USER'S GUIDE

CGNV2

VERSION 1.0
MAY 2014

DEFAULT LOGIN DETAILS	
IP Address	192.168.0.1
Username	cusadmin
Password	password

HitronTechnologies

ABOUT THIS USER’S GUIDE

INTENDED AUDIENCE

This manual is intended for people who want to configure the CGNV2’s features via its Graphical User Interface (GUI).

HOW TO USE THIS USER’S GUIDE

This manual contains information on each the CGNV2’s GUI screens, and describes how to use its various features.

- Use the Introduction (page 15) to see an overview of the topics covered in this manual.
- Use the Table of Contents (page 7), List of Figures (page 11) and List of Tables (page 13) to quickly find information about a particular GUI screen or topic.
- Use the Index (page 113) to find information on a specific keyword.
- Use the rest of this User’s Guide to see in-depth descriptions of the CGNV2’s features.

RELATED DOCUMENTATION

- **Quick Installation Guide**: see this for information on getting your CGNV2 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 CGNV2’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.

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.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

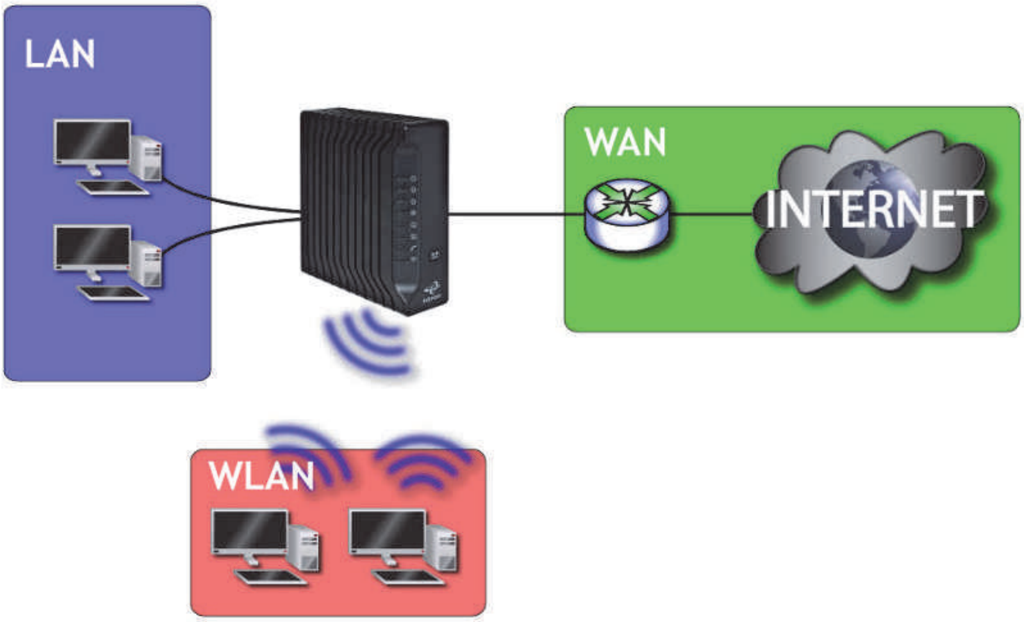
This chapter introduces the CGNV2 and its GUI (Graphical User Interface).

1.1 CGNV2 OVERVIEW

Your CGNV2 is a voice-enabled cable modem and wireless access point that allows you to connect your computers, analog telephones, wireless devices, and other network devices to one another, and to the Internet via the cable connection.

Computers with a wired connection to the CGNV2 are on the Local Area Network (LAN), computers with a wireless connection to the CGNV2 are on the Wireless Local Area Network (WLAN) and the CGNV2 connects to the service provider over the Wide Area Network (WAN).

FIGURE 1: Application Overview



1.1.1 KEY FEATURES

The CGNV2 provides:

- Internet connection to cable modem service via **CATV** port (F-type RF connector)
- Voice over IP (VoIP) connection to your voice service provider.
- 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 and MAC filtering
- Wired security: stateful inspection firewall with intrusion detection system, IP and MAC filtering, port forwarding and port triggering, and De-Militarized Zone (DMZ)
- 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 CGNV2's physical ports and buttons.

FIGURE 2: Hardware Connections

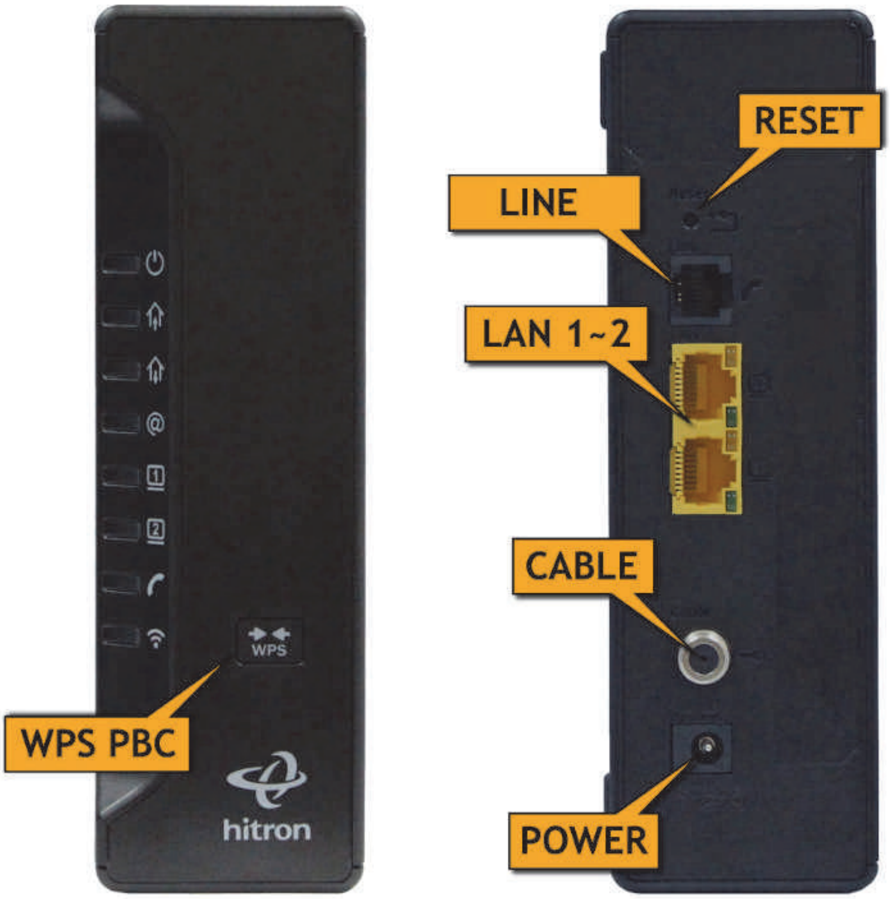


TABLE 1: Hardware Connections

WPS	Use this button to turn the wireless network on or off, and to begin the WiFi Protected Setup (WPS) Push-Button Configuration (PBC) procedure (see WPS on page 79 for more information.) ▸ To turn the wireless network on or off, press the button for between one and five seconds. ▸ To begin the WPS PBC connection procedure, press and hold the button for between five and ten seconds. Press the PBC button on your wireless clients in the coverage area within two minutes to enable them to join the wireless network.
Reset	Use this button to reboot or reset your CGNV2. ▸ Press the button and hold it for less than five seconds to reboot the CGNV2. The CGNV2 restarts, using your existing settings. ▸ Press the button and hold it for more than ten seconds to delete all user-configured settings and restart the CGNV2 using its factory default settings.

TABLE 1: Hardware Connections

LAN1	Use these ports to connect your computers and other network devices, using Category 5 or 6 Ethernet cables with RJ45 connectors.
LAN2	
LINE	Use this port to connect your analog phones for VoIP services, using cables with RJ11 connector.
CABLE	Use this to connect to the Internet via an F-type RF cable.
POWER	Use this to connect to the 12v/2A power adapter that came with your CGNV2. **NEVER use another power adapter with your CGNV2. Doing so could harm your CGNV2.**

1.3 LEDS

This section describes the CGNV2's LEDs (lights).

FIGURE 3: LEDs

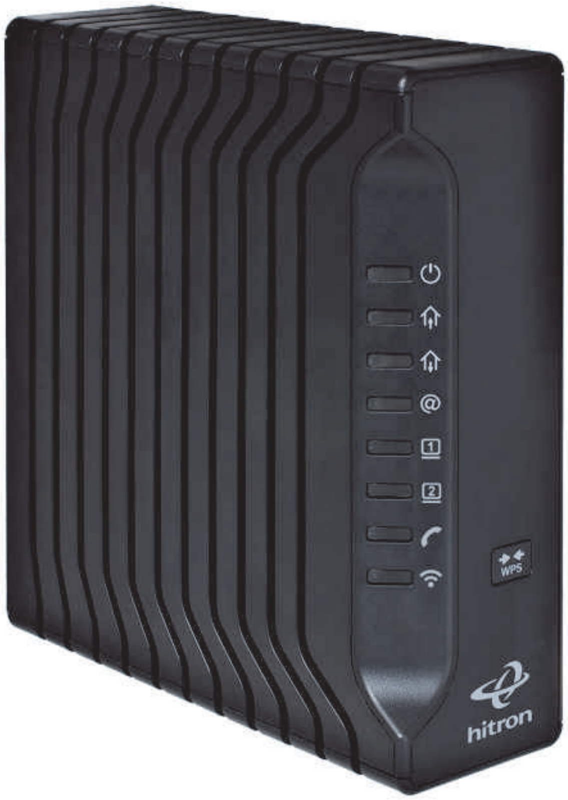


TABLE 2: LEDs

LED	STATUS	**DESCRIPTION**
WIRELESS 📶	Off	No data is being transmitted or received over the wireless network.
	Blinking	Data is being transmitted or received over the wireless network.
LINE ☎	Off	Your service plan does not include voice service.
	Blinking	A telephone is connected to the relevant **Line** port, and is off-hook.
	On	Your service plan includes voice service.
ETH 1 2	Off	No device is connected to any **LAN** port.
	Blinking	A device is connected to a **LAN** port via a fast Ethernet link, and is transmitting or receiving data.
	On	A device is connected to a **LAN** port via a fast ethernet link, but is not transmitting or receiving data.
Status @	Blinking	The CGNV2's cable modem is registering with the service provider.
	On	The CGNV2's cable modem has successfully registered with the service provider.

TABLE 2: LEDs

US ⌂	Blinking	The CGNV2 is searching for an upstream frequency on the **CATV** connection.
	On	The CGNV2 has successfully located and locked onto an upstream frequency on the **CATV** connection.
DS ⌂	Blinking	The CGNV2 is searching for a downstream frequency on the **CATV** connection.
	On	The CGNV2 has successfully located and locked onto a downstream frequency on the **CATV** connection.
POWER ⏻	On	The CGNV2 is receiving power.
	Off	The CGNV2 is not receiving power.

When you turn on the CGNV2, the LEDs light up in the following order:

- **Power**
- **US**
- **DS**
- **Status**
- The **ETH 1~2** LEDs light up as soon as there is activity on the relevant port, the **LINE** port light up if your service contract includes voice service, and the **WIRELESS** LED lights up once the wireless network is ready.

1.4 IP ADDRESS SETUP

Before you log into the CGNV2's GUI, your computer's IP address must be in the same subnet as the CGNV2. This allows your computer to communicate with the CGNV2.

NOTE: See IP Addresses and Subnets on page 25 for background information.

The CGNV2 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 CGNV2 (see Login to the CGNV2 on page 22).

- If the login screen displays, your computer is already configured correctly.
- If the login screen does not display, either the CGNV2'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 CGNV2's IP settings may have been changed from their defaults. If you do not know the CGNV2's new address, you should return it to its factory defaults. See Resetting the CGNV2 on page 23. Bear in mind that ALL user-configured settings are lost.

1.4.1 MANUAL IP ADDRESS SETUP

By default, your CGNV2's local IP address is **192.168.0.1**. If your CGNV2 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 CGNV2 DHCP server is active, set your computer to get an IP address automatically in step 5. The CGNV2 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 CGNV2:

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 CGNV2's DHCP server is active, select **Get an IP address automatically**.
    - If your CGNV2's DHCP server is not 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 CGNV2 is not using the default IP address, enter an IP address and subnet mask that places your computer in the same subnet as the CGNV2.

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 CGNV2, or uses the IP address that you specified, and can communicate with the CGNV2.

1.5 LOGIN TO THE CGNV2

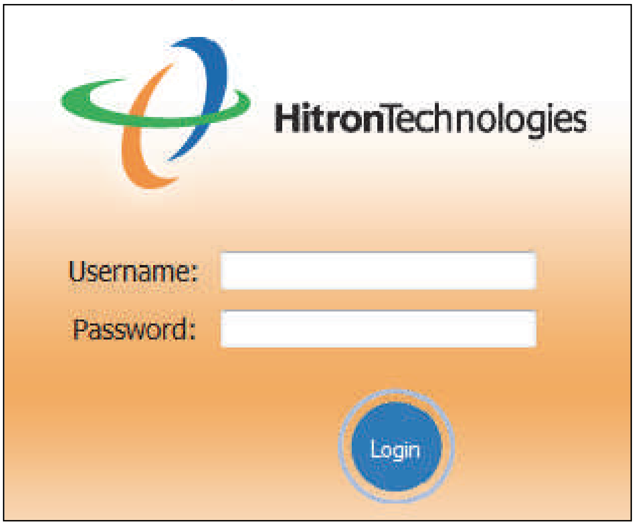
Take the following steps to login to the CGNV2's GUI.

NOTE: You can login to the CGNV2's GUI via the wireless interface. However, it is strongly recommended that you configure the CGNV2 via a wired connection on the LAN.

1 Open a browser window.

2 Enter the CGNV2's IP address (default **192.168.0.1**) in the URL bar. The **Login** screen displays.

FIGURE 4: Login



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

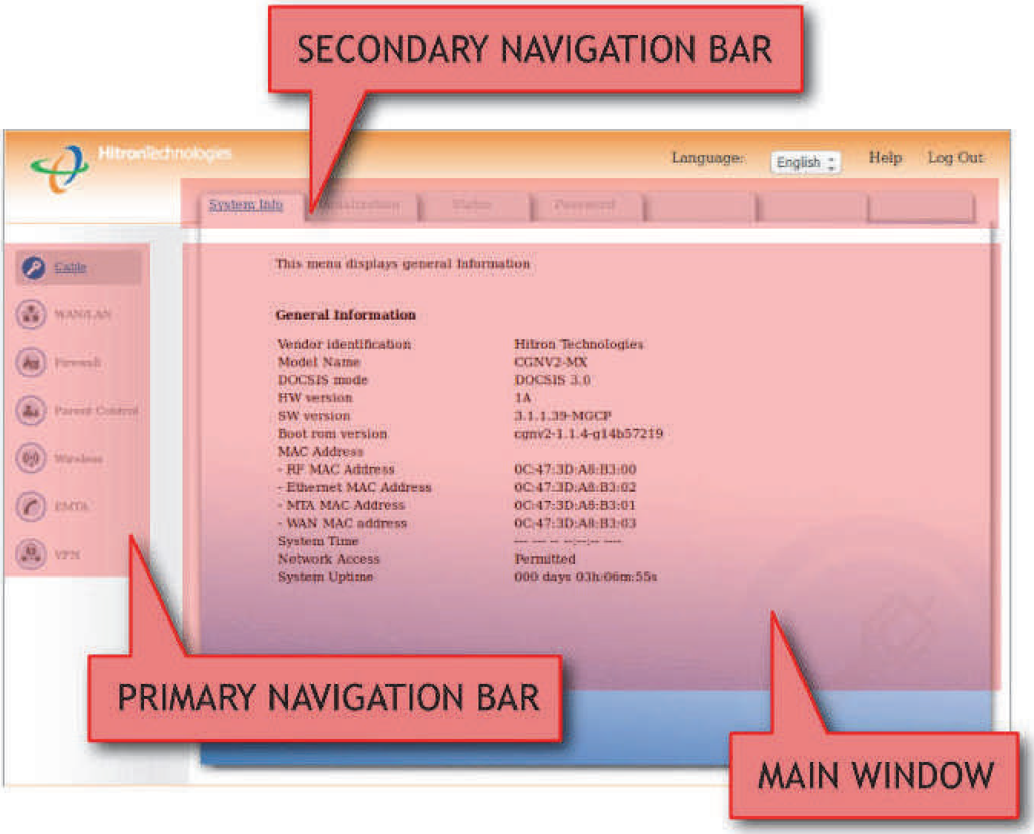
NOTE: The Username and Password are case-sensitive; "cusadmin" is not the same as "Cusadmin".

4 Click **Login**. The **System Info** screen displays (see The System Info Screen on page 30).

1.6 GUI OVERVIEW

This section describes the CGNV2's GUI.

FIGURE 5: GUI Overview



This menu displays general information

General Information

Vendor identification	Hitron Technologies
Model Name	CGNV2-MX
DOCSIS mode	DOCSIS 3.0
HW version	1A
SW version	3.1.1.39-MGCP
Boot rom version	cgnv2-1.1.4-g14b57219
MAC Address	
- RF MAC Address	0C:47:3D:A8:B3:00
- Ethernet MAC Address	0C:47:3D:A8:B3:02
- MTA MAC Address	0C:47:3D:A8:B3:01
- WAN MAC address	0C:47:3D:A8:B3:03
System Time	--- --- -- --:--:-- ----
Network Access	Permitted
System Uptime	000 days 03h:06m:55s

TABLE 3: 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 CGNV2's configuration, and make configuration changes.

1.7 RESETTING THE CGNV2

When you reset the CGNV2 to its factory defaults, all user-configured settings are lost, and the CGNV2 is returned to its initial configuration state.

There are two ways to reset the CGNV2:

- Press the **RESET** button on the CGNV2, and hold it in for ten seconds or longer.
- Click **WAN/LAN** > **Backup**. In the screen that displays, click the **Factory Reset** button.

The CGNV2 turns off and on again, using its factory default settings.

NOTE: Depending on your CGNV2's previous configuration, you may need to re-configure your computer's IP settings; see IP Address Setup on page 20.

2

CABLE

This chapter describes the screens that display when you click **Cable** in the toolbar.

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 CGNV2 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 CGNV2:

- The public network (Wide Area Network or WAN) is the link between the cable (CATV) connector and your Internet Service Provider. Your CGNV2's IP address on this network is assigned by your service provider.
- The private network (in routing mode - see Routing Mode on page 28) 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 CGNV2 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 4: 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 CGNV2'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 5: 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 6: 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 CGNV2 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 CGNV2 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 DNS

2.1.6 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 CGNV2 via one of the **LAN** ports) and also has a wireless card (to connect to your CGNV2 over the wireless interface) the MAC addresses of the two cards will be different. In the case of the CGNV2, each internal module (cable modem module, Ethernet module, wireless module, etc.) possesses its own MAC address.

2.1.7 ROUTING MODE

When your CGNV2 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 CGNV2 on the WAN, and all traffic for LAN computers is sent to that IP address. The CGNV2 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 CGNV2 in routing mode, each computer on the LAN must be assigned an IP address in the CGNV2's subnet manually.

When the CGNV2 is not in routing mode, the service provider assigns an IP address to each computer connected to the CGNV2 directly. The CGNV2 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 CGNV2’s configuration file.

2.1.8 CONFIGURATION FILES

The CGNV2’s configuration (or config) file is a document that the CGNV2 obtains automatically over the Internet from the service provider’s server, which specifies the settings that the CGNV2 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.

2.1.9 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 CGNV2, and “upstream” refers to traffic from the CGNV2 to the service provider.

2.1.10 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.

2.1.11 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.

2.1.12 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.

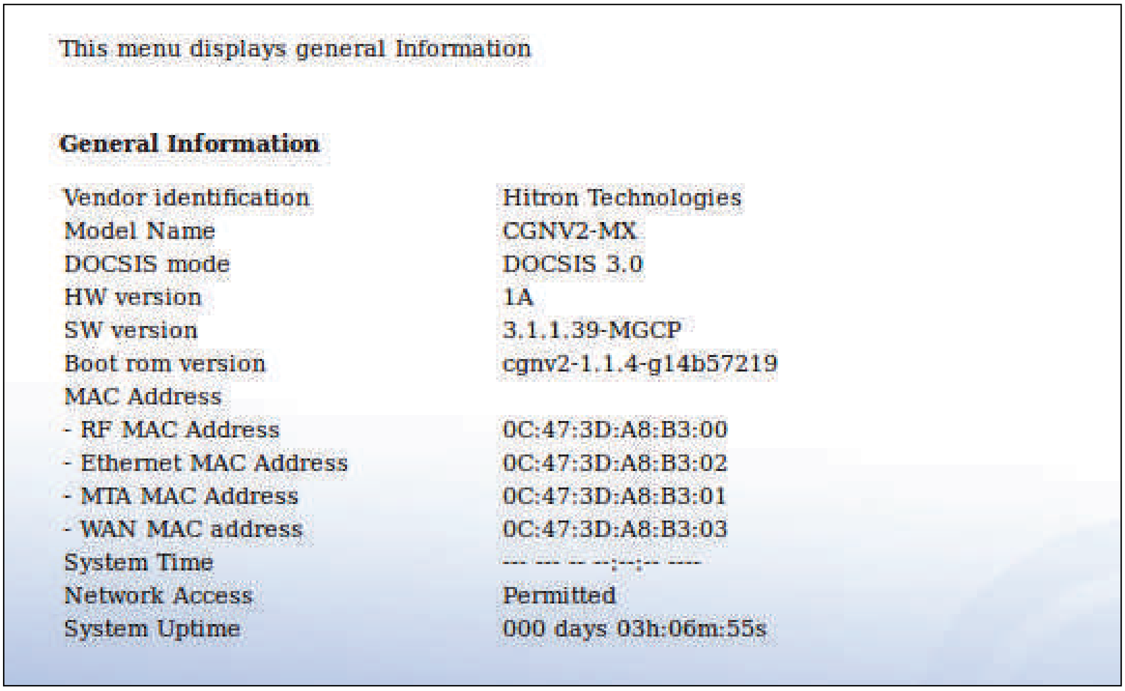
2.2 THE SYSTEM INFO SCREEN

Use this screen to see general information about your CGNV2'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 **Cable** > **System Info**. The following screen displays.

