CGNV4 DOCSIS 3.0 eMTA WiFi Gateway

User's Guide DRAFT

Version 1.1 - 02/2014

hitron

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the CGNV4's features via its Graphical User Interface (GUI).

How to Use this User's Guide

This manual contains information on each the CGNV4's GUI screens, and describes how to use its various features.

- Use the Introduction on page 14 to see an overview of the topics covered in this manual.
- Use the Table of Contents (page 6), List of Figures (page 10) and List of Tables (page 12) to quickly find information about a particular GUI screen or topic.
- Use the Index (page 108) to find information on a specific keyword.
- Use the rest of this User's Guide to see in-depth descriptions of the CGNV4's features.

Related Documentation

- **Quick Installation Guide**: see this for information on getting your CGNV4 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 CGNV4's Graphical User Interface (GUI) contains a **Help** button. Click this button to see additional information about configuring the screen.

Document Conventions

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

- Bulleted paragraphs are used to list items, and to indicate options.

1 Numbered paragraphs indicate procedural steps.

NOTE: Notes provide additional information on a subject.

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

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

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

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

> Click **Settings** > **Advanced Settings**.

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

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

> Press [ENTER] to continue.

Customer Support

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

Default Login Details

The CGNV4's default IP address and login credentials are as follows. For more information, see Logging in to the CGNV4 on page 23.

Table 1: Default Credentials

IP Address	192.168.0.1
Username	admin
Password	admin

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

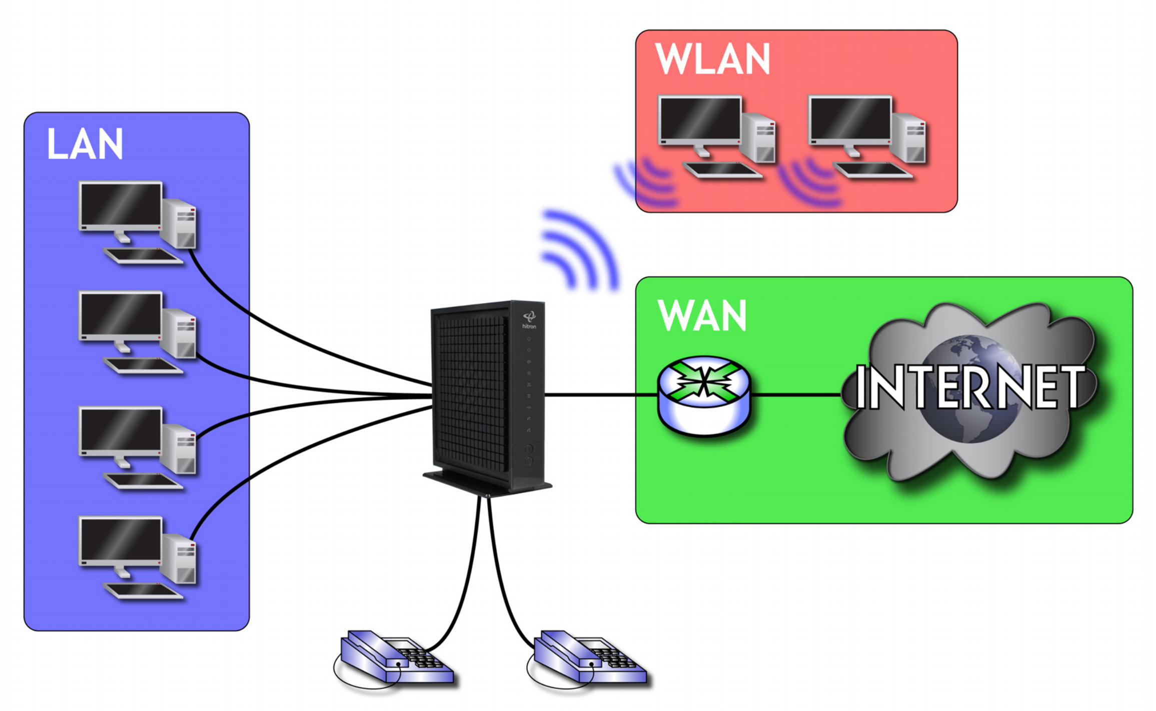
Introduction

This chapter introduces the CGNV4 and its GUI (Graphical User Interface).

1.1 CGNV4 Overview

Your CGNV4 is a DOCSIS cable modem, router, embedded Multimedia Terminal Adapter (eMTA) and wireless access point that allows you to connect your cabled Ethernet, wireless devices and analog telephones to one anotherand to the Internet via your building's cable connection.

Figure 1: Application Overview



1.1.1 Key Features

The CGNV4 provides:

- DOCSIS/EuroDOCSIS 3.0 compliance
- IEEE 802.11ac WiFi access point 3x3 dual band MIMO internal antennas
- Local Area Network connection via four 10/100/1000 Mbps Ethernet ports
- Two FXS analog telephone ports using SIP or MGCP
- USB 2.0 host port
- Quality of Service (QoS) for optimal video and data performance
- External LEDs clearly displaying device and network status
- Full operator control via configuration file and SNMP
- TR-069 and HNAP for easy setup and remote management
- Wireless security: WEP, WPA-PSK and WPA2-PSK encryption, Wifi Protected Setup (WPS) push-button and PIN configuration, MAC filtering
- Settings backup and restore
- Secure configuration interface, accessible by Web browser

1.2 Hardware Connections

This section describes the CGNV4's physical ports and buttons.

Figure 2: Hardware Connections

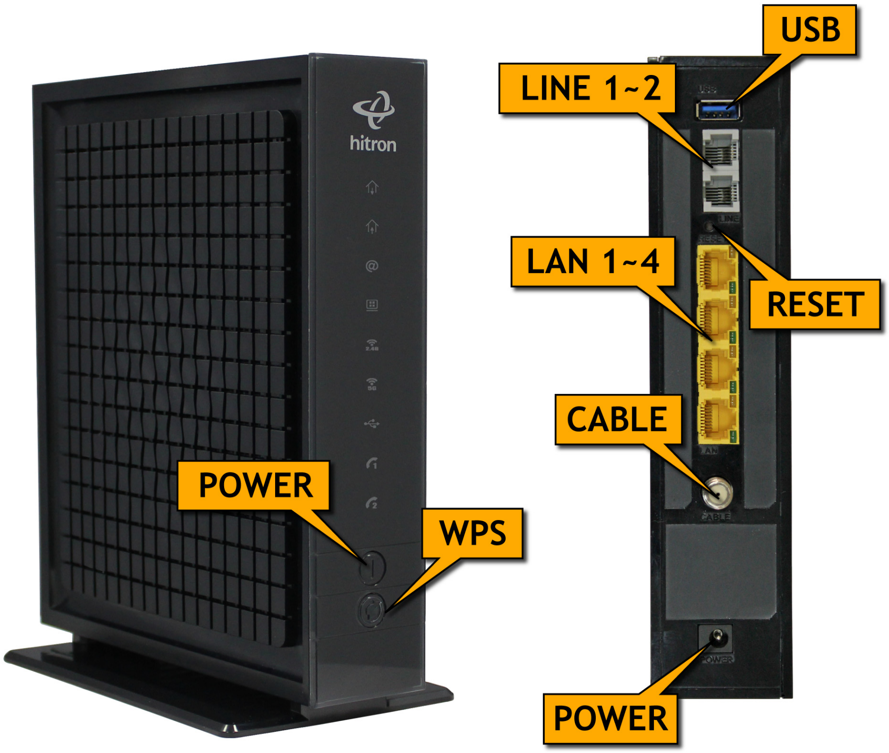


Table 2: Hardware Connections

WPS	Press this button to begin the WiFi Protected Setup (WPS) Push-Button Configuration (PBC) procedure. Press the PBC button on your wireless clients in the coverage area within two minutes to enable them to join the wireless network. See WPS on page 63 for more information.
USB	The CGNV4 provides a USB 2.0 host port, allowing you to plug in USB flash disks for mounting and sharing through the LAN interfaces via the Samba protocol (network neighborhood). The CGNV4 supports the following Windows file systems: - FAT16 - FAT32 - NTFS **USB devices must not drain more than 500mA from the USB port. USB devices requiring more than 500mA should be provided with their own power source(s).**
LINE 1	Use these ports to connect your analog phones for VoIP services, using cables with RJ11 connectors.
LINE 2	
RESET	Use this button to reboot or reset your CGNV4 to its factory default settings. To reboot the CGNV4, press the button and hold it for less than five seconds. The CGNV4 restarts, using your existing settings. To reset the CGNV4, press the button and hold it for more than ten seconds. All user-configured settings are deleted, and the CGNV4 restarts using its factory default settings.
LAN1	Use these ports to connect your computers and other network devices, using Category 5 or 6 Ethernet cables with RJ45 connectors.
LAN2	
LAN3	
LAN4	

Table 2: Hardware Connections

CABLE	Use this to connect to the Internet via an F-type RF cable.
POWER	Use the **POWER** port to connect to the 12v/2A power adapter that came with your CGNV4. Use the **POWER** switch to turn the CGNV4 on or off. **NEVER use another power adapter with your CGNV4. Doing so could harm your CGNV4.** Figure 3: Power Adaptor

1.3 LEDs

This section describes the CGNV4’s LEDs (lights).

Figure 4: LEDs

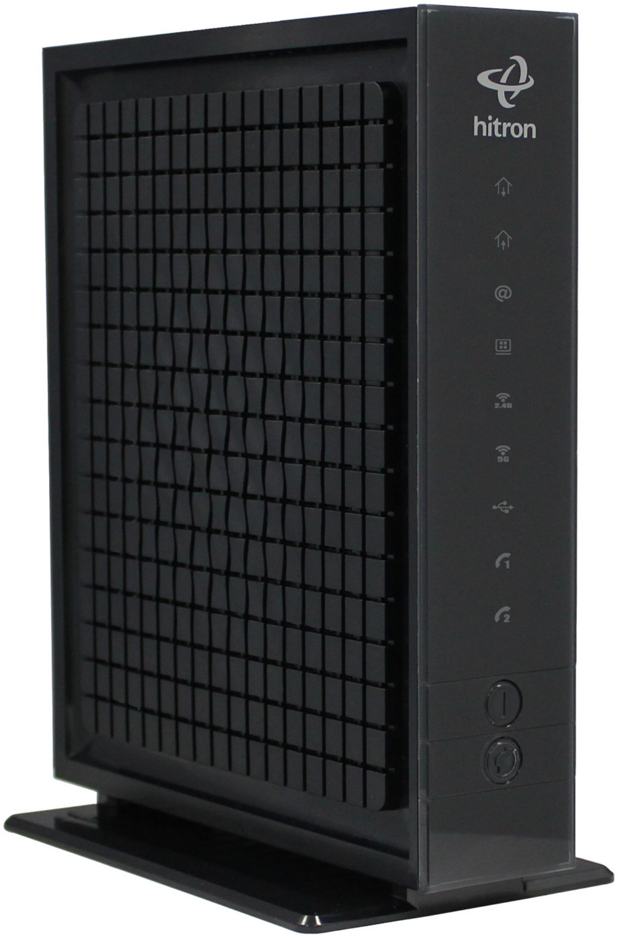


Table 3: LEDs

LED	STATUS	DESCRIPTION
US ⇅	Green, blinking	The CGNV4 is searching for an upstream frequency on the **CABLE** connection.
	Green, steady	The CGNV4 has successfully located and locked onto an upstream frequency on the **CABLE** connection.
	Blue	The CGNV4 is engaged in channel bonding on the upstream connection.
	Off	There is no upstream activity on the **CABLE** connection.

Table 3: LEDs

DS	Green, blinking	The CGNV4 is searching for a downstream frequency on the **CABLE** connection.
	Green, steady	The CGNV4 has successfully located and locked onto a downstream frequency on the **CABLE** connection.
	Blue	The CGNV4 is engaged in channel bonding on the downstream connection.
	Off	There is no downstream activity on the **CABLE** connection.
Status @	Blinking	The CGNV4's cable modem is registering with the service provider's CMTS.
	On	The CGNV4's cable modem has successfully registered with the service provider and is ready for data transfer.
LAN	Off	No device is connected to one of the **LAN** ports.
	Green, blinking	A device is connected to one of the **LAN** ports via a Fast Ethernet (100Mbps) link, and is transmitting or receiving data.
	Green, steady	A device is connected to one of the **LAN** ports via a Fast Ethernet (100Mbps) link, but is not transmitting or receiving data.
	Blue, blinking	A device is connected to one of the **LAN** ports via a Gigabit Ethernet (1000Mbps) link, and is transmitting or receiving data.
	Blue, steady	A device is connected to one of the **LAN** ports via a Gigabit Ethernet (1000Mbps) link, but is not transmitting or receiving data.
WIRELESS (2.4GHZ) 2.4G	Off	The 2.4GHz wireless network is not enabled.
	Green, steady	The 2.4GHz wireless network is enabled, and no data is being transmitted or received over the 2.4GHz wireless network.
	Green, blinking	The 2.4GHz wireless network is enabled, and data is being transmitted or received over the 2.4GHz wireless network.
	Bi-color	Wi-Fi Protected Setup (WPS) is in operation on the 2.4GHz wireless network.

Table 3: LEDs

WIRELESS (5GHZ) 5G	Off	The 5GHz wireless network is not enabled.
	Green, steady	The 5GHz wireless network is enabled, and no data is being transmitted or received over the 5GHz wireless network.
	Green, blinking	The 5GHz wireless network is enabled, and data is being transmitted or received over the 5GHz wireless network.
	Bi-color	Wi-Fi Protected Setup (WPS) is in operation on the 5GHz wireless network.
USB	Off	No USB device is connected to a USB port.
	Green, steady	A USB device is connected to a USB port, and is not transmitting or receiving data.
	Green, blinking	A USB device is connected to a USB port, and is transmitting or receiving data.
Line 1 Line 2 ☎	Off	No telephone is connected to the relevant **Line** port.
	Blinking	A telephone is connected to the relevant **Line** port, and is off-hook.
	On	A telephone is connected to the relevant **Line** port, and is on-hook.

1.4 IP Address Setup

Before you log into the CGNV4’s GUI, your computer’s IP address must be in the same subnet as the CGNV4. This allows your computer to communicate with the CGNV4.

NOTE: See IP Addresses and Subnets on page 27 for background information.

If your computer is configured to get an IP address automatically, or if you are not sure, try to log in to the CGNV4 (see GUI Overview on page 24).

- If the login screen displays, your computer is already configured correctly.

- If the login screen does not display, your computer is not configured correctly. Follow the procedure in Manual IP Address Setup on page 22 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 CGNV4’s IP settings may have been changed from their defaults. If you do not know the CGNV4’s new address, you should return it to its factory defaults. See Resetting the CGNV4 on page 25. Bear in mind that ALL user-configured settings are lost.

1.4.1 Manual IP Address Setup

By default, your CGNV4’s local IP address is **192.168.0.1**. If your CGNV4 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**.

Take the following steps to manually set up your computer’s IP address to connect to the CGNV4:

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 network has an active DHCP server, select **Get an IP address automatically**.
   - If your network does not have an active DHCP server, 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 CGNV4 is not using the default IP address, enter an IP address and subnet mask that places your computer in the same subnet as the CGNV4.

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 CGNV4, or uses the IP address that you specified, and can communicate with the CGNV4.

1.5 Logging in to the CGNV4

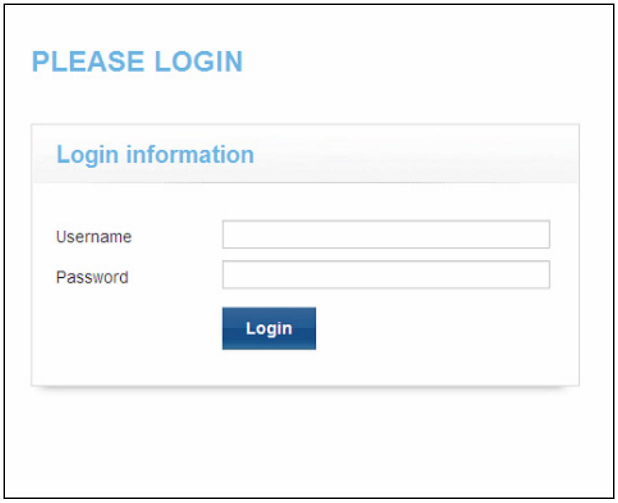
Take the following steps to log into the CGNV4's GUI.

NOTE: You can log into the CGNV4's GUI via the wireless interface. However, it is strongly recommended that you configure the CGNV4 via a wired connection on the LAN.

1 Open a browser window.

2 Enter the CGNV4's IP address (default **192.168.0.1**) in the URL bar. The **Login** screen displays.

Figure 5: Login



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

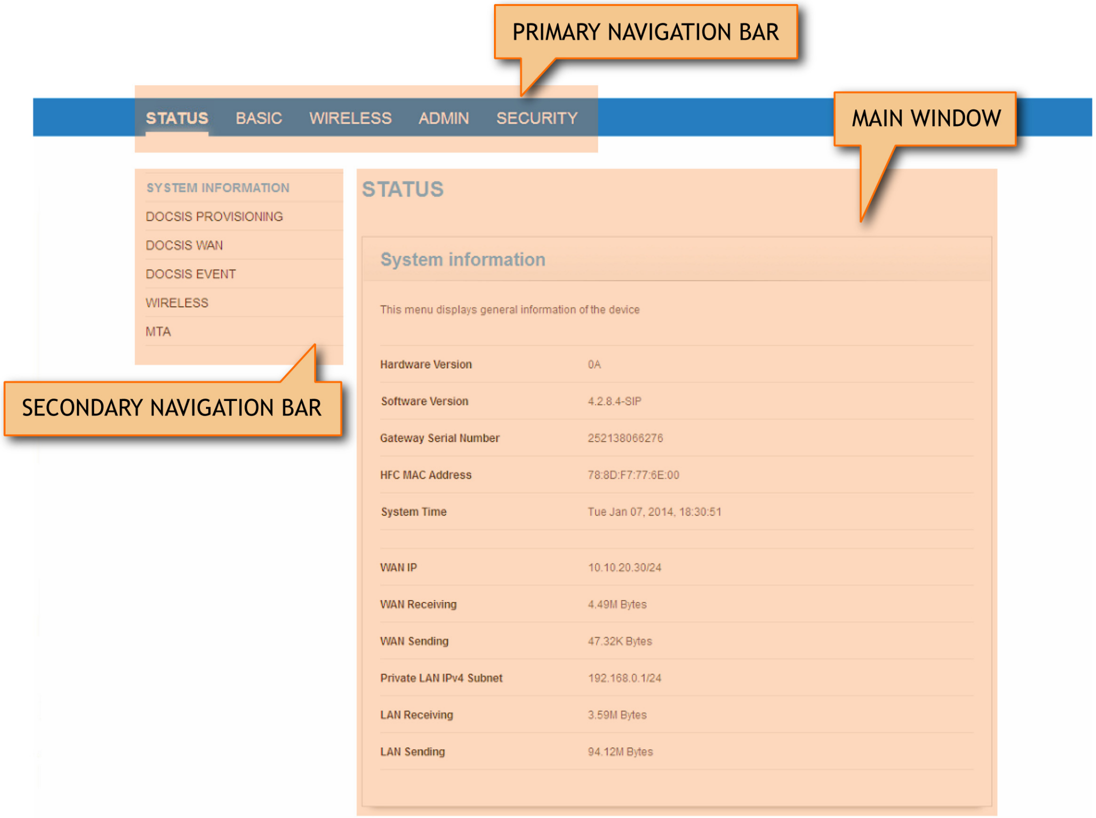
NOTE: The Username and Password are case-sensitive; “admin” is not the same as “Admin”.

4 Click **Login**. The **System Information** screen displays (see The System Information Screen on page 33).

1.6 GUI Overview

This section describes the CGNV4's GUI.

Figure 6: GUI Overview



STATUS

System information

This menu displays general information of the device

Hardware Version	0A
Software Version	4.2.8.4-SIP
Gateway Serial Number	252138066276
HFC MAC Address	78:8D:F7:77:6E:00
System Time	Tue Jan 07, 2014, 18:30:51
WAN IP	10.10.20.30/24
WAN Receiving	4.49M Bytes
WAN Sending	47.32K Bytes
Private LAN IPv4 Subnet	192.168.0.1/24
LAN Receiving	3.59M Bytes
LAN Sending	94.12M Bytes

Table 4: GUI Overview

Primary Navigation Bar	Use this section to move from one part of the GUI to another.

Table 4: GUI Overview (continued)

Secondary Navigation Bar	Use this section to move from one related screen to another.
Main Window	Use this section to read information about your CGNV4's configuration, and make configuration changes.

