net", and "www.example.org". If you enter a full web address - for instance, "www.exampleonline.com", you will only block this address.

Web Site Blocking Options

Enable Web Site Blocking Enabled

New Key Word/URL Blocking Add

Blocked Key Words/URLs

Remove Clear List

Trusted Computers

New Computer MAC Address Add

Trusted Computer List

connected computers Remove Clear List

Apply Cancel Help

The following table describes the labels in this screen.

Table 24: [The Parental Control > Web Site Blocking Screen](#)

Web Site Blocking Options	
Enable Web Site Blocking	<p>Use this field to turn web site blocking on or off.</p> <ul style="list-style-type: none"> ▶ Select the checkbox to enable web site blocking. ▶ Deselect the checkbox to disable web site blocking.
New Key Word/URL Blocking	<p>Use these fields to configure the websites to which users on the LAN are denied access:</p> <ul style="list-style-type: none"> ▶ Enter a URL (for example, "www.example.com") to block access to that website only. ▶ Enter a keyword (for example, "example") to block access to all websites that contain the keyword in their URL (for example, "www.example.com", "www.example.org", "www.someotherwebsite.com/example" and so forth). <p>Click Add to add the URL or keyword to the Blocked Key Words/URLs list.</p>
Blocked Key Words/URLs	<p>This displays the list of websites and keywords to which users on the LAN are denied access.</p> <ul style="list-style-type: none"> ▶ Select a URL or keyword and click Remove to delete it from the list. ▶ Click Clear List to delete all the URLs and keywords from the list.
Trusted Computers	
New Computer MAC Address	<p>Enter a computer's Media Access Control (MAC) address and click Add to include it in the trusted computer list.</p>
Trusted Computer List	<p>This displays a list of the computers which are exempt from the website blocking filter, identified by their MAC addresses.</p>
Connected Computers	<p>Click this to see a list of the computers that are currently connected to the CGN. To add a computer to the New Computer MAC Address field, select its Add checkbox and click Apply in the screen that displays.</p>
Remove	<p>Select a computer's MAC address from the Connected Computers list and click this to delete it from the list.</p>

Table 24: [The Parental Control > Web Site Blocking Screen \(continued\)](#)

Clear List	Click this to delete all the computers' MAC addresses from the list.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

5.3 THE SCHEDULING SCREEN

Use this screen to control when the website blocking filter should be in effect.

NOTE: To configure the website blocking filter, use the [Parent Control > Web Site Blocking](#) screen.

Click **Parent Control > Scheduling**. The following screen displays.

Figure 24: [The Parental Control > Scheduling Screen](#)

Web Site Blocking Schedule allows you to apply your Web Site Blocking rules at different times of the day and week. Please select the hours of the day that you **Allow** your children to surf the Internet.

Days of the week

Please select the days that you wish to apply Web Site Blocking settings to

Blocking Everyday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

Time of the day

Please select the hours of the day that you wish to apply Web Site Blocking settings to

All Day Enabled

Hour Minute

Start 12 0 AM ▼

End 12 0 AM ▼

Apply Cancel Help

The following table describes the labels in this screen.

 Table 25: [The Parental Control > Scheduling Screen](#)

Days of the Week	Select the days of the week on which you want the website blocking filter to be in effect.
Time of Day	Use these fields to control the time that the website blocking filter should be in effect: <ul style="list-style-type: none"> ▶ Select All Day to apply the website blocking filter at all times. ▶ To apply the website blocking filter only at certain times of day, deselect All Day. Use the Start fields to define the time that the filter should come into effect, and use the End fields to define the time that the filter should cease being in effect.
Apply	Click this to save your changes to the fields in this screen.

Table 25: [The Parental Control > Scheduling Screen \(continued\)](#)

Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

5.4 THE EMAIL / SYSLOG ALERT SCREEN

Use this screen to forward information to a target email address or system log each time the firewall alert is triggered, and to define the time at which emails should be sent and/or log entries created.

The firewall must be enabled for alerts to be triggered.

Click **Parent Control > Email/Syslog Alert**. The following screen displays.

Figure 25: [The Parental Control > Email / Syslog Alert Screen](#)

Email/Syslog Alert

When the firewall feature is enabled, The user can be notified about the blocked traffic by email and/or syslog. The CGN2-BIZ firewall can notify the user about the intrusion and/or the attempts to access the blocked URL, also the notification could be sent out immediately or by the predefined time schedule.

Mail Server Configuration

SMTP Server Address

Sender's E-mail Address

Mail Server Authentication

User Name

Password

Recipient list (up to 4 items)

	Name	Email Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>		

Syslog Server Configuration

Syslog Server Address

Alert Options

When intrusion is detected

Send Email **Send Syslog**

The following table describes the labels in this screen.

Table 26: [The Parental Control > Email / Syslog Alert Screen](#)

Mail Server Configuration	Use this section to define the location of the transmitting email server, and the email address from which admin emails appear to originate.
SMTP Server Address	Enter the address of the email server from which admin emails should be sent.
Sender's Email Address	Enter the email address from which admin emails should appear to originate.
Mail Server Authentication	Use this section to enter the user credentials for the defined email server.
User Name	Enter the user name for your account on the defined email server.
Password	Enter the password associated with the above user name.

Table 26: The Parental Control > Email / Syslog Alert Screen (continued)

<p>Recipient List (up to 4 items)</p>	<p>Use this section to define up to four target email address to which admin emails will be sent.</p> <ul style="list-style-type: none"> ▶ To enter a new target email address, click Add. Enter the target email address's Name and Recipient's Address in the fields that display, then click Apply to save your changes. Alternatively, click Cancel to return to the previous screen without saving your changes. <p>Figure 26: Add Target Email Address</p> <div data-bbox="561 763 1364 1106" style="border: 1px solid black; padding: 5px;"> <p>Recipient Adding</p> <p>Users could input and edit the email alert recipient list here.</p> <p>Name <input type="text"/></p> <p>Recipient's Email Address <input type="text"/></p> <p style="text-align: right;"> <input type="button" value="Back"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/> </p> </div> <ul style="list-style-type: none"> ▶ To make changes to an existing target email address, select its radio button and click Edit. The screen that displays is the same as the Add Target Email Address screen. ▶ To remove an email address, select its radio button and click Delete. The email address is removed from the list.
<p>Syslog Server Configuration</p>	<p>Use this section to define the server on which the system log is stored.</p>
<p>Syslog Server Address</p>	<p>Enter the address of the server on which the system log is stored.</p>
<p>Alert Options</p>	<p>Use this section to define the actions to be taken when an intrusion event is detected.</p>
<p>When Intrusion is Detected</p>	<ul style="list-style-type: none"> ▶ Select Send Email to send an email to the list when an intrusion event is detected. ▶ Select Send Syslog to send an entry to the system log when an intrusion event is detected.
<p>Apply</p>	<p>Click this to save your changes to the fields in this screen.</p>