FIGURE 6: The Cable > System Info Screen



This menu displays general Information

General Information

Vendor identification	Hitron Technologies
Model Name	CGNV2-MX
DOCSIS mode	DOCSIS 3.0
HW version	1A
SW version	3.1.1.39-MGCP
Boot rom version	cgnv2-1.1.4-g14b57219
MAC Address	
- RF MAC Address	0C:47:3D:A8:B3:00
- Ethernet MAC Address	0C:47:3D:A8:B3:02
- MTA MAC Address	0C:47:3D:A8:B3:01
- WAN MAC address	0C:47:3D:A8:B3:03
System Time	--- --- -- --:--:-- ----
Network Access	Permitted
System Uptime	000 days 03h:06m:55s

The following table describes the labels in this screen.

TABLE 7: The Cable > System Info Screen

General Information	
Vendor Identification	This displays the name of the company that supplied the CGNV2.
Model Name	This displays the device's model name (CGNV2).
DOCSIS Mode	This displays the version of the Data Over Cable Service Interface Specification (DOCSIS) standard to which the CGNV2 complies.
HW Version	This displays the version number of the CGNV2's physical hardware.
SW Version	This displays the version number of the software that controls the CGNV2.
Boot ROM Version	This displays the version number of the program that controls the CGNV2's boot procedure (in which the main software is loaded).
MAC Address	
RF MAC Address	This displays the Media Access Control (MAC) address of the CGNV2's RF module. This is the module that connects to the Internet through the **CATV** connection.
Ethernet MAC Address	This displays the Media Access Control (MAC) address of the CGNV2's Ethernet module. This is the module to which you connect through the **LAN** ports.
MTA MAC Address	This displays the Media Access Control (MAC) address of the CGNV2's **MTA** module.

TABLE 7: The Cable > System Info Screen (continued)

Primary BSSID MAC Address	This displays the Media Access Control (MAC) address of the CGNV2's Basic Service Set IDentifier (BSSID). This is the MAC address of the wireless module to which wireless clients connect. *NOTE:* You may have additional BSSIDs, depending on your contract with your service provider.
WAN MAC Address	This displays the Media Access Control (MAC) address of the module that connects to the Internet through the **CATV** connection when the CGNV2 is in routing mode.
System Time	This displays the current date and time.
Network Access	This field displays when you are connected to your service provider, and shows whether or not your service provider allows you to access the Internet over the **CATV** connection. ▶ **Permitted** displays if you can access the Internet. ▶ **Denied** displays if you cannot access the Internet.
System Uptime	This displays the number of days, hours, minutes and seconds since the CGNV2 was last switched on or rebooted.

2.3 THE INITIALIZATION SCREEN

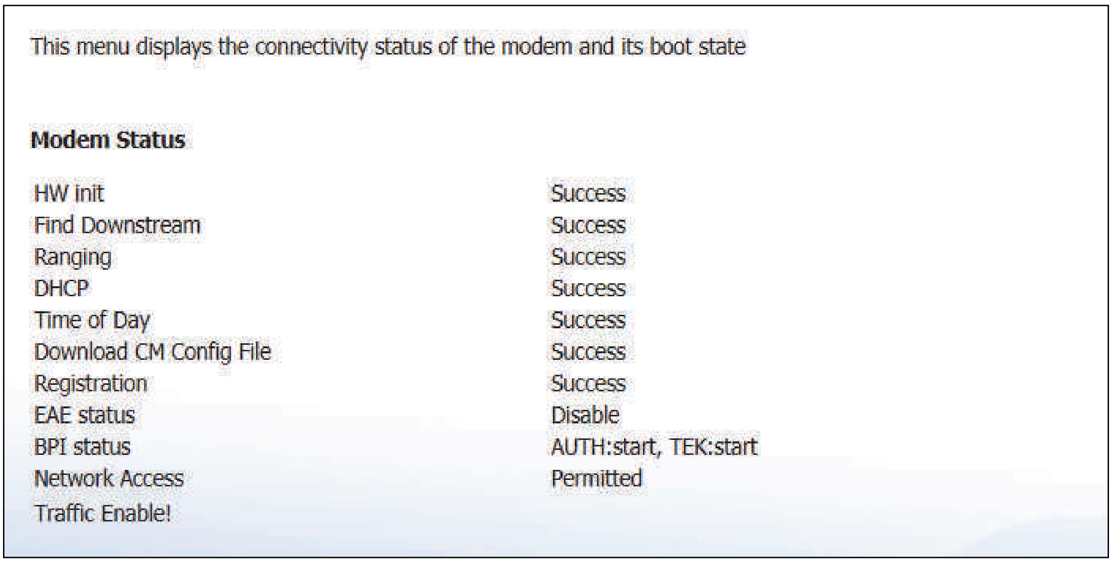
This screen displays the steps successfully taken to connect to the Internet over the **CATV** connection.

Use this screen for troubleshooting purposes to ensure that the CGNV2 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 CGNV2.

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

FIGURE 7: The Cable > 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 CGNV2 is attempting to complete a connection step.
- **Success** displays when the CGNV2 has completed a connection step.

2.4 THE STATUS SCREEN

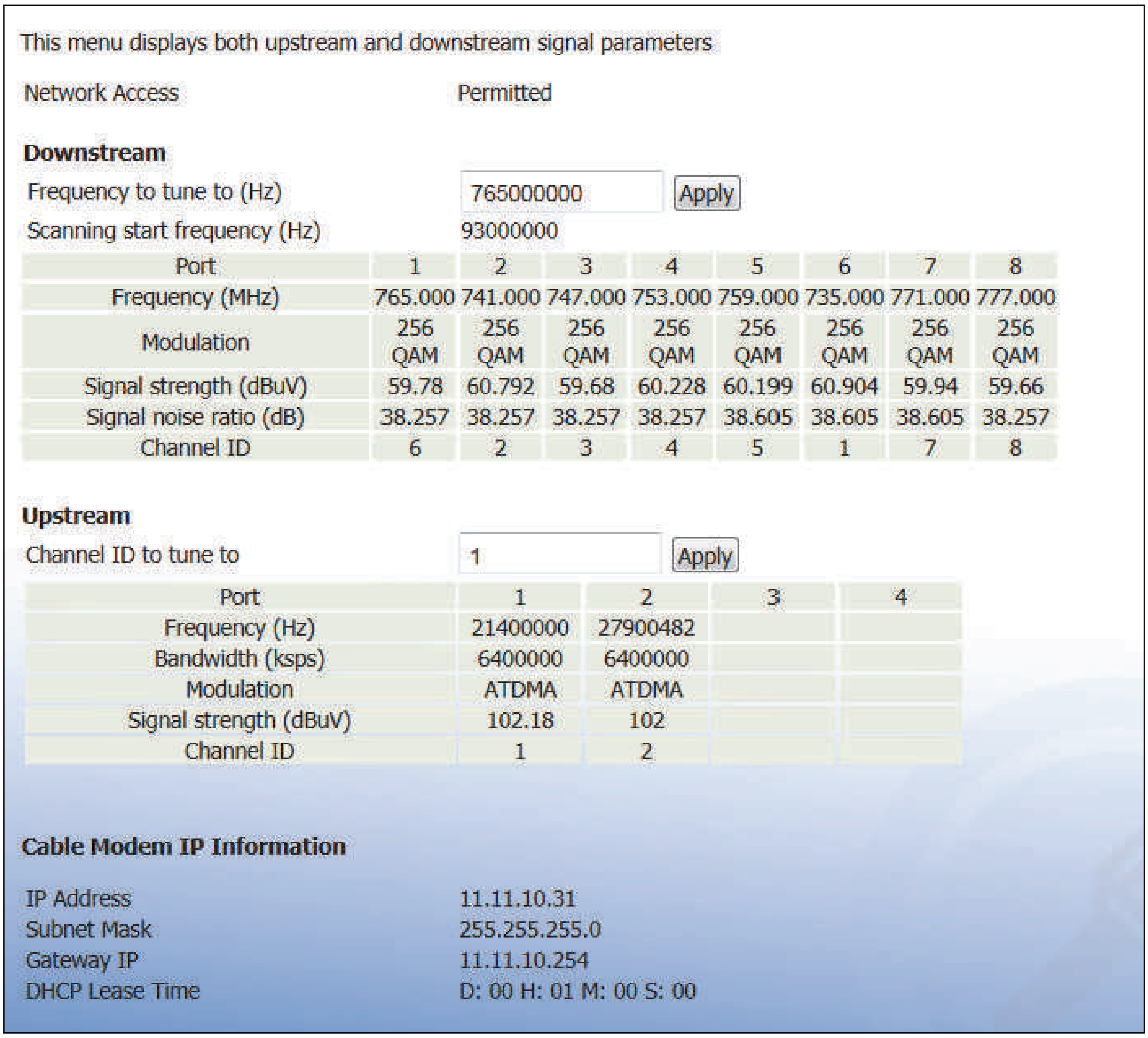
Use this screen to discover information about:

- The nature of the upstream and downstream connection between the CGNV2 and the device to which it is connected through the **CATV** interface.
- IP details of the CGNV2's WAN connection.

You can also configure the CGNV2's downstream center frequency.

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

FIGURE 8: The Cable > Status Screen



This menu displays both upstream and downstream signal parameters

Network Access Permitted

Downstream

Frequency to tune to (Hz) 765000000 Apply

Scanning start frequency (Hz) 93000000

Port	1	2	3	4	5	6	7	8
Frequency (MHz)	765.000	741.000	747.000	753.000	759.000	735.000	771.000	777.000
Modulation	256 QAM	256 QAM	256 QAM	256 QAM	256 QAM	256 QAM	256 QAM	256 QAM
Signal strength (dBuV)	59.78	60.792	59.68	60.228	60.199	60.904	59.94	59.66
Signal noise ratio (dB)	38.257	38.257	38.257	38.257	38.605	38.605	38.605	38.257
Channel ID	6	2	3	4	5	1	7	8

Upstream

Channel ID to tune to 1 Apply

Port	1	2	3	4
Frequency (Hz)	21400000	27900482		
Bandwidth (ksps)	6400000	6400000		
Modulation	ATDMA	ATDMA		
Signal strength (dBuV)	102.18	102		
Channel ID	1	2		

Cable Modem IP Information

IP Address	11.11.10.31
Subnet Mask	255.255.255.0
Gateway IP	11.11.10.254
DHCP Lease Time	D: 00 H: 01 M: 00 S: 00

The following table describes the labels in this screen.

TABLE 8: The Cable > Status Screen

Network Access	This displays whether or not your service provider allows you to access the Internet over the **CATV** connection. ▶ **Permitted** displays if you can access the Internet. ▶ **Denied** displays if you cannot access the Internet.
Downstream *NOTE:* The downstream signal is the signal transmitted to the CGNV2.	

TABLE 8: The Cable > Status Screen (continued)

Frequency to Tune to	This displays the current center frequency in Hertz (Hz) over which data is transmitted to the CGNV2 over the **CATV** interface. This is the frequency to which the CGNV2 is locked in; it will only scan for another frequency if this frequency becomes unavailable. If you want the CGNV2 to attempt to connect at a different frequency, enter it in the field and click **Apply**. *NOTE:* Do not change the frequency unless you have a good reason to do so.
Scanning Start Frequency	This displays the frequency in Hertz (Hz) at which the CGNV2 begins scanning for a connection over the **CATV** interface (if a frequency is not already locked in).
Port	This displays the number of the downstream connection's port.
Frequency (MHz)	This displays the actual frequency of each downstream data channel to which the CGNV2 is connected.
Modulation	This displays the type of modulation that each downstream channel uses. Possible modulation types
Signal Strength (dBmV)	This displays the power of the signal of each downstream data channel to which the CGNV2 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 CGNV2 is connected, in dB (decibels).
Channel ID	This displays the ID number of each channel on which the upstream signal is transmitted.
Upstream *NOTE:* The upstream signal is the signal transmitted from the CGNV2.	
Channel ID to tune to	This displays the current upstream channel ID over which data is transmitted from the CGNV2 over the **CATV** interface. If you want the CGNV2 to attempt to connect at a different channel ID, enter it in the field and click **Apply**. Do not change the channel ID unless you have a good reason to do so.
Port	This displays the number of the downstream connection's port.
Frequency (MHz)	This displays the frequency in Herz (Hz) of each upstream data channel to which the CGNV2 is connected.
Bandwidth (ksps)	This displays the bandwidth of each upstream data channel to which the CGNV2 is connected.

TABLE 8: The Cable > Status Screen (continued)

Modulation	This displays the type of modulation that each downstream channel uses. Possible modulation types
Signal Strength (dBuV)	This displays the transmitted power of the signal of each upstream data channel to which the CGNV2 is connected, in dBuV.
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 CGNV2's WAN IP address. This IP address is automatically assigned to the CGNV2
Subnet Mask	This displays the CGNV2's WAN subnet mask.
Gateway IP	This displays the gateway IP address of the device on the WAN to which the CGNV2 is connected.
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.

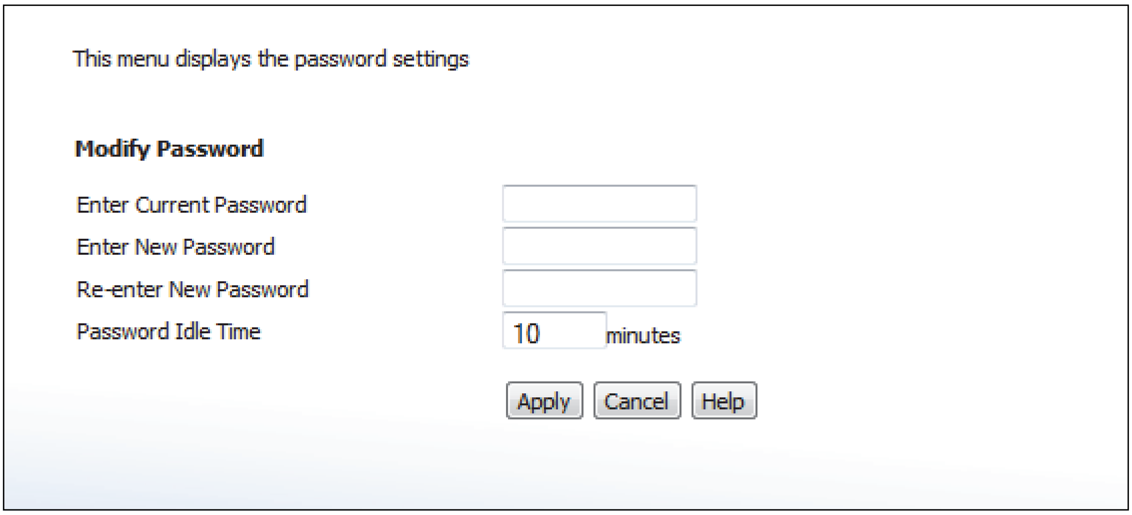
2.5 THE PASSWORD SCREEN

Use this screen to change the password with which you log in to the CGNV2.

NOTE: If you forget your password, you will need to reset the CGNV2 to its factory defaults.

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

FIGURE 9: The Cable > Password Screen



This menu displays the password settings

Modify Password

Enter Current Password
Enter New Password
Re-enter New Password
Password Idle Time 10 minutes

The following table describes the labels in this screen.

TABLE 9: The Cable > Password Screen

Enter Current Password	Enter the password with which you currently log into the CGNV2
Enter New Password	Enter and re-enter the password you want to use to log into the CGNV2.
Re-Enter New Password	
Password Idle Time	Enter the number of minutes of inactivity after which you should be automatically logged out of the CGNV2. Once this period elapses, you will need to login 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.

3

WAN/LAN

This chapter describes the screens that display when you click **WAN/LAN** in the toolbar.

3.1 WAN/LAN OVERVIEW

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

3.1.1 WIDE AREA NETWORKS AND LOCAL AREA NETWORKS

A Wide Area Network (WAN) is a network that has at least two parts separated by a distance requiring the use of a telecommunications infrastructure often supplied by a ISP.

A Local Area Network (LAN) is a network of computers that are physically linked together on a single site without the use of telephone lines of any sort. Your CGNV2's LAN consists of all the computers and other networking devices connected to the **LAN 1~2** ports. This is your private network (in routing mode - see Routing Mode on page 28).

The LAN is a separate network from the Wide Area Network (WAN). In the case of the CGNV2, the WAN refers to all computers and other devices available on the cable (**CATV**) connection.

By default, computers on the WAN cannot identify individual computers on the LAN; they can see only the CGNV2. The CGNV2 handles routing to and from individual computers on the LAN.

3.1.2 WAN/LAN IP ADDRESSES AND SUBNETS

IP addresses of the CGNV2 WAN/LAN are either controlled by the DHCP server (see DHCP on page 27), 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 25.

3.1.3 DNS

A DNS server is a server software program that performs Domain Name Services (DNS). This involves taking a full host name such as **www.example.com** or a domain name such as **example.com** and returning the corresponding Internet Protocol (IP) address such as 93.184.216.119.

3.1.4 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 (DNS). 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 CGNV2 allows you to define a **Domain Suffix** to the LAN. When you enter the domain suffix into your browser, you can reach the CGNV2 no matter what IP address it has on the LAN.

3.1.5 MTU

The maximum transmission unit (MTU) of a communications protocol of a layer is the size (in bytes) of the largest protocol data unit that the layer can pass onwards.

3.1.6 DEBUGGING (PING AND TRACEROUTE)

The CGNV2 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 CGNV2 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 LAN IP SCREEN

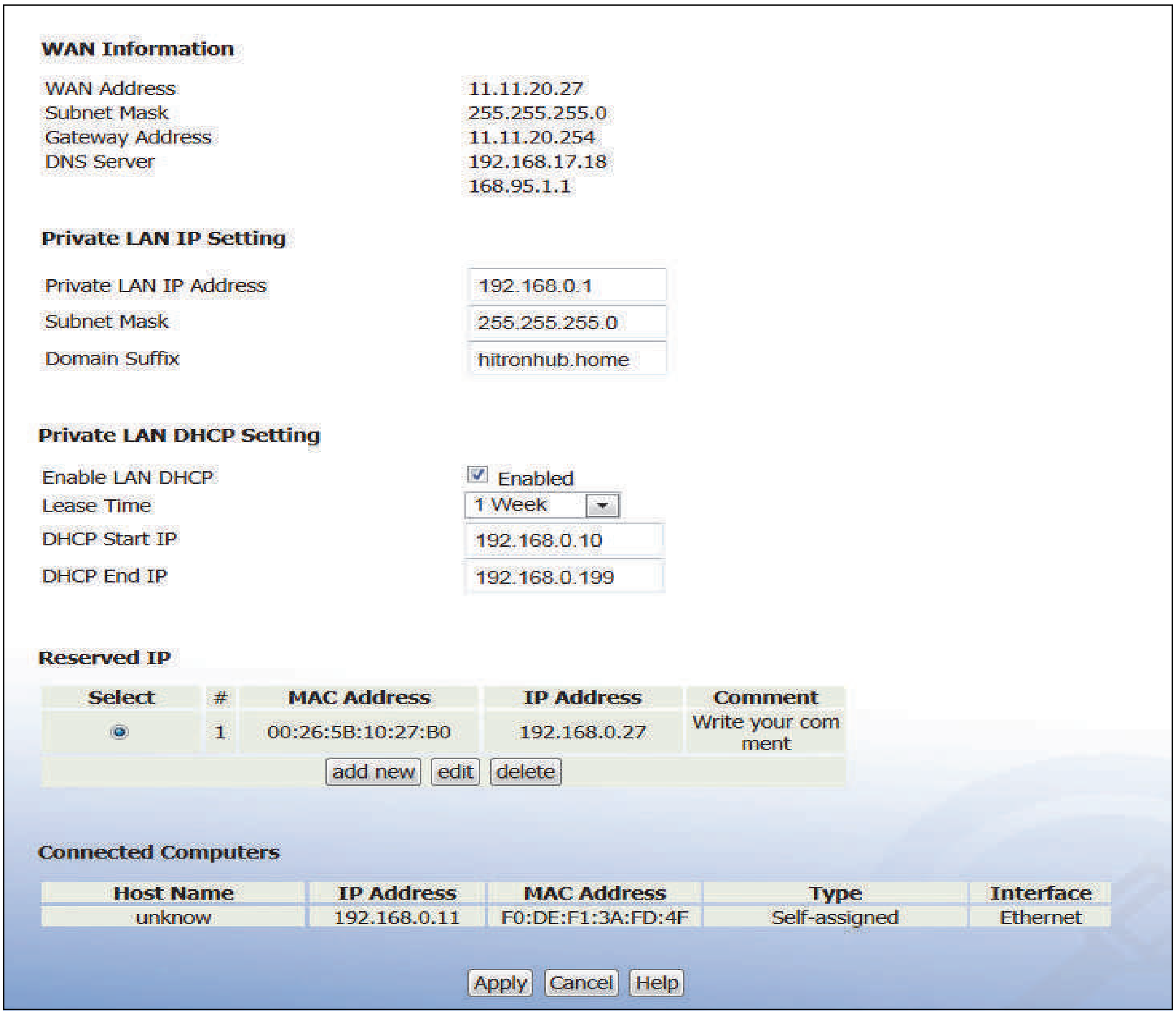
Use this screen to:

- Configure the CGNV2's LAN IP address, subnet mask and domain suffix
- Configure the CGNV2's internal DHCP server

- See information about the network devices connected to the CGNV2 on the LAN.

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

FIGURE 10: The WAN/LAN > LAN IP Screen



WAN Information

WAN Address	11.11.20.27
Subnet Mask	255.255.255.0
Gateway Address	11.11.20.254
DNS Server	192.168.17.18 168.95.1.1

Private LAN IP Setting

Private LAN IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Domain Suffix	hitronhub.home

Private LAN DHCP Setting

Enable LAN DHCP	☑ Enabled
Lease Time	1 Week
DHCP Start IP	192.168.0.10
DHCP End IP	192.168.0.199

Reserved IP

Select	#	MAC Address	IP Address	Comment
●	1	00:26:5B:10:27:B0	192.168.0.27	Write your com ment

Connected Computers

Host Name	IP Address	MAC Address	Type	Interface
unknow	192.168.0.11	F0:DE:F1:3A:FD:4F	Self-assigned	Ethernet

The following table describes the labels in this screen.