1.7 Resetting the CGNV4

When you reset the CGNV4 to its factory defaults, all user-configured settings are lost, and the CGNV4 is returned to its initial configuration state.

To reset the CGNV4, click **Admin** > **Device Reset**. In the screen that displays, click the **Factory Default** button.

The CGNV4 turns off and on again, using its factory default settings.

NOTE: Depending on your CGNV4's previous configuration, you may need to re-configure your computer's IP settings; see IP Address Setup on page 21.

2

Status

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

2.1 Status Overview

This section describes some of the concepts related to the **Status** 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 CGNV4 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 CGNV4:

- The public network (Wide Area Network or WAN) is the link between the cable connector and your Internet Service Provider. Your CGNV4's IP address on this network is assigned by your service provider.

- The private network 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 CGNV4 to assign them automatically via DHCP (Dynamic Host Configuration Protocol). IANA has reserved the following blocks of IP addresses to be used for private networks only:

Table 5: Private IP Address Ranges

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

If you assign addresses manually, they must be within the CGNV4's LAN subnet.

2.1.2.3 Subnets

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

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

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

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

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

Table 6: IP Address: Decimal and Binary

192	168	0	1
11000000	10101000	00000000	00000001

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

Table 7: Subnet Mask: Decimal and Binary

255	255	255	0
11111111	11111111	11111111	00000000

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

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

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

2.1.3 DHCP

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

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

If a computer is not configured to request an IP address via DHCP, you must configure an IP address manually if you want to access other computers and devices on the network. See IP Address Setup on page 21 for more information.

By default, the CGNV4 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 CGNV4 is a DHCP server on the LAN; it provides IP addresses to computers on the LAN which request them.

2.1.4 DHCP Lease

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

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

2.1.5 MAC Addresses

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

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

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

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

Bear in mind that a MAC address does not precisely represent a computer on your network (or elsewhere), it represents a network device, which may be part of a computer (or other device). For example, if a single computer has an Ethernet card (to connect to your CGNV4 via one of the **LAN** ports) and also has a wireless card (to connect to your CGNV4 over the wireless interface) the MAC addresses of the two cards will be different. In the case of the CGNV4, each internal module (cable modem module, Ethernet module, wireless module, etc.) possesses its own MAC address.

2.1.6 Routing Mode

When your CGNV4 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 CGNV4 on the WAN, and all traffic for LAN computers is sent to that IP address. The CGNV4 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 CGNV4 in routing mode, each computer on the LAN must be assigned an IP address in the CGNV4's subnet manually.

When the CGNV4 is not in routing mode, the service provider assigns an IP address to each computer connected to the CGNV4 directly. The CGNV4 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 CGNV4's configuration file.

2.1.7 Configuration Files

The CGNV4's configuration (or config) file is a document that the CGNV4 obtains automatically over the Internet from the service provider's server, which specifies the settings that the CGNV4 should use. It contains a variety of settings that are not present in the user-configurable Graphical User Interface (GUI) and can be specified only by the service provider.

2.1.8 Downstream and Upstream Transmissions

The terms "downstream" and "upstream" refer to data traffic flows, and indicate the direction in which the traffic is traveling. "Downstream" refers to traffic from the service provider to the CGNV4, and "upstream" refers to traffic from the CGNV4 to the service provider.

2.1.9 Cable Frequencies

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

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

2.1.10 Modulation

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

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

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

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

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

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

2.1.11 TDMA, FDMA and SCDMA

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

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

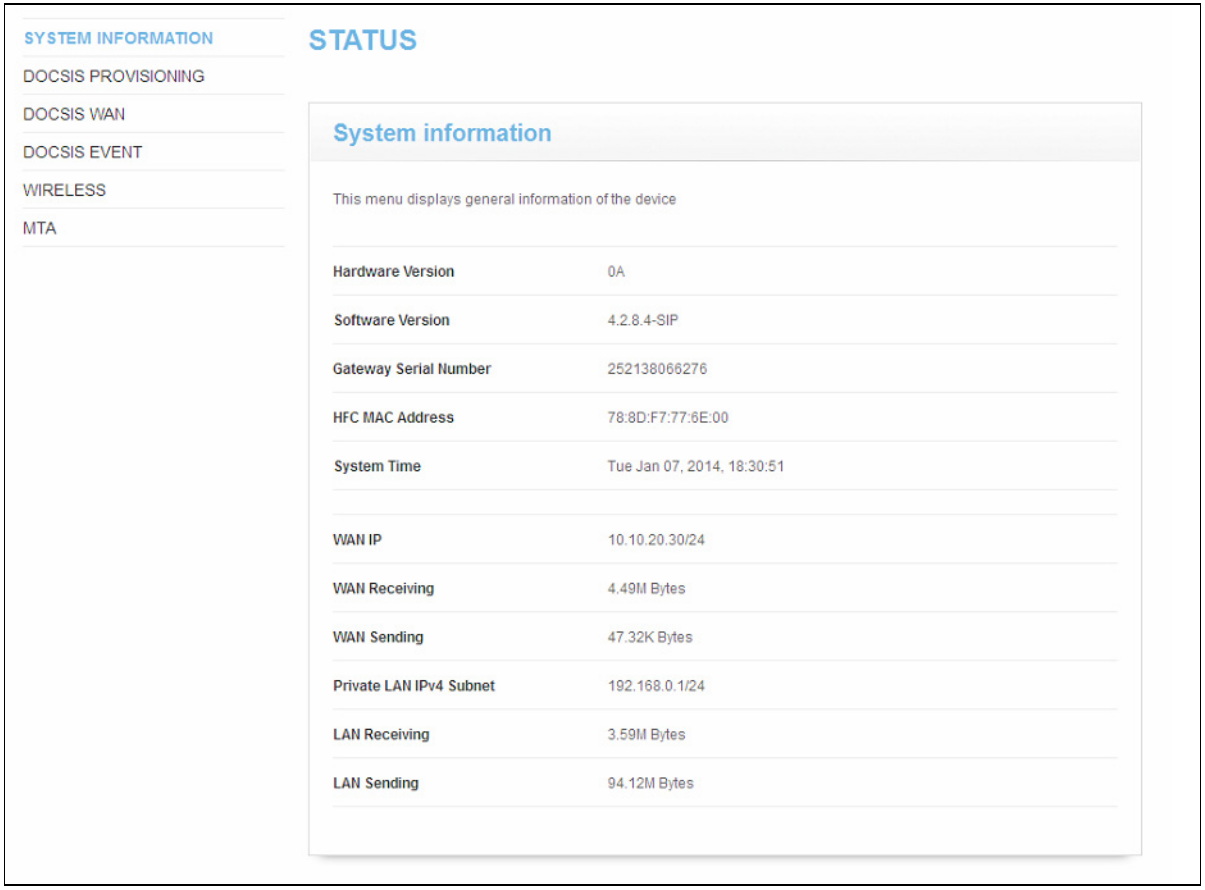
- SCDMA allows multiple users to share the same frequency channel by assigning a unique orthogonal code to each user.

2.2 The System Information Screen

Use this screen to see general information about your CGNV4's hardware, its software, and its connection to the Internet.

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

Figure 7: The Status: System Information Screen



STATUS

System information

This menu displays general information of the device

Hardware Version	0A
Software Version	4.2.8.4-SIP
Gateway Serial Number	252138066276
HFC MAC Address	78:8D:F7:77:6E:00
System Time	Tue Jan 07, 2014, 18:30:51
WAN IP	10.10.20.30/24
WAN Receiving	4.49M Bytes
WAN Sending	47.32K Bytes
Private LAN IPv4 Subnet	192.168.0.1/24
LAN Receiving	3.59M Bytes
LAN Sending	94.12M Bytes

The following table describes the labels in this screen.

Table 8: The Status: System Information Screen

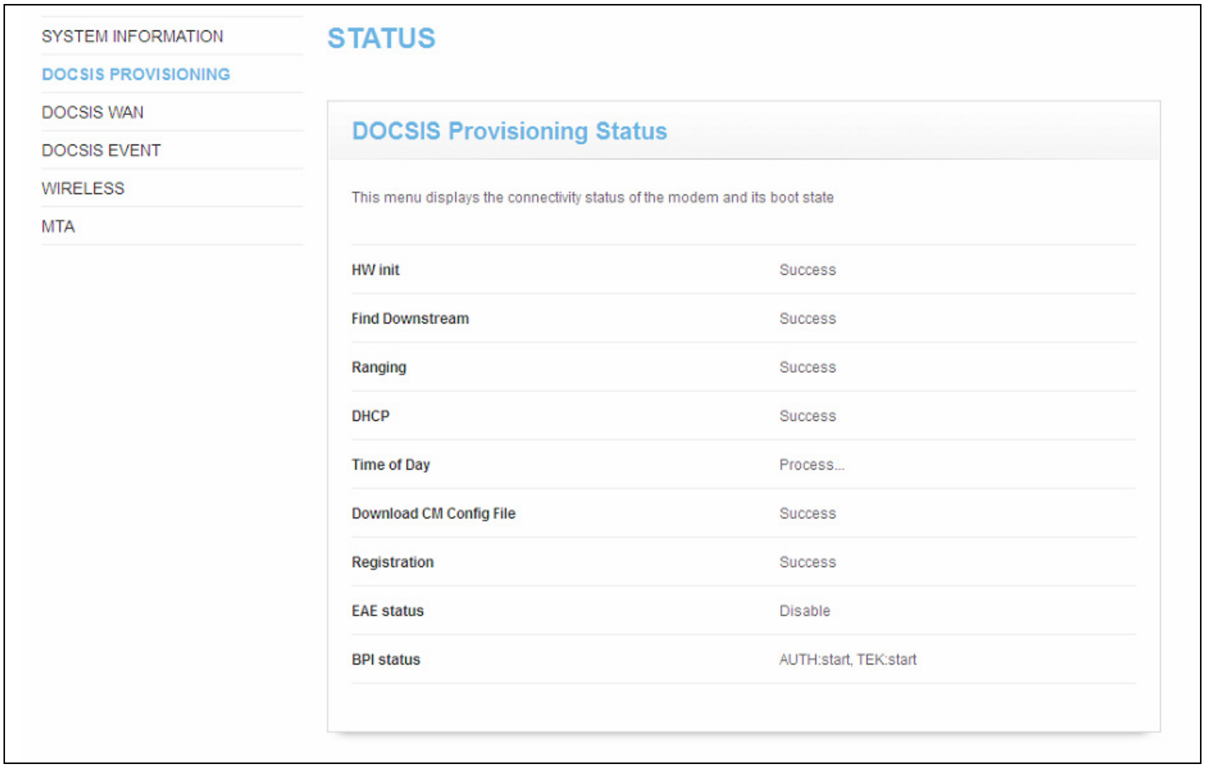
Hardware Version	This displays the version number of the CGNV4's physical hardware.
Software Version	This displays the version number of the software that controls the CGNV4.
Gateway Serial Number	This displays a number that uniquely identifies the device.
HFC MAC Address	This displays the Media Access Control (MAC) address of the CGNV4's Hybrid-Fiber Coax (HFC) module. This is the module that connects to the Internet through the **CATV** connection.
System Time	This displays the current date and time.
WAN IP	This displays the CGNV4's WAN IP address. This IP address is automatically assigned to the CGNV4
WAN Receiving	This displays the amount of data received over the WAN connection since the device was last started.
WAN Sending	This displays the amount of data transmitted over the WAN connection since the device was last started.
Private LAN IPv4 Subnet	This displays the CGNV4's LAN subnet mask.
LAN Receiving	This displays the amount of data received over the LAN connection since the device was last started.
LAN Sending	This displays the amount of data transmitted over the LAN connection since the device was last started.

2.3 The DOCSIS Provisioning Screen

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

Use this screen for troubleshooting purposes to ensure that the CGNV4 has successfully connected to the Internet; if an error has occurred you can identify the stage at which the failure occurred.Click **Status** > **DOCSIS Provisioning**. The following screen displays.

Figure 8: The Status: DOCSIS Provisioning Screen



DOCSIS Provisioning Status

This menu displays the connectivity status of the modem and its boot state

HW init	Success
Find Downstream	Success
Ranging	Success
DHCP	Success
Time of Day	Process...
Download CM Config File	Success
Registration	Success
EAE status	Disable
BPI status	AUTH:start, TEK:start

For each step:

- **Process** displays when the CGNV4 is attempting to complete a connection step.
- **Success** displays when the CGNV4 has completed a connection step.

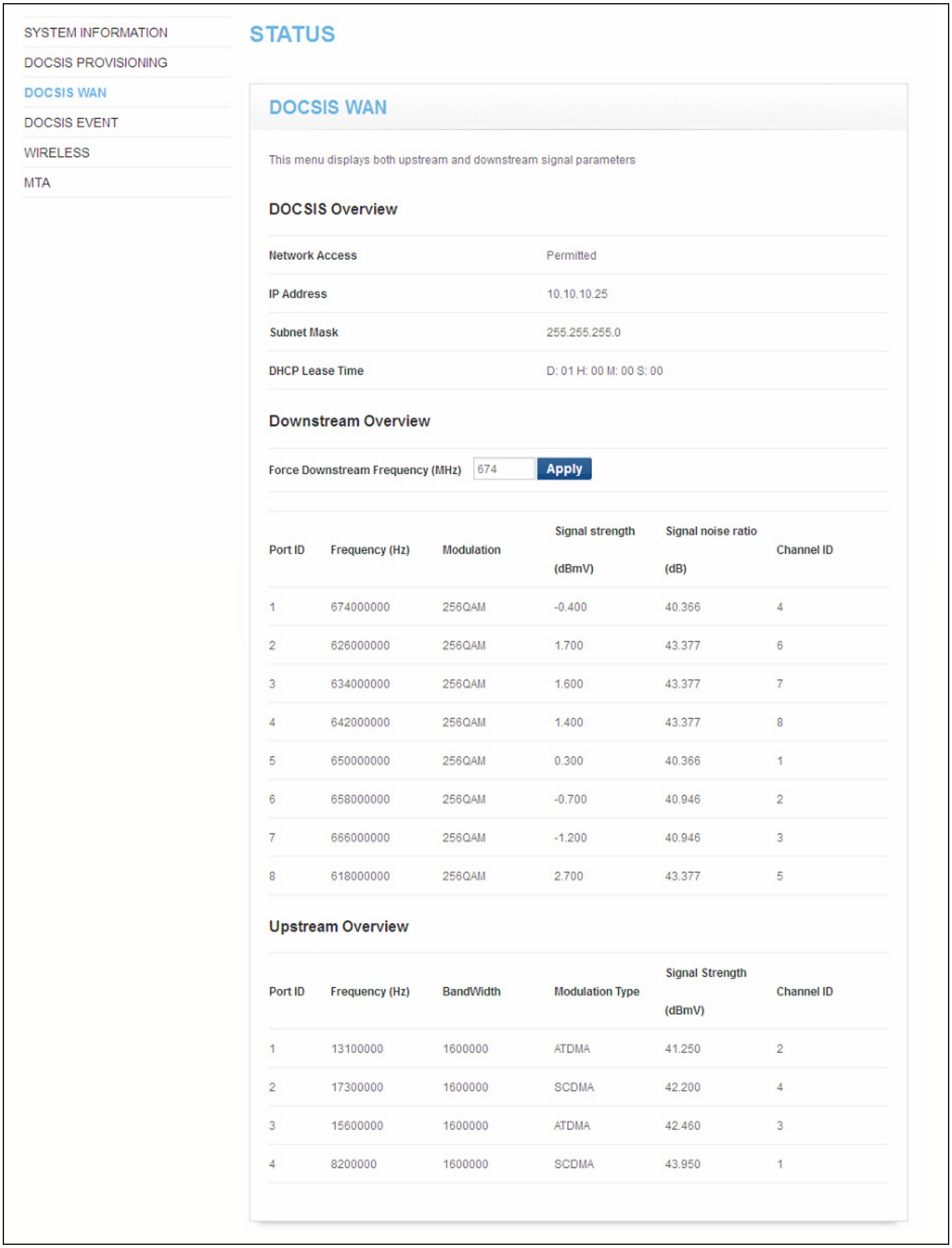
2.4 The DOCSIS WAN Screen

Use this screen to discover information about:

- The nature of the upstream and downstream connection between the CGNV4 and the device to which it is connected through the **CABLE** interface.
- IP details of the CGNV4's WAN connection.

Click **Status** > **DOCSIS WAN**. The following screen displays.Click **Status** > **DOCSIS WAN**. The following screen displays.

Figure 9: The Status: DOCSIS WAN Screen



DOCSIS WAN

This menu displays both upstream and downstream signal parameters

DOCSIS Overview

Network Access	Permitted
IP Address	10.10.10.25
Subnet Mask	255.255.255.0
DHCP Lease Time	D: 01 H: 00 M: 00 S: 00

Downstream Overview

Force Downstream Frequency (MHz) 674

Port ID	Frequency (Hz)	Modulation	Signal strength (dBmV)	Signal noise ratio (dB)	Channel ID
1	674000000	256QAM	-0.400	40.366	4
2	626000000	256QAM	1.700	43.377	6
3	634000000	256QAM	1.600	43.377	7
4	642000000	256QAM	1.400	43.377	8
5	650000000	256QAM	0.300	40.366	1
6	658000000	256QAM	-0.700	40.946	2
7	666000000	256QAM	-1.200	40.946	3
8	618000000	256QAM	2.700	43.377	5

Upstream Overview

Port ID	Frequency (Hz)	BandWidth	Modulation Type	Signal Strength (dBmV)	Channel ID
1	13100000	1600000	ATDMA	41.250	2
2	17300000	1600000	SCDMA	42.200	4
3	15600000	1600000	ATDMA	42.460	3
4	8200000	1600000	SCDMA	43.950	1

The following table describes the labels in this screen.

Table 9: The Status: DOCSIS WAN Screen

DOCSIS Overview	
Network Access	This displays whether or not your service provider allows you to access the Internet over the **CABLE** connection. **Permitted** displays if you can access the Internet. **Denied** displays if you cannot access the Internet.
IP Address	This displays the CGNV4’s WAN IP address. This IP address is automatically assigned to the CGNV4
Subnet Mask	This displays the CGNV4’s WAN subnet mask.
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.
Downstream Overview NOTE: The downstream signal is the signal transmitted to the CGNV4.	
Force Downstream Frequency (MHz)	Use this to configure the CGNV4 to use a specific downstream frequency. Enter the desired frequency in Megahertz (MHz) and click **Apply**.
Port ID	This displays the ID number of the downstream connection’s port.
Frequency (Hz)	This displays the actual frequency in Hertz (Hz) of each downstream data channel to which the CGNV4 is connected.
Modulation	This displays the type of modulation that each downstream channel uses.
Signal Strength (dBmV)	This displays the power of the signal of each downstream data channel to which the CGNV4 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 CGNV4 is connected, in dB (decibels).
Channel ID	This displays the ID number of each channel on which the downstream signal is transmitted.
Upstream Overview NOTE: The upstream signal is the signal transmitted from the CGNV4.	