Table 26: [The Parental Control > Email / Syslog Alert Screen \(continued\)](#)

Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

6

WIRELESS

This chapter describes the screens that display when you click **Wireless** in the toolbar. It contains the following sections:

- ▶ [Wireless Overview](#) on page 83
- ▶ [The Setup Screen](#) on page 86
- ▶ [The Access Control Screen](#) on page 93
- ▶ [The Advanced Screen](#) on page 95

6.1 WIRELESS OVERVIEW

This section describes some of the concepts related to the **Wireless** screens.

6.1.1 WIRELESS NETWORKING BASICS

Your CGN's wireless network is part of the Local Area Network (LAN), known as the Wireless LAN (WLAN). The WLAN is a network of radio links between the CGN and the other computers and devices that connect to it.

6.1.2 ARCHITECTURE

The wireless network consists of two types of device: access points (APs) and clients.

- ▶ The access point controls the network, providing a wireless connection to each client.

- ▶ The wireless clients connect to the access point in order to receive a wireless connection to the WAN and the wired LAN.

The CGN is the access point, and the computers you connect to the CGN are the wireless clients.

6.1.3 WIRELESS STANDARDS

The way in which wireless devices communicate with one another is standardized by the Institute of Electrical and Electronics Engineers (IEEE). The IEEE standards pertaining to wireless LANs are identified by their 802.11 designation. There are a variety of WLAN standards, but the CGN supports the following (in order of adoption - old to new - and data transfer speeds - low to high):

- ▶ IEEE 802.11b
- ▶ IEEE 802.11g
- ▶ IEEE 802.11n

6.1.4 SERVICE SETS AND SSIDS

Each wireless network, including all the devices that comprise it, is known as a Service Set.

NOTE: Depending on its capabilities and configuration, a single wireless access point may control multiple Service Sets; this is often done to provide different service or security levels to different clients.

Each Service Set is identified by a Service Set Identifier (SSID). This is the name of the network. Wireless clients must know the SSID in order to be able to connect to the AP. You can configure the CGN to broadcast the SSID (in which case, any client who scans the airwaves can discover the SSID), or to "hide" the SSID (in which case it is not broadcast, and only users who already know the SSID can connect).

6.1.5 WIRELESS SECURITY

Radio is inherently an insecure medium, since it can be intercepted by anybody in the coverage area with a radio receiver. Therefore, a variety of techniques exist to control authentication (identifying who should be allowed to join the network) and encryption (signal scrambling so that only authenticated users can decode the transmitted data). The sophistication of each security method varies, as does its effectiveness. The CGN supports the following wireless security protocols (in order of effectiveness):

- ▶ **WEP** (the Wired Equivalency Protocol): this protocol uses a series of “keys” or data strings to authenticate the wireless client with the AP, and to encrypt data sent over the wireless link. WEP is a deprecated protocol, and should only be used when it is the only security standard supported by the wireless clients. WEP provides only a nominal level of security, since widely-available software exists that can break it in a matter of minutes.
- ▶ **WPA-PSK** (WiFi Protected Access - Pre-Shared Key): WPA was created to solve the inadequacies of WEP. There are two types of WPA: the “enterprise” version (known simply as WPA) requires the use of a central authentication database server, whereas the “personal” version (supported by the CGN) allows users to authenticate using a “pre-shared key” or password instead. While WPA provides good security, it is still vulnerable to “brute force” password-guessing attempts (in which an attacker simply barrages the AP with join requests using different passwords), so for optimal security it is advised that you use a random password of thirteen characters or more, containing no “dictionary” words.
- ▶ **WPA2-PSK**: WPA2 is an improvement on WPA. The primary difference is that WPA uses the Temporal Key Integrity Protocol (TKIP) encryption standard (which has been shown to have certain possible weaknesses), whereas WPA2 uses the stronger Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP), which has received the US government’s seal of approval for communications up to the Top Secret security level. Since WPA2-PSK uses the same pre-shared key mechanism as WPA-PSK, the same caveat against using insecure or simple passwords applies.

6.1.5.1 WPS

WiFi-Protected Setup (WPS) is a standardized method of allowing wireless devices to quickly and easily join wireless networks, while maintaining a good level of security. The CGN provides two methods of WPS authentication:

- ▶ **Push-Button Configuration (PBC):** when the user presses the **PBC** button on the AP (either a physical button, or a virtual button in the GUI), any user of a wireless client that supports WPS can press the corresponding **PBC** button on the client within two minutes to join the network.
- ▶ **Personal Identification Number (PIN) Configuration:** all WPS-capable devices possess a PIN (usually to be found printed on a sticker on the device's housing). When you configure another device to use the same PIN, the two devices authenticate with one another.

Once authenticated, devices that have joined a network via WPS use the WPA2 security standard.

6.1.6 WMM

WiFi MultiMedia (WMM) is a Quality of Service (QoS) enhancement that allows prioritization of certain types of data over the wireless network. WMM provides four data type classifications (in priority order; highest to lowest):

- ▶ Voice
- ▶ Video
- ▶ Best effort
- ▶ Background

If you wish to improve the performance of voice and video (at the expense of other, less time-sensitive applications such as Internet browsing and FTP transfers), you can enable WMM. You can also edit the WMM QoS parameters, but are disadvised to do so unless you have an extremely good reason to make the changes.