TABLE 10: The WAN/LAN > LAN IP Screen

WAN Information	
WAN Address	This field displays the CGNV2’s IP address on the WAN (Wide Area Network) interface.
Subnet Mask	This field displays the CGNV2’s WAN subnet mask.
Gateway Address	This field displays the address of the device on the WAN to which the CGNV2 is connected.
DNS Server	This field displays the Domain Name Servers that the CGNV2 uses to resolve domain names into IP addresses.
Private LAN IP Setting	
Private LAN IP Address	Use this field to define the IP address of the CGNV2 on the Private LAN.

TABLE 10: The WAN/LAN > LAN IP Screen (continued)

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 CGNV2 on the LAN. *NOTE:* The **Domain Suffix** is **hitronhub.home** by default.
Private LAN DHCP Setting	
Enable LAN DHCP	Select this if you want the CGNV2 to provide IP addresses to network devices on the LAN automatically. 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.
Lease Time	Use this field to define the time after which the CGNV2 renews the IP addresses of all the network devices connected to the CGNV2 on the LAN (when DHCP is enabled).
DHCP Start IP	Use this field to specify the IP address at which the CGNV2 begins assigning IP addresses to devices on the LAN (when DHCP is enabled).
DHCP End IP	Use this field to specify the IP address at which the CGNV2 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.
Reserved IP	
Select	Select a reserved IP's radio button before clicking **Edit** or **Delete**.
#	This displays the arbitrary identification number assigned to the reserved IP.
MAC Address	This displays the Media Access Control (MAC) address of network device connected on the LAN with a reserved IP.
IP Address	This displays the IP address of network device connected on the LAN with reserved IP.
Comment	This displays the comment entered while adding a reserved IP.
Add New	Click this to define a new reserved IP. See Adding or Editing a Reserved IP on page 43 for information on the screen that displays.
Edit	Select a reserved IP's radio button and click this to make changes. See Adding or Editing a Reserved IP on page 43 for information on the screen that displays.

TABLE 10: The WAN/LAN > LAN IP Screen (continued)

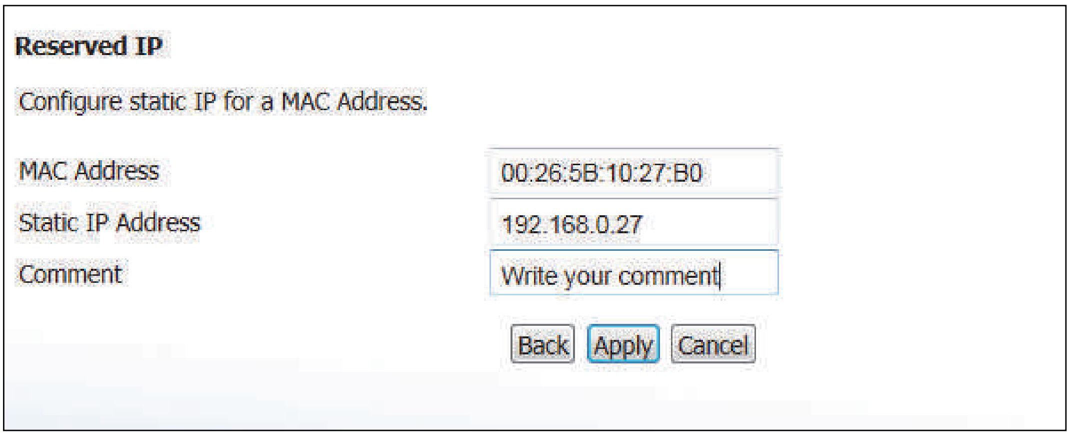
Delete	Select a reserved IP's radio button and click this to remove. The deleted information cannot be retrieved.
Connected Computers	
Host Name	This displays the name of each network device connected on the LAN.
IP Address	This displays the IP address of each network device connected on the LAN.
MAC 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.

3.2.1 ADDING OR EDITING A RESERVED IP

- To add a new reserved IP, click **Add New** in the **WAN/LAN** > **LAN IP** screen.
- To edit an existing reserved IP, select the IP's radio button in the **WAN/LAN** > **LAN IP** and click the **Edit** button.
- To delete an existing reserved IP, select the IP's radio button in the **WAN/LAN** > **LAN IP** and click the **Delete** button.

The following screen displays.

FIGURE 11: The WAN/LAN > LAN IP > Add/Edit Screen



Reserved IP

Configure static IP for a MAC Address.

MAC Address	00:26:5B:10:27:B0
Static IP Address	192.168.0.27
Comment	Write your comment

The following table describes the labels in this screen.

TABLE 11: The WAN/LAN > LAN IP > Add/Edit Screen

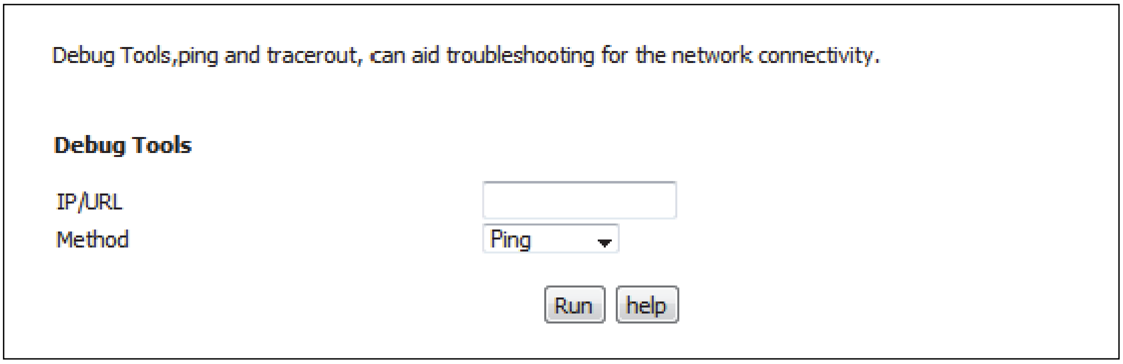
Reserved IP	
MAC Address	Use this field to enter the Media Access Control (MAC) address of the network device.
Static IP Address	Use this field to enter the static IP address.
Comment	Use this field to enter your comment.
Back	Click this to return to the previous screen without saving changes.
Apply	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.

3.3 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 12: The WAN/LAN > Debug Screen



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

Debug Tools

IP/URL

Method: Ping

The following table describes the labels in this screen.

TABLE 12: The WAN/LAN > Debug Screen

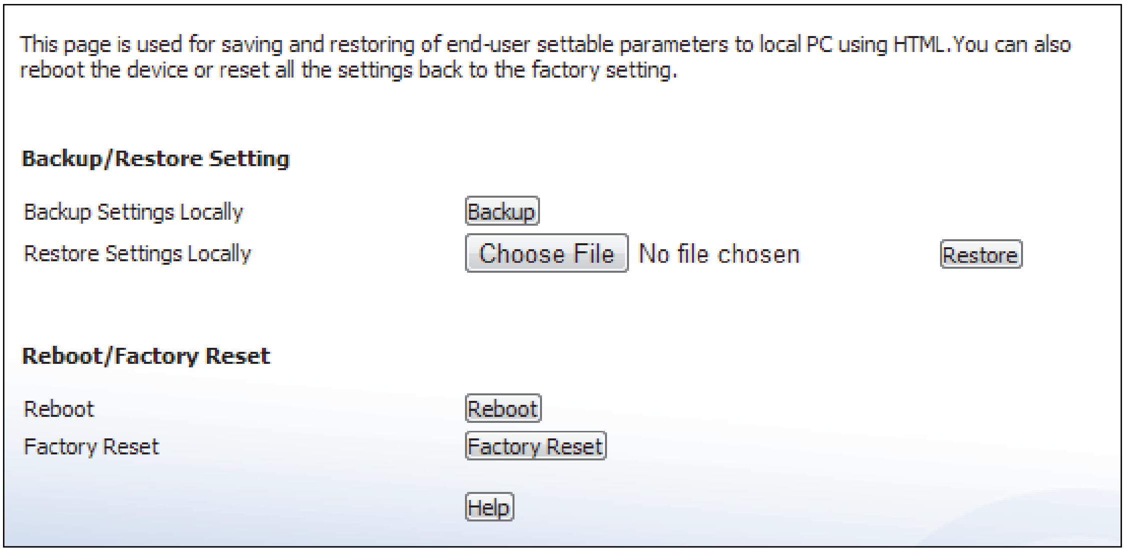
IP/URL	Enter the IP address or URL that you want to test.
Method	Select the type of test that you want to run on the **IP/URL** that you specified.
Run	Click this to perform the test.
Help	Click this to see information about the fields in this screen.

3.4 THE BACKUP SCREEN

Use this screen to back up your CGNV2's settings to your computer, to load settings from a backup you created earlier, to reboot your CGNV2, or to return it to its factory default settings.

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

FIGURE 13: The WAN/LAN > Backup Screen



This page is used for saving and restoring of end-user settable parameters to local PC using HTML.You can also reboot the device or reset all the settings back to the factory setting.

Backup/Restore Setting

Backup Settings Locally

Restore Settings Locally — No file chosen

Reboot/Factory Reset

Reboot

Factory Reset

The following table describes the labels in this screen.

TABLE 13: The WAN/LAN > Backup Screen

Backup/Restore Setting	
Backup Settings Locally	Click this to create a backup of all your CGNV2's settings on your computer.
Restore Settings Locally	Use these fields to return your CGNV2'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 CGNV2's settings to those specified in the backup.
Reboot/Factory Reset	
Reboot	Click this to restart your CGNV2.
Factory Reset	Click this to return your CGNV2 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.

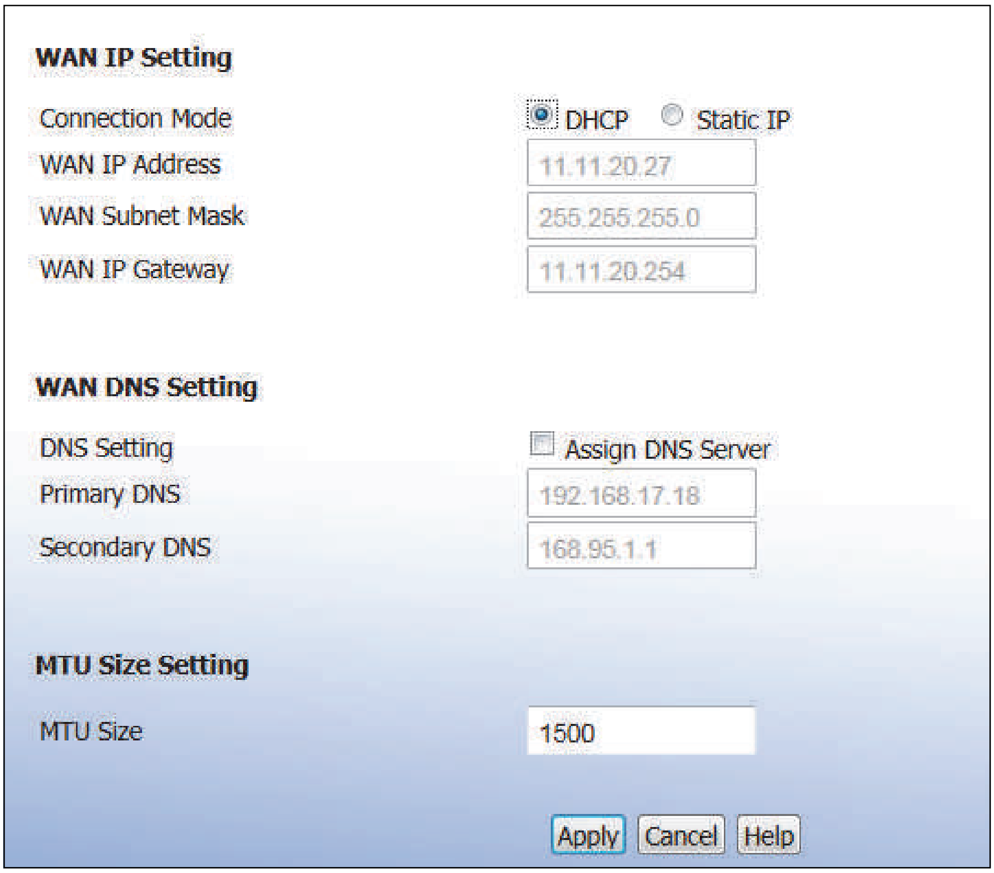
3.5 THE WAN IP SCREEN

Use this screen to:

- Configure the CGNV2's WAN IP address, subnet mask and domain suffix
- Configure the CGNV2's internal DNS server
- See the current MTU size of the CGNV2 on the WAN.

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

FIGURE 14: The WAN/LAN > WAN IP Screen



WAN IP Setting

Connection Mode	● DHCP ○ Static IP
WAN IP Address	11.11.20.27
WAN Subnet Mask	255.255.255.0
WAN IP Gateway	11.11.20.254

WAN DNS Setting

DNS Setting	□ Assign DNS Server
Primary DNS	192.168.17.18
Secondary DNS	168.95.1.1

MTU Size Setting

MTU Size	1500

The following table describes the labels in this screen.

TABLE 14: The WAN/LAN > WAN IP Screen

WAN IP Setting	
Connection Mode	Use this field to select the connection mode. ▸ Select **DHCP** to automatically get an IP address from DHCP server. ▸ Select **Static IP** to manually enter an IP address.
WAN IP Address	This displays the CGNV2's WAN IP address. If you select static IP mode, use this field to enter the static IP address.

TABLE 14: The WAN/LAN > WAN IP Screen (continued)

WAN Subnet Mask	This displays the CGNV2’s WAN subnet mask. If you select static IP mode, use this field to enter the subnet mask.
WAN IP Gateway	This displays the CGNV2’s WAN gateway IP address. If you select static IP mode, use this field to enter the gateway IP address.
WAN DNS Setting	
DNS Setting	Click the checkbox if you want to manually assign the DNS server.
Primary DNS	This displays the CGNV2’s WAN primary DNS. If you select assign DNS server, use this field to enter the primary DNS IP address.
Secondary DNS	This displays the CGNV2’s WAN secondary DNS. If you select assign DNS server, use this field to enter the secondary DNS IP address.
MTU Size Setting	
MTU Size	This displays the current maximum transmission unit size (**MTU**) or use this field to enter the desired MTU size and click **Apply**.
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 FIREWALL

This chapter describes the screens that display when you click **Firewall** in the toolbar.

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 CGNV2’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.

4.1.3 PING

The CGNV2 allows you to use the ping utility on the LAN (in the **LAN** > **Debug** screen) and also on the WAN (in the **Firewall** > **Firewall Options** screen). For more information, see Debugging (Ping and Traceroute) on page 40.

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 CGNV2’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 CGNV2 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 CGNV2 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 CGNV2 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.

NOTE: This feature is not available when the DS-lite function is enabled.

4.1.7 PORT TRIGGERING

Port triggering is a means of automating port forwarding. The CGNV2 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 CGNV2 automatically opens the incoming ports specified in the rule, in anticipation of incoming traffic.

NOTE: This feature is not available when the DS-lite function is enabled.

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.

NOTE: This feature is not available when the DS-lite function is enabled.

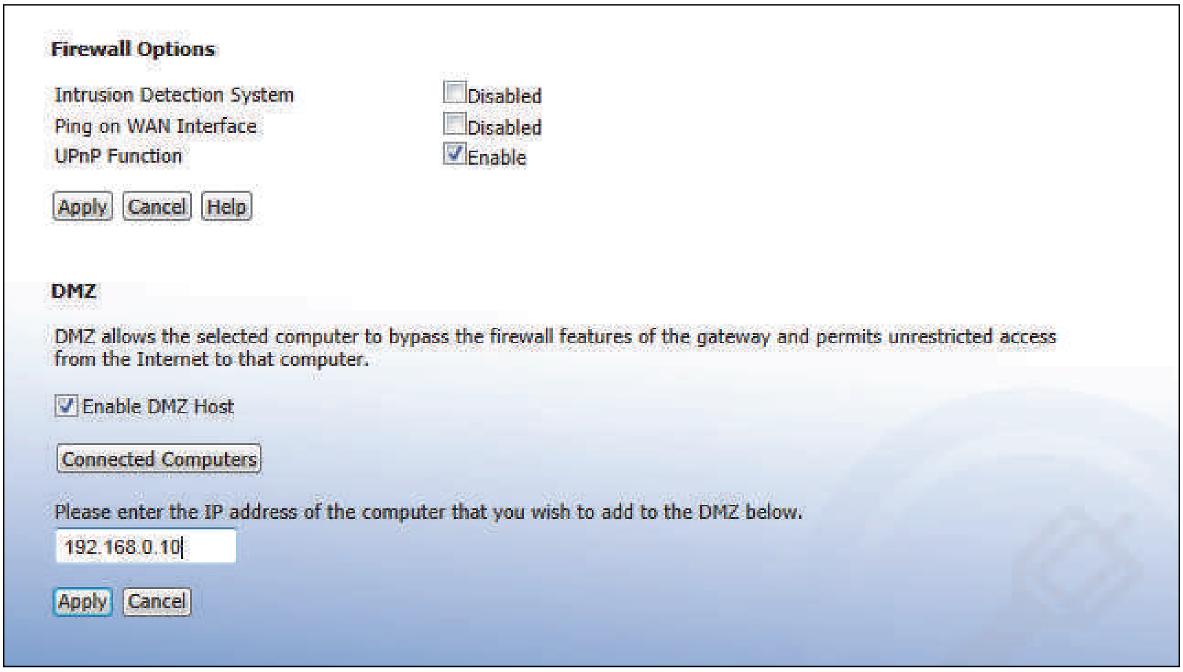
4.2 THE FIREWALL OPTIONS SCREEN

Use this screen to turn firewall features on or off, and to configure your network's Demilitarized Zone (DMZ). You can enable or disable the CGNV2's intrusion detection system, and allow or prevent responses to ICMP requests from the WAN.

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

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

FIGURE 15: The Firewall > Firewall Options Screen



Firewall Options

Intrusion Detection System ☐ Disabled
Ping on WAN Interface ☐ Disabled
UPnP Function ☑ Enable

DMZ

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

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

192.168.0.10

The following table describes the labels in this screen.

TABLE 15: The Firewall > Firewall Options Screen

Intrusion Detection System	- **Select** Disable to turn the intrusion detection system off. - **Deselect** Disable to turn the intrusion detection system on.
Ping on WAN Interface	- **Select** Disable to prevent responses to ICMP requests originating from the WAN. - **Deselect** Disable to allow responses to ICMP requests originating from the WAN.
UPnP Function	- **Select** Enable to turn the UPnP Function on . - **Deselect** Enable to turn the UPnP Function off.
Enable DMZ Host	Use this field to turn the DMZ on or off. - **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 CGNV2 on the LAN.
[...] 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.

4.3 THE MAC FILTERING SCREEN

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

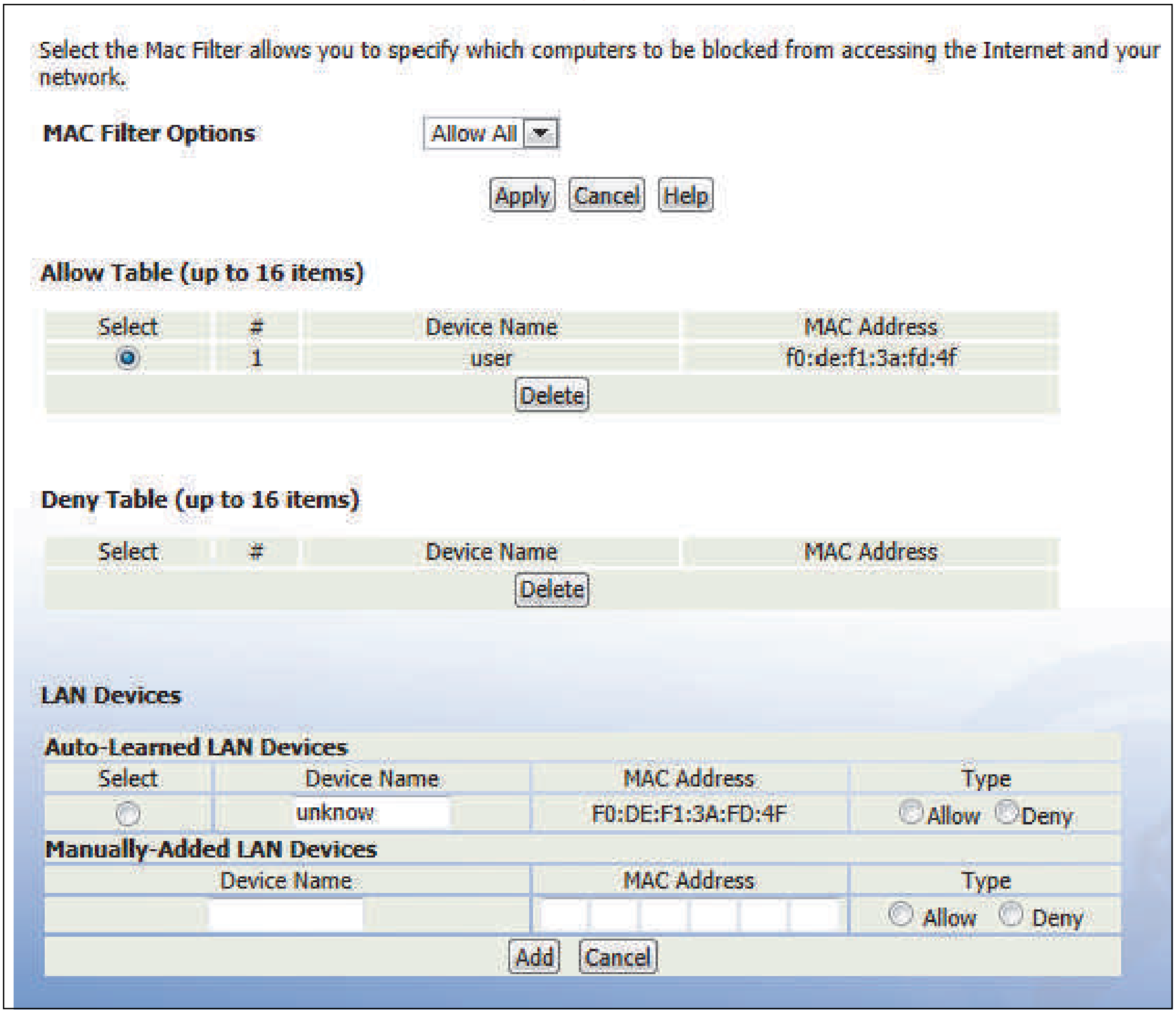
NOTE: To configure MAC address filtering on the wireless network, see The Access Control Screen on page 86.