Table 9: The Status: DOCSIS WAN Screen (continued)

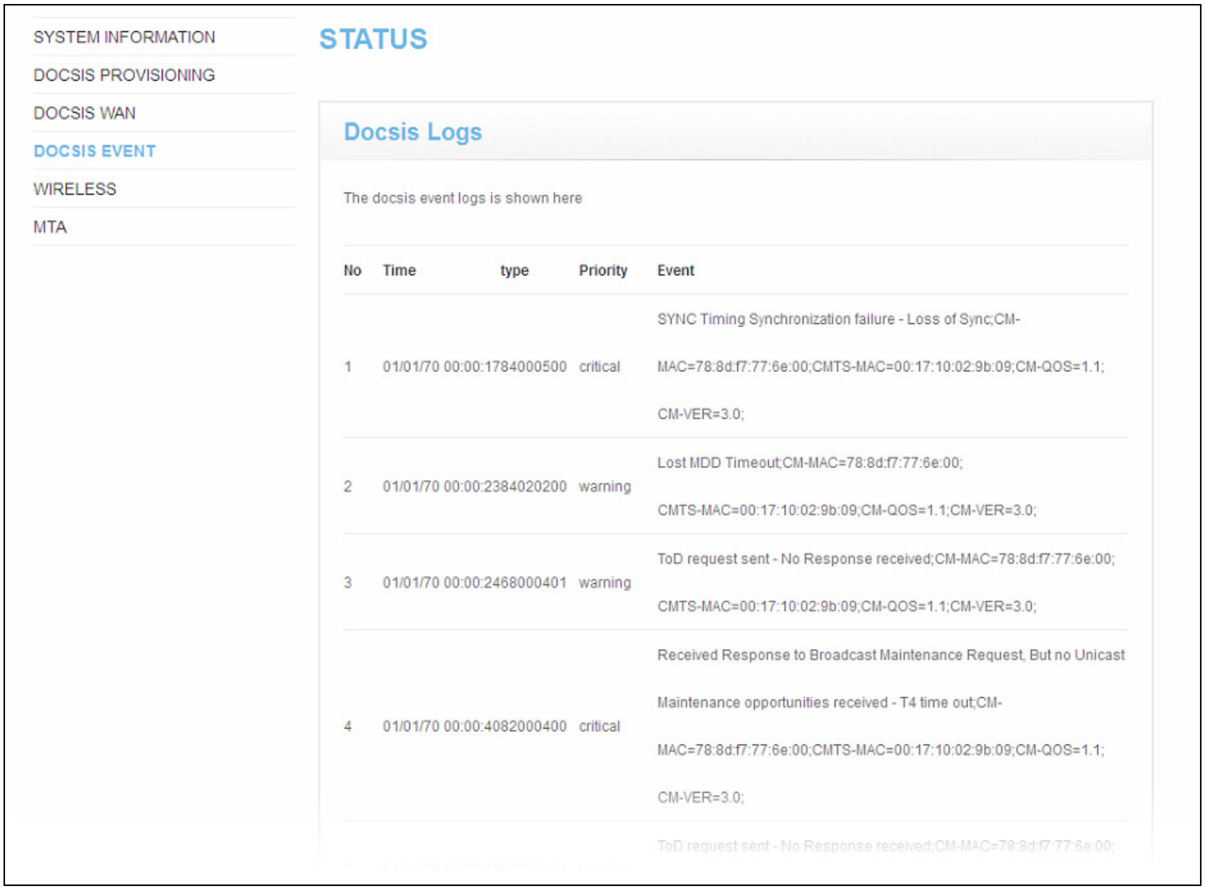
Force Downstream Frequency (MHz)	Use this to configure the CGNV4 to use a specific upstream frequency. Enter the desired frequency in Megahertz (MHz) and click **Apply**.
Port ID	This displays the ID number of the upstream connection’s port.
Frequency (Hz)	This displays the actual frequency in Hertz (Hz) of each upstream data channel to which the CGNV4 is connected.
Modulation	This displays the type of modulation that each upstream channel uses.
Signal Strength (dBmV)	This displays the power of the signal of each upstream data channel to which the CGNV4 is connected, in dBmV (decibels above/below 1 millivolt).
Signal Noise Ratio (dB)	This displays the Signal to Noise Ratio (SNR) of each upstream data channel to which the CGNV4 is connected, in dB (decibels).
Channel ID	This displays the ID number of each channel on which the upstream signal is transmitted.

2.5 The DOCSIS Event Screen

Use this screen to view information about local WAN activity events.

Click **Status** > **DOCSIS Event**. The following screen displays.

Figure 10: The Status: DOCSIS Event Screen



The docsis event logs is shown here

No	Time	type	Priority	Event
1	01/01/70 00:00:1784000500	critical		SYNC Timing Synchronization failure - Loss of Sync;CM-MAC=78:8d:f7:77:6e:00;CMTS-MAC=00:17:10:02:9b:09;CM-QOS=1.1;CM-VER=3.0;
2	01/01/70 00:00:2384020200	warning		Lost MDD Timeout;CM-MAC=78:8d:f7:77:6e:00;CMTS-MAC=00:17:10:02:9b:09;CM-QOS=1.1;CM-VER=3.0;
3	01/01/70 00:00:2468000401	warning		ToD request sent - No Response received;CM-MAC=78:8d:f7:77:6e:00;CMTS-MAC=00:17:10:02:9b:09;CM-QOS=1.1;CM-VER=3.0;
4	01/01/70 00:00:4082000400	critical		Received Response to Broadcast Maintenance Request, But no Unicast Maintenance opportunities received - T4 time out;CM-MAC=78:8d:f7:77:6e:00;CMTS-MAC=00:17:10:02:9b:09;CM-QOS=1.1;CM-VER=3.0;
[illegible]	[illegible]	[illegible]		ToD request sent - No Response received;CM-MAC=78:8d:f7:77:6e:00;

The following table describes the labels in this screen.

Table 10: The Status: DOCSIS Event Screen

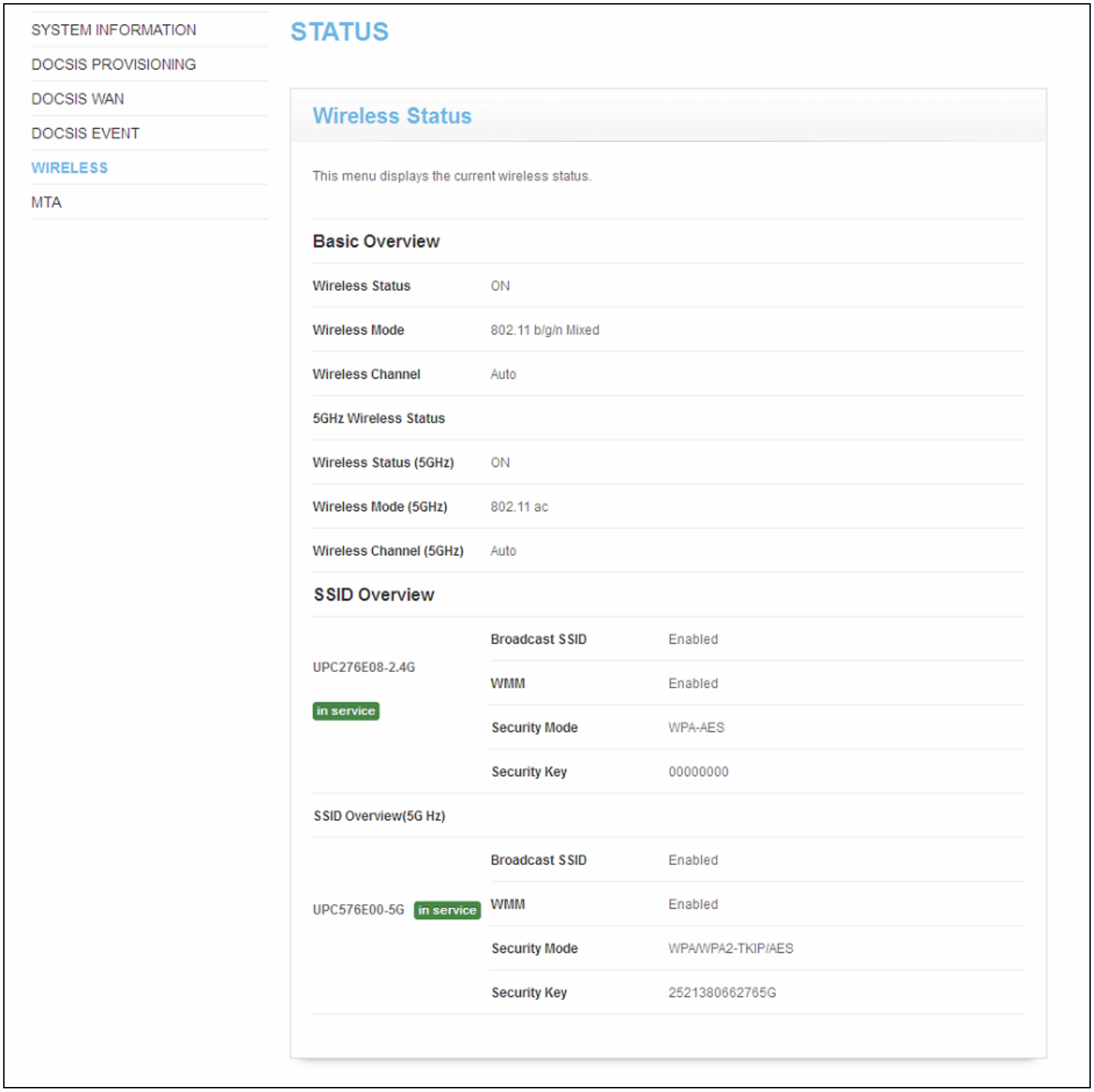
No	This displays the arbitrary, incremental index number assigned to the event.
Time	This displays the date and time at which the event occurred.
Type	This displays the nature of the event.
Priority	This displays the severity of the event.
Event	This displays a description of the event.

2.6 The Wireless Status Screen

Use this screen to view information about the CGNV4's wireless network.

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

Figure 11: The Status: Wireless Status Screen



Wireless Status

This menu displays the current wireless status.

Basic Overview

Wireless Status	ON
Wireless Mode	802.11 b/g/n Mixed
Wireless Channel	Auto
5GHz Wireless Status	
Wireless Status (5GHz)	ON
Wireless Mode (5GHz)	802.11 ac
Wireless Channel (5GHz)	Auto

SSID Overview

UPC276E08-2.4G in service	Broadcast SSID	Enabled
	WMM	Enabled
	Security Mode	WPA-AES
	Security Key	00000000
SSID Overview(5G Hz)		
UPC576E00-5G in service	Broadcast SSID	Enabled
	WMM	Enabled
	Security Mode	WPA/WPA2-TKIP/AES
	Security Key	2521380662765G

The following table describes the labels in this screen.

Table 11: The Status: Wireless Status Screen

Basic Overview	
Wireless Status	This field displays **ON** when the CGNV4’s 2.4 GHz wireless network is active, and displays **OFF** when it is inactive.

Table 11: The Status: Wireless Status Screen (continued)

Wireless Mode	This displays the type of 2.4 GHz wireless network that the CGNV4 is using.
Wireless Channel	This displays the wireless channel on which the CGNV4’s 2.4 GHz wireless network is transmitting and receiving.
5GHz Wireless Status	
Wireless Status (5GHz)	This field displays **ON** when the CGNV4’s 5 GHz wireless network is active, and displays **OFF** when it is inactive.
Wireless Mode (5GHz)	This displays the type of 5 GHz wireless network that the CGNV4 is using.
Wireless Channel (5GHz	This displays the wireless channel on which the CGNV4’s 5 GHz wireless network is transmitting and receiving.
SSID Overview	
(SSID)	This displays the 2.4 GHz wireless network’s Service Set Identifier. This is the name of the wireless network, to which wireless clients connect.
Broadcast SSID	This field displays **Enabled** when the 2.4 GHz wireless network’s SSID is being broadcast, and displays **Disabled** when it is not.
WMM	This field displays **Enabled** when the 2.4 GHz wireless network, and displays **Disabled** when it is not.
Security Mode	This displays the type of security the CGNV4’s 2.4 GHz wireless network is currently using.
Security Key	This displays the password for the CGNV4’s 2.4 GHz wireless network.
SSID Overview (5GHz)	
(SSID)	This displays the 5 GHz wireless network’s Service Set Identifier. This is the name of the wireless network, to which wireless clients connect.
Broadcast SSID	This field displays **Enabled** when the 5 GHz wireless network’s SSID is being broadcast, and displays **Disabled** when it is not.
WMM	This field displays **Enabled** when the 5 GHz wireless network, and displays **Disabled** when it is not.

Table 11: The Status: Wireless Status Screen (continued)

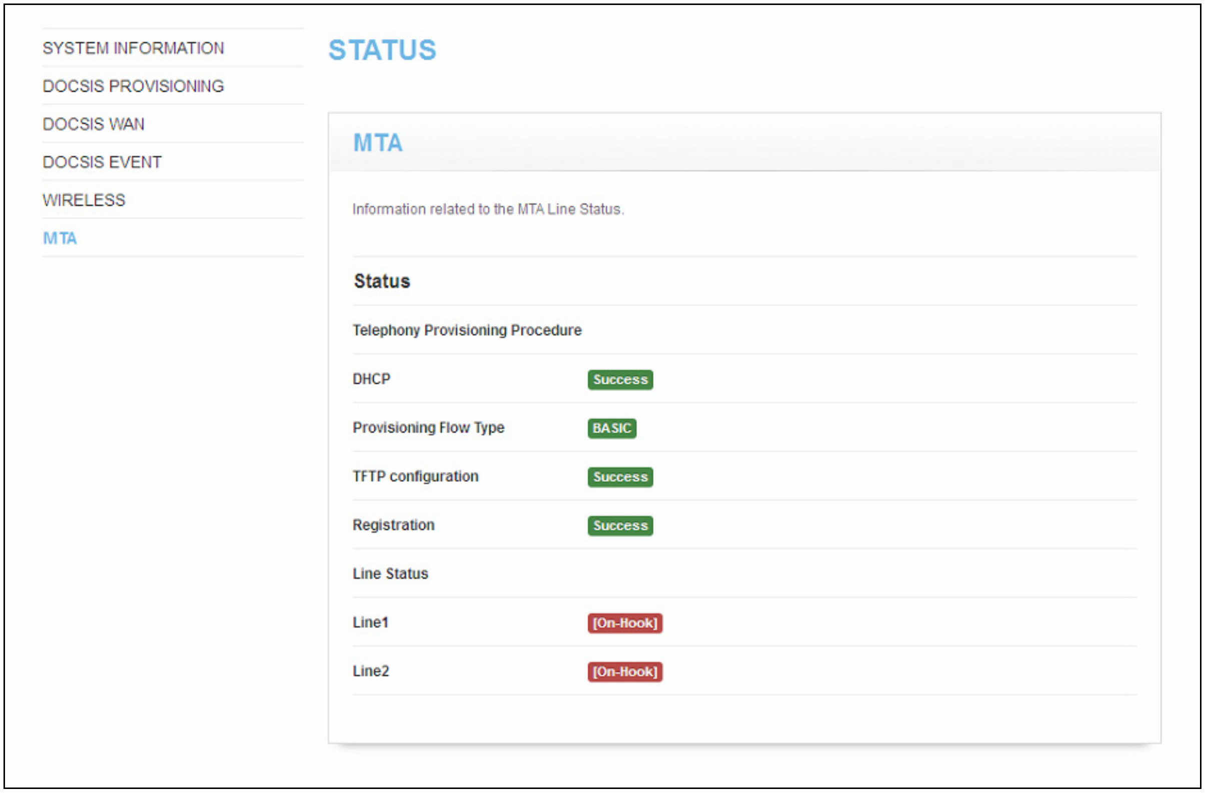
Security Mode	This displays the type of security the CGNV4’s 5 GHz wireless network is currently using.
Security Key	This displays the password for the CGNV4’s 5 GHz wireless network.

2.7 The MTA Screen

Use this screen to see general information about the CVE-30360’s embedded Multimedia Terminal Adapter module.

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

Figure 12: The Status: MTA Screen



STATUS

MTA

Information related to the MTA Line Status.

Status	
Telephony Provisioning Procedure	
DHCP	Success
Provisioning Flow Type	BASIC
TFTP configuration	Success
Registration	Success
Line Status	
Line1	[On-Hook]
Line2	[On-Hook]

The following table describes the labels in this screen.

Table 12: The Status: MTA Screen

Telephony Provisioning Procedure	
DHCP	This field displays the status of the remote telephony DHCP server.
Provisioning Flow Type	This displays the type of security used for voice calls through the CGNV4.
TFTP Configuration	This field displays the status of the remote telephony TFTP server.
Registration	This field displays the overall status of voice call registration.
Line Status	
Line 1	These fields display the current status of each phone connected to the CGNV4.
Line 2	

3

Basic

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

3.1 Basic Overview

This section describes some of the concepts related to the **Basic** screens (see also Status Overview on page 26).

3.1.1 The Domain Name System

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.

3.1.2 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 CGNV4 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.

3.1.3 Port Triggering

Port triggering is a means of automating port forwarding. The CGNV4 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 CGNV4 automatically opens the incoming ports specified in the rule, in anticipation of incoming traffic.

3.1.4 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.

3.1.5 Routing Mode

When your CGNV4 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 CGNV4 on the WAN, and all traffic for LAN computers is sent to that IP address. The CGNV4 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 CGNV4 in routing mode, each computer on the LAN must be assigned an IP address in the CGNV4's subnet manually.

When the CGNV4 is not in routing mode, the service provider assigns an IP address to each computer connected to the CGNV4 directly. The CGNV4 does not perform any routing operations, and traffic flows between the computers and the service provider.

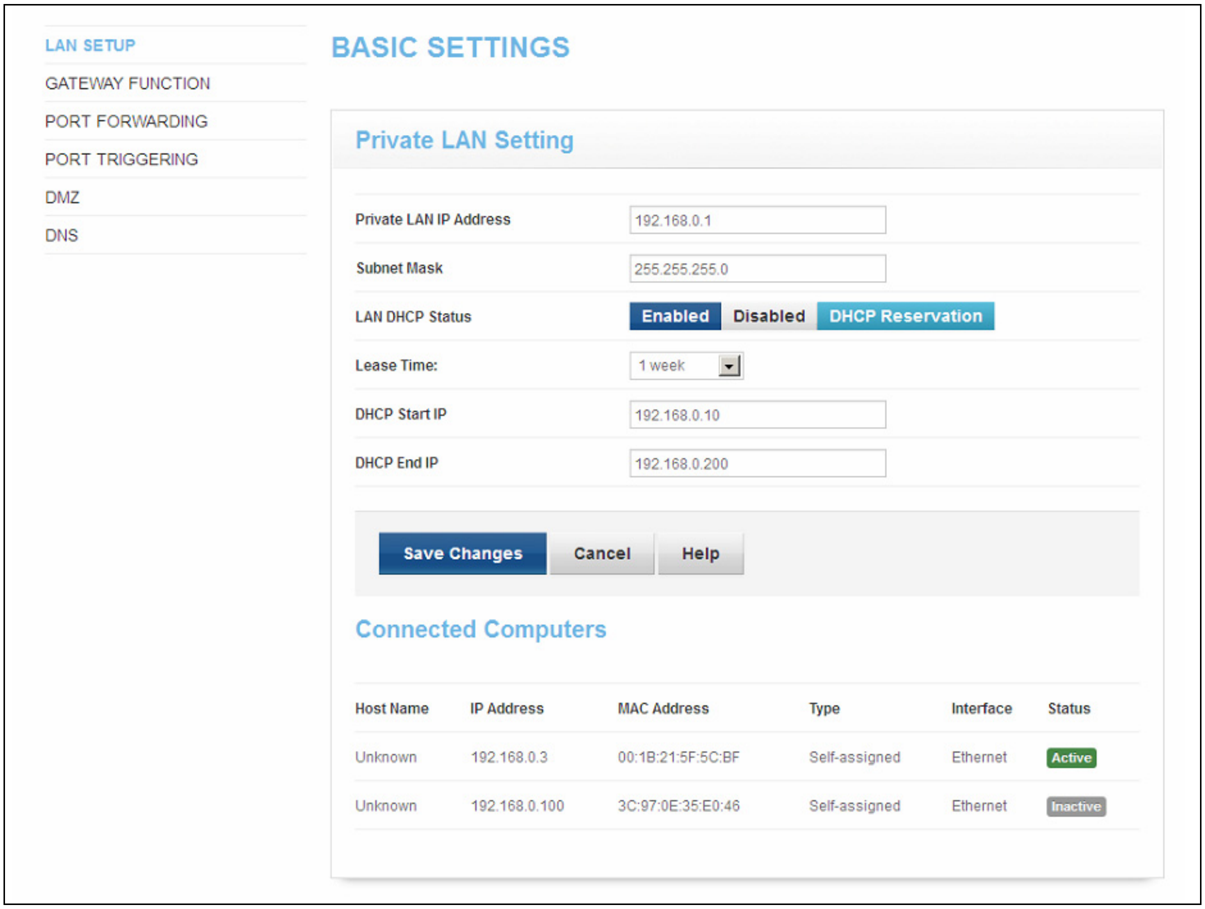
3.2 The LAN Setup Screen

Use this screen to:

- View information about the CGNV4's connection to the WAN
- Configure the CGNV4's internal DHCP server
- Define how the CGNV4 assigns IP addresses on the LAN
- See information about the network devices connected to the CGNV4 on the LAN.

Click **Basic** > **LAN Setup**. The following screen displays.

Figure 13: The Basic: LAN Setup Screen



BASIC SETTINGS

Private LAN Setting

Private LAN IP Address	192.168.0.1
Subnet Mask	255.255.255.0
LAN DHCP Status	Enabled Disabled DHCP Reservation
Lease Time:	1 week
DHCP Start IP	192.168.0.10
DHCP End IP	192.168.0.200

Connected Computers

Host Name	IP Address	MAC Address	Type	Interface	Status
Unknown	192.168.0.3	00:1B:21:5F:5C:BF	Self-assigned	Ethernet	Active
Unknown	192.168.0.100	3C:97:0E:35:E0:46	Self-assigned	Ethernet	Inactive

The following table describes the labels in this screen.