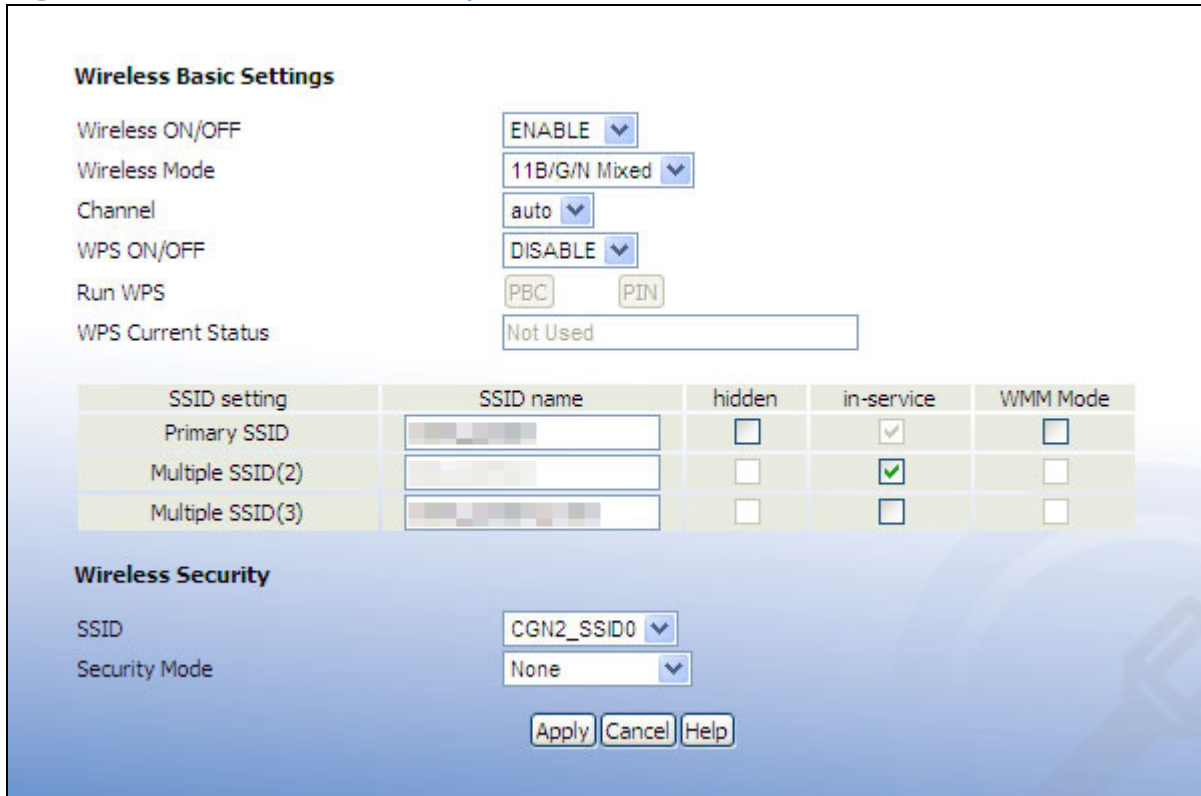
6.2 THE SETUP SCREEN

Use this screen to configure your CGN's basic wireless settings. You can turn the wireless module on or off, select the wireless mode and channel, run WPS and configure the wireless network's SSID. You can also configure authentication and encryption on your wireless network.

NOTE: It is strongly recommended that you set up security on your network; otherwise, anyone in the radio coverage area can access your network.

Click **Wireless > Setup**. The following screen displays.

Figure 27: [The Wireless > Setup Screen](#)



Wireless Basic Settings

Wireless ON/OFF: ENABLE

Wireless Mode: 11B/G/N Mixed

Channel: auto

WPS ON/OFF: DISABLE

Run WPS: PBC PIN

WPS Current Status: Not Used

SSID setting	SSID name	hidden	in-service	WMM Mode
Primary SSID		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Multiple SSID(2)		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Multiple SSID(3)		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Wireless Security

SSID: CGN2_SSID0

Security Mode: None

Apply Cancel Help

The following table describes the labels in this screen.

Table 27: [The Wireless > Setup Screen](#)

Wireless Basic Settings	
Wireless ON/OFF	Use this field to turn the wireless network on or off. <ul style="list-style-type: none"> ▶ Select ENABLE to turn the wireless network on. ▶ Deselect DISABLE to turn the wireless network off.

Table 27: [The Wireless > Setup Screen \(continued\)](#)

Wireless Mode	Select the type of wireless network that you want to use: <ul style="list-style-type: none"> ▶ 11B/G Mixed: use IEEE 802.11b and 802.11n ▶ 11B Only: use IEEE 802.11b ▶ 11G Only: use IEEE 802.11g ▶ 11N Only: use IEEE 802.11n ▶ 11G/N Mixed: use IEEE 802.11g and 802.11N ▶ 11B/G/N Mixed: use IEEE 802.11b, 802.11g and 802.11N NOTE: Only wireless clients that support the network protocol you select can connect to the wireless network. If in doubt, use 11B/G/N (default).
Channel	Select the wireless channel that you want to use, or select Auto to have the CGN select the optimum channel to use. NOTE: Use the Auto setting unless you have a specific reason to do otherwise.
WPS ON/OFF	Use this field to turn Wifi Protected Setup (WPS) on or off. <ul style="list-style-type: none"> ▶ Select ENABLE to turn WPS on. ▶ Deselect DISABLE to turn WPS off.

Table 27: [The Wireless > Setup Screen \(continued\)](#)

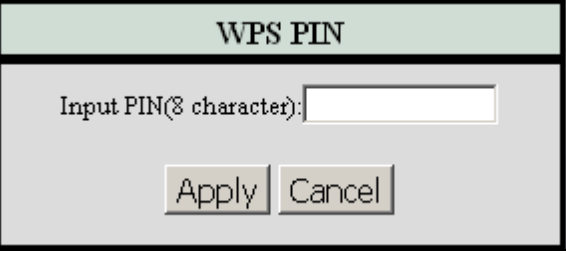
Run WPS	Use these buttons to run Wifi Protected Setup (WPS): <ul style="list-style-type: none"> ▶ Click the PBC button to begin the Push-Button Configuration process. You must then press the PBC button on your client wireless devices within two minutes in order to register them on your wireless network. ▶ Click the PIN button to begin the PIN configuration process. In the screen that displays, enter the WPS PIN that you want to use for the CGN, or the WPS PIN of the client device you want to add to the network. <p>Figure 28: WPS PIN</p> 
WPS Current Status	This displays whether or not the CGN is using Wifi Protected Setup.
SSID Setting	This displays an entry for each of the CGN's SSIDs. NOTE: You may have additional BSSIDs, depending on your contract with your service provider.
SSID Name	Enter the name that you want to use for your wireless network. This is the name that identifies your network, and to which wireless clients connect. NOTE: It is suggested that you change the SSID from its default, for security reasons.