You can set the CGNV2 to allow only certain devices to access the CGNV2 and the network, or to deny certain devices access.

NOTE: To see a list of all the computers connected to the CGNV2 on the LAN, click the **Connected Computers** button in the **Firewall** > **IP Filtering**, **Forwarding**, **Port Triggering** or **Firewall Options** screens.

Click **Firewall** > **MAC Filtering**. The following screen displays.

FIGURE 16: The Firewall > MAC Filtering Screen



Select the Mac Filter allows you to specify which computers to be blocked from accessing the Internet and your network.

MAC Filter Options Allow All

Allow Table (up to 16 items)

Select	#	Device Name	MAC Address
●	1	user	f0:de:f1:3a:fd:4f

Deny Table (up to 16 items)

Select	#	Device Name	MAC Address

LAN Devices

Auto-Learned LAN Devices

Select	Device Name	MAC Address	Type
○	unknow	F0:DE:F1:3A:FD:4F	○ Allow ○ Deny

Manually-Added LAN Devices

Device Name	MAC Address	Type
		○ Allow ○ Deny

The following table describes the labels in this screen.

TABLE 16: The Firewall > MAC Filtering Screen

MAC Filter Options	
MAC Filter Options	Use this field to control whether the CGNV2 performs MAC filtering. ▶ Select **Allow-All** to turn MAC filtering off. All devices may access the CGNV2 and the network. ▶ Select **Allow** to permit only devices with the MAC addresses you set up in the **Allow Table** to access the CGNV2 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 CGNV2 and the network. The specified devices are denied access.
Allow Table (up to 16 Items)	
Select	Select a MAC address's radio button before clicking **Delete**.
#	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	Select a permitted device's radio button (◉) and click this to remove the device from the list. The device may no longer access the CGNV2 and the network. *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 CGNV2.
Deny Table (up to 16 Items)	
Select	Select a MAC address's radio button before clicking **Delete**.
#	This displays the index number assigned to the permitted 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	Select a denied device's radio button (◉) and click this to remove the device from the list. The device may now access the CGNV2 and the network.
Auto-Learned LAN Devices	
Select	Select a MAC address's radio button before clicking **Add** or **Cancel**.

TABLE 16: The Firewall > MAC Filtering Screen (continued)

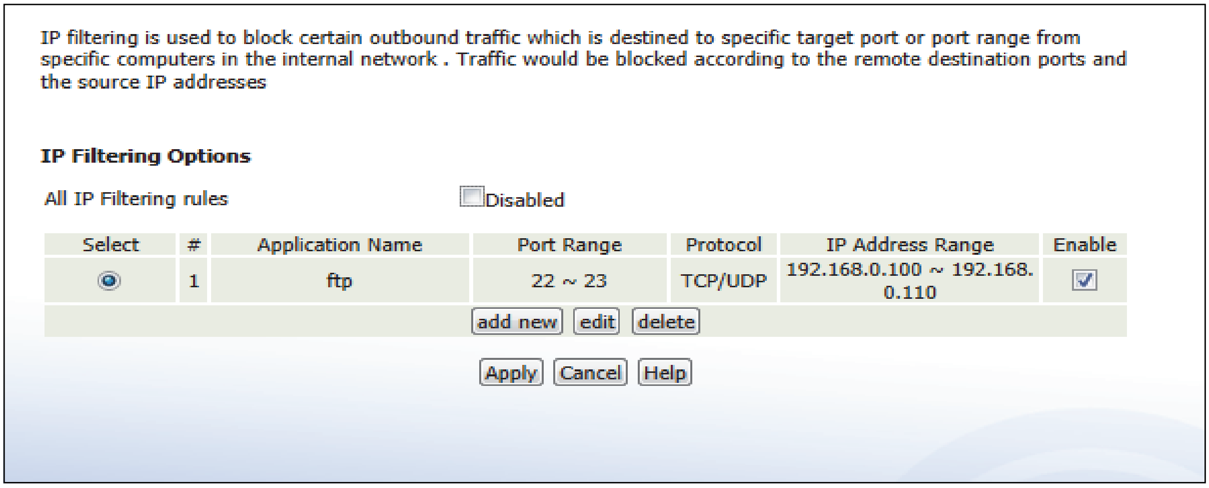
Device Name	This displays the name of each network device that has connected to the CGNV2 on the LAN.
MAC Address	This displays the MAC address of each network device that has connected to the CGNV2 on the LAN.
Type	Use this field to specify the list to which you want to add the device. - Select **Allow** 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 CGNV2 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 CGNV2 and the network.
Type	Use this field to specify the list to which you want to add the device. - 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 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.

4.4 THE IP FILTERING SCREEN

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

Click **Firewall** > **IP Filtering**. The following screen displays.

FIGURE 17: The Firewall > IP Filtering Screen



IP filtering is used to block certain outbound traffic which is destined to specific target port or port range from specific computers in the internal network . Traffic would be blocked according to the remote destination ports and the source IP addresses

IP Filtering Options

All IP Filtering rules □Disabled

Select	#	Application Name	Port Range	Protocol	IP Address Range	Enable
●	1	ftp	22 ~ 23	TCP/UDP	192.168.0.100 ~ 192.168.0.110	☑

The following table describes the labels in this screen.

TABLE 17: The Firewall > IP Filtering Screen

All IP Filtering Rules	Use this to turn IP filtering on or off. - **Deselect** the checkbox to enable IP filtering. - **Select** the checkbox to disable IP filtering (default). *NOTE:* You can add, edit or delete IP filtering rules only when this checkbox is deselected.
Select	Select an IP filtering rule's radio button (◉) before clicking **Add New**, **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	This displays the type of communications that are not permitted: - **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.

TABLE 17: The Firewall > IP Filtering Screen (continued)

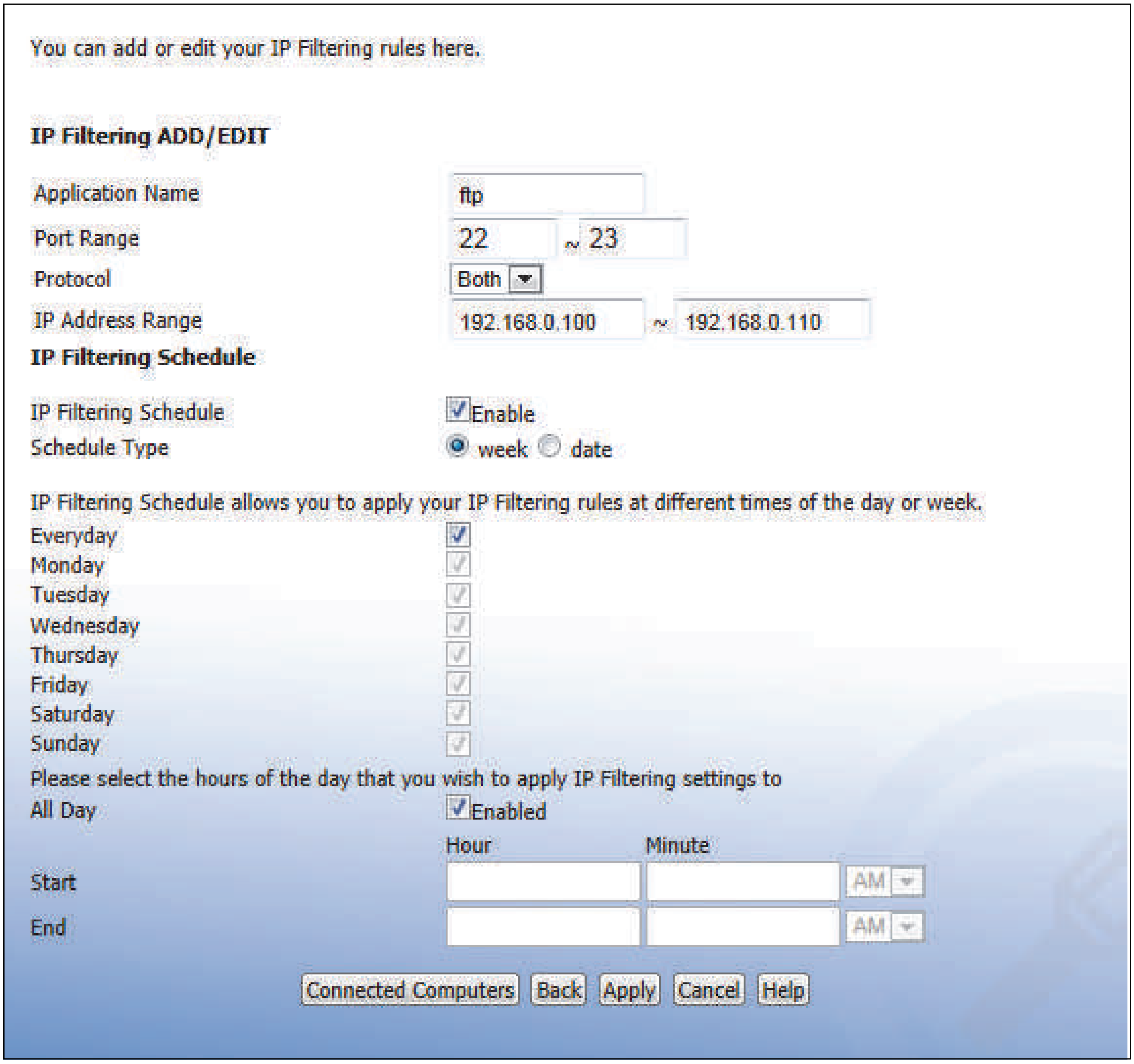
Enable	Use this field to turn each IP filtering rule on or off. - **Select** this checkbox to enable the IP filtering rule. - **Deselect** this checkbox to disable the IP filtering rule.
Add New	Click this to define a new IP filtering rule. See Adding or Editing an IP Filtering Rule on page 57 for information on the screen that displays.
Edit	Select an IP filtering rule's radio button (◉) and click this to make changes to the rule. See Adding or Editing an IP Filtering Rule on page 57 for information on the screen that displays.
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 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.

4.4.1 ADDING OR EDITING AN IP FILTERING RULE

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

The following screen displays.

FIGURE 18: The Firewall > IP Filtering > Add/Edit Screen



You can add or edit your IP Filtering rules here.

IP Filtering ADD/EDIT

Application Name	ftp
Port Range	22 ~ 23
Protocol	Both
IP Address Range	192.168.0.100 ~ 192.168.0.110

IP Filtering Schedule

IP Filtering Schedule	☑ Enable
Schedule Type	● week ○ date

IP Filtering Schedule allows you to apply your IP Filtering rules at different times of the day or week.

Everyday	☑
Monday	☑
Tuesday	☑
Wednesday	☑
Thursday	☑
Friday	☑
Saturday	☑
Sunday	☑

Please select the hours of the day that you wish to apply IP Filtering settings to

All Day	☑ Enabled		
	Hour	Minute	
Start			AM
End			AM

The following table describes the labels in this screen.

TABLE 18: The Firewall > IP Filtering > Add/Edit Screen

IP Filtering Add/Edit	
Application Name	Enter a name for the application that you want to block. *NOTE:* This name is arbitrary, and does not affect functionality in any way.
Port Range	Use these fields to specify the target port range to which communication should be blocked. Enter the start port number in the first field, and the end port number in the second field. To specify only a single port, enter its number in both fields.

TABLE 18: The Firewall > IP Filtering > Add/Edit Screen

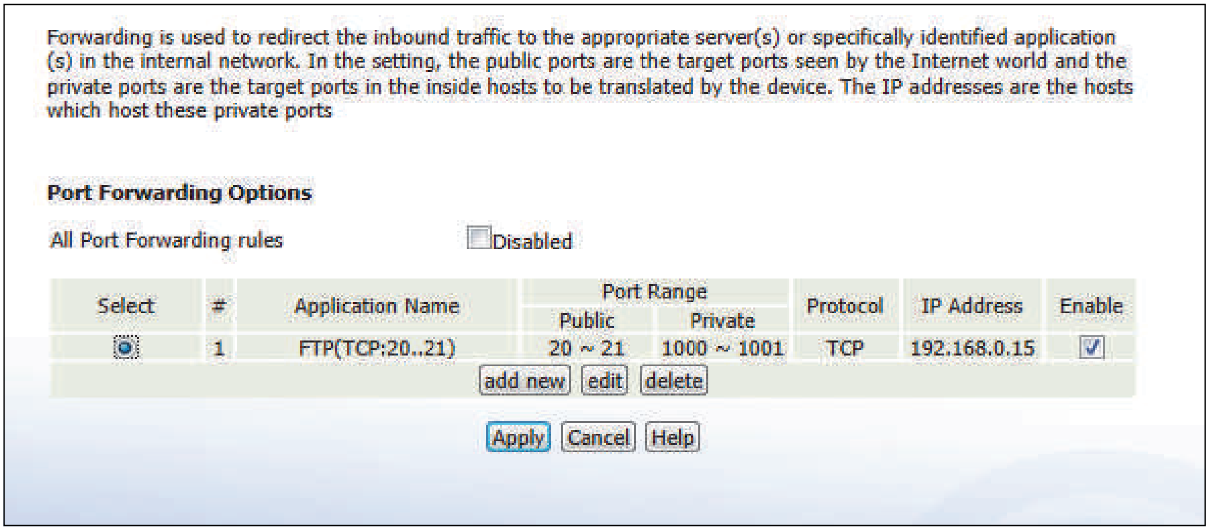
Protocol	Use this field to specify whether the CGNV2 should block communication via: - Transmission Control Protocol (**TCP**) - User Datagram Protocol (**UDP**) - **Both** TCP and UDP. *NOTE:* If in doubt, leave this field at its default (**Both**).
IP Address Range	Use these fields to specify the range of local computers’ IP addresses from which communications should be blocked. Enter the start IP address in the first field, and the end IP address in the second. To specify only a single IP address, enter it in both fields.
IP Filtering Schedule	
IP Filtering Schedule	
Schedule Type	
All Day	
Start	
End	
Connected Computers	Click this to see a list of the computers currently connected to the CGNV2 on the LAN.
Back	Click this to return to the **Firewall** > **IP filtering** screen without saving your changes to the IP filtering rule.
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 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 19: 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			
◉	1	FTP(TCP:20..21)	20 ~ 21	1000 ~ 1001	TCP	192.168.0.15	☑

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. - Select the checkbox to enable port forwarding. - Deselect the checkbox to disable port forwarding.
Select	Select a port forwarding rule's radio button (◉) 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.
Port Range	These fields display the ports to which the rule applies: - The **Public** field displays the incoming port range. These are the ports on which the CGNV2 received traffic from the originating host on the WAN. - The **Private** field displays the port range to which the CGNV2 forwards traffic to the device on the LAN.
Protocol	This field displays the protocol or protocols to which this rule applies: - 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	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.

TABLE 19: The Firewall > Forwarding Screen (continued)

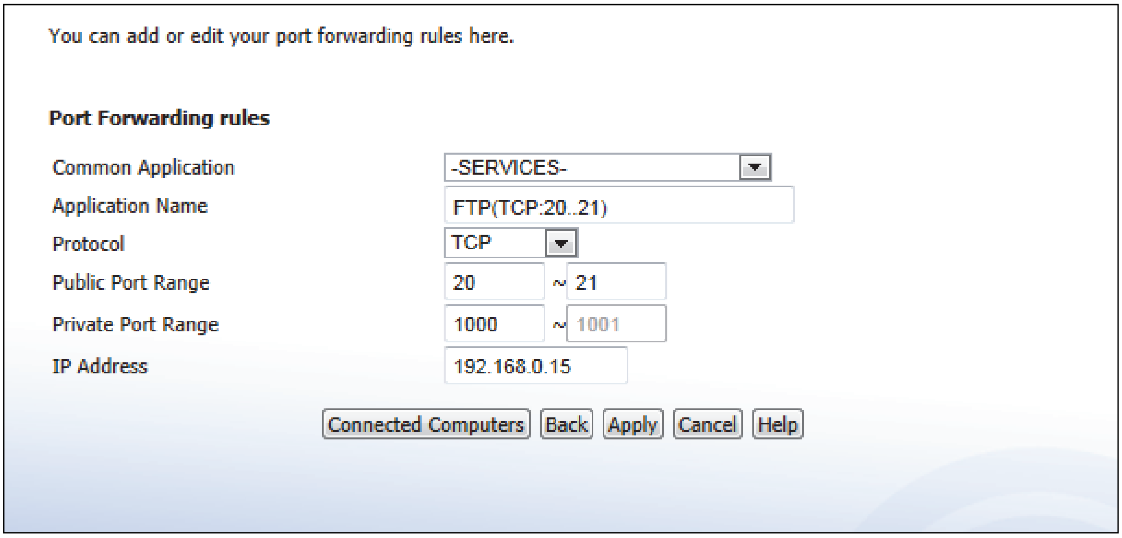
Enable	Use this field to turn each port forwarding rule on or off. - Select this checkbox to enable the port forwarding rule. - Deselect this checkbox to disable the port forwarding rule.
Add New	Click this to define a new port forwarding rule. See Adding or Editing a Port Forwarding Rule on page 61 for information on the screen that displays.
Edit	Select a port forwarding rule's radio button (◉) and click this to make changes to the rule. See Adding or Editing a Port Forwarding Rule on page 61 for information on the screen that displays.
Delete	Select a port forwarding 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 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 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.

The following screen displays.

FIGURE 20: The Firewall > Forwarding > Add/Edit Screen



You can add or edit your port forwarding rules here.

Port Forwarding rules

Common Application	-SERVICES-
Application Name	FTP(TCP:20..21)
Protocol	TCP
Public Port Range	20 ~ 21
Private Port Range	1000 ~ 1001
IP Address	192.168.0.15

The following table describes the labels in this screen.

TABLE 20: The Firewall > Forwarding > Add/Edit Screen

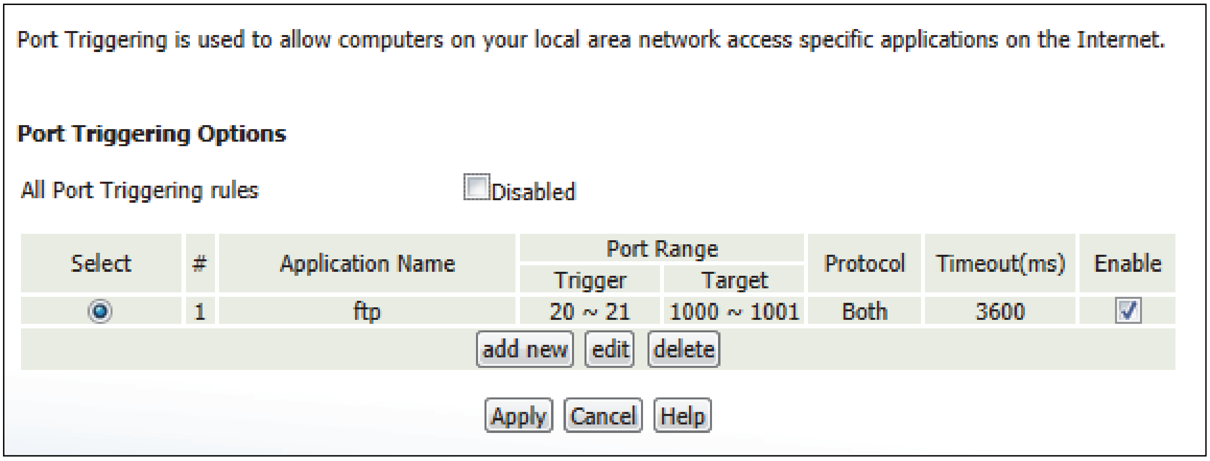
Common Application	
Application Name	Enter a name for the application for which you want to create the rule. *NOTE:* This name is arbitrary, and does not affect functionality in any way.
Public Port Range	Use these fields to specify the incoming port range. These are the ports on which the CGNV2 received traffic from the originating host on the WAN. Enter the start port number in the first field, and the end port number in the second field. To specify only a single port, enter its number in both fields.
Private Port Range	Use these fields to specify the ports to which the received traffic should be forwarded. Enter the start port number in the first field. The number of ports must match that specified in the **Public Port Range**, so the CGNV2 completes the second field automatically.
Protocol	Use this field to specify whether the CGNV2 should forward traffic via: - 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**) *NOTE:* If in doubt, leave this field at its default (**TCP/UDP**).
IP Address	Use this field to enter the IP address of the computer on the LAN to which you want to forward the traffic.
Connected Computers	Click this to see a list of the computers currently connected to the CGNV2 on the LAN.
Back	Click this to return to the **Firewall** > **Forwarding** screen without saving your changes to the port forwarding rule.
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.

4.6 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 21: 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			
●	1	ftp	20 ~ 21	1000 ~ 1001	Both	3600	☑

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. - Select the checkbox to enable port triggering. - Deselect the checkbox to disable port triggering.
Select	Select a port triggering rule's radio button (●) before clicking **Edit** or **Delete**.
#	This displays the arbitrary identification number assigned to the port triggering rule.
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: - The **Trigger** field displays the range of outgoing ports. When the CGNV2 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 CGNV2 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 CGNV2 opens the **Target** ports that it should close them.