Table 13: The Basic: LAN Setup Screen

Private LAN Setting	
Private LAN IP Address	Use this field to define the IP address of the CGNV4 on the LAN.
Subnet Mask	Use this field to define the LAN subnet. Use dotted decimal notation (for example, **255.255.255.0**).
LAN DHCP Status	Use this field to configure whether or not the CGNV4's DHCP server is active. ▸ To turn the DHCP server on, click **Enabled**. ▸ To turn the DHCP server off, click **Disabled**.
Lease Time	Use this to select 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.

Table 13: The Basic: LAN Setup Screen (continued)

DHCP Start IP	Use this field to specify the IP address at which the CGNV4 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 CGNV4 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.
Save	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.
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**).
Status	This displays **Active** when the connected computer is online, and **Inactive** when the connected computer is offline.

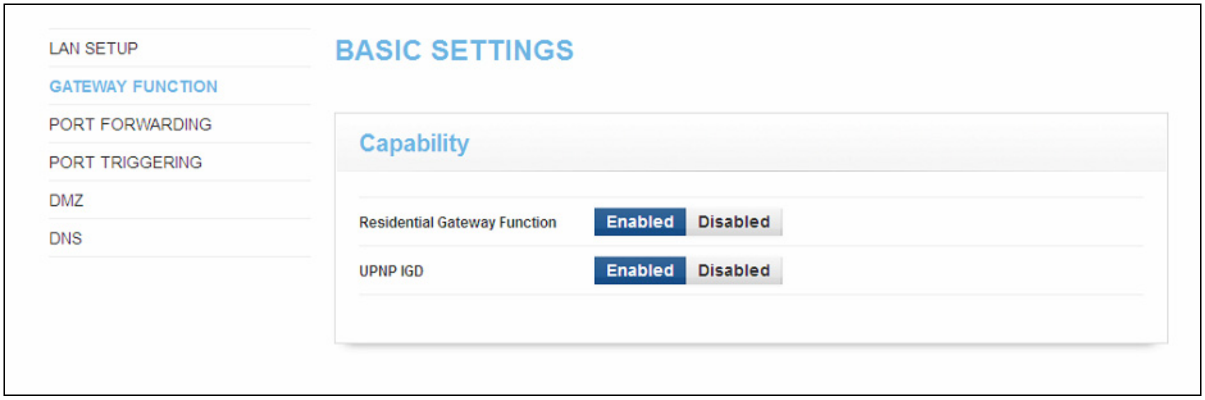
3.3 The Gateway Function Screen

Use this screen to enable or disable the CGNV4's residential gateway and Universal Plug n Play (UPnP) functions.

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

Click **Basic** > **Gateway Function**. The following screen displays.

Figure 14: The Basic: Gateway Function Screen



Residential Gateway Function [✓ Enabled] Disabled

UPNP IGD [✓ Enabled] Disabled

The following table describes the labels in this screen.

Table 14: The Basic: Gateway Function Screen

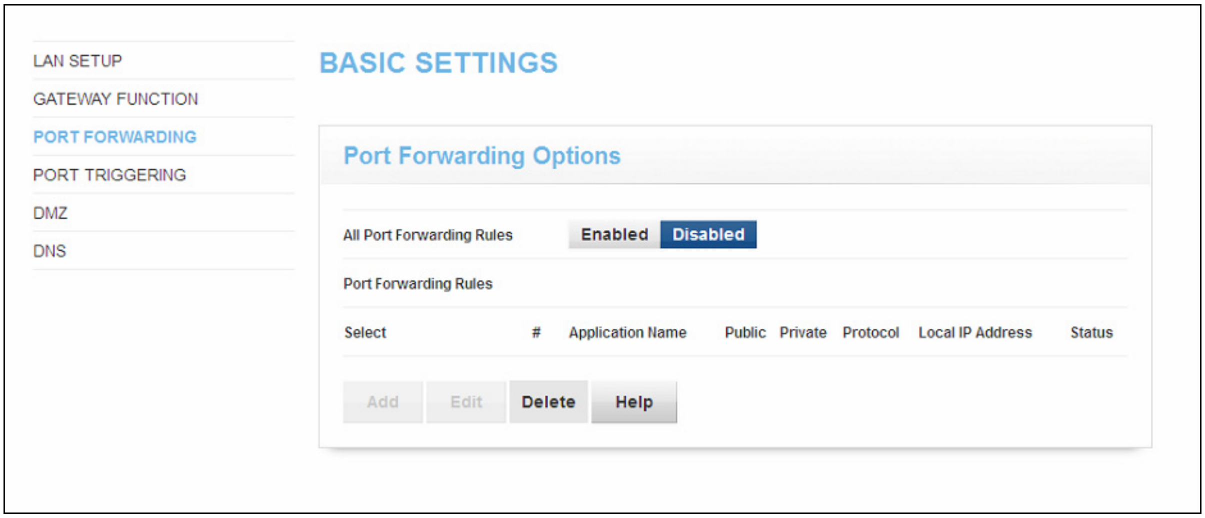
Residential Gateway Function	Select the checkbox to enable the CGNV4's residential gateway features, or deselect the checkbox to disable them.
UPnP IGD	Select the checkbox to enable the CGNV4's Universal Plug n Play Internet Gateway Device features, or deselect the checkbox to disable them.

3.4 The Port 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 **Basic** > **Port Forwarding**. The following screen displays.

Figure 15: The Basic: Port Forwarding Screen



Port Forwarding Options

All Port Forwarding Rules: Enabled [✓ Disabled]

Port Forwarding Rules

Select	#	Application Name	Public	Private	Protocol	Local IP Address	Status

The following table describes the labels in this screen.

Table 15: The Basic: Port Forwarding Screen

All Port Forwarding Rules	Use this field to turn port forwarding on or off. ▸ Select **Enabled** to turn port forwarding on. ▸ Select **Disabled** to turn port forwarding off.
Port Forwarding Rules	
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.
Public	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 CGNV4 received traffic from the originating host on the WAN. ▸ The **Private** field displays the port range to which the CGNV4 forwards traffic to the device on the LAN.
Private	

Table 15: The Basic: Port Forwarding Screen (continued)

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**)
Local 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.
Status	Use this to turn the port forwarding rule on or off. - Select **ON** to activate the port forwarding rule. - Select **OFF** to deactivate the port forwarding rule.
Add	Click this to define a new port forwarding rule. See Adding or Editing a Port Forwarding Rule on page 51 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 51 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.
Help	Click this to see information about the fields in this screen.

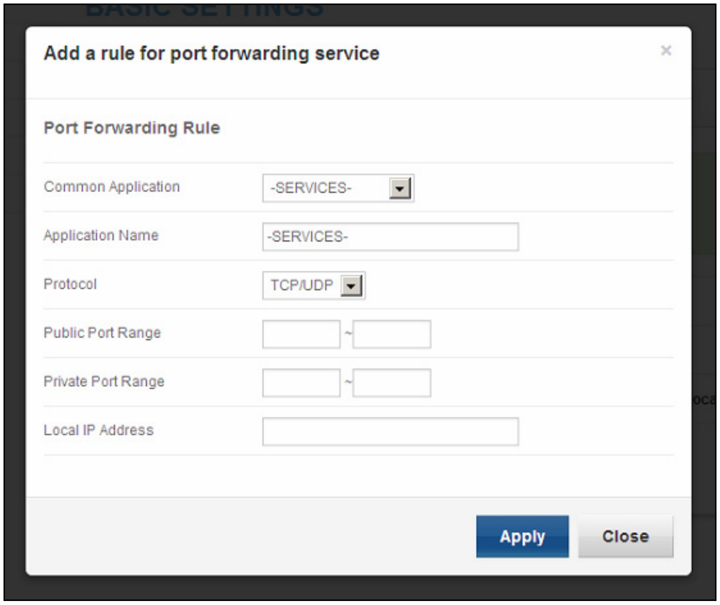
3.4.1 Adding or Editing a Port Forwarding Rule

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

NOTE: Ensure that **Enabled** is selected in the **Basic** > **Port Forwarding** screen in order to add or edit port forwarding rules.

The following screen displays.

Figure 16: The Basic: Port Forwarding Add/Edit Screen



Add a rule for port forwarding service

Port Forwarding Rule

Common Application	-SERVICES-
Application Name	-SERVICES-
Protocol	TCP/UDP
Public Port Range	~
Private Port Range	~
Local IP Address	

The following table describes the labels in this screen.

Table 16: The Basic: Port Forwarding Add/Edit Screen

Common Application	Use this field to select the application for which you want to create a port forwarding rule, if desired.
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.
Protocol	Use this field to specify whether the CGNV4 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**).

Table 16: The Basic: Port Forwarding Add/Edit Screen

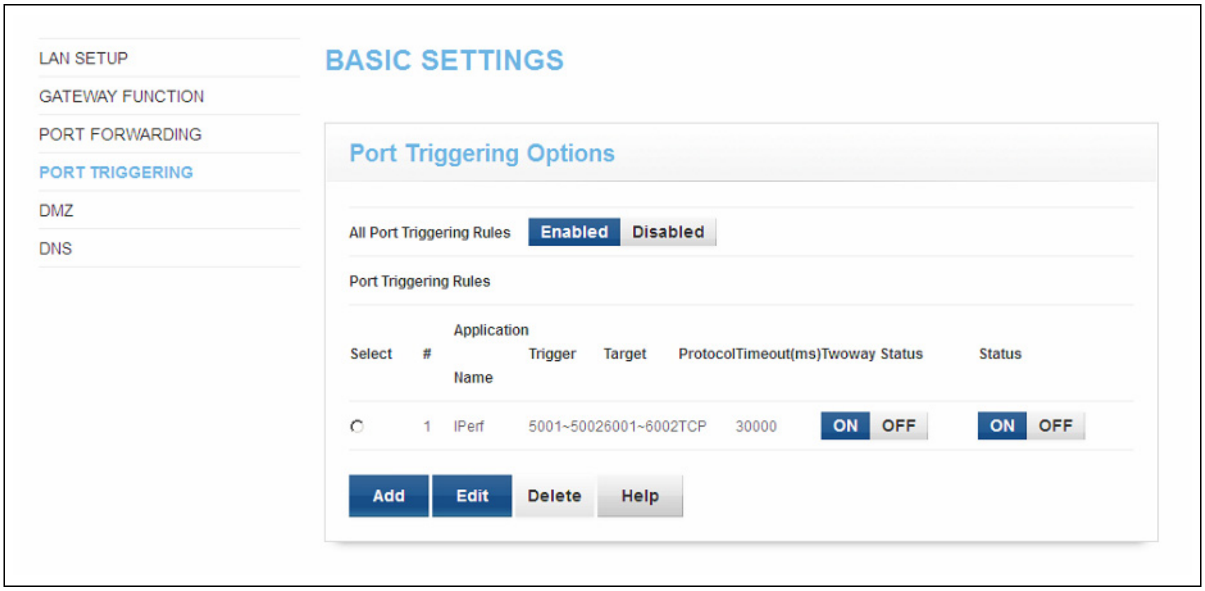
Public Port Range	Use these fields to specify the incoming port range. These are the ports on which the CGNV4 receives traffic from the originating host on the WAN. Enter the start port number in the first field, and the end port number in the second field. To specify only a single port, enter its number 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 CGNV4 completes the second field automatically.
Local IP Address	Use this field to enter the IP address of the computer on the LAN to which you want to forward the traffic.
Apply	Click this to save your changes to the fields in this screen.
Close	Click this to return to the **Port Forwarding** screen without saving your changes to the rule.

3.5 The Port Triggering Screen

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

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

Figure 17: The Basic: Port Triggering Screen



All Port Triggering Rules [✓ Enabled] Disabled

Port Triggering Rules

Select	#	Application Name	Trigger	Target	Protocol	Timeout(ms)	Twoway Status	Status
○	1	IPerf	5001~5002	6001~6002	TCP	30000	[✓ ON] OFF	[✓ ON] OFF

The following table describes the labels in this screen.

Table 17: The Basic: Port Triggering Screen

All Port Triggering Rules	Use this field to turn port triggering on or off. - Select **Enabled** to turn port triggering on. - Select **Disabled** to turn port triggering off.
Port Triggering Rules	
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 name you assigned to the rule when you created it.
Trigger	This displays the range of outgoing ports. When the CGNV4 detects activity (outgoing traffic) on these ports from computers on the LAN, it automatically opens the **Target** ports.
Target	This displays the range of triggered ports. These ports are opened automatically when the CGNV4 detects activity on the **Trigger** ports from computers on the LAN.
Protocol	This displays the protocol of the port triggering rule (**TCP**, **UDP** or **Both**).

Table 17: The Basic: Port Triggering Screen (continued)

Timeout (ms)	This displays the time (in milliseconds) after the CGNV4 opens the **Target** ports that it should close them.
Twoway Status	Usually a port triggering rule works for two IP addresses; when a rule is enabled, other IPs will also be allowed to use the rule as a trigger.
Status	Use this field to turn the rule **On** or **Off**.
Add	Click this to define a new port triggering rule. Port triggering must first be set to **Enabled**. See Adding or Editing a Port Triggering Rule on page 55 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. Port triggering must first be set to **Enabled**. See Adding or Editing a Port Triggering Rule on page 55 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.
Help	Click this to see information about the fields in this screen.

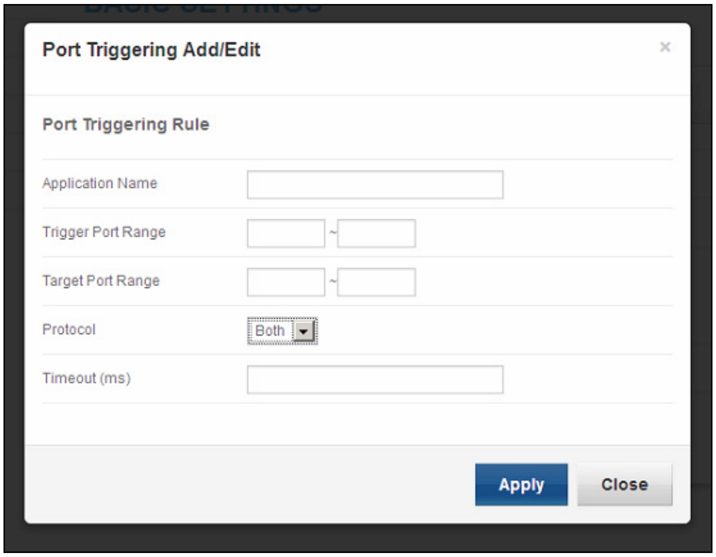
3.5.1 Adding or Editing a Port Triggering Rule

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

NOTE: Ensure that **Enabled** is selected in the **Basic** > **Port Triggering** screen in order to add or edit port triggering rules.

The following screen displays.

Figure 18: The Basic: Port Triggering Add/Edit Screen


Port Triggering Add/Edit

Port Triggering Rule

Application Name

Trigger Port Range ~

Target Port Range ~

Protocol: Both

Timeout (ms)

The following table describes the labels in this screen.

Table 18: The Basic: 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 CGNV4 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 CGNV4 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.

Table 18: The Basic: Port Triggering Add/Edit Screen

Protocol	Use this field to specify whether the CGNV4 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 CGNV4 opens the **Target** ports that it should close them.
Apply	Click this to save your changes to the fields in this screen.
Close	Click this to return to the **Port Triggering** screen without saving your changes to the rule.

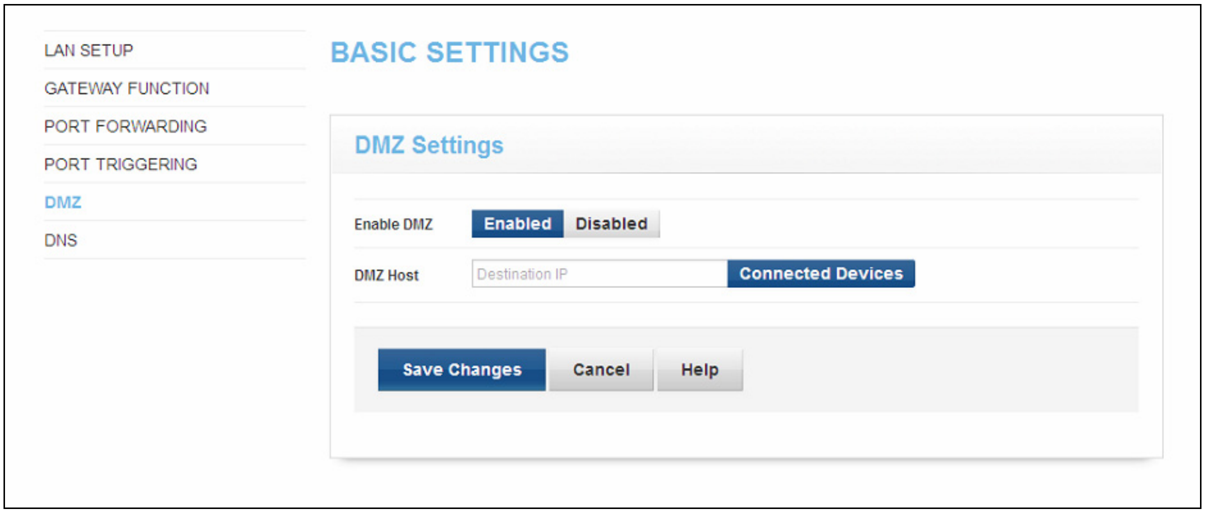
3.6 The DMZ Screen

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

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

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

Figure 19: The Basic: DMZ Screen



The following table describes the labels in this screen.

Table 19: The Basic: DMZ Screen

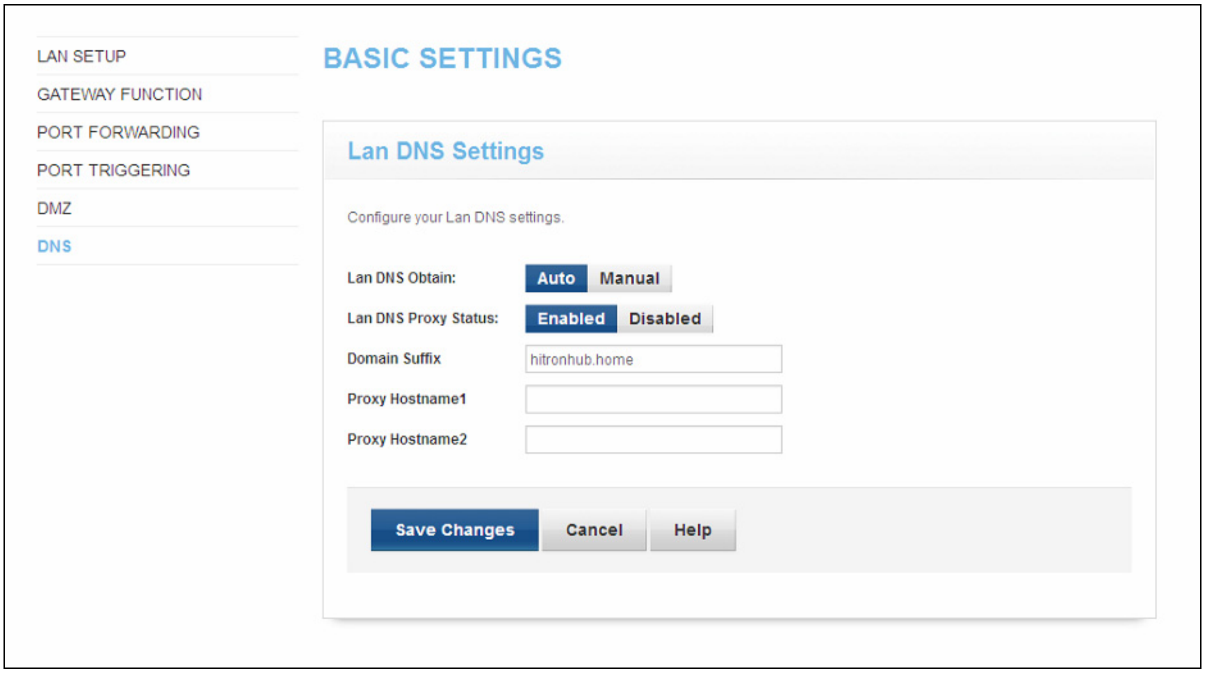
Enable DMZ	Use this field to turn the DMZ on or off. - Select **Enabled** to turn the DMZ on. - Select **Disabled** to turn the DMZ off. Computers that were previously in the DMZ are now on the LAN.
DMZ Host	Enter the IP address of the computer that you want to add to the DMZ.
Connected Devices	Click this to see a list of the computers currently connected to the CGNV4 on the LAN.
Save Changes	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.

3.7 The DNS Screen

Use this screen to configure the CGNV4’s LAN DNS settings, including its subnet mask, domain suffix and proxy hostname.

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

Figure 20: The Basic: DNS Screen



Configure your Lan DNS settings.