Table 27: **The Wireless > Setup Screen (continued)**

Hidden	Use this field to make your network visible or invisible to other wireless devices. <ul style="list-style-type: none"> ▶ Select the checkbox if you do not want the CGN to broadcast the network name (SSID) to all wireless devices in the coverage area. Anyone who wants to connect to the network must know the SSID. ▶ Deselect the checkbox if you want your network name (SSID) to be public. Anyone with a wireless device in the coverage area can discover the SSID, and attempt to connect to the network.
In Service	This field controls whether or not the SSID is in operation. NOTE: This field is user-configurable for the Primary SSID only.
WMM Mode	Select the checkbox if you want to apply Wifi MultiMedia (WMM) Quality of Service (QoS) settings to this SSID.
Wireless Security	
SSID	Select the SSID for which you want to configure security.
Security Mode	Select the type of security that you want to use. <ul style="list-style-type: none"> ▶ Select None to use no security. Anyone in the coverage area can enter your network. ▶ Select WEP to use the Wired Equivalent Privacy security protocol. ▶ Select WPA-Personal to use the WiFi Protected Access (Personal) security protocol. NOTE: Due to inherent security vulnerabilities, it is suggested that you use WEP only if it is the only security protocol your wireless clients support. Under almost all circumstances, you should use WPA-Personal .
WEP Settings NOTE: These fields are only configurable when you select WEP from the Security Mode list.	

Table 27: [The Wireless > Setup Screen \(continued\)](#)

WEP Key Length	Use this field to specify the length of the security key used to allow wireless devices to join the network. The longer the key, the more secure it is. <ul style="list-style-type: none"> ▶ Select 64-bit to use a ten-digit security key. ▶ Select 128-bit to use a twenty-six-digit security key.
WEP Key 1~4	Use these fields to define the security keys that all wireless devices on the network must use to join the network. <p>The CGN supports up to four WEP keys, of which you can select one as the default. You should input the same four keys, in the same order, in your network's wireless clients. Your CGN and your wireless clients can use different default keys, as long as all four keys are present and in the same order. If your wireless client supports only a single WEP key, use the CGN's default key.</p> <p>Enter the keys in hexadecimal format (using the digits 0~9 and the letters A~F).</p>
Default WEP Key	Select the number of the security key that you want the CGN to use as its default authentication key for transmissions.
Authentication	Select the authentication mode that you want to use: <ul style="list-style-type: none"> ▶ Select Open System to allow wireless clients to authenticate (identify themselves) to the CGN before presenting their security credentials (WEP keys). ▶ Select Shared Key to use the WEP key in the authentication process. When a client wants to associate, the CGN sends an unencrypted challenge message. The client must use the WEP key to encrypt the challenge message and return it to the CGN, which then decrypts the message and compares the result with its original message. <p>Open System authentication is the more secure of the two authentication types, since while the Shared Key system appears more robust, it is possible to derive secure data by capturing the challenge messages.</p> <ul style="list-style-type: none"> ▶ Select Automatic to have the CGN choose the authentication method.

Table 27: [The Wireless > Setup Screen \(continued\)](#)

WPA_Personal	
NOTE: These fields display only when you select WPA-Personal from the Security Mode list.	
WPA Mode	Select the type of WPA security that you want to use: <ul style="list-style-type: none"> ▶ Select WPA-PSK to use Wifi Protected Access (Pre-Shared Key) mode ▶ Select WPA2-PSK to use Wifi Protected Access 2 (Pre-Shared Key) mode ▶ Select Auto (WPA-PSK or WPA2-PSK) to allow clients operating in either mode to connect to the CGN.
Cipher Type	Select the type of encryption that you want to use: <ul style="list-style-type: none"> ▶ Select TKIP to use the Temporal Key Integrity Protocol. ▶ Select AES to use the Advanced Encryption Standard. ▶ Select TKIP and AES to allow clients using either encryption type to connect to the CGN.
Group Key Update Interval	Enter the frequency (in seconds) with which you want the CGN to create new pre-shared keys, and issue them to the wireless client.
Pre-Shared Key	Enter the pre-shared key that you want to use for your wireless network. You will need to enter this key into your wireless clients in order to allow them to connect to the network.
Pre-Authentication	Use this field to allow pre-authentication (Enable) in WPA2, or deny pre-authentication requests (Disable). In preauthentication, a WPA2 wireless client can perform authentication with other wireless access points in its range when it is still connected to its current wireless access point. This allows mobile wireless clients to connect to new access points more quickly, permitting more efficient roaming.
Apply	Click this to save your changes to the fields in this screen.

Table 27: [The Wireless > Setup Screen \(continued\)](#)

Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

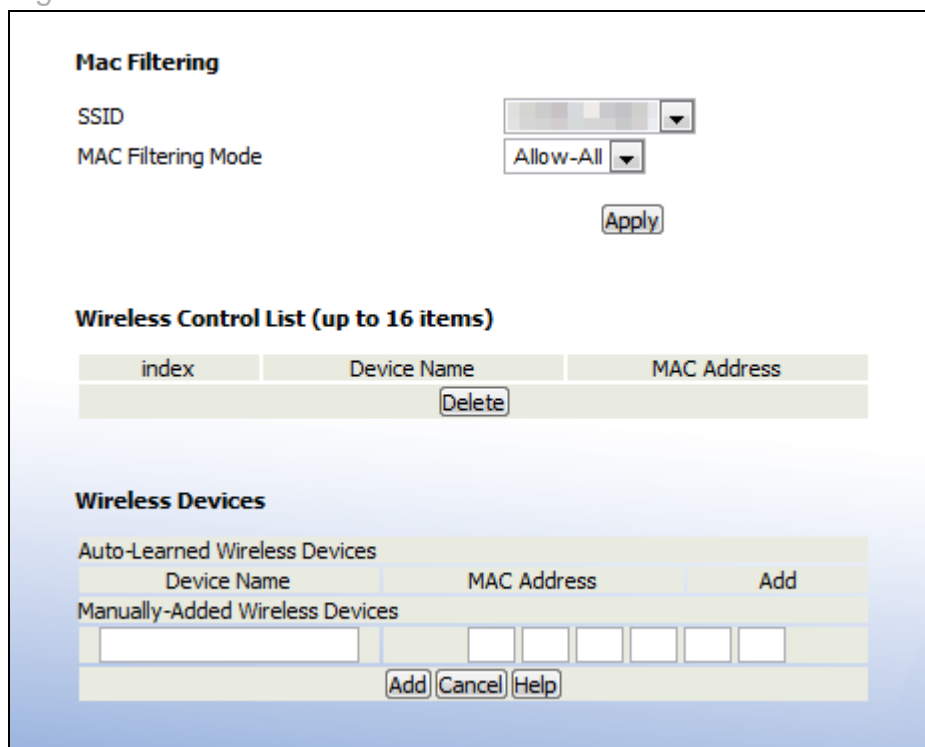
6.3 THE ACCESS CONTROL SCREEN

Use this screen to configure Media Access Control (MAC) address filtering on the wireless network.