TABLE 21: The Firewall > Port Triggering Screen

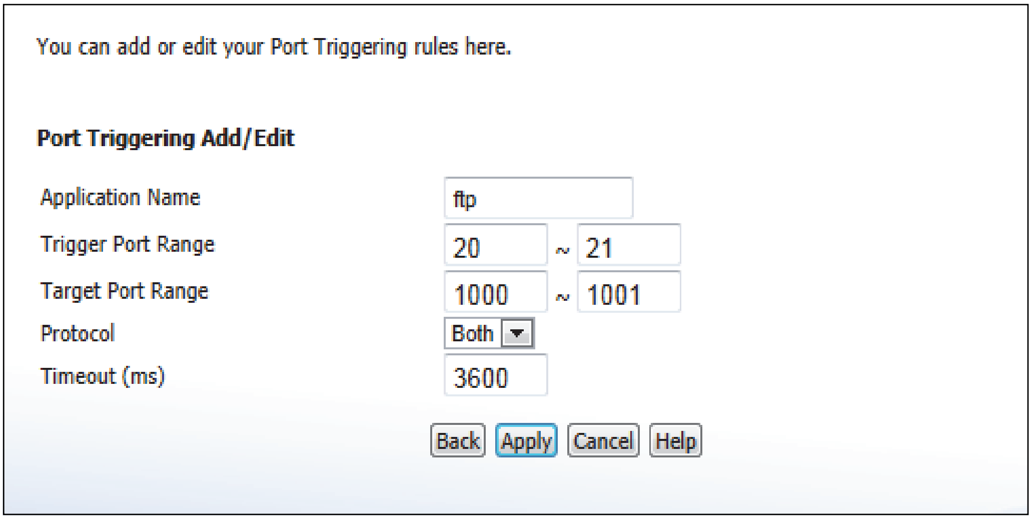
Enable	Use this field to turn each port triggering rule on or off. ▶ Select this checkbox to enable the port triggering rule. ▶ Deselect this checkbox to disable the port triggering rule.
Add New	Click this to define a new port triggering rule. See Adding or Editing a Port Triggering Rule on page 64 for information on the screen that displays.
Edit	Select a port triggering rule's radio button (◉) and click this to make changes to the rule. See Adding or Editing a Port Triggering Rule on page 64 for information on the screen that displays.
Delete	Select a port triggering 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 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.

4.6.1 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 22: The Firewall > Port Triggering > Add/Edit Screen



You can add or edit your Port Triggering rules here.

Port Triggering Add/Edit

Application Name	ftp
Trigger Port Range	20 ~ 21
Target Port Range	1000 ~ 1001
Protocol	Both ▾
Timeout (ms)	3600

The following table describes the labels in this screen.

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

Application Name	Enter a name for the application for which you want to create the rule. *NOTE:* This name is arbitrary, and does not affect functionality in any way.
Trigger Port Range	Use these fields to specify the trigger ports. When the CGNV2 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. Enter the start port number in the first field, and the end port number in the second field. To specify only a single port, enter its number in both fields.
Target Port Range	Use these fields to specify the target ports. The CGNV2 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. Enter the start port number in the first field, and the end port number in the second field. To specify only a single port, enter its number in both fields.
Protocol	Use this field to specify whether the CGNV2 should activate this trigger when it detects activity via: ▸ Transmission Control Protocol (**TCP**) ▸ User Datagram Protocol (**UDP**) ▸ Transmission Control Protocol and User Datagram Protocol (**Both**) *NOTE:* If in doubt, leave this field at its default (**Both**).
Timeout (ms)	Enter the time (in milliseconds) after the CGNV2 opens the **Target** ports that it should close them.
Connected Computers	Click this to see a list of the computers currently connected to the CGNV2 on the LAN.
Back	Click this to return to the **Firewall** > **Forwarding** screen without saving your changes to the port forwarding rule.
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.

5.1 PARENTAL CONTROL OVERVIEW

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

5.1.1 WEBSITE BLOCKING

The **Parent 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).

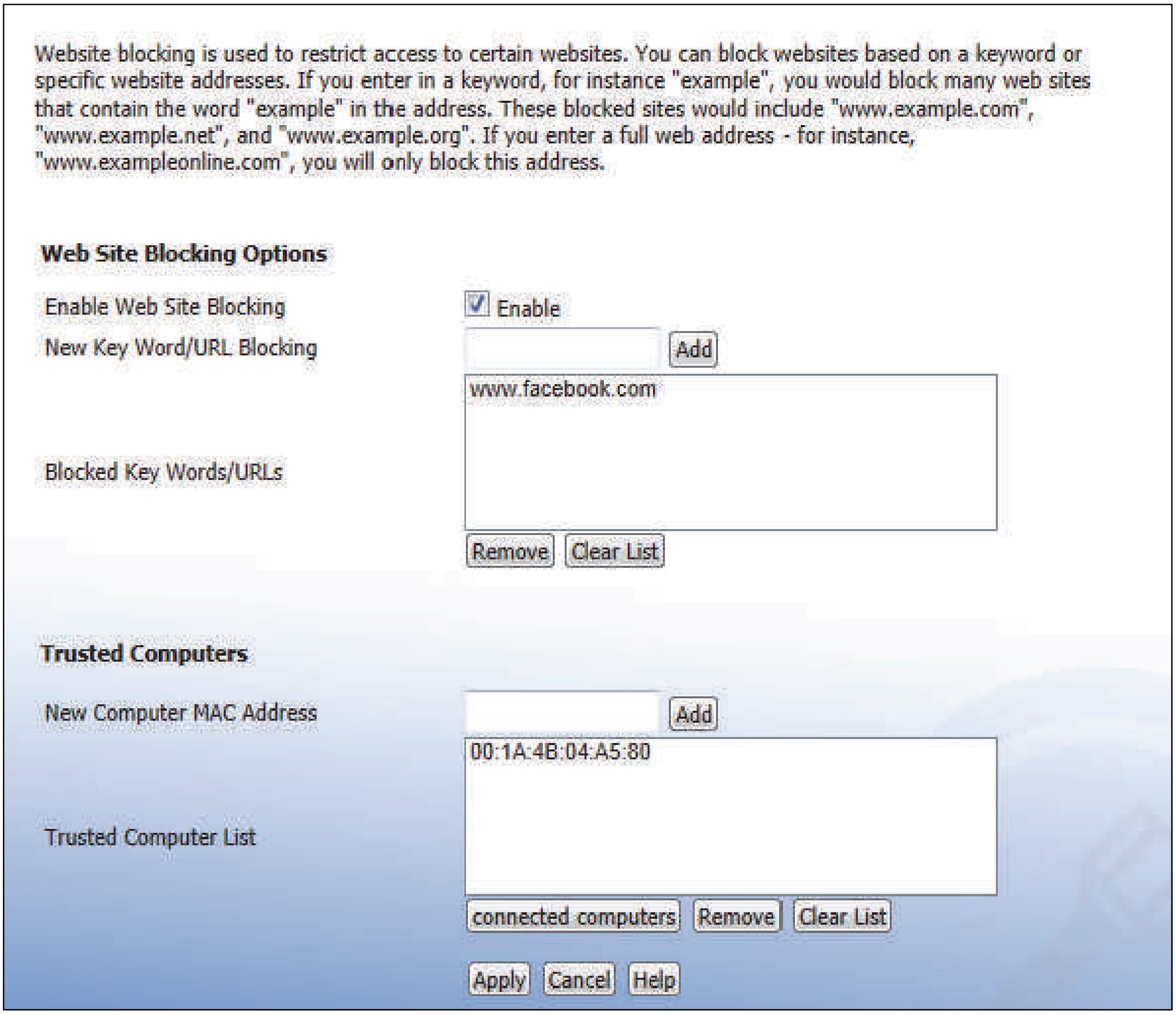
5.2 THE WEB SITE BLOCKING SCREEN

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 **Parent Control** > **Scheduling** screen.

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

FIGURE 23: The Parent 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 many web sites 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 ☑ Enable

New Key Word/URL Blocking [ ] Add

Blocked Key Words/URLs: www.facebook.com

Remove Clear List

Trusted Computers

New Computer MAC Address [ ] Add

Trusted Computer List: 00:1A:4B:04:A5:80

connected computers Remove Clear List

Apply Cancel Help

The following table describes the labels in this screen.

TABLE 23: The Parent Control > Web Site Blocking Screen

Web Site Blocking Options	
Enable Web Site Blocking	Use this field to turn web site blocking on or off. ▶ **Select** the checkbox to enable web site blocking. ▶ **Deselect** the checkbox to disable web site blocking.
New Key Word/URL Blocking	Use these fields to configure the websites to which users on the LAN are denied access: ▶ 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). Click **Add** to add the URL or keyword to the **Blocked Key Words/URLs** list.

TABLE 23: The Parent Control > Web Site Blocking Screen (continued)

Blocked Key Words/ URLs	This displays the list of websites and keywords to which users on the LAN are denied access. ▸ 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	Enter a computer's Media Access Control (MAC) address and click **Add** to include it in the trusted computer list.
Trusted Computer List	This displays a list of the computers which are exempt from the website blocking filter, identified by their MAC addresses.
Connected Computers	Click this to see a list of the computers that are currently connected to the CGNV2.
Remove	Select a computer's MAC address from the **Connected Computers** list and click this to delete it from the list.
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.

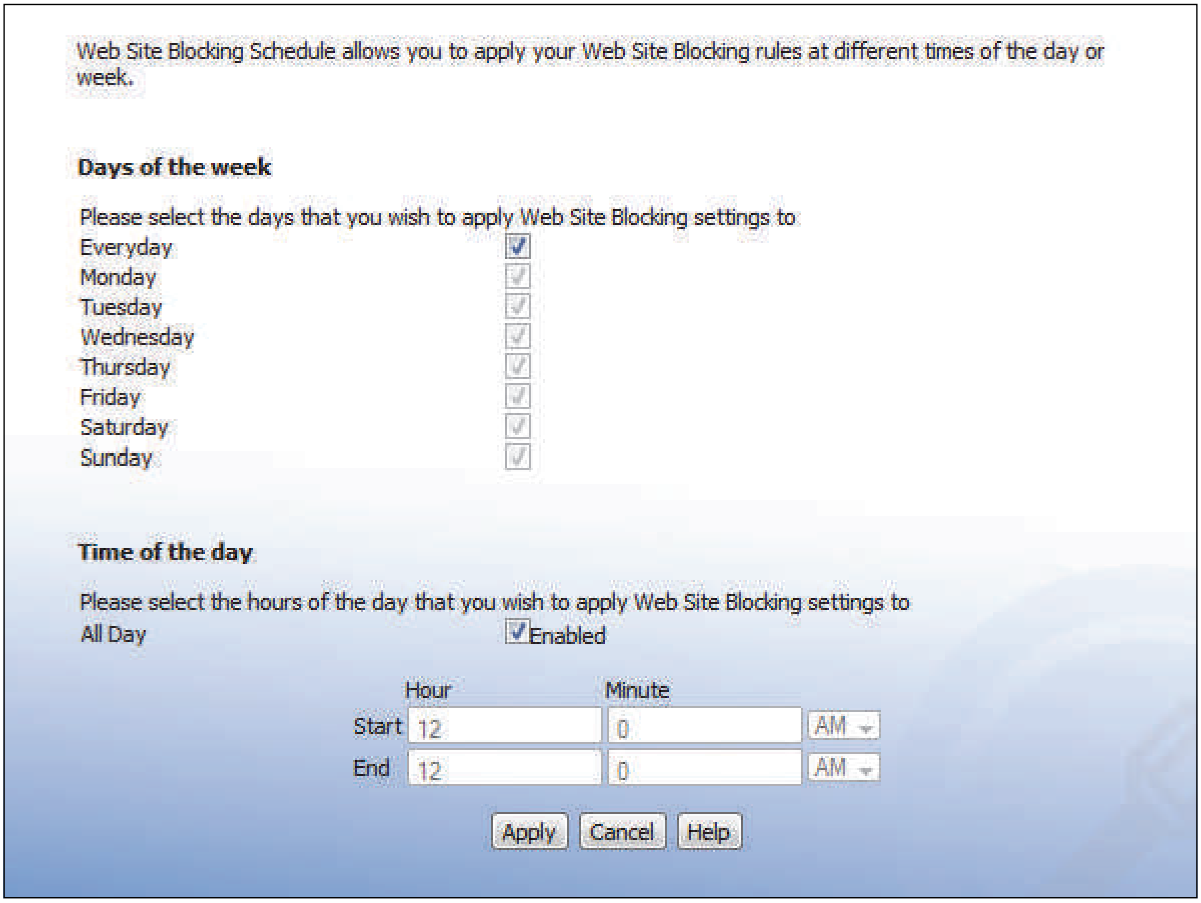
5.3 THE SCHEDULING SCREEN

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 Parent Control > Scheduling Screen



Web Site Blocking Schedule allows you to apply your Web Site Blocking rules at different times of the day or week.

Days of the week

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

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

The following table describes the labels in this screen.

TABLE 24: The Parent Control > Scheduling Screen

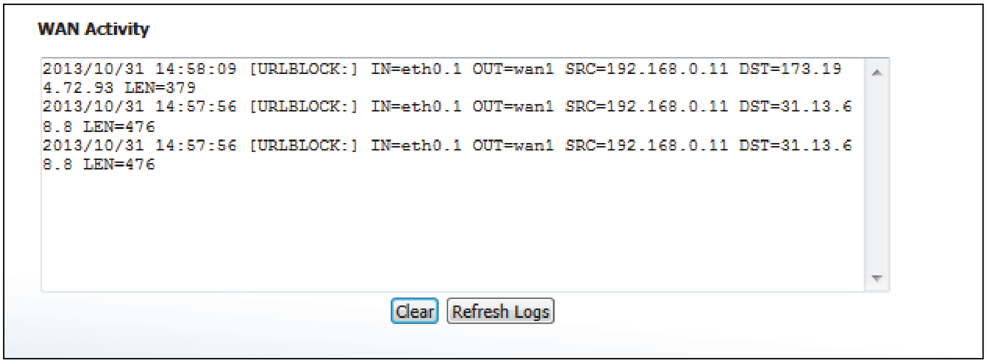
Days of the Week	Select the days of the week on which you want the website blocking filter to be in effect.
Time of the Day	Use these fields to control the time that the website blocking filter should be in effect: ▸ Select **All Day** to apply the website blocking filter at all times. ▸ To apply the 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.
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 LOCAL LOGS SCREEN

Use this screen to see information about events that have triggered the website blocking filter.

Click **Parent Control** > **Local Logs**. The following screen displays.

FIGURE 25: The Parent Control > Local Logs Screen



```
2013/10/31 14:58:09 [URLBLOCK:] IN=eth0.1 OUT=wan1 SRC=192.168.0.11 DST=173.19
4.72.93 LEN=379
2013/10/31 14:57:56 [URLBLOCK:] IN=eth0.1 OUT=wan1 SRC=192.168.0.11 DST=31.13.6
8.8 LEN=476
2013/10/31 14:57:56 [URLBLOCK:] IN=eth0.1 OUT=wan1 SRC=192.168.0.11 DST=31.13.6
8.8 LEN=476
```

The following table describes the labels in this screen.

TABLE 25: The Parental Control > Local Logs Screen

WAN Activity	This field displays information about website blocking filter events in the following format: ▶ Date (DD/MM/YY) ▶ Time (HH:MM:SS) ▶ IP Address ▶ Event type
Clear	Click this to remove the log events. Deleted information cannot be retrieved.
Refresh Logs	Click this to reload the information in the **WAN Activity** list. Events that have occurred since you last refreshed the list display.

6

WIRELESS

- This chapter provides an introduction to wireless networking, describes some common wireless network setup procedures, and documents the screens that display when you click **Wireless** in the toolbar. It contains the following sections:Wireless Basics on page 73: this section describes how wireless networks work and are secured.Wireless Tutorials on page 75: this section describes how to perform some common wireless network configuration tasks using your CGNV2.
- Advanced Wireless Networking on page 78: this section provides more in-depth information. If you are just interested in setting up your wireless network in a standard configuration you do not need to read this section.
- The Wireless Screens on page 80: this section provides detailed information on each of the CGNV2's wireless screens.
  Use this section as a reference to find out about a particular screen or field.

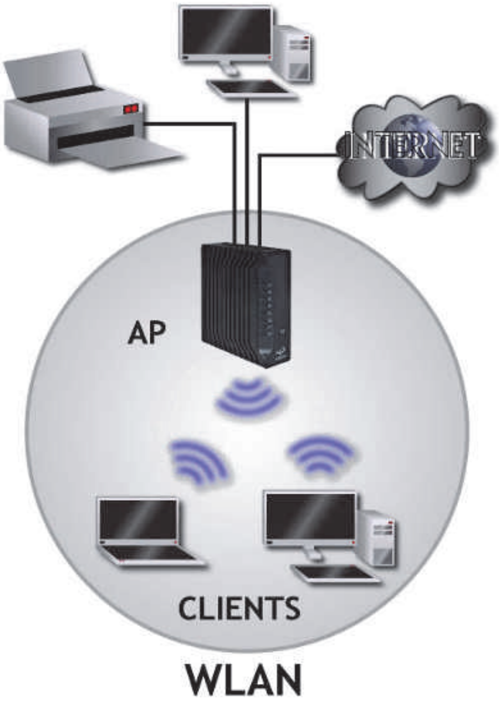
6.1 WIRELESS BASICS

This section describes how wireless networks and wireless security work.

Your CGNV2'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 CGNV2 and the other computers and devices that connect to it.

In the following figure, the wireless network is the part in the circle. The laptop and the PC are called “wireless clients” and connect to the CGNV2, which is called the “access point” or “AP”. The wireless clients can use the AP to access other devices (such as the printer) or the Internet.

FIGURE 26: Example Wireless Network



6.1.1 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 CGNV2 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

6.1.2 SERVICE SETS AND SSIDS

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

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 CGNV2 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). See Hiding the Network on page 77 for more information.

6.1.3 BASIC 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 in an attempt to secure it.

These techniques 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 CGNV2 supports the following wireless security protocols (in order of effectiveness):

Least secure	No security
↕	WEP
	WPA-PSK
Most secure	WPA2-PSK

For more information on these security protocols, see Advanced Wireless Security on page 78.

6.2 WIRELESS TUTORIALS

This section walks you through some of the more common wireless networking tasks.

NOTE: For basic wireless network setup, please see the Quick Installation Guide that came with your CGNV2.

These tasks include:

- Choosing a Security Method on page 75
- Changing the Wireless Password on page 76
- Changing the Network Name (SSID) on page 77
- Hiding the Network on page 77
- Improving the Wireless Network's Performance on page 77

6.2.1 CHOOSING A SECURITY METHOD

The security method that you choose to use for your wireless network depends upon the security methods supported by the devices on the network (the CGNV2, your PC, your laptop, and so on).

Not all devices support the same security methods, so you must find out what security methods each of the supports, and choose a method that they all support.

You should choose the best security method available; see Basic Wireless Security on page 75 for a list of methods the CGNV2 supports, in order of effectiveness.

In order to find out which security methods your other wireless devices support, you can:

- Look at the wireless device and see if it has a label listing the methods supported.
- Look at any documentation or packaging that came with the device.
- Go into the device’s configuration utility and look for a list of supported methods. This is often displayed as a drop-down list from which you can select an option.
- Go to the device’s manufacturer’s website and look for an information page that lists the device’s specifications.

If you want to use WPS (see WPS on page 79) all the wireless clients must also support WPS. There are two ways to determine if this is the case (in addition to those described above):

- Look at the wireless device and see if it has a physical button labeled “WPS” or something similar, a wireless “wave” icon (something like ((•))), or the “Wi-Fi Protected Setup” logo. If any of these are the case, the device probably supports the WPS PBC (“Push-Button Configuration”) method.
- Go into the wireless device’s configuration utility and look for a “WPS” or “Wi-Fi Protected Setup” screen. This screen should let you know whether the device supports WPS PBC method, the WPS PIN method, or both (some devices have a PBC button in their configuration utilities, in addition to or instead of a physical button).

Once you have chosen a security method, you can select it on the CGNV2 in the **Wireless** > **Security** screen’s **Security Mode** field (see The Security Screen on page 83).

6.2.2 CHANGING THE WIRELESS PASSWORD

Only wireless clients with the correct password can access the network. It’s a good idea to change your wireless network’s password every so often, if you think someone knows it who shouldn’t, or if there’s suspicious activity on your network.

You should change the password on the CGNV2, then change the password on each of your wireless clients.

The procedure for changing the password on the CGNV2 depends on the security method your network is using.

- If you are using the WPS PBC (“Push-Button Configuration”) security method, where you press a button on the CGNV2 and the other wireless devices, which connect automatically, just run the WPS PBC process again; see the Quick Installation Guide that came with your CGNV2 for more information on how to do this.

- If you are using the WPS PIN security, where you have a WPS password that you enter into each device on the network, go to the **Wireless** > **Basic** screen and click the **PIN** button. In the screen that displays, enter the WPS PIN that you want to use for the CGNV2, or the WPS PIN of the client device you want to add to the network.
- If you are using WEP, go to the **Wireless** > **Security** screen. Use the **WEP Settings** section to define the key(s) you want to use. Click **Apply** when you have finished.
- If you are using WPA-PSK or WPA2-PSK, go to the **Wireless** > **Security** screen. In the **WPA_Personal** section, enter the new password in the **Pre-Shared Key** field. Click **Apply** when you have finished.

Whichever security method you are using, when you change the password on the CGNV2, the other devices will not be able to connect to the network until you change their passwords as well.

The way in which you change the password on the client devices differs according to manufacturer and model. In general, you will need to log in to the device's configuration utility and perform a similar procedure to the one you just performed on the CGNV2, unless you are using the WPS PBC method, in which case you must press the button within two minutes of pressing the button on the CGNV2.

NOTE: If you are using WPS PBC, bear in mind that any device that also supports WPS can connect to the CGNV2 during the connection period. It is therefore not an ideal method to use in public places, or if you suspect someone is attempting to gain unauthorized access to the network.

6.2.3 CHANGING THE NETWORK NAME (SSID)

To change your wireless network's SSID (the name that displays when you scan for wireless networks on your wireless client), go to the **Wireless** > **Basic** screen. Enter the new network name in the **SSID Name** field and click **Apply**.

NOTE: Since the SSID is required to connect to a network, you will need to re-connect your wireless client devices to the new SSID.

6.2.4 HIDING THE NETWORK

There are various reasons that you might not want your network to be visible to people scanning for available networks. To do this, go to the **Wireless** > **Basic** screen. Select the **Hidden** checkbox and click **Apply**.

6.2.5 IMPROVING THE WIRELESS NETWORK'S PERFORMANCE

There are two main factors that affect how well your wireless devices can communicate:

1. Interference from physical objects
2. Radio Frequency (RF) interference

To minimize interference from physical objects:

- Move the CGNV2 away from walls, heavy furniture, other massive or metallic objects like refrigerators, and so forth.
- Install the CGNV2 in a higher location.