Lan DNS Obtain: [✓ Auto] Manual

Lan DNS Proxy Status: [✓ Enabled] Disabled

Domain Suffix: hitronhub.home

Proxy Hostname1:

Proxy Hostname2:

The following table describes the labels in this screen.

Table 20: The Basic: DNS Screen

LAN DNS Obtain	Use this to select whether to obtain DNS information automatically over the network, or to define it manually. Select **Auto** to obtain DNS information automatically. Select **Manual** to obtain DNS information manually.
LAN DNS Proxy Status	Use this to turn DNS proxy on or off on the LAN. When DNS proxy is turned on (default) the DHCP server provides the CGNV4’s LAN IP address as the DNS server for name resolution. Selected **Enabled** to turn DNS proxy on. Selected **Disabled** to turn DNS proxy off.
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 CGNV4 on the LAN. NOTE: It is suggested that you make a note of your device’s **Domain Suffix** in case you ever need to access the CGNV4’s GUI without knowledge of its IP address.

Table 20: The Basic: DNS Screen (continued)

Proxy Hostname 1 Proxy Hostname 2	When **LAN DNS Obtain** is set to **Manual**, enter the IP addresses of up to two computers for which you want to manually add to the DNS.
Save Changes	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 Wireless

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

4.1 Wireless Overview

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

4.1.1 Wireless Networking Basics

Your CGNV4'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 CGNV4 and the other computers and devices that connect to it.

4.1.2 Architecture

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

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

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

The CGNV4 is the access point, and the computers you connect to the CGNV4 are the wireless clients.

4.1.3 Wireless Standards

The way in which wireless devices communicate with one another is standardized by the Institute of Electrical and Electronics Engineers (IEEE). The IEEE standards pertaining to wireless LANs are identified by their 802.11 designation. There are a variety of WLAN standards, but the CGNV4 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

4.1.4 Service Sets and SSIDs

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

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

Each Service Set is identified by a Service Set IDentifier (SSID). This is the name of the network. Wireless clients must know the SSID in order to be able to connect to the AP. You can configure the CGNV4 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).

4.1.5 Wireless Security

Radio is inherently an insecure medium, since it can be intercepted by anybody in the coverage area with a radio receiver. Therefore, a variety of techniques exist to control authentication (identifying who should be allowed to join the network) and encryption (signal scrambling so that only authenticated users can decode the transmitted data). The sophistication of each security method varies, as does its effectiveness. The CGNV4 supports the following wireless security protocols (in order of effectiveness):

- **WEP** (the Wired Equivalency Protocol): this protocol uses a series of “keys” or data strings to authenticate the wireless client with the AP, and to encrypt data sent over the wireless link. WEP is a deprecated protocol, and should only be used when it is the only security standard supported by the wireless clients. WEP provides only a nominal level of security, since widely-available software exists that can break it in a matter of minutes.
- **WPA-PSK** (WiFi Protected Access - Pre-Shared Key): WPA was created to solve the inadequacies of WEP. There are two types of WPA: the “enterprise” version (known simply as WPA) requires the use of a central authentication database server, whereas the “personal” version (supported by the CGNV4) 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.

4.1.5.1 WPS

WiFi-Protected Setup (WPS) is a standardized method of allowing wireless devices to quickly and easily join wireless networks, while maintaining a good level of security. The CGNV4 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.

4.1.6 WMM

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

- Voice
- Video
- Best effort
- Background

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

4.2 The Wireless Basic Settings Screen

Use this screen to configure your CGNV4's basic 2.4GHz and 5GHz wireless settings. You can turn the wireless modules on or off, select the wireless mode and channel, and configure the wireless networks' SSID settings.

The CGNV4 has separate 2.4GHz and 5GHz wireless networks:

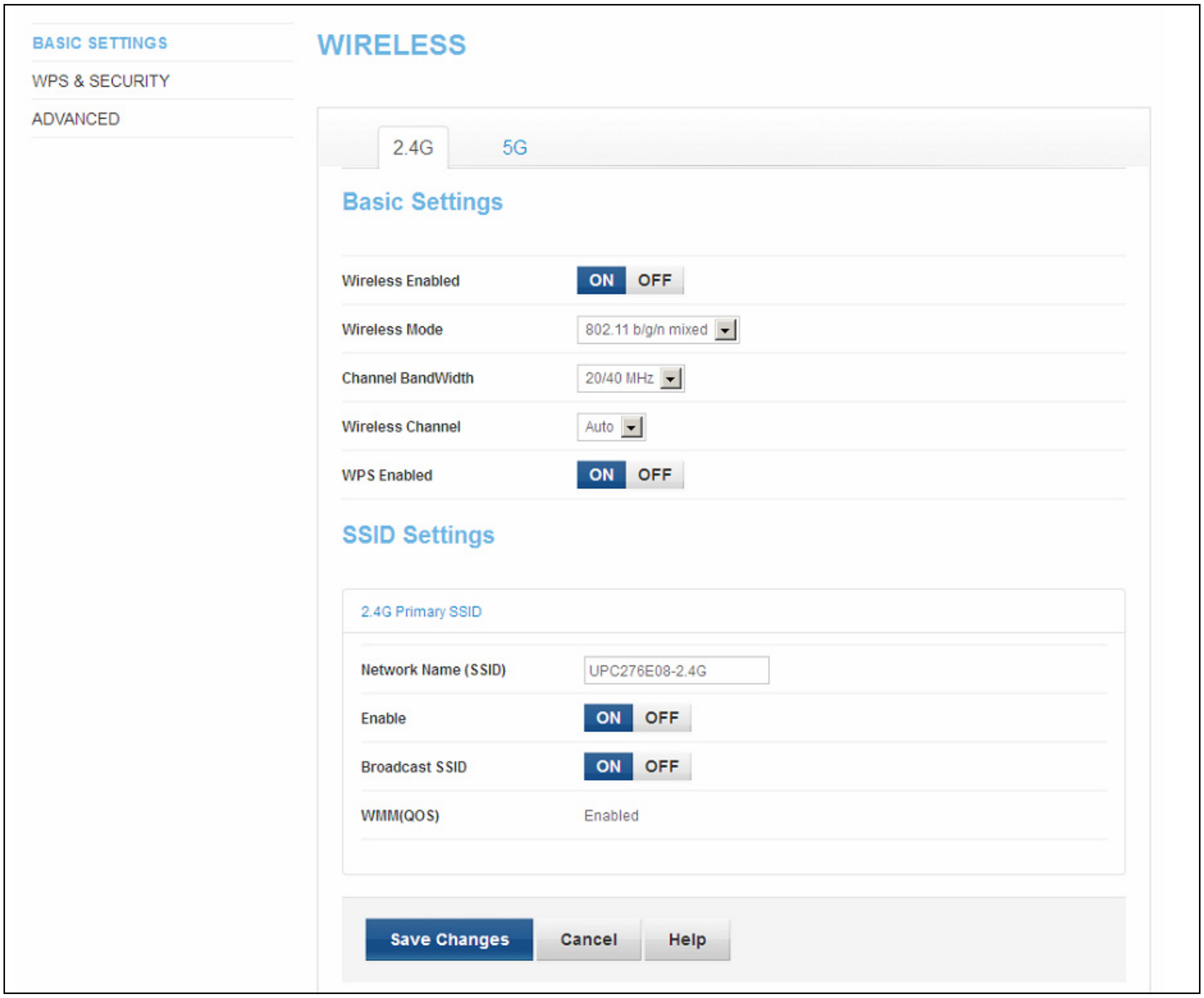
- To configure the CGNV4's 2.4GHz wireless network, click **Wireless** > **Basic Settings**, then click the **2.4G** tab. See 2.4G Settings on page 65 for information on the screen that displays.
- To configure the CGNV4's 5GHz wireless network, click **Wireless** > **Basic Settings**, then click the **5G** tab. See 5G Settings on page 68 for information on the screen that displays.

4.2.1 2.4G Settings

Use this screen to configure the CGNV4's 2.4GHz wireless network.

Click **Wireless** > **Basic Settings**, then click the **2.4G** tab. The following screen displays.

Figure 21: The Wireless: Basic Settings 2.4GHz Screen



Basic Settings

Wireless Enabled	ON OFF
Wireless Mode	802.11 b/g/n mixed
Channel BandWidth	20/40 MHz
Wireless Channel	Auto
WPS Enabled	ON OFF

SSID Settings

2.4G Primary SSID

Network Name (SSID)	UPC276E08-2.4G
Enable	ON OFF
Broadcast SSID	ON OFF
WMM(QOS)	Enabled

The following table describes the labels in this screen.

Table 21: The Wireless: Basic Settings 2.4GHz Screen

Basic Settings	
Wireless Enabled	Use this field to turn the 2.4GHz wireless network on or off. - Select **ON** to enable the wireless network. - Select **OFF** to disable the wireless network.
Wireless Mode	Select the type of 2.4GHz wireless network that you want to use: - **802.11 11b Only**: use IEEE 802.11b - **802.11 11g Only**: use IEEE 802.11g - **802.11 11n Only**: use IEEE 802.11n - **802.11 B/G/N Mixed**: use IEEE 802.11b, 802.11g and 802.11n - **802.11 G/N Mixed**: use IEEE 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 Mixed** (default).
Channel Bandwidth	This field allows you to configure the width of the radio channel the CGNV4 uses to communicate with its wireless clients (IEEE 802.11n only). Using the full 40MHz bandwidth can double your data speed. - Select **20 MHz** to only use a 20 megahertz band. - Select **20/40 MHz** to use a 40 megahertz band when possible, and a 20 megahertz band when a 40Mhz band is unavailable. - Select **40 MHz** to only use a 40 megahertz band.
Wireless Channel	Select the 2.4GHz wireless channel that you want to use, or select **Auto** to have the CGNV4 select the optimum channel to use. NOTE: Use the **Auto** setting unless you have a specific reason to do otherwise.

Table 21: The Wireless: Basic Settings 2.4GHz Screen (continued)

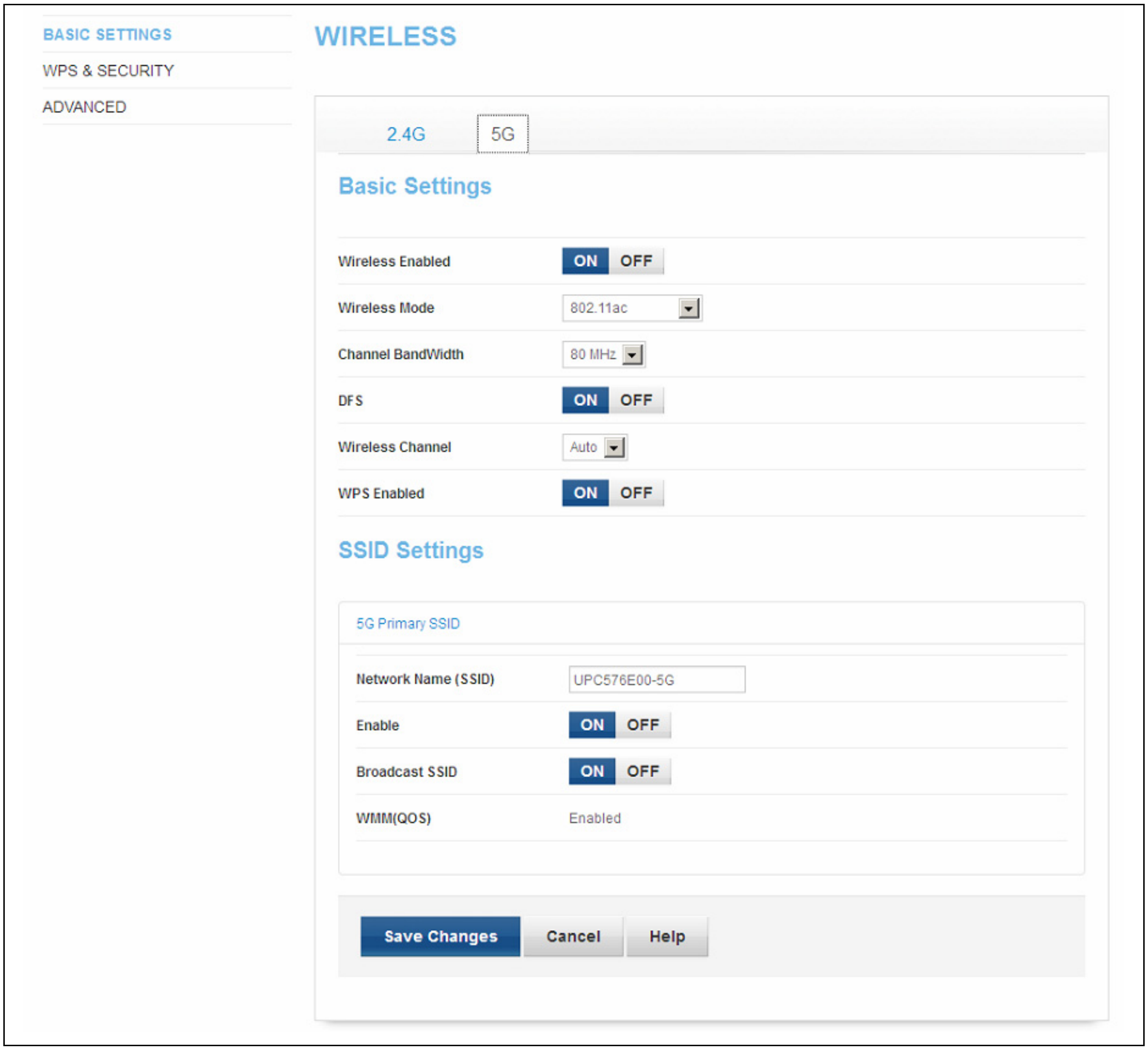
WPS Enabled	Use this field to turn Wifi Protected Setup (WPS) on or off on the 2.4GHz network. ▸ Select **ON** to enable WPS. ▸ Deselect **OFF** to disable WPS. See The WPS & Security Screen on page 71 for more information on using WPS.
SSID Settings	
Network Name (SSID)	Enter the name that you want to use for this SSID. 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.
Enable	Use this field to enable or disable the SSID. ▸ Select **ON** to enable the SSID. ▸ Deselect **OFF** to disable the SSID.
Broadcast SSID	Use this field to make this SSID visible or invisible to other wireless devices. ▸ Select **ON** 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. ▸ Select **OFF** if you do not want the CGNV4 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.
WMM(QoS)	This field displays whether Wifi MultiMedia (WMM) Quality of Service (QoS) settings are **Enabled** or **Disabled** on this SSID.
Save Changes	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.

4.2.2 5G Settings

Use this screen to configure the CGNV4’s 5GHz wireless network.

Click **Wireless** > **Basic Settings**, then click the **5G** tab. The following screen displays.

Figure 22: The Wireless: Basic Settings 5GHz Screen



Wireless Enabled	ON OFF
Wireless Mode	802.11ac
Channel BandWidth	80 MHz
DFS	ON OFF
Wireless Channel	Auto
WPS Enabled	ON OFF
Network Name (SSID)	UPC576E00-5G
Enable	ON OFF
Broadcast SSID	ON OFF
WMM(QOS)	Enabled

The following table describes the labels in this screen.

Table 22: The Wireless: Basic Settings 5GHz Screen

Basic Settings	
Wireless Enabled	Use this field to turn the 5GHz wireless network on or off. ▸ Select **ON** to enable the wireless network. ▸ Select **OFF** to disable the wireless network.
Wireless Mode	Select the type of 5GHz wireless network that you want to use: ▸ **802.11 11n 5G**: use IEEE 802.11n (5GHz) ▸ **802.11 11a**: use IEEE 802.11a ▸ **802.11 B/G/N Mixed**: use IEEE 802.11a and 802.11n ▸ **802.11 11ac**: use IEEE 802.11ac (5GHz only) NOTE: Only wireless clients that support the network protocol you select can connect to the wireless network. If in doubt, use **11B/G/N Mixed**.
Channel Bandwidth	This field allows you to configure the width of the radio channel the CGNV4 uses to communicate with its wireless clients. Using the full 40MHz bandwidth can double your data speed. ▸ Select **20 MHz** to only use a 20 megahertz band. ▸ Select **40 MHz** to only use a 40 megahertz band. ▸ Select **80 MHz** to only use a 80 megahertz band.
Wireless Channel	Select the 5GHz wireless channel that you want to use, or select **Auto** to have the CGNV4 select the optimum channel to use. NOTE: Use the **Auto** setting unless you have a specific reason to do otherwise.

Table 22: The Wireless: Basic Settings 5GHz Screen (continued)

WPS Enabled	Use this field to turn Wifi Protected Setup (WPS) on or off on the 5GHz network. - Select **ON** to enable WPS. - Deselect **OFF** to disable WPS. See The WPS & Security Screen on page 71 for more information on using WPS.
SSID Settings	
Network Name (SSID)	Enter the name that you want to use for this SSID. 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.
Enable	Use this field to enable or disable the SSID. - Select **ON** to enable the SSID. - Deselect **OFF** to disable the SSID.
Broadcast SSID	Use this field to make this SSID visible or invisible to other wireless devices. - Select **ON** 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. - Select **OFF** if you do not want the CGNV4 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.
WMM(QoS)	This field displays whether Wifi MultiMedia (WMM) Quality of Service (QoS) settings are **Enabled** or **Disabled** on this SSID.
Save Changes	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.

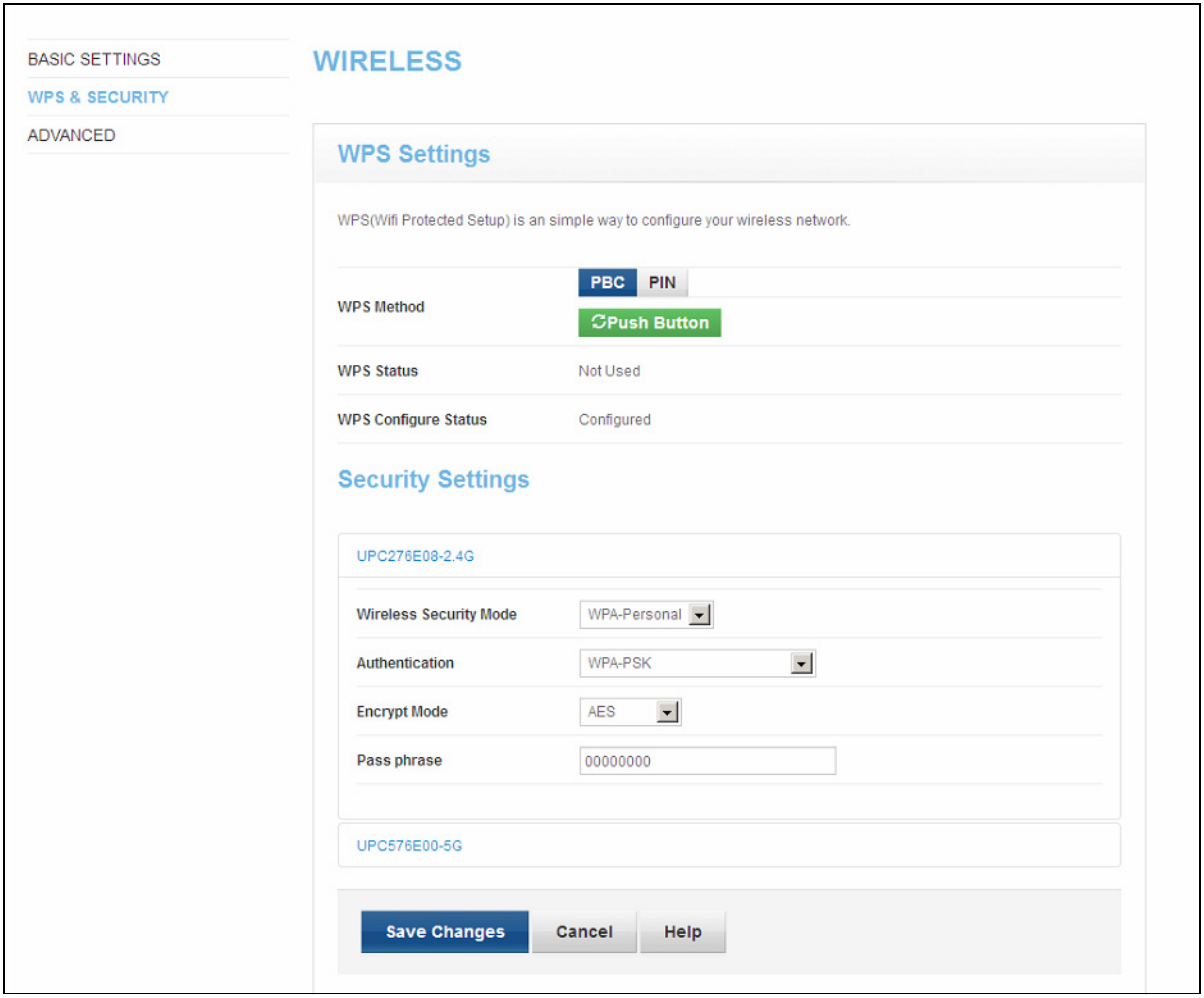
4.3 The WPS & Security Screen

Use this screen to configure your CGNV4's 2.4GHz and 5GHz wireless networks' authentication and encryption, and manage Wifi Protected Setup (WPS).