NOTE: To configure MAC address filtering on the wired LAN, see [The Filter Setting Screen on page 57](#).

You can set the CGN to allow only certain devices to access the CGN and the network wirelessly, or to deny certain devices access.

Click **Wireless > Access Control**. The following screen displays.

 Figure 29: [The Wireless > Access Control Screen](#)


The screenshot shows the 'Mac Filtering' configuration screen. It includes a dropdown for SSID, a dropdown for MAC Filtering Mode (set to 'Allow-All'), and an 'Apply' button. Below this is the 'Wireless Control List (up to 16 items)' section, which contains a table with columns for 'index', 'Device Name', and 'MAC Address', and a 'Delete' button. The bottom section is 'Wireless Devices', which is divided into 'Auto-Learned Wireless Devices' and 'Manually-Added Wireless Devices'. The 'Manually-Added' section has input fields for device name and MAC address, and 'Add', 'Cancel', and 'Help' buttons.

The following table describes the labels in this screen.

Table 28: [The Wireless > Access Control Screen](#)

MAC Filtering	
SSID	Select the SSID for which you want to configure wireless access control. NOTE: At the time of writing, the CGN supports a single SSID.
MAC Filtering Mode	Use this field to control whether the CGN performs MAC filtering on the wireless network. <ul style="list-style-type: none"> ▶ Select Allow-All to turn MAC filtering off. All devices may access the CGN and the network wirelessly. ▶ Select Allow to permit only devices with the MAC addresses you set up in the Wireless Control List to access the CGN and the network wirelessly. All other devices are denied access. ▶ Select Deny to permit all devices except those with the MAC addresses you set up in the Wireless Control List to access the CGN and the network wirelessly. The specified devices are denied access.
Apply	Click this to save your changes in the MAC filtering section.
Wireless Control List (up to 16 Items)	
# Index	This displays the index number assigned to the permitted or denied wireless device.
Device Name	This displays the name you gave to the permitted or denied wireless device.
MAC Address	This displays the MAC address of the permitted or denied wireless device.
Delete	Select a permitted or denied wireless device's radio button (☐) and click this to remove the device from the list. The device may no longer access the CGN and the network.
Wireless Devices	
Auto-Learned Wireless Devices	
Device Name	This displays the name of each network device that has connected to the CGN on the wireless network.

Table 28: [The Wireless > Access Control Screen \(continued\)](#)

MAC Address	This displays the MAC address of each network device that has connected to the CGN on the wireless network.
Add	Select a device's checkbox and click Add to add the device to the Wireless Control List .
Manually-Added Wireless Devices	
Device Name	Enter the name to associate with a network device that you want to permit or deny access to the CGN and the network wirelessly. NOTE: This name is arbitrary, and does not affect functionality in any way.
MAC Address	Specify the MAC address of the network device that you want to permit or deny access to the CGN and the network wirelessly.
Add	Click this to add any Manually-Added Wireless Devices , and Auto-Learned Wireless Devices with their Add boxes checked, to the Wireless Control List .
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

6.4 THE ADVANCED SCREEN

Click **Wireless > Advanced**. The following screen displays.

Figure 30: The Wireless > Advanced Screen

Wireless Advanced Settings

BG Protection Mode

IGMP Snooping Disable Enable

WMM Configuration

HT Physical Mode

Operating Mode Mixed Mode Green Field

Channel BandWidth 20 20/40

Guard Interval long short

MCS

Reverse Direction Grant(RDG) Disable Enable

Extension Channel

Aggregation MSDU(A-MSDU) Disable Enable

Auto Block ACK Disable Enable

Decline BA Request Disable Enable

Other

HT TxStream

HT RxStream

The following table describes the labels in this screen.

Table 29: [The Wireless > Advanced Screen](#)

Wireless Advanced Settings	
BG Protection Mode	<p>Use this field to configure IEEE 802.11b/g protection.</p> <p>Both 802.11b and 802.11g wireless communications occur at the same radio frequencies. When the CGN is wirelessly connected to 802.11b clients and 802.11g clients simultaneously, the performance of the link to 802.11g clients can deteriorate due to the presence of the 802.11b clients. Because 802.11b and 802.11g use different modulation techniques, 802.11b clients do not understand 802.11g's Request To Send (RTS) and Clear To Send (CTS) messages, which ensure that each wireless device transmits only when other devices are not transmitting.</p> <p>When B/G protection is active, the CGN prevents 802.11b clients transmitting over 802.11g transmissions by first transmitting an announcement (known as a CTS-to-Self) to 802.11b clients, stating that it intends to transmit to 802.11g clients.</p> <ul style="list-style-type: none"> ▶ Select Auto to have the CGN control whether B/G protection is active or not. ▶ Select Always-on to use B/G protection at all times. ▶ Select Always-off to never use B/G protection.