To minimize RF interference:

- Move the CGNV2 away from sources of RF energy such as wireless telephone base stations, microwaves, and so forth.
- Conduct a wireless site audit to see if other wireless networks are interfering with yours. If so, you can change the wireless channel to one that isn't so congested.

  To conduct a site audit on the CGNV2, go to the **Wireless** > **WiFi Site Survey** screen. Click **Scan**. The screen that displays shows the wireless networks in the area, the **Ch** field shows the channel they are using, and the **Signal (%)** field shows how strongly the CGNV2 is receiving their signal (bear in mind that the strength of a network at the CGNV2's location is not necessarily the same as at your wireless client's location; it may be much stronger there).

  If there are a lot of networks or a very strong network using a single channel or a group of channels, you can change the CGNV2's channel to one further away from the congested channel. To do this on the CGNV2, go to the **Wireless** > **Basic** screen and choose an option from the **Channel** list. You should choose a channel as far away from the congested area as possible; ideally a difference of five channels is desirable.

  Depending on their configuration, you may also then need to change the channel on your wireless client devices.

6.3 ADVANCED WIRELESS NETWORKING

This section provides more technical information about wireless networks.

NOTE: If you are just setting up your wireless network in a standard configuration (covered in Wireless Tutorials on page 75) you do not need to read this section.

6.3.1 ADVANCED WIRELESS SECURITY

This section describes the CGNV2's supported security protocols in greater detail.

- **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 CGNV2) 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.

6.3.2 OTHER WIRELESS CONCEPTS

This section provides information on wireless-related topics not covered in previous sections.

6.3.2.1 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 CGNV2 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.

6.3.2.2 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.

6.4 THE WIRELESS SCREENS

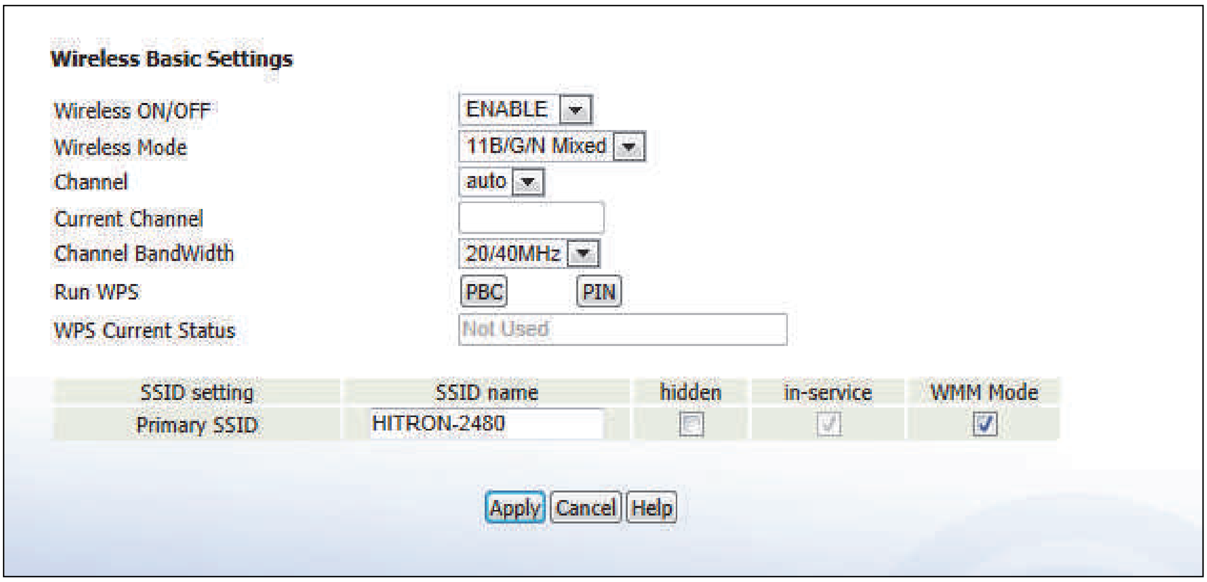
This section describes each of the screens that display when you click **Wireless** in the toolbar.

6.4.1 THE BASIC SCREEN

Use this screen to configure your CGNV2'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.

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

FIGURE 27: The Wireless > Basic Screen



Wireless Basic Settings

Wireless ON/OFF	ENABLE
Wireless Mode	11B/G/N Mixed
Channel	auto
Current Channel	
Channel BandWidth	20/40MHz
Run WPS	PBC PIN
WPS Current Status	Not Used

SSID setting	SSID name	hidden	in-service	WMM Mode
Primary SSID	HITRON-2480	□	☑	☑

The following table describes the labels in this screen.

TABLE 26: The Wireless > Basic Screen

Wireless Basic Settings	
Wireless ON/OFF	Use this field to turn the wireless network on or off. ▶ Select **ENABLE** to turn the wireless network on. ▶ Select **DISABLE** to turn the wireless network off.
Wireless Mode	Select the type of wireless network that you want to use: ▶ **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 CGNV2 select the optimum channel to use. *NOTE:* Use the **Auto** setting unless you have a specific reason to do otherwise.
Current Channel	This displays the current WiFi channel.
Channel Bandwidth	Use this field to select the channel bandwidth (20MHz, 40MHz, 20/40MHz).

TABLE 26: The Wireless > Basic Screen (continued)

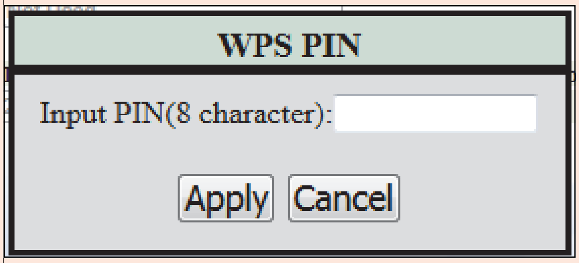
Run WPS	Use these buttons to run Wifi Protected Setup (WPS): - Click the **PBC** button to begin the Push-Button Configuration process. You must then press the PBC button on your client wireless devices within two minutes in order to register them on your wireless network. - Click the **PIN** button to begin the PIN configuration process. In the screen that displays, enter the WPS PIN that you want to use for the CGNV2, or the WPS PIN of the client device you want to add to the network. *FIGURE 28:* WPS PIN  WPS PIN Input PIN(8 character):
WPS Current Status	This displays whether the WPS function is active, idle or not used.
SSID Setting	This displays **Primary SSID**. *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.
Hidden	Use this field to make your network visible or invisible to other wireless devices. - Select the checkbox if you do not want the CGNV2 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.

TABLE 26: The Wireless > Basic Screen (continued)

In Service	This field controls whether or not the SSID is in operation. *NOTE:* At the time of writing, this field is not user-configurable.
WMM Mode	Select the checkbox if you want to apply Wifi MultiMedia (WMM) Quality of Service (QoS) settings to this SSID.

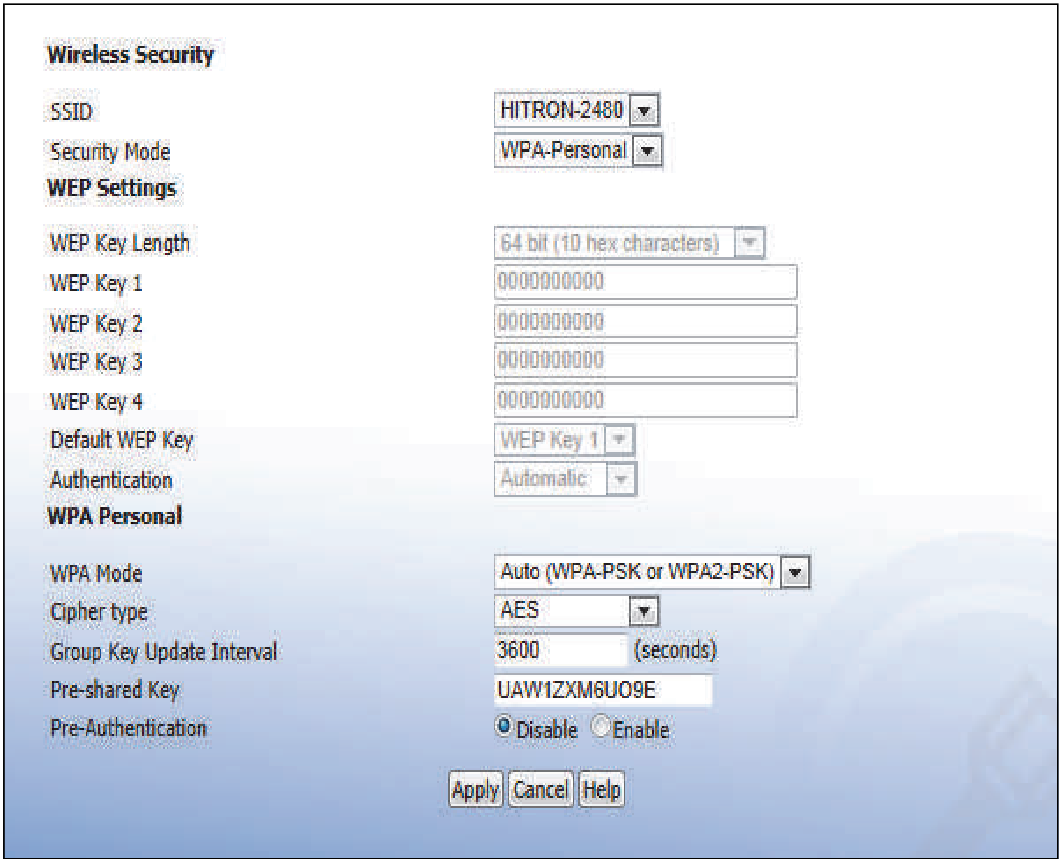
6.4.2 THE SECURITY SCREEN

Use this screen to 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** > **Security**. The following screen displays.

FIGURE 29: The Wireless > Security Screen



Wireless Security

SSID	HITRON-2480
Security Mode	WPA-Personal
WEP Settings	
WEP Key Length	64 bit (10 hex characters)
WEP Key 1	0000000000
WEP Key 2	0000000000
WEP Key 3	0000000000
WEP Key 4	0000000000
Default WEP Key	WEP Key 1
Authentication	Automatic
WPA Personal	
WPA Mode	Auto (WPA-PSK or WPA2-PSK)
Cipher type	AES
Group Key Update Interval	3600 (seconds)
Pre-shared Key	UAW1ZXM6UO9E
Pre-Authentication	● Disable ○ Enable

The following table describes the labels in this screen.

TABLE 27: The Wireless > Security Screen

Wireless Security	
SSID	Select the SSID for which you want to configure security. *NOTE:* At the time of writing, only one SSID is available.
Security Mode	Select the type of security that you want to use. ▶ 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.	
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. ▶ 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. The CGNV2 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 CGNV2 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 CGNV2's default key. Enter the keys in hexadecimal format (using the digits **0~9** and the letters **A~F**).
Default WEP Key	Select the number of the security key that you want the CGNV2 to use as its default authentication key for transmissions.

TABLE 27: The Wireless > Security Screen (continued)

Authentication	Select the authentication mode that you want to use: - Select **Open System** to allow wireless clients to authenticate (identify themselves) to the CGNV2 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 CGNV2 sends an unencrypted challenge message. The client must use the WEP key to encrypt the challenge message and return it to the CGNV2, which then decrypts the message and compares the result with its original message. **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. - Select **Automatic** to have the CGNV2 choose the authentication method.
WPA_Personal *NOTE:* These fields are only configurable when you select **WPA-Personal** from the **Security Mode** list.	
WPA Mode	Select the type of WPA security that you want to use: - 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 CGNV2.
Cipher Type	Select the type of encryption that you want to use: - 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 CGNV2.
Group Key Update Interval	Enter the frequency (in seconds) with which you want the CGNV2 to create new pre-shared keys, and issue them to the wireless client.

TABLE 27: The Wireless > Security Screen (continued)

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.
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.

6.4.3 THE ACCESS CONTROL SCREEN

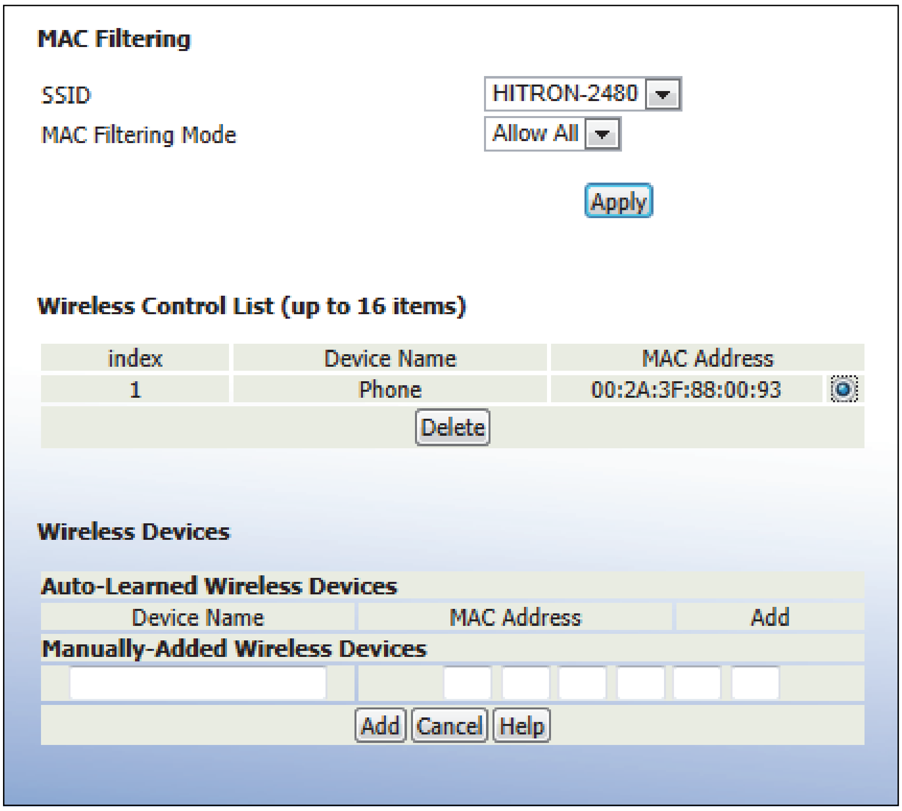
Use this screen to configure Media Access Control (MAC) address filtering on the wireless network.

NOTE: To configure MAC address filtering on the wired LAN, see **The MAC Filtering Screen** on page 52.

You can set the CGNV2 to allow only certain devices to access the CGNV2 and the network wirelessly, or to deny certain devices access.

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

FIGURE 30: The Wireless > Access Control Screen



MAC Filtering

SSID: HITRON-2480

MAC Filtering Mode: Allow All

Apply

Wireless Control List (up to 16 items)

index	Device Name	MAC Address	
1	Phone	00:2A:3F:88:00:93	◉

Delete

Wireless Devices

Auto-Learned Wireless Devices

Device Name	MAC Address	Add

Manually-Added Wireless Devices

Add Cancel Help

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 CGNV2 supports a single SSID.
MAC Filtering Mode	Use this field to control whether the CGNV2 performs MAC filtering on the wireless network. - Select **Allow-All** to turn MAC filtering off. All devices may access the CGNV2 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 CGNV2 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 CGNV2 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)	

TABLE 28: The Wireless > Access Control Screen (continued)

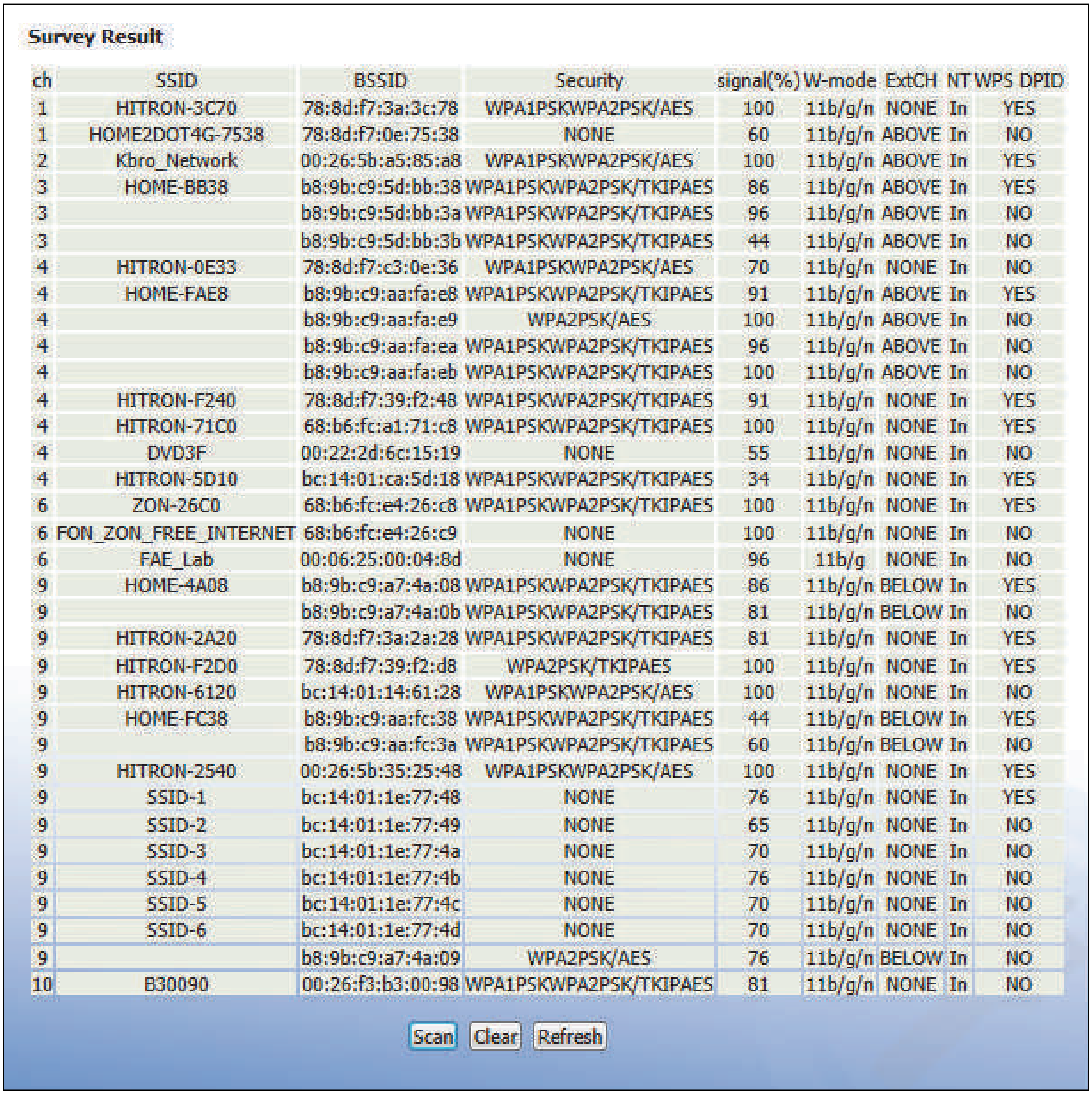
# Index	This displays the index number assigned to the permitted or denied wireless device.
Device Name	This displays the name you gave to the permitted or denied wireless device.
MAC Address	This displays the MAC address of the permitted or denied wireless device.
Delete	Select a permitted or denied wireless device's radio button (◉) and click this to remove the device from the list. The device may no longer access the CGNV2 and the network.
Auto-Learned Wireless Devices	
Device Name	This displays the name of each network device that has connected to the CGNV2 on the wireless network.
MAC Address	This displays the MAC address of each network device that has connected to the CGNV2 on the wireless network.
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 CGNV2 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 CGNV2 and the network wirelessly.
Add	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.

6.4.4 THE WIFI SITE SURVEY SCREEN

Use this screen to view information about the wireless networks within the CGNV2's coverage area.

Click **Wireless** > **WiFi Site Survey**. The following screen displays.