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** > **WPS & Security**. The following screen displays.

Figure 23: The Wireless: WPS & Security Screen



WPS Settings

WPS(Wifi Protected Setup) is an simple way to configure your wireless network.

WPS Method	PBC PIN
WPS Status	Not Used
WPS Configure Status	Configured

Security Settings

UPC276E08-2.4G

Wireless Security Mode	WPA-Personal
Authentication	WPA-PSK
Encrypt Mode	AES
Pass phrase	00000000

UPC576E00-5G

The following table describes the labels in this screen.

Table 23: The Wireless: WPS & Security Screen

WPS Settings	
WPS Method	Use these buttons to run Wifi Protected Setup (WPS): ▸ Click the **PBC** button and then **Push 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 CGNV4, or the WPS PIN of the client device you want to add to the network.
WPS Status	This displays whether or not the CGNV4 is using Wifi Protected Setup.
WPS Configure Status	This displays the Wifi Protected Setup configuration.
Security Settings	
(SSID)	Your CGNV4 has multiple SSIDs. Click the SSID you wish to configure to see its security fields.
Wireless 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 the **WPA** option.

Table 23: The Wireless: WPS & Security Screen (continued)

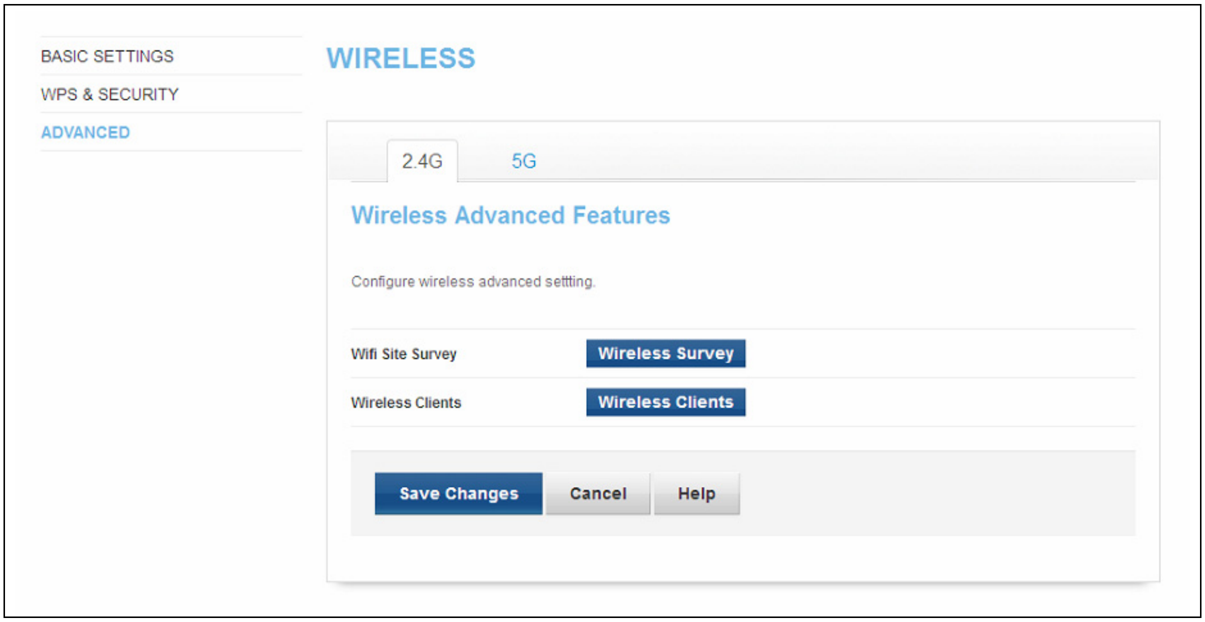
Authentication	Select the type of authentication that you want to use. - Select **WPA-PSK** to use the WiFi Protected Access (Personal) security protocol. - Select **WPA2-PSK** to use the WiFi Protected Access 2 (Personal) security protocol. - Select **Auto (WPA-PSK or WPA2-PSK)** to use both the WPA and the WPA2 security protocols; clients that support WPA2 connect using this protocol, whereas those that support only WPA connect using this protocol.
Encrypt Mode	Select the type of encryption you want to use. The options that display depend on the options you selected in the other fields in this screen. **WEP**: - Select **WEP64** to use a ten-digit security key. - Select **WEP128** to use a twenty-six-digit security key. **WPA-PSK**, **WPA2-PSK** and **Auto**: - Select **TKIP** to use the Temporal Key Integrity Protocol. - Select **AES** to use the Advanced Encryption Standard. - Select **TKIP/AES** to allow clients using either encryption type to connect to the CGNV4.
Pass phrase	Enter the security key or password 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.
Save Changes	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 Advanced Wireless Screen

Use this screen to view information about the wireless networks within the CGNV4’s coverage area.

Click **Wireless** > **Advanced**. The following screen displays. Click the **2.4G** tab to see information about the 2.4GHz wireless network, or click the **5G** tab to see information about the 5GHz wireless network.

Figure 24: The Wireless: Advanced Screen



Wireless Advanced Features

Configure wireless advanced settting.

Wifi Site Survey

Wireless Clients

The following table describes the labels in this screen.

Table 24: The Wireless: Advanced Screen

WiFi Site Survey	Click this to view information about the wireless networks within the CGNV4’s coverage area. See The WiFi Site Survey Screen on page 75 for information on the screen that displays.
Wireless Clients	Click this to view information about the wireless clients connected to the CGNV4’s wireless network. See The Wireless Clients Screen on page 77 for information on the screen that displays.
Save Changes	Click this to save your changes to the fields in this screen.

Table 24: The Wireless: Advanced Screen (continued)

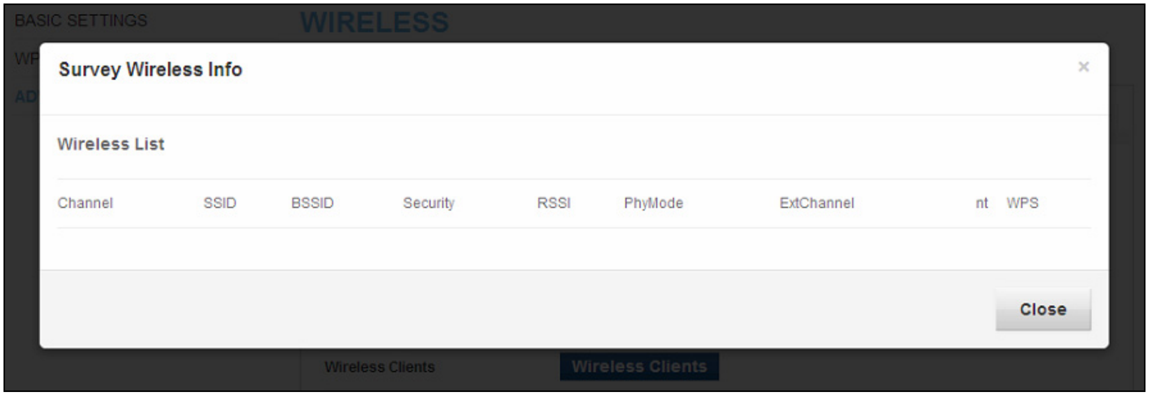
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.4.1 The WiFi Site Survey Screen

Use this screen to view information about the wireless networks within the CGNV4's coverage area.

Click **Wireless** > **Advanced**, then click the **Wireless Survey** button. The following screen displays.

Figure 25: The Wireless: WiFi Site Survey Screen



Channel	SSID	BSSID	Security	RSSI	PhyMode	ExtChannel	nt	WPS

The following table describes the labels in this screen.

Table 25: The Wireless: WiFi Site Survey Screen

Survey Results	
Channel	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 25: The Wireless: WiFi Site Survey Screen

RSSI	This field displays the Received Signal Strength Indication from each wireless network.
PhyMode	This displays the Physical Mode (the IEEE 802.11 version) of each wireless network.
ExtCH	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 networks using channel bonding, where the extension channel is above the main channel, **ABOVE** displays. ▸ For 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.
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.

Table 25: The Wireless: WiFi Site Survey Screen

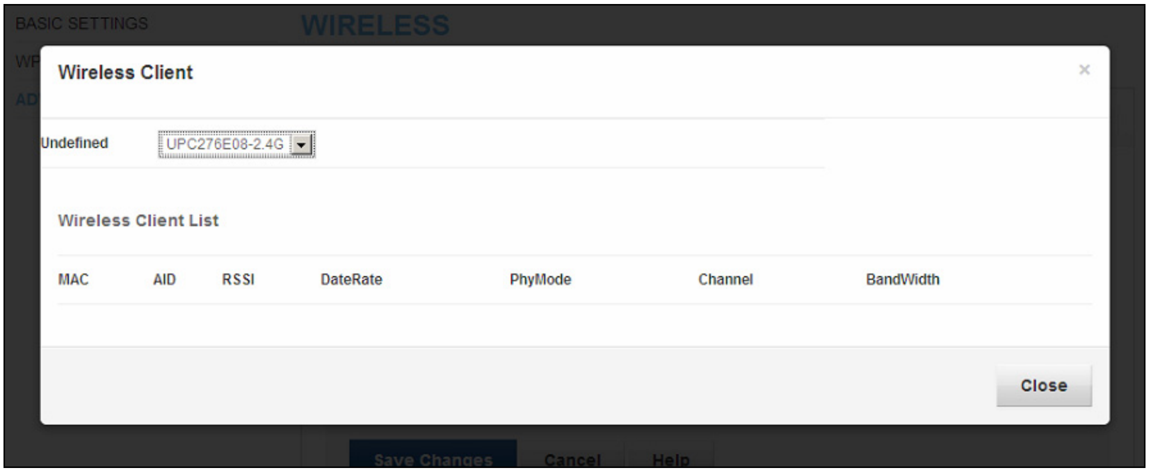
WPS	This field displays whether the target network is using WiFi Protected Setup (WPS) or not. If the target network is using WPS, this field displays whether it is using PIN mode, or Push-Button Configuration (PBC) mode. - If the target network is not using WPS, **NO** displays. - If the target network 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 63 for more information on WPS, and the difference between PIN and PBC modes.
Close	Click this to close the lightbox.

4.4.2 The Wireless Clients Screen

Use this screen to view information about the wireless clients connected to the CGNV4's wireless network.

Click **Wireless** > **Advanced**, then click the **Wireless Clients** button. The following screen displays.

Figure 26: The Wireless: Wireless Clients Screen



Wireless Client

Undefined UPC276E08-2.4G

Wireless Client List

MAC	AID	RSSI	DateRate	PhyMode	Channel	BandWidth

The following table describes the labels in this screen.

Table 26: The Wireless: Wireless Clients Screen

Wireless Client Lists	
(SSID)	Select the SSID of the network that you want to query.
MAC	This displays the MAC (Media Access Control) address of each wireless client connected to the CGNV4's wireless network.
AID	This displays the Association Identifier (AID) of the connection between the CGNV4 and the client. The Association Identifier is the logical port the CGNV4 assigns to the wireless client.
RSSI	This field displays the Received Signal Strength Indication from each wireless client connected to the CGNV4's wireless network.
Date	This displays the date the wireless client last connected to the CGNV4's wireless network.
Rate	This displays the transfer speed of each wireless client connected to the CGNV4's wireless network.
PhyMode	This displays the Physical Mode (the IEEE 802.11 version) of each wireless client connected to the CGNV4's wireless network.
Channel	This displays the wireless channel on which the client is connected to the CGNV4.
Bandwidth	This displays the bandwidth (20/40MHz) of each wireless client connected to the CGNV4's wireless network.

5 Admin

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

5.1 Admin Overview

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

5.1.1 Debugging (Ping and Traceroute)

The CGNV4 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 CGNV4 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.

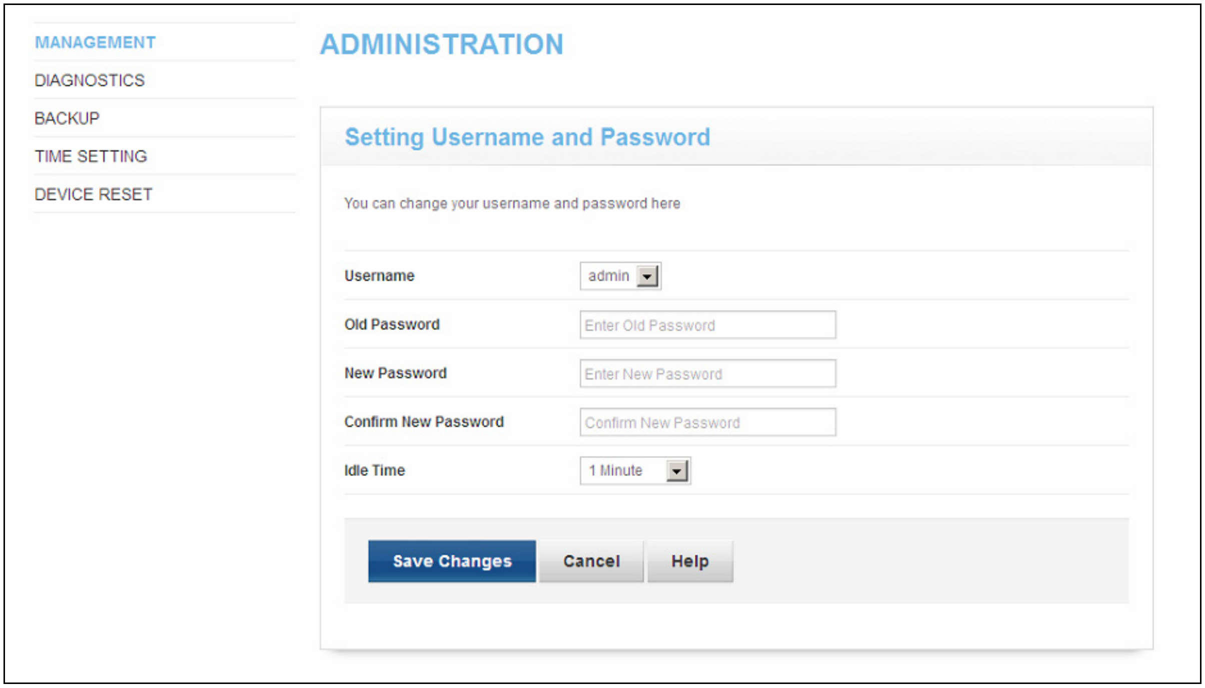
5.2 The Management Screen

Use this screen to make changes to the CGNV4's login credentials (username and password) and inactivity idle time.

NOTE: If you forget your password, you will need to reset the CGNV4 to its factory defaults.

Click **Admin** > **Management**. The following screen displays.

Figure 27: The Admin: Management Screen



You can change your username and password here

Username	admin
Old Password	Enter Old Password
New Password	Enter New Password
Confirm New Password	Confirm New Password
Idle Time	1 Minute

The following table describes the labels in this screen.

Table 27: The Admin: Management Screen

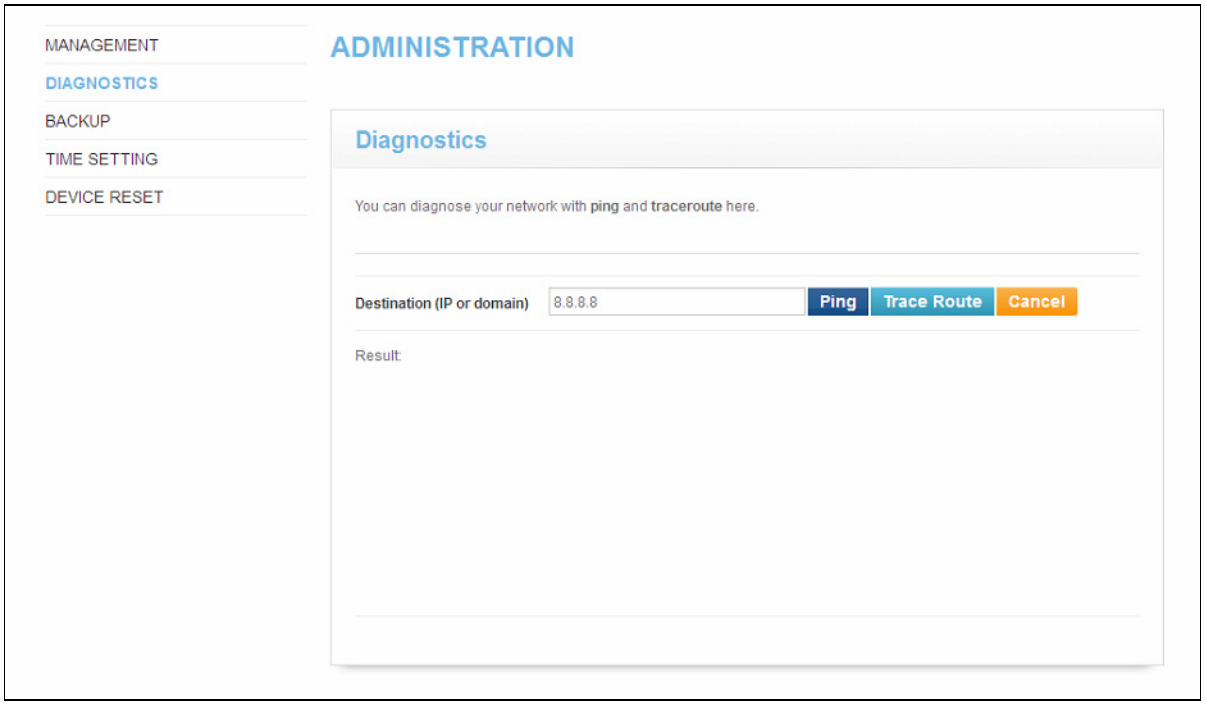
Username	If your CGNV4 supports multiple user accounts, select the account you want to modify from the list.
Old Password	Enter the password with which you currently log into the CGNV4 for this account.
New Password	Enter and re-enter the password you want to use to log into the CGNV4 for this account.
Confirm New Password	
Idle Time	Select the time interval after which an inactive user should be logged out of the CGNV4's admin interface.
Save Changes	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 Diagnostics Screen

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

Click **Admin** > **Diagnostics**. The following screen displays.

Figure 28: The Admin: Diagnostics Screen



You can diagnose your network with **ping** and **traceroute** here.

Destination (IP or domain) 8.8.8.8

Result:

The following table describes the labels in this screen.

Table 28: The Admin: Diagnostics Screen

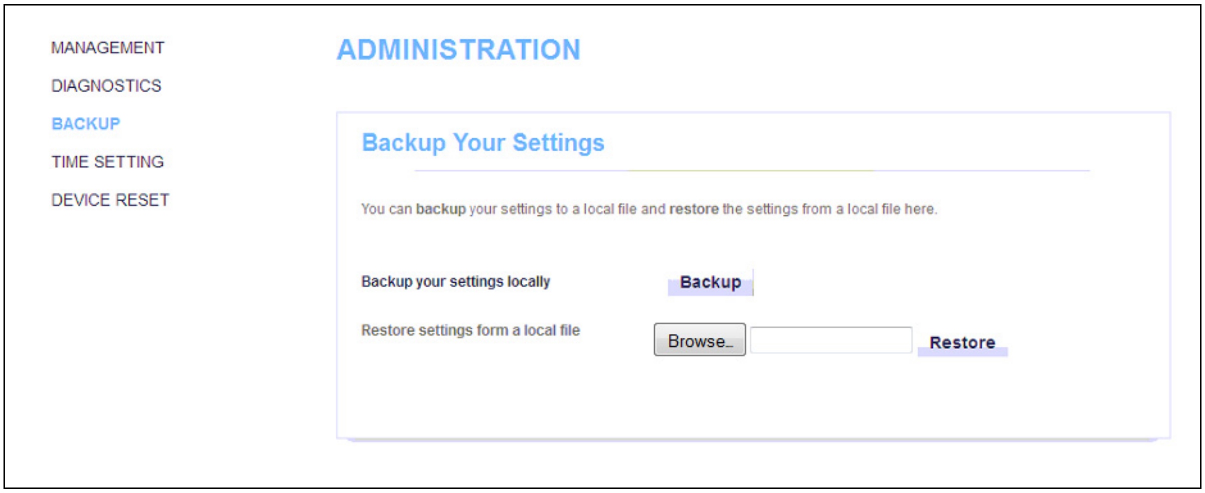
Destination (IP or Domain)	Enter the IP address or URL that you want to test.
Ping	Select the type of test that you want to run on the **Destination** that you specified.
Traceroute	
Result	This field displays a report of the test most recently performed.
Cancel	Click this to terminate a test in progress.