Table 29: [The Wireless > Advanced Screen \(continued\)](#)

IGMP Snooping	<p>Use this field to turn Internet Group Management Protocol (IGMP) snooping on or off.</p> <p>IGMP is used to manage multicast groups. In multicast groups, data is transmitted to numerous IP addresses simultaneously. This is the most efficient method of providing the same data to many different recipients at the same time, since each data packet needs to be sent only once. Multicast groups are often used for Internet TV and real-time streaming applications such as online gaming.</p> <p>IGMP snooping allows the CGN to “snoop” or listen in on IGMP traffic, and to determine which computers on the LAN belong to which IGMP groups. By keeping lists of which computers belong to IGMP groups, the CGN can send the IGMP data to only those computers that have requested it, and can refrain from sending unsolicited multicast data. This can improve your connection to wireless clients.</p> <ul style="list-style-type: none"> ▶ Select Disable to turn IGMP snooping off. ▶ Select Enable to turn IGMP snooping on.
WMM Configuration	<p>Click this to set up your Wifi Multimedia (WMM) Quality of Service (QoS) settings. See Configuring WMM Parameters on page 103 for information on the screen that displays.</p> <p>NOTE: Turn WMM on and off in the Wireless > Basic Settings screen.</p>
HT Physical Mode	

Table 29: [The Wireless > Advanced Screen \(continued\)](#)

Operating Mode	<p>Use this field to configure how the CGN transmits in IEEE 802.11n mode.</p> <p>Mixed mode, on the other hand, allows 802.11a/b/g stations to tell when 802.11n transmissions are occurring, by transmitting RTS, CTS and CTS-to-Self messages in a format the legacy stations can understand. You should select this option if you have 802.11a/b/g stations in your networks, or if there are other 802.11a/b/g networks in your area.</p> <p>Green Field, also known is High Throughput (HT) mode, assumes that there are no existing IEE 802.11a/b/g stations using the same radio channel. In greenfield mode, the 802.11a/b/g stations are unable to tell when 802.11n transmissions are occurring. You should select this mode only if there are no 802.11a/b/g stations in your network (or other networks in your location). Otherwise these stations' wireless transmissions will interfere with your 802.11n transmissions. When no 802.11a/b/g stations are present, greenfield mode allows greater wireless network speeds, because the legacy messages (RTS, CTS and CTS-to-Self) do not need to be sent.</p>
Channel Bandwidth	<p>This field allows you to configure the width of the radio channel the CGN uses to communicate with its wireless clients (IEEE 802.11n only). Using the full 40MHz bandwidth can double your data speed.</p> <ul style="list-style-type: none"> ▶ Select 20 to only use a 20 megahertz band. ▶ Select 20/40 to use a 40 megahertz band when possible, and a 20 megahertz band when a 40Mhz band is unavailable.

Table 29: [The Wireless > Advanced Screen \(continued\)](#)

<p>Guard Interval</p>	<p>In 802.11n networks, the guard interval is the amount of time that elapses between the transmission of symbols. This is to prevent Inter-Symbol Interference, or ISI, caused by echoes.</p> <p>NOTE: In modulated signals, each distinct modulated character (for example, each audible tone produced by a modem for transmission over telephone lines) is known as a symbol.</p> <ul style="list-style-type: none"> ▶ Select Long to use a long guard interval of 800 nanoseconds. ▶ Select Short to use a short guard interval of 400 nanoseconds.
<p>MCS</p>	<p>Use this field to configure the Modulation and Coding Scheme (MCS) that the CGN uses for IEEE 802.11n transmissions.</p> <p>The 802.11n protocol specifies 77 Modulation and Coding Schemes. Each MCS refers to a combination of a modulation technique, a coding rate, a guard interval, and a certain number of spatial streams. The CGN supports MCS 0~15, and 32.</p> <p>Select the MCS that you wish to use for 802.11n transmissions. If unsure, select Auto (default).</p>

Table 29: [The Wireless > Advanced Screen \(continued\)](#)

Reverse Direction Grant (RDG)	<p>Use this field to configure Reverse Direction Grant in IEEE 802.11n transmissions.</p> <p>Each data transfer requires that the wireless station initiating the transfer acquires permission from the access point to perform the transfer. This is known as a transmission opportunity, or TXOP. Each TXOP is time-limited; the initiating station may transmit for only a certain length of time, and then must cease.</p> <p>Normally, if the receiving station wishes to return data to the initiating station, it must also acquire its own TXOP.</p> <p>However, when you enable Reverse Direction Grants, a wireless station that has already obtained a TXOP may issue a Reverse Direction Grant to the receiving station. This allows the receiving station to transmit data back to the initiating station for the remaining time specified in the original TXOP. It does not need to acquire its own TXOP.</p> <ul style="list-style-type: none"> ▶ Select Disable to disallow Reverse Direction Grants. ▶ Select Enable to allow Reverse Direction Grants.
Extension Channel	<p>This field displays the secondary wireless radio channel that the CGN uses for channel bonding (combining two channels for faster data transfer) in IEEE 802.11n transmissions.</p> <p>NOTE: At the time of writing, you cannot select the Extension channel. It is selected automatically by the CGN.</p>
Aggregation MSDU (A-MSDU)	<p>Use this field to control whether the CGN supports Aggregation MSDUs (A-MSDUs) in IEEE 802.11n transmissions.</p> <p>Each A-MSDU consists of multiple MSDUs, added together (aggregated) to create one large packet. This reduces the overhead associated with transmission, but can result in a reduced data rate if your network suffers from a high error rate since each lost A-MSDU will require retransmission.</p> <ul style="list-style-type: none"> ▶ Select Disable to not use A-MSDUs. ▶ Select Enable to use A-MSDUs.

Table 29: [The Wireless > Advanced Screen \(continued\)](#)

Auto Block ACK	<p>Use this field to control how the CGN sends acknowledgement (ACK) requests in IEEE 802.11n transmissions.</p> <p>Normally, an ACK request is sent after every data or management frame in order to ensure that it has been received correctly. However, when you enable Auto Block ACK the CGN sends a burst of multiple frames together, and follows it with a single, block ACK request.</p> <ul style="list-style-type: none"> ▶ Select Disable to not use block ACKs. ▶ Select Enable to use block ACKs. <p>NOTE: Block ACK can increase your network's speed, as fewer ACK messages are sent. However, you should not use it if your network is prone to interference, since if the transmitting station needs to retransmit information, the required retransmission will be much longer.</p>
Decline BA Request	<p>Use this field to control how the CGN receives acknowledgement (ACK) requests in IEEE 802.11n transmissions.</p> <p>Select Disable to accept block ACK requests. The transmitting device may then send multiple data frames together, followed by the block ACK request.</p> <p>Select Enable to decline block ACK requests. The transmitting device must then follow each data frame with an ACK request in the traditional manner.</p>
Other	
HT TxStream	Select the number of 802.11n radio transmitting channels (1 or 2) for High Throughput (HT) transmission.
HT RxStream	Select the number of 802.11n radio receiving channels (1 or 2) for High Throughput (HT) transmission.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

6.4.1 CONFIGURING WMM PARAMETERS

To set up your CGN's Wifi MultiMedia (WMM) Quality of Service (QoS) settings, click the **Configuration** button in the **Wireless > Advanced** screen. The following screen displays.