FIGURE 31: The Wireless > WiFi Site Survey Screen



Survey Result

ch	SSID	BSSID	Security	signal(%)	W-mode	ExtCH	NT	WPS	DPID
1	HITRON-3C70	78:8d:f7:3a:3c:78	WPA1PSKWPA2PSK/AES	100	11b/g/n	NONE	In	YES	
1	HOME2DOT4G-7538	78:8d:f7:0e:75:38	NONE	60	11b/g/n	ABOVE	In	NO	
2	Kbro_Network	00:26:5b:a5:85:a8	WPA1PSKWPA2PSK/AES	100	11b/g/n	ABOVE	In	YES	
3	HOME-BB38	b8:9b:c9:5d:bb:38	WPA1PSKWPA2PSK/TKIPAES	86	11b/g/n	ABOVE	In	YES	
3		b8:9b:c9:5d:bb:3a	WPA1PSKWPA2PSK/TKIPAES	96	11b/g/n	ABOVE	In	NO	
3		b8:9b:c9:5d:bb:3b	WPA1PSKWPA2PSK/TKIPAES	44	11b/g/n	ABOVE	In	NO	
4	HITRON-0E33	78:8d:f7:c3:0e:36	WPA1PSKWPA2PSK/AES	70	11b/g/n	NONE	In	NO	
4	HOME-FAE8	b8:9b:c9:aa:fa:e8	WPA1PSKWPA2PSK/TKIPAES	91	11b/g/n	ABOVE	In	YES	
4		b8:9b:c9:aa:fa:e9	WPA2PSK/AES	100	11b/g/n	ABOVE	In	NO	
4		b8:9b:c9:aa:fa:ea	WPA1PSKWPA2PSK/TKIPAES	96	11b/g/n	ABOVE	In	NO	
4		b8:9b:c9:aa:fa:eb	WPA1PSKWPA2PSK/TKIPAES	100	11b/g/n	ABOVE	In	NO	
4	HITRON-F240	78:8d:f7:39:f2:48	WPA1PSKWPA2PSK/TKIPAES	91	11b/g/n	NONE	In	YES	
4	HITRON-71C0	68:b6:fc:a1:71:c8	WPA1PSKWPA2PSK/TKIPAES	100	11b/g/n	NONE	In	YES	
4	DVD3F	00:22:2d:6c:15:19	NONE	55	11b/g/n	NONE	In	NO	
4	HITRON-5D10	bc:14:01:ca:5d:18	WPA1PSKWPA2PSK/TKIPAES	34	11b/g/n	NONE	In	YES	
6	ZON-26C0	68:b6:fc:e4:26:c8	WPA1PSKWPA2PSK/TKIPAES	100	11b/g/n	NONE	In	YES	
6	FON_ZON_FREE_INTERNET	68:b6:fc:e4:26:c9	NONE	100	11b/g/n	NONE	In	NO	
6	FAE_Lab	00:06:25:00:04:8d	NONE	96	11b/g	NONE	In	NO	
9	HOME-4A08	b8:9b:c9:a7:4a:08	WPA1PSKWPA2PSK/TKIPAES	86	11b/g/n	BELOW	In	YES	
9		b8:9b:c9:a7:4a:0b	WPA1PSKWPA2PSK/TKIPAES	81	11b/g/n	BELOW	In	NO	
9	HITRON-2A20	78:8d:f7:3a:2a:28	WPA1PSKWPA2PSK/TKIPAES	81	11b/g/n	NONE	In	YES	
9	HITRON-F2D0	78:8d:f7:39:f2:d8	WPA2PSK/TKIPAES	100	11b/g/n	NONE	In	YES	
9	HITRON-6120	bc:14:01:14:61:28	WPA1PSKWPA2PSK/AES	100	11b/g/n	NONE	In	NO	
9	HOME-FC38	b8:9b:c9:aa:fc:38	WPA1PSKWPA2PSK/TKIPAES	44	11b/g/n	BELOW	In	YES	
9		b8:9b:c9:aa:fc:3a	WPA1PSKWPA2PSK/TKIPAES	60	11b/g/n	BELOW	In	NO	
9	HITRON-2540	00:26:5b:35:25:48	WPA1PSKWPA2PSK/AES	100	11b/g/n	NONE	In	YES	
9	SSID-1	bc:14:01:1e:77:48	NONE	76	11b/g/n	NONE	In	YES	
9	SSID-2	bc:14:01:1e:77:49	NONE	65	11b/g/n	NONE	In	NO	
9	SSID-3	bc:14:01:1e:77:4a	NONE	70	11b/g/n	NONE	In	NO	
9	SSID-4	bc:14:01:1e:77:4b	NONE	76	11b/g/n	NONE	In	NO	
9	SSID-5	bc:14:01:1e:77:4c	NONE	70	11b/g/n	NONE	In	NO	
9	SSID-6	bc:14:01:1e:77:4d	NONE	70	11b/g/n	NONE	In	NO	
9		b8:9b:c9:a7:4a:09	WPA2PSK/AES	76	11b/g/n	BELOW	In	NO	
10	B30090	00:26:f3:b3:00:98	WPA1PSKWPA2PSK/TKIPAES	81	11b/g/n	NONE	In	NO	

The following table describes the labels in this screen.

TABLE 29: The Wireless > WiFi Site Survey Screen

Survey Results	
ch	This field displays the number of the radio channel that the target wireless network is using.
SSID	This field displays the Service Set IDentifier of the target wireless network.
BSSID	This field displays the Basic Service Set IDentifier of the target wireless network. This is usually the Media Access Control (MAC) address of the target network device.
Security	This field displays the type of security that the target wireless network is using.

TABLE 29: The Wireless > WiFi Site Survey Screen (continued)

Signal (%)	This field displays the signal strength of the target wireless network, as received by the CGNV2, as a percentage fro 0 (no reception) to 100 (perfect reception)
W-mode	This field displays the wireless network standard (for instance, 11n) that the target wireless network is using.
ExtCH	For IEEE 802.11n networks that support 40MHz wireless transmissions, this field displays whether the network uses channel bonding, and specifies whether the extension channel is above or below the primary control channel. *NOTE:* Channel bonding allows an access point to increase data throughput by using two wireless channels simultaneously, instead of a single channel. When you use channel bonding, you have a primary control channel, and an extension channel. The extension channel may be either directly above the control channel, or directly below. ▶ For IEEE 802.11n networks using channel bonding, where the extension channel is above the main channel, **ABOVE** displays. ▶ For IEEE 802.11n networks using channel bonding, where the extension channel is above the main channel, **BELOW** displays. ▶ For networks that do not use channel bonding, **NONE** displays.

TABLE 29: The Wireless > WiFi Site Survey Screen (continued)

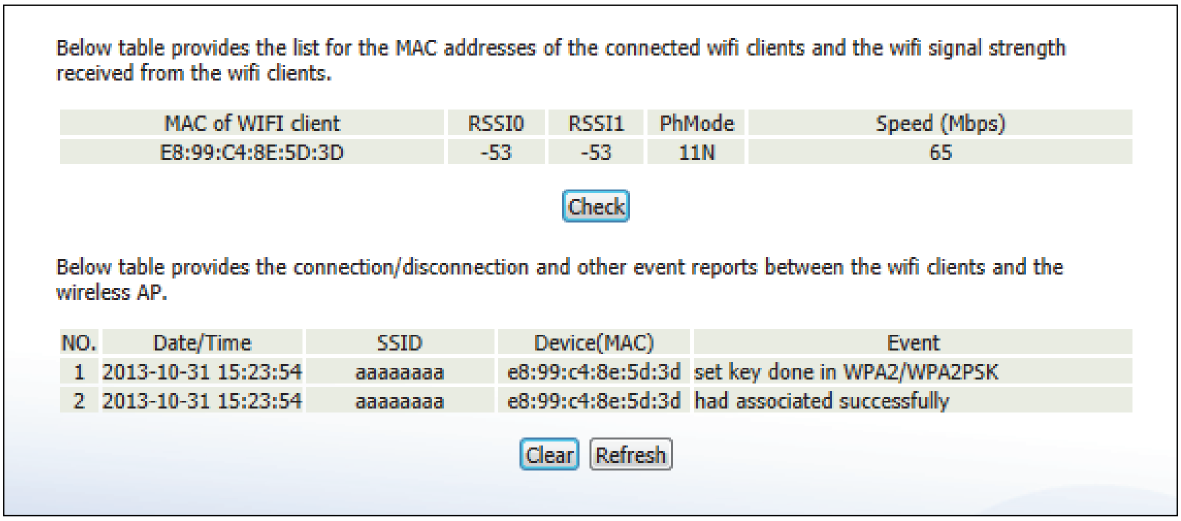
Nt	This field displays whether the network is using infrastructure mode, or ad-hoc mode. *NOTE:* In infrastructure mode, wireless devices connect to a central Access Point (AP), which usually connects to the Internet or another network via a wired connection. In ad-hoc mode, wireless devices connect to one another, as peers.
WPS DPID	This field displays whether the target network is using WiFi Protected Setup (WPS) or not. If the target network is using WPS, this field displays whether it is using PIN mode, or Push-Button Configuration (PBC) mode. - If the target network is not using WPS, **NO** displays. - If the target network is using WPS, and allows wireless devices to connect using the PIN mode, **PIN** displays. - If the target network is using WPS, and allows wireless devices to connect using the push-button mode, **PBC** displays. *NOTE:* See WPS on page 79 for more information on WPS, and the difference between PIN and PBC modes.

6.4.5 THE CONNECTION LIST SCREEN

Use this screen to view information about the wireless clients connected to the CGNV2.

Click **Wireless** > **Connection List**. The following screen displays.

FIGURE 32: The Wireless > Connection List Screen



Below table provides the list for the MAC addresses of the connected wifi clients and the wifi signal strength received from the wifi clients.

MAC of WIFI client	RSSI0	RSSI1	PhMode	Speed (Mbps)
E8:99:C4:8E:5D:3D	-53	-53	11N	65

Below table provides the connection/disconnection and other event reports between the wifi clients and the wireless AP.

NO.	Date/Time	SSID	Device(MAC)	Event
1	2013-10-31 15:23:54	aaaaaaaa	e8:99:c4:8e:5d:3d	set key done in WPA2/WPA2PSK
2	2013-10-31 15:23:54	aaaaaaaa	e8:99:c4:8e:5d:3d	had associated successfully

The following table describes the labels in this screen.

TABLE 30: The Wireless > Connection List Screen

MAC of WiFi Client	This displays the MAC address of each device connected to the SSID.
RSSI0-1	This displays the value of the Received Signal Strength Indicator.
PhMode	This displays the WiFi operation mode.
Speed (Mbps)	This displays current connection speed.
NO.	This displays the arbitrary identification number assigned to the WiFi event.
Date/Time	This displays the date and time at which the WiFi event occurred.
SSID	This field displays the SSID on which the WiFi event occured.
Device (MAC)	This field displays the WiFi client’s MAC address on which the WiFi event occured..
Event	This field describes the WiFi event.

7

eMTA

This chapter describes the screens that display when you click **eMTA** in the toolbar. These screens display information about the CGNV2's embedded Multimedia Terminal Adapter module.

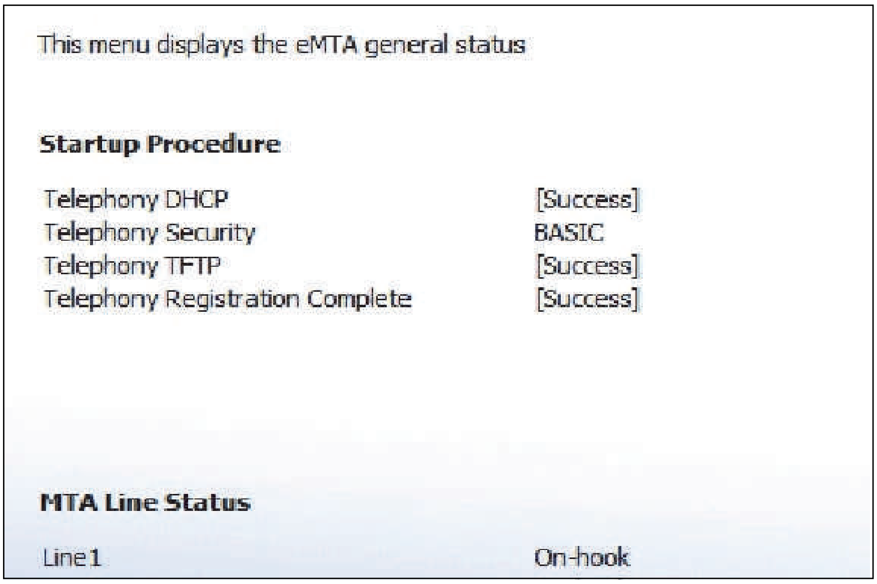
NOTE: The fields in these screens are read-only, and are provided for troubleshooting purposes only.

7.1 THE STATUS SCREEN

Use this screen to see general information about the eMTA module.

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

FIGURE 33: The eMTA > Status Screen



This menu displays the eMTA general status

Startup Procedure

Telephony DHCP	[Success]
Telephony Security	BASIC
Telephony TFTP	[Success]
Telephony Registration Complete	[Success]

MTA Line Status

Line1	On-hook

The following table describes the labels in this screen.

TABLE 31: The eMTA > Status Screen

Startup Procedure	
Telephony DHCP	This field displays the status of the remote telephony DHCP server.

TABLE 31: The eMTA > Status Screen (continued)

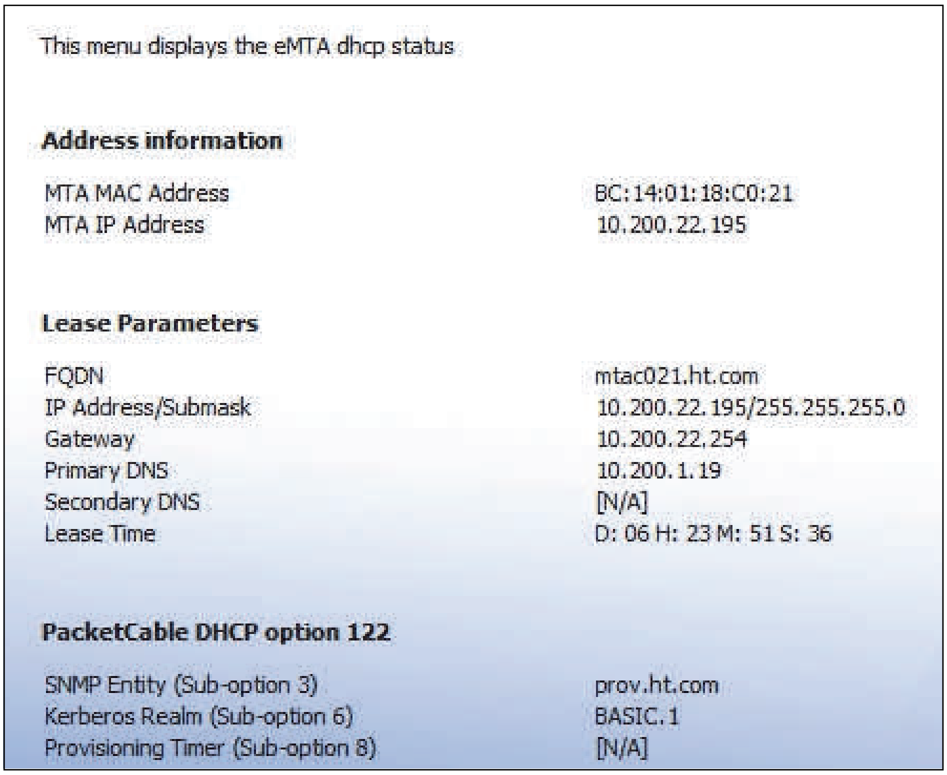
Telephony Security	This displays the type of security used for voice calls through the CGNV2.
Telephony TFTP	This field displays the status of the remote telephony TFTP server.
Telephony Registration Complete	This field displays the overall status of voice call registration.
MTA Line State	
Line	This displays the current status of the phone connected to the CGNV2. This field do not display when a phone is not connected to the port.

7.2 THE DHCP SCREEN

Use this screen to see information about the MTA module's connections to the service provider.

Click **eMTA** > **DHCP**. The following screen displays.

FIGURE 34: The eMTA > DHCP Screen



This menu displays the eMTA dhcp status

Address information

MTA MAC Address	BC:14:01:18:C0:21
MTA IP Address	10.200.22.195

Lease Parameters

FQDN	mtac021.ht.com
IP Address/Submask	10.200.22.195/255.255.255.0
Gateway	10.200.22.254
Primary DNS	10.200.1.19
Secondary DNS	[N/A]
Lease Time	D: 06 H: 23 M: 51 S: 36

PacketCable DHCP option 122

SNMP Entity (Sub-option 3)	prov.ht.com
Kerberos Realm (Sub-option 6)	BASIC.1
Provisioning Timer (Sub-option 8)	[N/A]

The following table describes the labels in this screen.

TABLE 32: The eMTA > DHCP Screen

Address Information	
MTA MAC Address	This field displays the Media Access Control (MAC) address of the Media Terminal Adapter (MTA) module.
MTA IP Address	This field displays the IP address of the MTA module.
Lease Parameters	
FQDN	This displays the Fully-Qualified Domain Name of the DHCP server from which the MTA module derives its IP address and subnet mask.
IP Address/Submask	This displays the MTA module's IP address and subnet mask, derived by DHCP.
Gateway	This displays the IP address of the MTA module's gateway on the WAN.
Primary DNS	This displays the IP address of the MTA module's primary Domain Name System (DNS) server.
Secondary DNS	This displays the IP address of the MTA module's secondary DNS server.
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.
Packet Cable DHCP Option 122 *NOTE:* DHCP Option 122 is defined in RFC 3495.	
SNMP Entity (Sub-Option 3)	This displays the Telephony Service Provider's provisioning server address.
Kerberos Realm (Sub-Option 6)	This displays the TSP's Kerberos realm name.
Provisioning Timer (Sub-Option 8)	This displays the TSP's provisioning timer value.

8

VPN

This chapter describes the screens that display when you click VPN in the toolbar.

NOTE: This chapter only applies for firmware which supports VPN function.

8.1 VPN OVERVIEW

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

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

8.1.1 IPSEC

The Internet Protocol Security (IPsec) is a technology protocol suite for securing IP communications by authenticating and/or encrypting each IP packet of a communication session.

8.1.1.1 FRAMEWORK PROTOCOLS

There are two main IPsec framework protocols are as follows:

- ESP

Encapsulated Security Payload (ESP) is a protocol protects the IP packet data from third party interference by encrypting the contents using symmetric cryptography algorithms.

- AH

Authentication Header (AH) is a protocol protects the IP packet header from third party interference and spoofing by computing a cryptographic checksum and hashing the IP packet header fields with a secure hashing function. This is then followed by an additional header that contains the hash, to allow the information in the packet to be authenticated.

8.1.1.2 IKE

The Internet Key Exchange (IKE) is an IPsec standard protocol used to ensure security for VPN negotiation and remote host or network access.

8.1.1.3 ENCRYPTION ALGORITHMS

- DES

Data Encryption Standard (DES) is used to encrypt and decrypt packet data.

- 3DES

Triple DES (3DES) applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

- AES

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data.

- TWOFISH

Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. Twofish is related to the earlier block cipher Blowfish.

- BLOWFISH

Blowfish is a symmetric key block cipher that can be used as a drop-in replacement for DES. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use.

8.1.1.4 CRYPTOGRAPHIC HASH FUNCTION

A cryptographic hash function is a hash function that takes an arbitrary block of data and returns a fixed-size bit string, the cryptographic hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the message, and the hash value is sometimes called the message digest or simply digest. There are some main cryptographic hash algorithms are as follows:

- MD5

The MD5 message-digest 5 (MD5) algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. MD5 has been utilized in a wide variety of security applications, and is also commonly used to check data integrity. An MD5 hash value is typically expressed as a hexadecimal number, 32 digits long.

- SHA

Secure Hash Algorithm (SHA). The four SHA algorithms are structured differently and are distinguished as SHA-0, SHA-1, SHA-2, and SHA-3. SHA-1 is very similar to SHA-0, but corrects an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-2 on the other hand significantly differs from the SHA-1 hash function.

8.1.2 PPTP

The Point-to-Point Tunneling Protocol (PPTP) is used for providing security levels and remote access levels comparable with typical VPN products.

8.1.3 L2TP

The Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs.

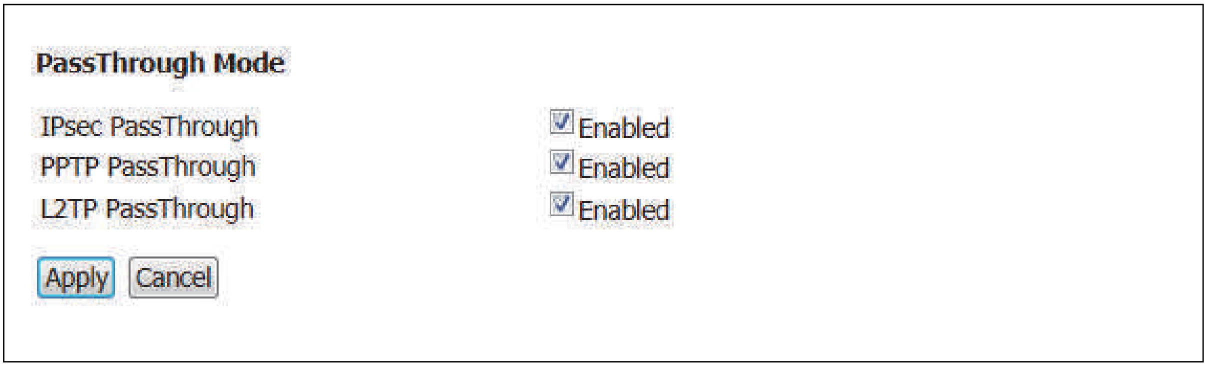
8.2 THE PASSTHROUGH SCREEN

Use this screen to select the VPN pass-through mode.

Click **VPN** > **PassThrough**. The following screen displays.

NOTE: This screen allows to choose which VPN protocols will be supported by CGNV2 in passthrough mode when the VPN client is a CPE connected to its LAN.

FIGURE 35: The VPN > PassThrough Screen



PassThrough Mode

IPsec PassThrough ☑ Enabled

PPTP PassThrough ☑ Enabled

L2TP PassThrough ☑ Enabled

The following table describes the labels in this screen.

TABLE 33: The VPN > PassThrough Screen

PassThrough Mode	
IPsec PassThrough	Use this field to select whether the IPsec Pass-through be active or not. ▶ **Select** Enabled to activate the IPsec Pass-through. ▶ **Deselect** Enabled to deactivate the IPsec Pass-through.