5.4 The Backup Screen

Use this screen to back up your CGNV4's settings to your computer or load settings from a backup you created earlier.

Click **Admin** > **Backup**. The following screen displays.

Figure 29: The Admin: Backup Screen



You can **backup** your settings to a local file and **restore** the settings from a local file here.

Backup your settings locally Backup

Restore settings form a local file Browse... Restore

The following table describes the labels in this screen.

Table 29: The Admin: Management Screen

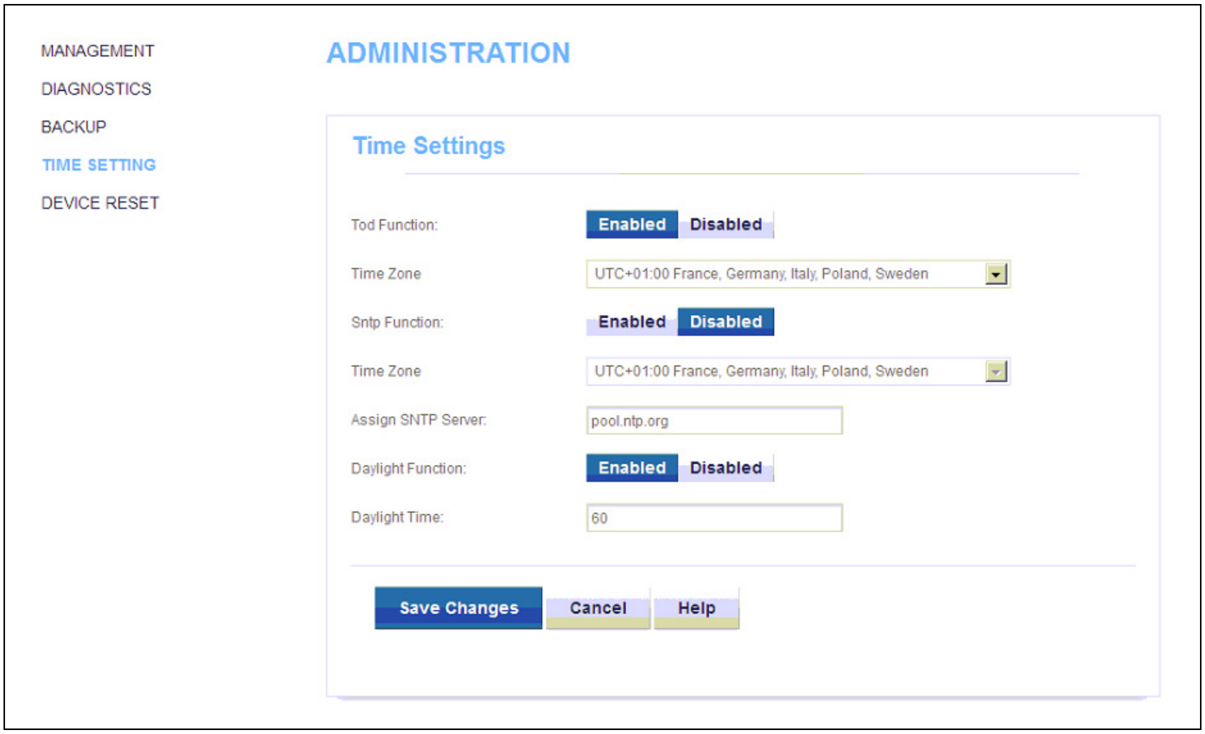
Back Up Your Settings Locally	Click this to create a backup of all your CGNV4's settings on your computer.
Restore Settings From a Local File	Use these fields to return your CGNV4's settings to those specified in a backup that you created earlier. Click **Browse** to select a backup, then click **Restore** to return your CGNV4's settings to those specified in the backup.

5.5 The Time Setting Screen

Use this screen to

Click **Admin** > **Time Setting**. The following screen displays.

Figure 30: The Admin: Time Setting Screen



Tod Function: Enabled Disabled

Time Zone: UTC+01:00 France, Germany, Italy, Poland, Sweden

Sntp Function: Enabled Disabled

Time Zone: UTC+01:00 France, Germany, Italy, Poland, Sweden

Assign SNTP Server: pool.ntp.org

Daylight Function: Enabled Disabled

Daylight Time: 60

The following table describes the labels in this screen.

Table 30: The Admin: Time Setting Screen

ToD Function	Use this field to turn the CGNV4’s internal Time of Day (ToD) function on or off. Time of Date functions are used for obtaining the data used for network event time stamps, and are useful for analysis and troubleshooting. - Select **Enabled** to turn Time of Day functions on. - Select **Disabled** to turn Time of Day functions off.
Time Zone	If **ToD Function** is **Enabled**, select the time zone in which the CGNV4 is located, or that you want to use for network administration. This time zone is used when adding time stamps to network events.
SNTP Function	Use this field to turn the CGNV4’s Simple Network Time Protocol (SNTP) function on or off. SNTP enables the CGNV4 to obtain time and date data from a remote SNTP/NTP server on the Internet. - Select **Enabled** to turn SNTP functions on. - Select **Disabled** to turn SNTP functions off.

Table 30: The Admin: Time Setting Screen (continued)

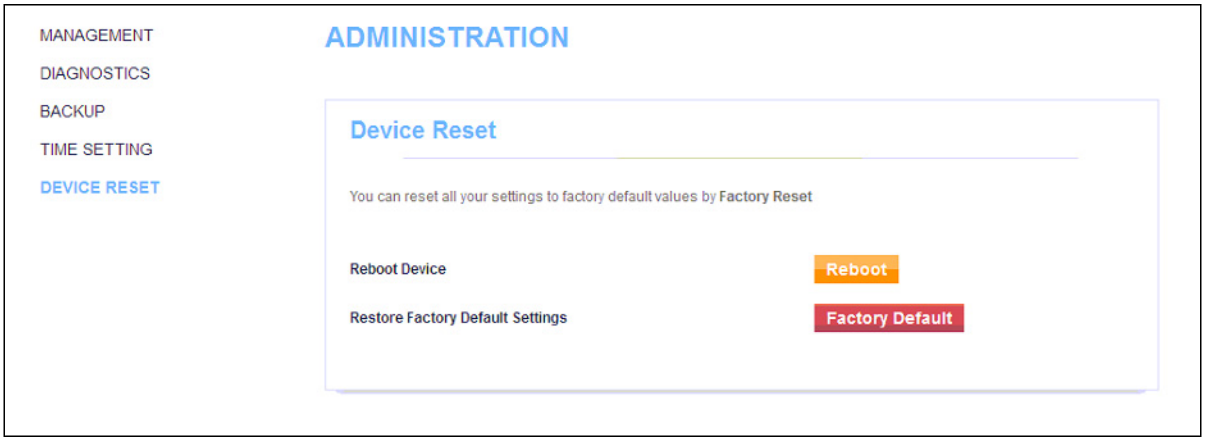
Time Zone	If **SNTP Function** is **Enabled**, select the time zone in which the CGNV4 is located, or that you want to use for network administration. This time zone is used when adding time stamps to network events.
Assign SNTP Server	If **SNTP Function** is **Enabled**, enter the URL of the SNTP server from which the CGNV4 should get its data.
Daylight Function Daylight Time	Use the **Daylight Function** field to turn daylight savings time on or off for the CGNV4's time stamps. ‣ Select **Enabled** to turn daylight savings on. ‣ Select **Disabled** to turn daylight savings off. If you select **Enabled** in the **Daylight Function** field, additionally enter the correct daylight savings offset time (in minutes) in the **Daylight Time** field.
Save Changes	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.

5.6 The Device Reset Screen

Use this screen to reboot your CGNV4, or to return it to its factory default settings.

Click **Admin** > **Device Reset**. The following screen displays.

Figure 31: The Admin: Device Reset Screen



You can reset all your settings to factory default values by **Factory Reset**

Reboot Device

Restore Factory Default Settings

The following table describes the labels in this screen.

Table 31: The Admin: Device Reset Screen

Reboot Device	Click this to restart your CGNV4.
Restore Factory Default Settings	Click this to return your CGNV4 to its factory default settings. When you do this, all your user-configured settings are lost, and cannot be retrieved.

6

Security

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

6.1 Security Overview

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

6.1.1 Firewall

The term "firewall" comes from a construction technique designed to prevent the spread of fire from one room to another. Similarly, your CGNV4'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.

6.1.2 Intrusion detection system

An intrusion detection system monitors network activity, looking for policy violations, and malicious or suspicious activity. The CGNV4's intrusion detection system logs all such activity to the **Security** > **Logs** screen.

6.1.3 Device Filtering

Every networking device has a unique Media Access Control (MAC) address that uniquely identifies it on the network. When you enable MAC address filtering on the CGNV4's firewall, you can set up a list of devices, identified by their MAC addresses, and then specify whether you want to:

- Deny the devices on the list access to the CGNV4 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).

6.1.4 Service Filtering

Service filtering is a way of preventing users on the LAN from connecting with devices on the WAN via specific services, protocols or applications. It achieves this by permitting or denying traffic from the LAN to pass to the WAN, based on the target port.

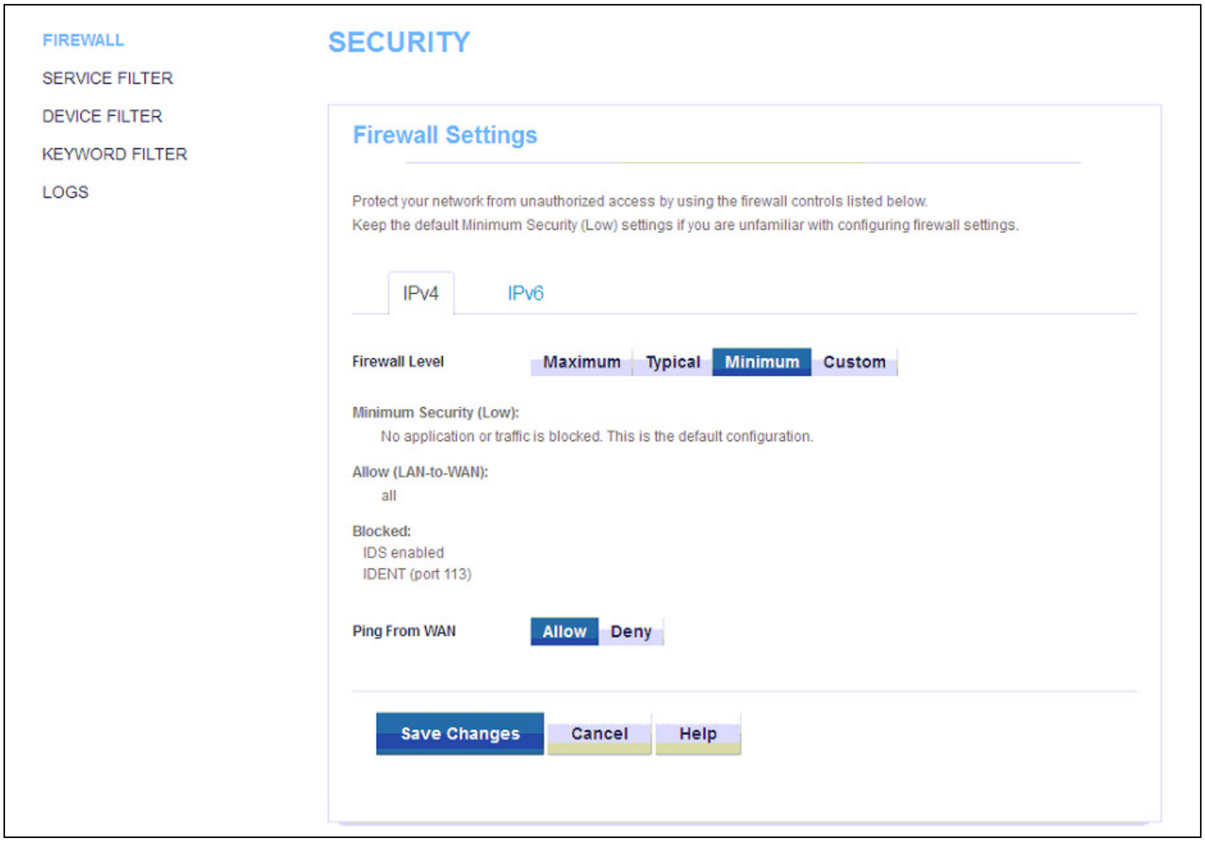
6.2 The Firewall Screen

Use this screen to turn firewall features on or off and to allow or permit certain applications and protocols. You can select the level of firewall protection from pre-defined options, or create a custom protection profile.

NOTE: To block specific ports, use the Service Filter screen (see The Service Filter Screen on page 91).

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

Figure 32: The Security: Firewall Screen



Firewall Settings

Protect your network from unauthorized access by using the firewall controls listed below.
Keep the default Minimum Security (Low) settings if you are unfamiliar with configuring firewall settings.

Firewall Level: Minimum

Minimum Security (Low):
No application or traffic is blocked. This is the default configuration.

Allow (LAN-to-WAN):
all

Blocked:
IDS enabled
IDENT (port 113)

Ping From WAN: Allow

IPv4 and IPv6 firewall features are configured separately. Click the **IPv4** tab (which displays by default) to configure IPv4 firewall features, or click the **IPv6** tab to configure IPv6 firewall features. The fields that display in each tab are identical.

The following table describes the labels in this screen.

Table 32: The Security: Firewall Screen

Firewall Level	Select the level of firewall protection that you want to apply to your LAN. Details about the protection level display beneath the buttons.
(Security Level)	These fields describe the specific protocols and applications that are permitted or denied by the firewall security level you select. When you select **Custom** in the **Firewall Level** field, additional fields display that allow you to toggle specific features on or off: - **Entire Firewall**: select **ON** to enable firewall security protection, or select **OFF** to disable it (not recommended). - **HTTP**: use this field to **Allow** or **Deny** HyperText Transfer Protocol traffic. - **ICMP**: use this field to **Allow** or **Deny** Internet Control Message Protocol traffic. - **P2P**: use this field to **Allow** or **Deny** peer-to-peer traffic (such as BitTorrent). - **Ident**: use this field to **Allow** or **Deny** Identification protocol traffic. The Identification protocol allows remote hosts to request identifying information about users of a device.
Ping from WAN	Use this field to permit or prohibit Internet Control Message Protocol (ICMP) echo requests from the WAN to the LAN. - Select **Allow** to permit pinging from the WAN. - Select **Deny** to prohibit pinging from the WAN. Echo requests from the WAN to the LAN are silently ignored.
Save Changes	Click this to save your changes to the fields in this screen.

Table 32: The Security: Firewall Screen (continued)

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

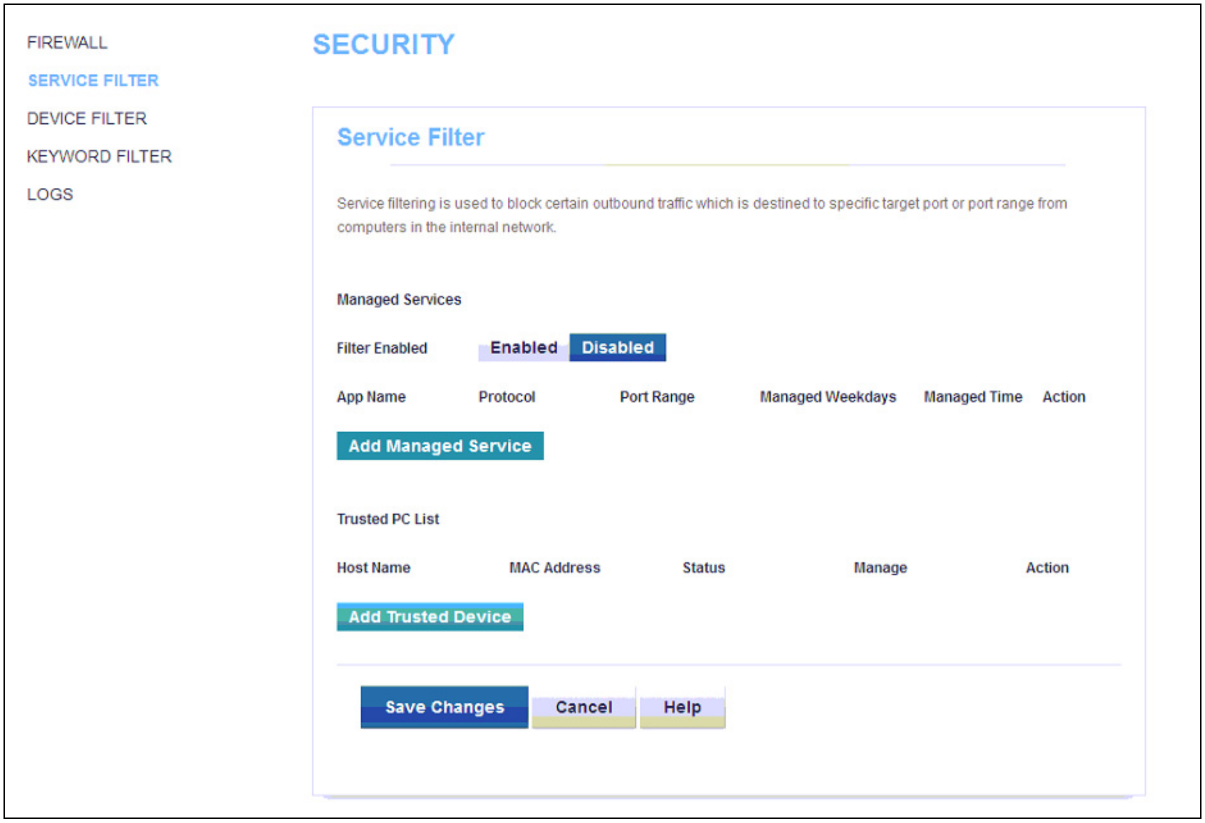
6.3 The Service Filter Screen

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

You can also create and edit trusted device rules. Trusted devices are those to which service filtering rules are not applied.

Click **Security** > **Service Filter**. The following screen displays.

Figure 33: The Security: Service Filter Screen



Service filtering is used to block certain outbound traffic which is destined to specific target port or port range from computers in the internal network.

Managed Services

Filter Enabled: Enabled [✓ Disabled]

App Name	Protocol	Port Range	Managed Weekdays	Managed Time	Action

Trusted PC List

Host Name	MAC Address	Status	Manage	Action

The following table describes the labels in this screen.

Table 33: The Security: Service Filter Screen

Managed Services	
Filter Enabled	Use this field to turn service filtering on or off. - Select **Enabled** to turn service filtering on. - Select **Disabled** to turn service filtering off.
App Name	This displays the name you assigned to the filtering rule when you created it.
Protocol	This field displays the protocol or protocols to which this filtering rule applies: - Transmission Control Protocol (**TCP**) - User Datagram Protocol (**UDP**)
Port Range	This displays the start and end port for which this filtering rule applies.
Managed Weekdays	This displays the days of the week on which this rule applies.
Managed Time	This displays the start (**From**) and end (**To**) of the time period during which this rule applies, on the specified **Managed Weekdays**.
Action	Click **Manage** to make changes to a filtering rule (see Adding or Editing a Service Filter Rule on page 93).
Add Managed Service	Click this to add a new service filtering rule (see Adding or Editing a Service Filter Rule on page 93).
Trusted PC List	
Host Name	This displays the arbitrary name of each trusted PC you configured.
MAC Address	This displays the Media Access Control (MAC) address of each trusted PC. Every network device has a MAC address that uniquely identifies it.
Status	This displays whether the device is currently trusted (**Enabled**) or untrusted (**Disabled**).
Manage	Click **Manage** to make changes to the trusted device rule. See Adding or Editing a Service Filter Trusted Device Rule on page 95 for information on the screen that displays.
Action	Click **Delete** to remove the trusted device rule.

Table 33: The Security: Service Filter Screen (continued)

Add Trusted Device	Click this to create a new trusted device rule. See Adding or Editing a Service Filter Trusted Device Rule on page 95 for information on the screen that displays.
Save Changes	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.