Figure 31: [The Wireless > Advanced > WMM Configuration Screen](#)

This page is used for WMM Configuration.

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	255	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	255	0	<input type="checkbox"/>
AC_BK	7	15	255	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>

NOTE: It is strongly recommended that you do not change the default values in this screen unless you have a good reason to do so.

The following table describes the labels in this screen.

Table 30: [The Wireless > Advanced > WMM Configuration Screen](#)

WMM Parameters of Access Point	
NOTE: This section controls the parameters of data transmitted from the CGN to the wireless clients.	
AC_BE	This row controls the Best Effort (BE) Access Category (AC)

Table 30: [The Wireless > Advanced > WMM Configuration Screen](#)

AC_BK	This row controls the Background (BK) Access Category (AC)
AC_VI	This row controls the Video (VI) Access Category (AC)
AC_VO	This row controls the Voice (VO) Access Category (AC)
AIFSN	This column controls the Arbitration Inter-Frame Space Number for each Access Category. WMM gives the highest priority to the AC with the lowest AIFSN.
CWMin	<p>This column controls the Contention Window Minimum for each Access Category. A smaller CWMin value increases priority for data of the relevant type.</p> <p>The contention window system is a mechanism for providing priority to important data on the wireless network. When a data collision occurs, each frame is assigned a random time to wait before attempting transmission again. This random time value is between zero and the data's CWMin value. If a collision occurs again, the time value is doubled, and transmission is attempted again. This continues until the time value reaches the CWMax value.</p>
CWMax	This column controls the Contention Window Maximum for each Access Category. A smaller CWMin value decreases the access delay for data of the relevant type, but can result in more data collisions.
TXOP	This field defines the Transmission Opportunity (TXOP) length for each Access Category. This is the length of time during which the wireless device may to transmit over the wireless network, once it receives a transmission opportunity.
ACM	This field specifies whether Admission Control is Mandatory (ACM) for each Access Category. Select the checkbox to have the CGN control ACM.

Table 30: [The Wireless > Advanced > WMM Configuration Screen](#)

AckPolicy	WMM defines two ACK policies: NormalAck and NoAck. <ul style="list-style-type: none"> ▶ NormalAck: the recipient of a transmission acknowledges each received packet. ▶ NoAck: the recipient of a transmission does not acknowledge received packets. This can improve data throughput in situations where signal quality is excellent, but in other situations can cause a significant increase in lost packets. Select the checkbox to use the NoAck policy.
WMM Parameters of Station NOTE: This section controls the parameters of data transmitted from the wireless clients to the CGN.	
AC_BE	This row controls the Best Effort (BE) Access Category (AC)
AC_BK	This row controls the Background (BK) Access Category (AC)
AC_VI	This row controls the Video (VI) Access Category (AC)
AC_VO	This row controls the Voice (VO) Access Category (AC)
AIFSN	This column controls the Arbitration Inter-Frame Space Number for each Access Category. WMM gives the highest priority to the AC with the lowest AIFSN.
CWMin	This column controls the Contention Window Minimum for each Access Category. A smaller CWMin value increases priority for data of the relevant type. The contention window system is a mechanism for providing priority to important data on the wireless network. When a data collision occurs, each frame is assigned a random time to wait before attempting transmission again. This random time value is between zero and the data's CWMin value. If a collision occurs again, the time value is doubled, and transmission is attempted again. This continues until the time value reaches the CWMax value.
CWMax	This column controls the Contention Window Maximum for each Access Category. A smaller CWMin value decreases the access delay for data of the relevant type, but can result in more data collisions.

Table 30: [The Wireless > Advanced > WMM Configuration Screen](#)

TXOP	This field defines the Transmission Opportunity (TXOP) length for each Access Category. This is the length of time during which the wireless device may to transmit over the wireless network, once it receives a transmission opportunity.
ACM	This field specifies whether Admission Control is Mandatory (ACM) for each Access Category. Select the checkbox to have the wireless client control ACM.

7

TROUBLESHOOTING

Use this section to solve common problems with the CGN and your network.

Problem: **None of the LEDs Turn On**

The CGN is not receiving power, or there is a fault with the device.

1 Ensure that you are using the correct power adaptor.



Using a power adaptor other than the one that came with your CGN can damage the CGN.

2 Ensure that the power adaptor is connected to the CGN and the wall socket (or other power source) correctly.

3 Ensure that the power source is functioning correctly. Replace any broken fuses or reset any tripped circuit breakers.

4 Disconnect and re-connect the power adaptor to the power source and the CGN.

5 If none of the above steps solve the problem, consult your vendor.

Problem: **One of the LEDs does not Display as Expected**

1 Ensure that you understand the LED's normal behavior (see [LEDs](#) on page 17).

2 Ensure that the CGN's hardware is connected correctly; see the Quick Installation Guide.

3 Disconnect and re-connect the power adaptor to the CGN.

4 If none of the above steps solve the problem, consult your vendor.

Problem: I Forgot the CGN's IP Address

- 1 The CGN's default LAN IP address is **192.168.0.1**.
- 2 You can locate the CGN's GUI by entering the LAN domain suffix into your browser's address bar (on a computer connected to the LAN). The default LAN domain suffix is displayed in the **WAN/LAN > IP** screen's **Domain Suffix** field. See [The IP Screen](#) on page 47 for more information.
- 3 Depending on your operating system and your network, you may be able to find the CGN's IP address by looking up your computer's default gateway. To do this on (most) Windows machines, click **Start > Run**, enter "cmd", and then enter "ipconfig". Get the IP address of the **Default Gateway**, and enter it in your browser's address bar.
- 4 If you still cannot access the CGN, you need to reset the CGN. See [Resetting the CGN](#) on page 24. All user-configured data is lost, and the CGN is returned to its default settings. If you previously backed-up a more recent version your CGN's settings, you can now upload them to the CGN; see [The Backup Screen](#) on page 52.

Problem: I Forgot the CGN's Admin Username or Password

- 1 The default username is **cusadmin**, and the default password is **password**.
- 2 If the default username and password do not work, you need to reset the CGN. See [Resetting the CGN](#) on page 24. All user-configured data is lost, and the CGN is returned to its default settings. If you previously backed-up a more recent version your CGN's settings, you can now upload them to the CGN; see [The Backup Screen](#) on page 52.