TABLE 33: The VPN > PassThrough Screen (continued)

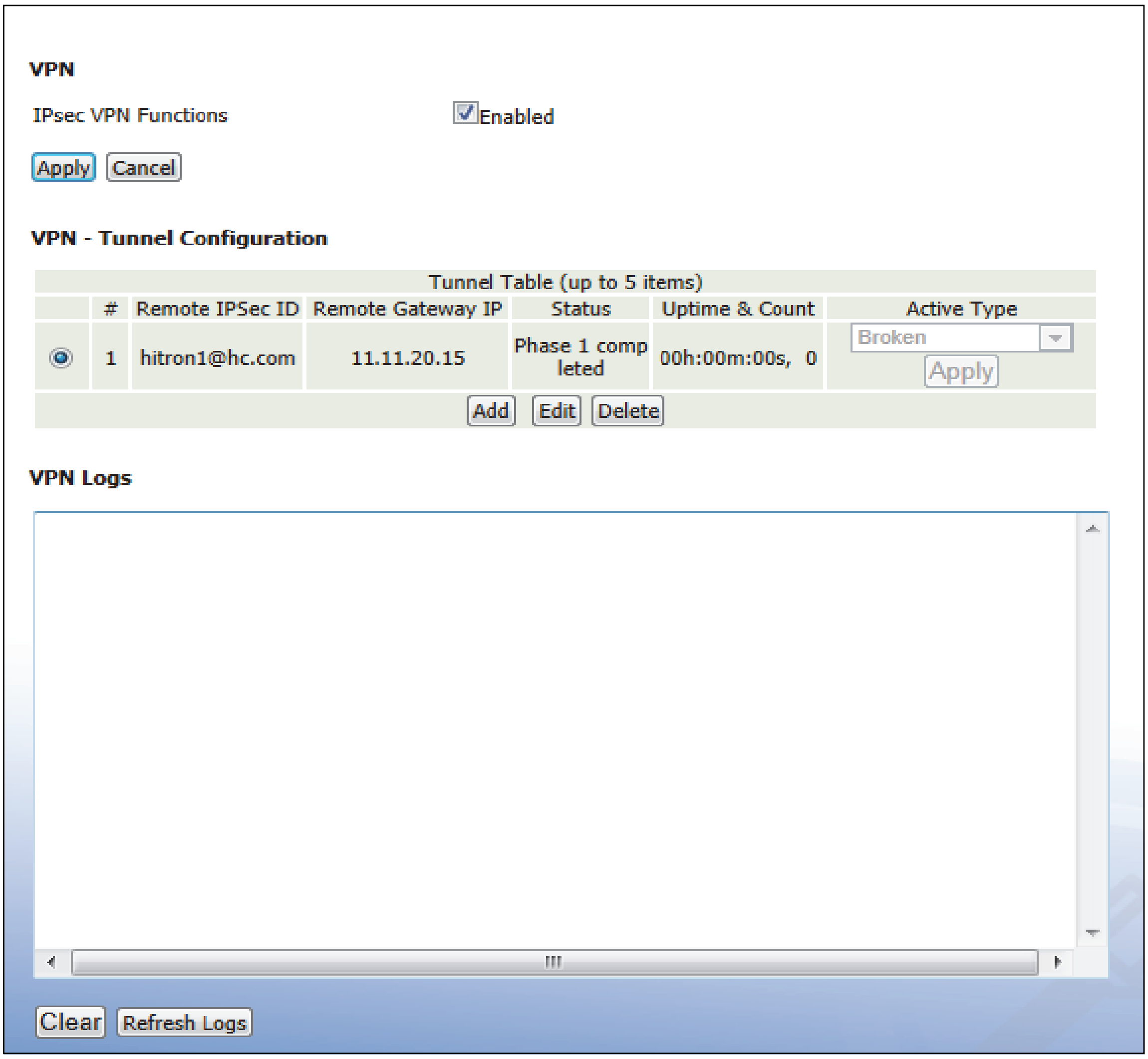
PPTP PassThrough	Use this field to select whether the PPTP Pass-through be active or not. - **Select** Enabled to activate the PPTP Pass-through. - **Deselect** Enabled to deactivate the PPTP Pass-through.
L2TP PassThrough	Use this field to select whether the L2TP Pass-through be active or not. - **Select** Enabled to activate the L2TP Pass-through. - **Deselect** Enabled to deactivate the L2TP Pass-through.

8.3 THE IP SEC SCREEN

Use this screen to configure IP Sec VPN functions. You can turn IP Sec VPN functions on or off and configure new and existing VPN tunnel.

Click **VPN** > **IPsec**. The following screen displays.

FIGURE 36: The VPN > IPsec Screen



VPN

IPsec VPN Functions ☑ Enabled

Apply Cancel

VPN - Tunnel Configuration

Tunnel Table (up to 5 items)

	#	Remote IPSec ID	Remote Gateway IP	Status	Uptime & Count	Active Type
●	1	hitron1@hc.com	11.11.20.15	Phase 1 completed	00h:00m:00s, 0	Broken Apply

Add Edit Delete

VPN Logs

Clear Refresh Logs

IPsecThe following table describes the labels in this screen.

TABLE 34: The VPN > IPsec Screen

VPN	
IPsec VPN Functions	Use this field to select whether the IPsec VPN functions be active or not. ▶ **Select** Enabled to activate the IPsFec VPN functions. ▶ **Deselect** Enabled to deactivate the IPsec VPN functions.
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.
VPN Tunnel Configuration	
#	This displays the arbitrary identification number assigned to the VPN tunnels.
Remote IPsec ID	This displays the ID number of the remote IPsec.

TABLE 34: The VPN > IPsec Screen (continued)

Remote Gateway IP	This displays the IP address of the remote gateway on WAN.
Status	This displays whether the tunnel is connected.
Uptime & Count	This displays the time period and number of times during the tunnel connected.
Active Type	This displays the active type of the VPN tunnel.
Add	Click this to define a new VPN tunnel. IPsec VPN Functions must first be set to **Enabled**. See Adding or Editing a VPN Tunnel on page 102 for information on the screen that displays.
Edit	Select a VPN tunnel's radio button and click this to make changes to the tunnel. IPsec VPN Functions must first be set to **Enabled**. See Adding or Editing a VPN Tunnel on page 102 for information on the screen that displays.
Delete	Select a VPN tunnel's radio button and click this to remove the tunnel. The deleted rule's information cannot be retrieved.
VPN Log	
Clear	Use this field to remove the VPN logs.
Refresh Logs	Use this field to obtain the VPN logs again.

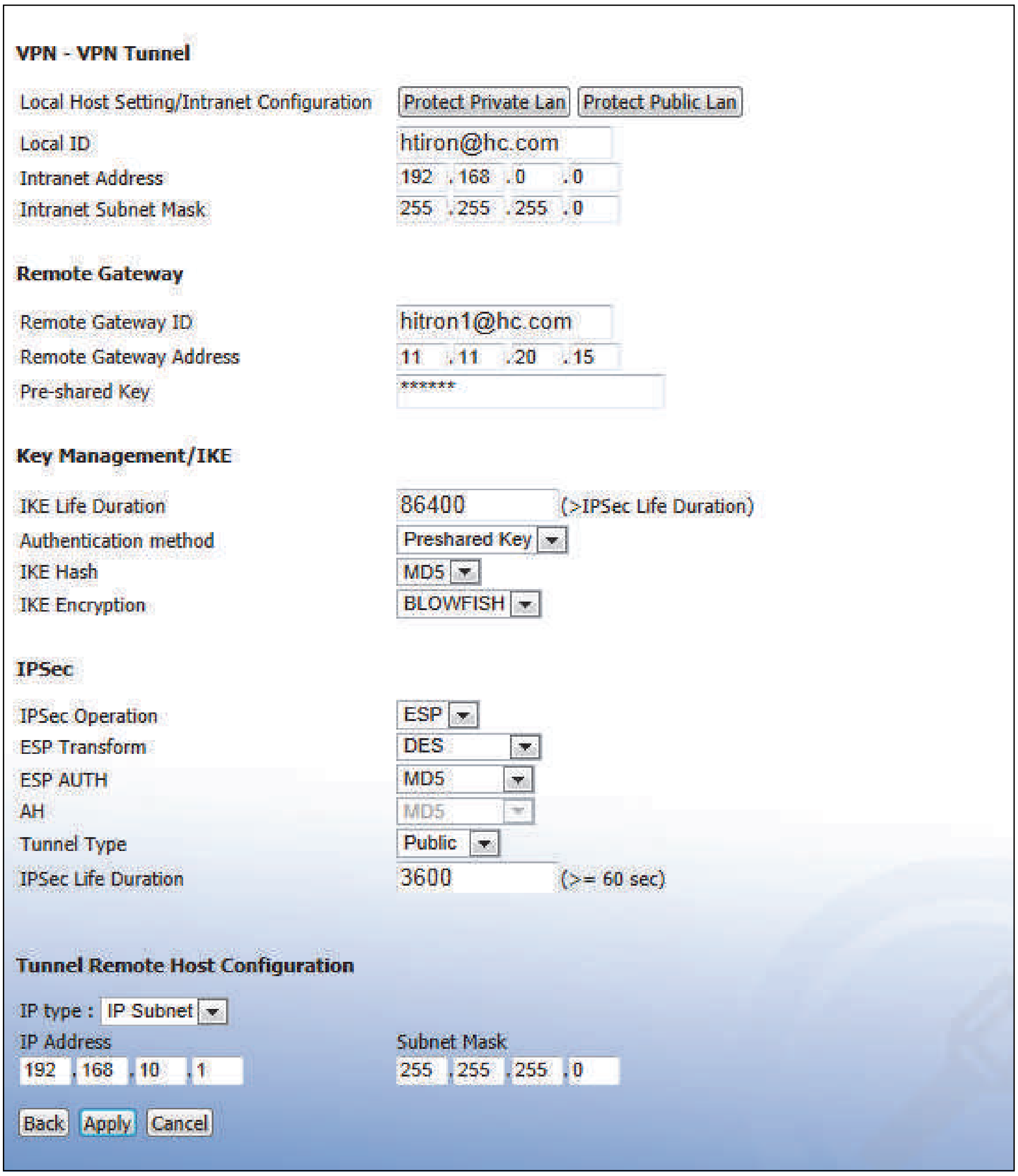
8.3.1 ADDING OR EDITING A VPN TUNNEL

- To add a new VPN tunnel, click **Add** in the **VPN** > **IP Sec** screen.
- To edit an existing VPN tunnel, select the tunnel's radio button in the **VPN** > **IP Sec** screen and click the **Edit** button.

NOTE: Ensure that Enabled is selected in the **VPN > IP Sec** screen in order to add or edit VPN tunnel.

The following screen displays.

FIGURE 37: The VPN > IPsec > Add/Edit Screen



VPN - VPN Tunnel

Local Host Setting/Intranet Configuration	Protect Private Lan · Protect Public Lan
Local ID	htiron@hc.com
Intranet Address	192 .168 .0 .0
Intranet Subnet Mask	255 .255 .255 .0

Remote Gateway

Remote Gateway ID	hitron1@hc.com
Remote Gateway Address	11 .11 .20 .15
Pre-shared Key	******

Key Management/IKE

IKE Life Duration	86400 (>IPSec Life Duration)
Authentication method	Preshared Key
IKE Hash	MD5
IKE Encryption	BLOWFISH

IPSec

IPSec Operation	ESP
ESP Transform	DES
ESP AUTH	MD5
AH	MD5
Tunnel Type	Public
IPSec Life Duration	3600 (>= 60 sec)

Tunnel Remote Host Configuration

IP type : IP Subnet

IP Address	Subnet Mask
192 .168 .10 .1	255 .255 .255 .0

The following table describes the labels in this screen.

TABLE 35: The VPN > IPsec > Add/Edit Screen

VPN - VPN Tunnel	
Local Host Setting/ Intranet Configuration	Use this field to select which LAN be protected. ▶ Select **Protect Private LAN** to protect the private LAN ▶ Deselect **Protect Public LAN** to protect the public LAN.
Local ID	Use this field to enter the local ID of the VPN tunnel.
Intranet Address	Use this field to enter the IP address of the Intranet.
Intranet Subnet Mask	Use this field to enter the Subnet Mask of the Intranet.
Remote Gateway	

TABLE 35: The VPN > IPsec > Add/Edit Screen (continued)

Remote Gateway ID	Use this field to configure the ID of the remote gateway.
Remote Gateway Address	Use this field to configure the IP address of the remote gateway.
Pre-shared Key	Use this field to enter the pre-shared key for connection to the remote gateway.
Key Management/IKE	
IKE Life Duration	Use this field to enter the IKE Life Duration value in seconds.
Authentication method	Use this field to select the method of authentication. *NOTE:* Leave this field at its default.
IKE Hash	Use this field to select the type of IKE hash you want to use. See Cryptographic Hash Function on page 98 for information on the screen that displays. ▶ MD5 ▶ SHA
IKE Encryption	Use this field to select the type of IKE encryption you want to use. See Encryption Algorithms on page 98 for information on the screen that displays. ▶ BLOWFISH ▶ 3DES ▶ AES
IPsec	
IPsec Operation	Use this field to select the protocol to protect the IP packet. See Framework Protocols on page 97 for information on the screen that displays. ▶ ESP ▶ AH
ESP Transform	Use this field to select the type of encryption you want to use. See Encryption Algorithms on page 98 for information on the screen that displays. ▶ DES ▶ 3DES ▶ BLOWFISH ▶ NONE ▶ AES ▶ TWOFISH *NOTE:* The options that display depend on the **IPsec Operation** you selected.

TABLE 35: The VPN > IPsec > Add/Edit Screen (continued)

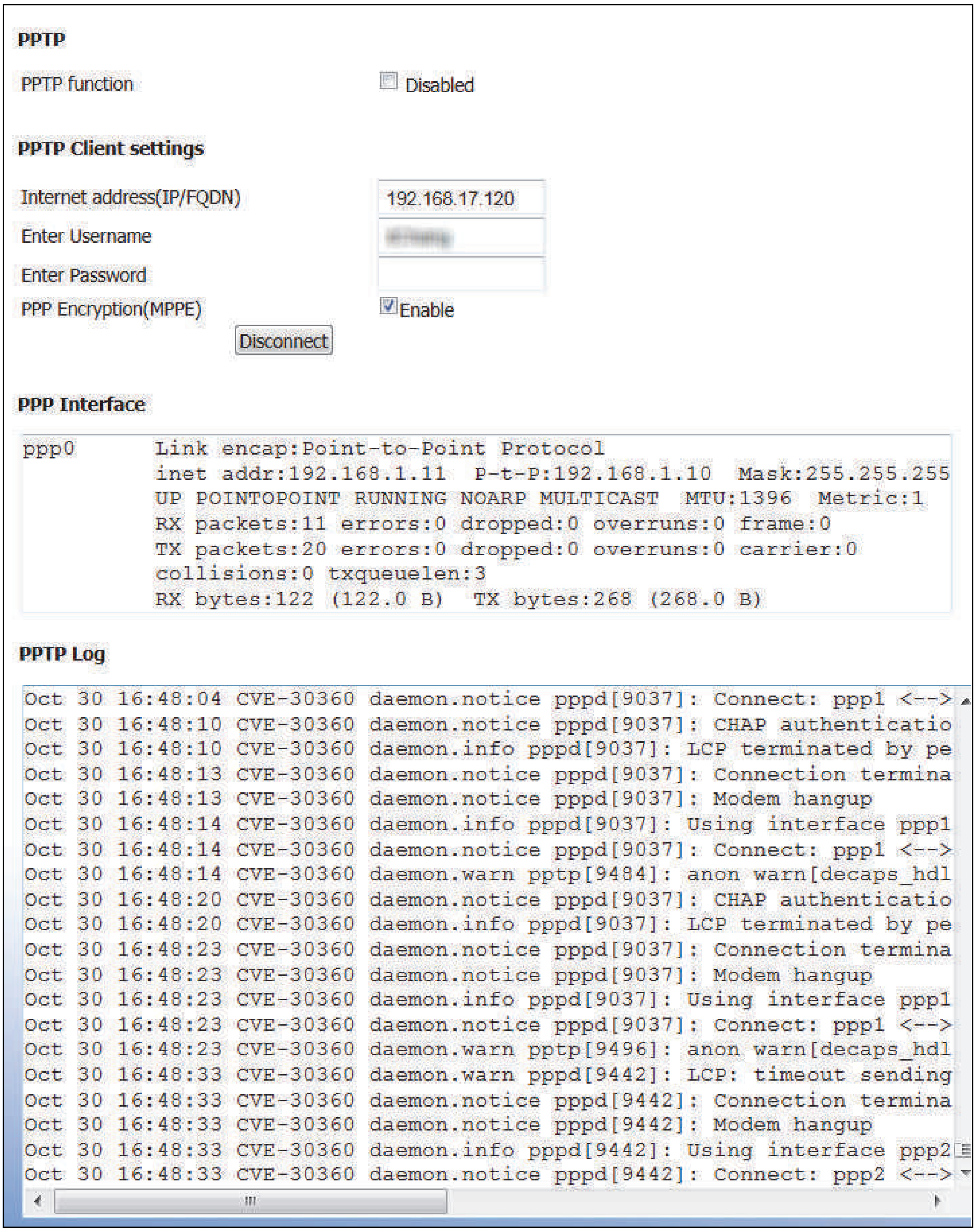
ESP AUTH	Use this field to select the type of ESP Authentication you want to use. See Cryptographic Hash Function on page 98 for information on the screen that displays. - MD5 - SHA - SHA2_256 *NOTE:* The options that display depend on the **IPsec Operation** you selected.
AH	Use this field to select the type of AH Authentication you want to use. See Cryptographic Hash Function on page 98 for information on the screen that displays. - MD5 - SHA - SHA2_256 *NOTE:* The options that display depend on the **IPsec Operation** you selected.
Tunnel Type	Use this field to select whether the type of the tunnel is public or private.
IPsec Life Duration	Use this field to enter the IPsec Life Duration value in seconds.
Tunnel Remote Host Configuration	
IP type	This displays the nature of the IP. *NOTE:* Leave this field at its default.
IP Address	Use this field to enter the allowed IP address for the tunnel’s connection.
Subnet Mask	Use this field to enter the tunnel’s subnet mask.
Back	Click this to return the fields in this screen to their last-saved values without saving your changes.
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.

8.4 THE PPTP SCREEN

Use this screen to configure PPTP function. You can turn PPTP function on or off and configure the settings.

Click **VPN** > **PPTP**. The following screen displays.

FIGURE 38: The VPN > PPTP Screen



PPTP

PPTP function □ Disabled

PPTP Client settings

Internet address(IP/FQDN) 192.168.17.120

Enter Username [redacted]

Enter Password

PPP Encryption(MPPE) ☑ Enable

PPP Interface

```
ppp0      Link encap:Point-to-Point Protocol
          inet addr:192.168.1.11  P-t-P:192.168.1.10  Mask:255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1396  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:122 (122.0 B)  TX bytes:268 (268.0 B)
```

PPTP Log

```
Oct 30 16:48:04 CVE-30360 daemon.notice pppd[9037]: Connect: ppp1 <-->
Oct 30 16:48:10 CVE-30360 daemon.notice pppd[9037]: CHAP authenticatio
Oct 30 16:48:10 CVE-30360 daemon.info pppd[9037]: LCP terminated by pe
Oct 30 16:48:13 CVE-30360 daemon.notice pppd[9037]: Connection termina
Oct 30 16:48:13 CVE-30360 daemon.notice pppd[9037]: Modem hangup
Oct 30 16:48:14 CVE-30360 daemon.info pppd[9037]: Using interface ppp1
Oct 30 16:48:14 CVE-30360 daemon.notice pppd[9037]: Connect: ppp1 <-->
Oct 30 16:48:14 CVE-30360 daemon.warn pptp[9484]: anon warn[decaps_hdl
Oct 30 16:48:20 CVE-30360 daemon.notice pppd[9037]: CHAP authenticatio
Oct 30 16:48:20 CVE-30360 daemon.info pppd[9037]: LCP terminated by pe
Oct 30 16:48:23 CVE-30360 daemon.notice pppd[9037]: Connection termina
Oct 30 16:48:23 CVE-30360 daemon.notice pppd[9037]: Modem hangup
Oct 30 16:48:23 CVE-30360 daemon.info pppd[9037]: Using interface ppp1
Oct 30 16:48:23 CVE-30360 daemon.notice pppd[9037]: Connect: ppp1 <-->
Oct 30 16:48:23 CVE-30360 daemon.warn pptp[9496]: anon warn[decaps_hdl
Oct 30 16:48:33 CVE-30360 daemon.warn pppd[9442]: LCP: timeout sending
Oct 30 16:48:33 CVE-30360 daemon.notice pppd[9442]: Connection termina
Oct 30 16:48:33 CVE-30360 daemon.notice pppd[9442]: Modem hangup
Oct 30 16:48:33 CVE-30360 daemon.info pppd[9442]: Using interface ppp2
Oct 30 16:48:33 CVE-30360 daemon.notice pppd[9442]: Connect: ppp2 <-->
```

The following table describes the labels in this screen.

TABLE 36: The VPN > PPTP Screen

PPTP	
PPTP function	Use this field to select whether the PPTP function be active or not. ▶ **Select** Disabled to deactivate the PPTP function. ▶ **Deselect** Disabled to activate the PPTP function.

TABLE 36: The VPN > PPTP Screen (continued)

PPTP Client settings	
Internet address (IP/ FQDN)	Use this field to enter the IP address or Fully-Qualified Domain Name of your PPTP Client.
Enter Username	Use this field to enter the username for your PPTP Client
Enter Password	Use this field to enter the password for your PPTP Client.
PPP Encryption (MPPE)	Use this field to select whether the PPP Encryption (MPPE) be active or not. ▶ **Select** Enabled to activate the PPP Encryption (MPPE). ▶ **Deselect** Enabled to deactivate the PPP Encryption (MPPE).
Connect	Click this to connect PPTP Client.
PPP Interface	This displays PPTP Interface connection information.
PPTP Log	This displays the PPTP section establish and termination.

9

TROUBLESHOOTING

Use this section to solve common problems with the CGNV2 and your network.

Problem: None of the LEDs Turn On

The CGNV2 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 CGNV2 can damage the CGNV2.

2. Ensure that the power adaptor is connected to the CGNV2 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 CGNV2.
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 18).
2. Ensure that the CGNV2’s hardware is connected correctly; see the Quick Installation Guide.
3. Disconnect and re-connect the power adaptor to the CGNV2.
4. If none of the above steps solve the problem, consult your vendor.

Problem: I Forgot the CGNV2's IP Address

1. The CGNV2's default LAN IP address is **192.168.0.1**.
2. You can locate the CGNV2'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 **hitronhub.home**. See The LAN IP Screen on page 40 for more information.
3. Depending on your operating system and your network, you may be able to find the CGNV2'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 CGNV2, you need to reset the CGNV2. See Resetting the CGNV2 on page 23. All user-configured data is lost, and the CGNV2 is returned to its default settings. If you previously backed-up a more recent version your CGNV2's settings, you can now upload them to the CGNV2; see The Backup Screen on page 45.

Problem: I Forgot the CGNV2'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 CGNV2 back to its factory defaults. See Resetting the CGNV2 on page 23. All user-configured data is lost, and the CGNV2 is returned to its default settings. If you previously backed-up a more recent version your CGNV2's settings, you can now upload them to the CGNV2; see The Backup Screen on page 45.

Problem: I Cannot Access the CGNV2 or the Internet

1. Ensure that you are using the correct IP address for the CGNV2.
2. Check your network's hardware connections, and that the CGNV2's LEDs display correctly (see LEDs on page 18).
3. Make sure that your computer is on the same subnet as the CGNV2; 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 CGNV2. See Resetting the CGNV2 on page 23. All user-configured data is lost, and the CGNV2 is returned to its default settings. If you previously backed-up a more recent version your

CGNV2's settings, you can now upload them to the CGNV2; see The Backup Screen on page 45.

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 30).

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 CGNV2'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 CGNV2's signal quality and coverage area.

3 Ensure that the CGNV2 and the wireless client are set to use the same wireless mode and SSID (see The Basic Screen on page 80) and security settings (see The Security Screen on page 83).

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 CGNV2 and the button on the wireless client within two minutes of one another.

INDEX