Problem: I Cannot Access the CGN or the Internet

- 1 Ensure that you are using the correct IP address for the CGN.
- 2 Check your network's hardware connections, and that the CGN's LEDs display correctly (see [LEDs](#) on page 17).
- 3 Make sure that your computer is on the same subnet as the CGN; see [IP Address Setup](#) on page 20.

- 4 If you are attempting to connect over the wireless network, there may be a problem with the wireless connection. Connect via a **LAN** port instead.
- 5 If the above steps do not work, you need to reset the CGN. See [Resetting the CGN](#) on page 24. All user-configured data is lost, and the CGN is returned to its default settings. If you previously backed-up a more recent version your CGN's settings, you can now upload them to the CGN; see [The Backup Screen](#) on page 52.
- 6 If the problem persists, contact your vendor.

Problem: I Cannot Access the Internet and the DS and US LEDs Keep Blinking

Your service provider may have disabled your Internet access; check the **Cable > System Info** screen's Network Access field (see [The System Info Screen](#) on page 33).

Problem: I Cannot Connect My Wireless Device

- 1 Ensure that your wireless client device is functioning properly, and is configured correctly. See the wireless client's documentation if unsure.
- 2 Ensure that the wireless client is within the CGN's radio coverage area. Bear in mind that physical obstructions (walls, floors, trees, etc.) and electrical interference (other radio transmitters, microwave ovens, etc) reduce your CGN's signal quality and coverage area.
- 3 Ensure that the CGN and the wireless client are set to use the same wireless mode and SSID (see [The Setup Screen](#) on page 86) and security settings (see [The Access Control Screen](#) on page 93).
- 4 Re-enter any security credentials (WEP keys, WPA(2)-PSK password, or WPS PIN).
- 5 If you are using WPS's PBC (push-button configuration) feature, ensure that you are pressing the button on the CGN and the button on the wireless client within 2 minutes of one another.

FCC STATEMENT

Federal Communication Commission 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 harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one 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.

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.

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

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

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.

INDEX

Numbers

802.11b/g/n 13, 84, 88, 97, 99

A

access control 93
access logs 13
access point 12, 83
accounts, login 23
address, IP 20
address, IP, local 21
AP 12, 83
attached network devices 38
authentication 91

B

backup 52
backup and restore 13
bar, navigation 24
BG protection mode 97
buttons 14

C

cable connection 12
cable connection status 37

cable modem 12
CATV 13, 26, 27
cipher type 92
clients, wireless 83
configuration file 31, 39
connection process 38
connection status, cable 37
conventions, document 3
customer support 3

D

debugging 46, 50, 51
default 52
default IP address 21
default username and password 23
defaults 41, 42, 52
De-Militarized Zone 56
DHCP 13, 20, 21, 29, 49
DHCP lease 30
diagnostics 46
DMZ 56
DMZ De-Militarized Zone 13
DNS 46
DOCSIS 26
document conventions 3
Domain Name System 46
domain suffix 46
downstream transmission 31
DS 20

E

ETH 19
Ethernet 13
Ethernet cables 16
Ethernet port 21
event logging 13

F

factory defaults 41, 42, 52
factory reset 16, 24
fast Ethernet 13
FDMA 32
firewall 54
forwarding, port 13, 56, 65
frequencies, cable 31
F-type RF connector 13

G

Graphical User Interface 12
graphical user interface 12
GUI 12, 23
GUI overview 23

H

hardware 14
HNAP 43
host ID 27
HT mode 98

I

IANA 27
ICMP 56, 72
IEEE 802.11b/g/n 13, 84
IGMP snooping 98
interface, user 12
intrusion detection 13, 55, 56, 72
IP address 20, 21, 27, 46, 108
IP address lease 30
IP address renewal 30
IP address setup 20, 21
IP address, default 21
IP address, format 27
IP address, local 21
IP filtering 13, 55
ISP 27

K

keyword blocking 76

L

LAN 12, 45, 83
LAN 1~4 16
LAN IP 47
LEDs 17, 107, 109
lights 17
Local Area Network 12
local IP address 21
logging in 22
login accounts 23
login screen 21
logs, access 13

M

MAC address 30
MAC address filtering 93
MAC filtering 13, 55, 57
main window 24
Media Access Control address 30
MIMO 13
modem 12
modulation 32
Multiple-In, Multiple-Out 13

N

navigation 24
navigation bar 24
network devices, attached 38
network diagnostics 46
network number 27
network, local 12
network, wide area 12
network, wireless 12

O

open system authentication 91
overview, GUI 23

P

parental control 13, 74
password 41, 42, 108
password and username 23
PBC configuration 85

PIN configuration 13, 85
ping 13, 46, 50, 51, 55, 56, 72
port forwarding 13, 56, 65
port triggering 13, 69
port, Ethernet 21
ports 14
pre-authentication 92
pre-shared key 92
private IP address 28
push-button configuration 13

Q

QAM 32
QAM TCM 32
QoS 86
QPSK 32

R

radio coverage 86
radio links 83
reboot 52
reset 16, 24
restore and backup 13
RF connector 13
RJ45 connectors 16
routing mode 28, 31, 45
rule, IP filtering 63
rule, port forwarding 67

S

SCDMA 32
scheduled website blocking 13

scheduling 77
security 90
security, wireless 13
service set 84
settings backup and restore 13
shared key authentication 91
SSID 84, 86
Status 20
status 38
status, cable connection 37
subnet 20, 21, 27, 46
subnet, IP 20
support, customer 3

T

TCP/IP 21
TDMA 32
traceroute 13, 46, 50, 51
triggering, port 13, 69
trusted computers 74

U

upstream transmission 31
URL blocking 76
US 20
user interface 12
username 108
username and password 23

W

WAN 12, 27
WAN connection 38

website blocking 74, 75, 79
website blocking, scheduled 13
WEP 13, 85
Wide Area Network 12
Wifi MultiMedia 86
Wifi Protected Setup 13, 85
window, main 24
Windows XP 21
wired security 13
wireless 83
wireless access point 12
wireless clients 83
wireless connection 109
Wireless Local Area Network 12
wireless networking standards 84
wireless security 13, 85, 90
wireless settings, basic 86
WLAN 12, 83
WMM 86, 98, 103
WPA2 86
WPA2-PSK 13, 85
WPA-PSK 13, 85
WPS 13, 85, 86, 90
WPS PBC 16

X

XP, Windows 21