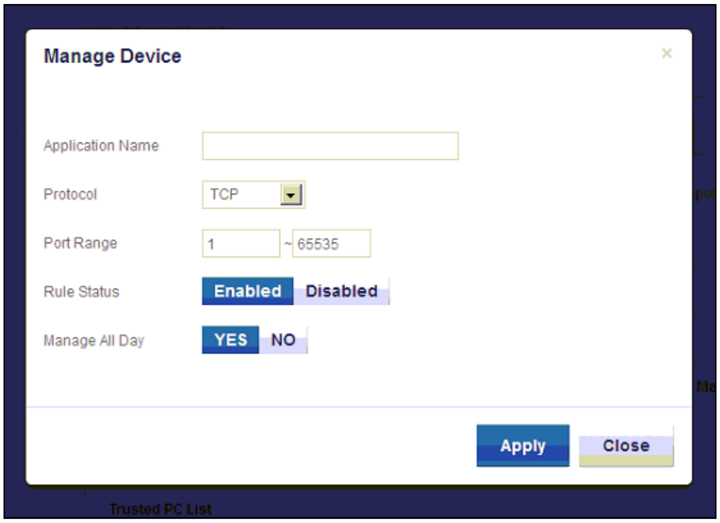
6.3.1 Adding or Editing a Service Filter Rule

- To add a new service filter rule, click **Add Managed Service** in the **Security** > **Service Filter** screen.
- To edit an existing service filter rule, locate the rule in the **Security** > **Service Filter** screen and click its **Manage** button.

NOTE: Ensure that **Enabled** is selected in the **Security** > **Service Filter** screen in order to add or edit service filtering rules.

The following screen displays.

Figure 34: The Security: Service Filter Add/Edit Screen



Manage Device

Application Name

Protocol TCP

Port Range 1 ~ 65535

Rule Status Enabled Disabled

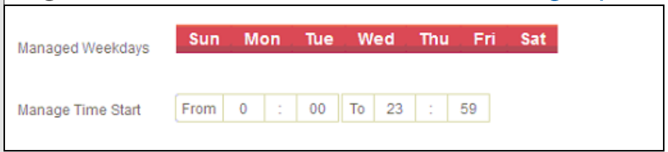
Manage All Day YES NO

The following table describes the labels in this screen.

Table 34: The Security: Service Filter 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.
Protocol	Use this field to specify whether the CGNV4 should filter via: ▸ Transmission Control Protocol (**TCP**) ▸ User Datagram Protocol (**UDP**) NOTE: If in doubt, leave this field at its default (**TCP**).
Port Range	Use these fields to specify the start and end port for which this filtering rule applies. These are the ports to which traffic will 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.
Rule Status	Use this field to select whether the filtering rule should be active or not. ▸ Select **Enabled** to activate the rule. Matching traffic will be blocked. ▸ Select **Disabled** to deactivate the rule. Matching traffic will not be blocked.

Table 34: The Security: Service Filter Add/Edit Screen

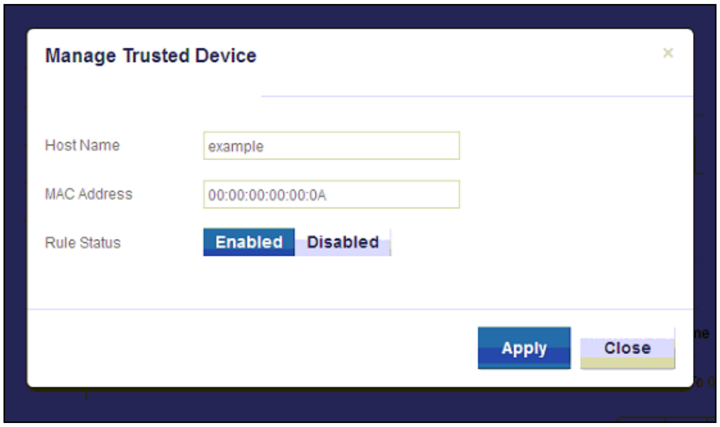
Manage All Day	Use this field to specify whether the filtering rule should apply on all days of the week, at all times, or whether the rule should be applied only at certain times. - Select **YES** to apply the rule at all times. - Select **NO** to apply the rule only at certain times. Additional fields display, allowing you to specify the times at which the rule should be applied. Figure 35: Additional Service Filtering Options  Managed Weekdays Sun Mon Tue Wed Thu Fri Sat Manage Time Start From 0 : 00 To 23 : 59 Use the **Managed Weekdays** fields to specify the days on which the rule should be applied. A red background indicates that the rule will be applied (traffic will be blocked), and a green background indicates that the rule will not be applied (traffic will not be blocked). Click a day to toggle the rule on or off for the relevant day. Use the **Manage Time Start** fields to specify the period during which the rule should be applied. Enter the start time in the **From** fields, using twenty-four hour notation, and enter the end time in the **To** fields.
Apply	Click this to save your changes to the fields in this screen.
Close	Click this to return to the **Service Filter** screen without saving your changes to the rule.

6.3.2 Adding or Editing a Service Filter Trusted Device Rule

- To add a new trusted device rule, click **Add Trusted PC** in the **Security** > **Service Filter** screen.
- To edit an existing trusted device rule, locate the rule in the **Security** > **Service Filter** screen and click its **Manage** button.

The following screen displays.

Figure 36: The Security: Service Filter Trusted Device Add/Edit Screen



Manage Trusted Device

Host Name: example

MAC Address: 00:00:00:00:00:0A

Rule Status: Enabled

The following table describes the labels in this screen.

Table 35: The Security: Service Filter Trusted Device Add/Edit Screen

Host Name	Enter a name to identify the device.
MAC Address	Enter the Media Access Control (MAC) address of the device.
Rule Status	Use this field to define whether the trusted device rule should be active or not. ▸ Select **Enabled** to activate the trusted device rule. ▸ Select **Disabled** to deactivate the trusted device rule.
Apply	Click this to save your changes to the fields in this screen.
Close	Click this to return to the **Service Filter** screen without saving your changes to the rule.

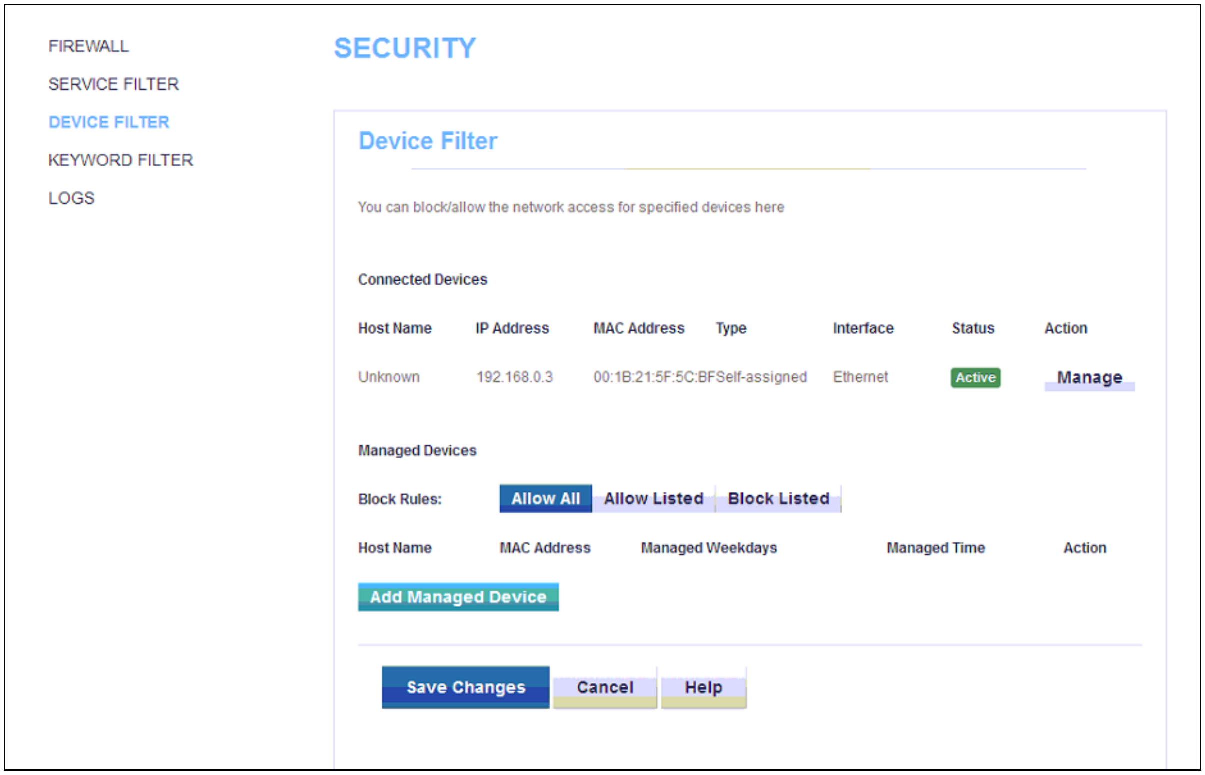
6.4 The Device Filter Screen

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

NOTE: To configure MAC address filtering on the wireless network, see The Wireless Access Control Screen on page 75.

Click **Security** > **Device Filter**. The following screen displays.

Figure 37: The Security: Device Filter Screen



You can block/allow the network access for specified devices here

Connected Devices

Host Name	IP Address	MAC Address	Type	Interface	Status	Action
Unknown	192.168.0.3	00:1B:21:5F:5C:BF	Self-assigned	Ethernet	Active	Manage

Managed Devices

Block Rules: Allow All | Allow Listed | Block Listed

Host Name	MAC Address	Managed Weekdays	Managed Time	Action

The following table describes the labels in this screen.

Table 36: The Security: Device Filter Screen

Connected Devices	
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 the name of the interface on which the relevant device is connected.
Status	This displays whether or not the connected device is active.
Action	Click **Manage** to make changes to the device's filtering status; see Adding or Editing a Managed Device on page 99 for information on the screen that displays.

Table 36: The Security: Device Filter Screen (continued)

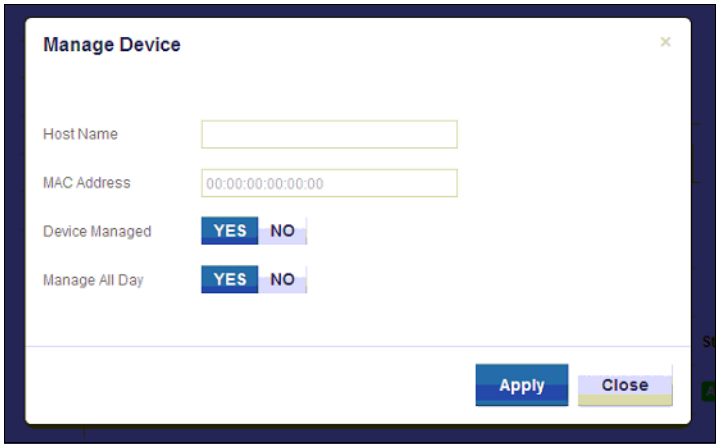
Managed Devices	
Block Rules	Use these buttons to control the action to be taken for the devices listed: - Select **Allow All** to ignore the **Managed Devices** list and let all devices connect to the CGNV4. - Select **Allow Listed** to permit only devices you added to the **Managed Devices** list to access the CGNV4 and the network. All other devices are denied access. - Select **Deny** to permit all devices except those you added to the **Managed Devices** list to access the CGNV4 and the network. The specified devices are denied access.
Host Name	This displays the name of each network device in the list.
MAC Address	This displays the Media Access Control (MAC) address of each network device in the list.
Managed Weekdays	This displays the days of the week on which the device is managed.
Managed Time	This displays the start (**From**) and end (**To**) of the time period during which the device is managed, on the specified **Managed Weekdays**.
Action	Click **Manage** to make changes to a managed device rule (see Adding or Editing a Managed Device on page 99).
Add Managed Device	Click this to add a new managed device rule (see Adding or Editing a Managed Device on page 99).
Save Changes	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

6.4.1 Adding or Editing a Managed Device

- To add a new managed device, click **Add Managed Device** in the **Security** > **Device Filter** screen.
- To edit an existing managed device, locate the device in the **Security** > **Device Filter** screen and click its **Manage** button.

The following screen displays.

Figure 38: The Security: Device Filter Add/Edit Screen

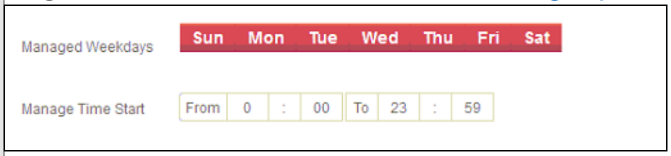


The following table describes the labels in this screen.

Table 37: The Security: Device Filter Add/Edit Screen

Host Name	If you are managing a device that already connected via the LAN, this field displays the device’s name. Alternatively, if you are managing a device that is not connected via the LAN, you can enter its name here if you know it.
MAC Address	If you are managing a device that already connected via the LAN, this field displays the device’s MAC (Media Access Control) address. Alternatively, if you are managing a device that is not connected via the LAN, you can enter its MAC address here if you know it.
Device Managed	Use this field to define whether the device should have its access privileges filtered or not. - Click **Yes** to filter the device’s access privileges. - Click **No** not to filter the device’s access privileges. When a device is not being managed, the **Manage All Day** field, and related fields, do not display.

Table 37: The Security: Device Filter Add/Edit Screen

Manage All Day	Use this field to specify whether the device should be managed on all days of the week, at all times, or whether the device should be managed only at certain times. - Select **YES** to managed the device at all times. - Select **NO** to managed the device only at certain times. Additional fields display, allowing you to specify the times at which the device should be managed. Figure 39: Additional Service Filtering Options  Managed Weekdays: Sun Mon Tue Wed Thu Fri Sat Manage Time Start: From 0 : 00 To 23 : 59 Use the **Managed Weekdays** fields to specify the days on which the device should be managed. A red background indicates that the device will be managed (access will be blocked), and a green background indicates that the device will not be managed (access will not be blocked). Click a day to toggle the rule on or off for the relevant day. Use the **Manage Time Start** fields to specify the period during which the device should be managed. Enter the start time in the **From** fields, using twenty-four hour notation, and enter the end time in the **To** fields.
Apply	Click this to save your changes to the fields in this screen.
Close	Click this to return to the **Device Filter** screen without saving your changes to the rule.

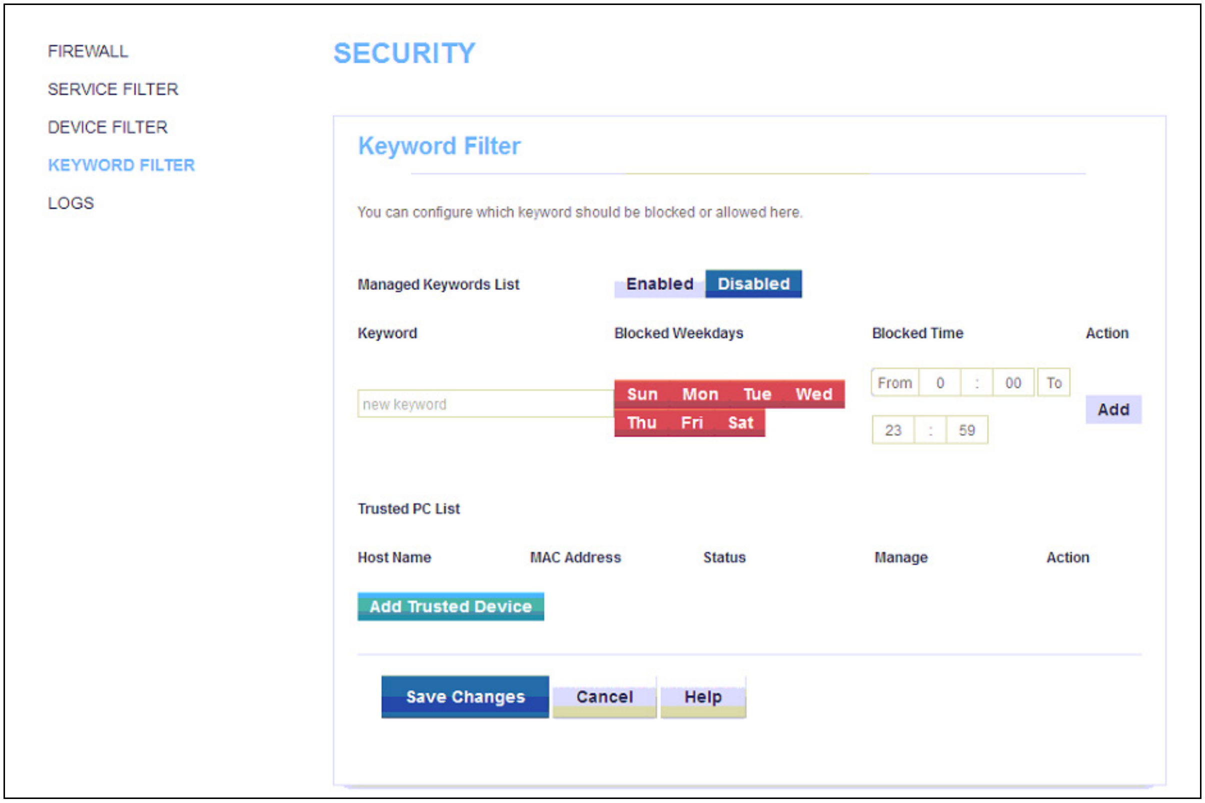
6.5 The Keyword Filter Screen

Use this screen to block access from the LAN to websites whose URLs (Web addresses) and page content (text) contain certain keywords. You can create multiple keyword blocking rules, and set them to apply on certain days and at certain times.

You can also create and edit trusted device rules. Trusted devices are those to which keyword filtering rules are not applied.

Click **Security** > **Keyword Filter**. The following screen displays.

Figure 40: The Security: Keyword Filter Screen



You can configure which keyword should be blocked or allowed here.

The following table describes the labels in this screen.

Table 38: The Security: Keyword Filter Screen

Managed Keywords List	Use this field to turn keyword filtering on or off. ▸ Select **Enabled** to turn keyword filtering on. ▸ Select **Disabled** to turn keyword filtering off.
Keyword	Enter the keyword that you want to block. The CGNV4 examines both the page's URL (Internet address) and its page content (text).
Blocked Weekdays	Use these fields to specify the times at which the keyword should be blocked. A red background indicates that the rule will be applied (access will be blocked), and a green background indicates that the device will not be applied (access will not be blocked). Click a day to toggle the rule on or off for the relevant day.

Table 38: The Security: Keyword Filter Screen (continued)

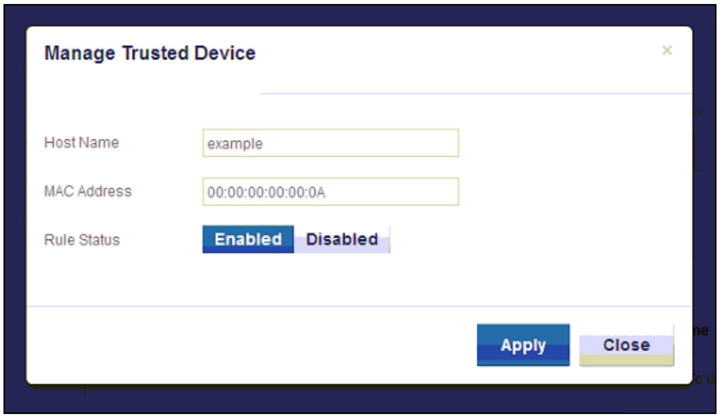
Blocked Time	Use these fields to specify the period during which the rule should be applied. Enter the start time in the **From** fields, using twenty-four hour notation, and enter the end time in the **To** fields.
Action	Click **Add** to create a new keyword blocking rule; a new row of fields display.
Trusted PC List	
Host Name	This displays the arbitrary name of each trusted PC you configured.
MAC Address	This displays the Media Access Control (MAC) address of each trusted PC. Every network device has a MAC address that uniquely identifies it.
Status	This displays whether the device is currently trusted (**Enabled**) or untrusted (**Disabled**).
Manage	Click **Manage** to make changes to the trusted device rule. See Adding or Editing a Keyword Filter Trusted Device Rule on page 102 for information on the screen that displays.
Action	Click **Delete** to remove the trusted device rule.
Add Trusted Device	Click this to create a new trusted device rule. See Adding or Editing a Keyword Filter Trusted Device Rule on page 102 for information on the screen that displays.
Save Changes	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.

6.5.1 Adding or Editing a Keyword Filter Trusted Device Rule

- To add a new trusted device rule, click **Add Trusted PC** in the **Security** > **Keyword Filter** screen.
- To edit an existing trusted device rule, locate the rule in the **Security** > **Keyword Filter** screen and click its **Manage** button.

The following screen displays.

Figure 41: The Security: Keyword Filter Trusted Device Add/Edit Screen



Host Name: example

MAC Address: 00:00:00:00:00:0A

Rule Status: Enabled

The following table describes the labels in this screen.

Table 39: The Security: Keyword Filter Trusted Device Add/Edit Screen

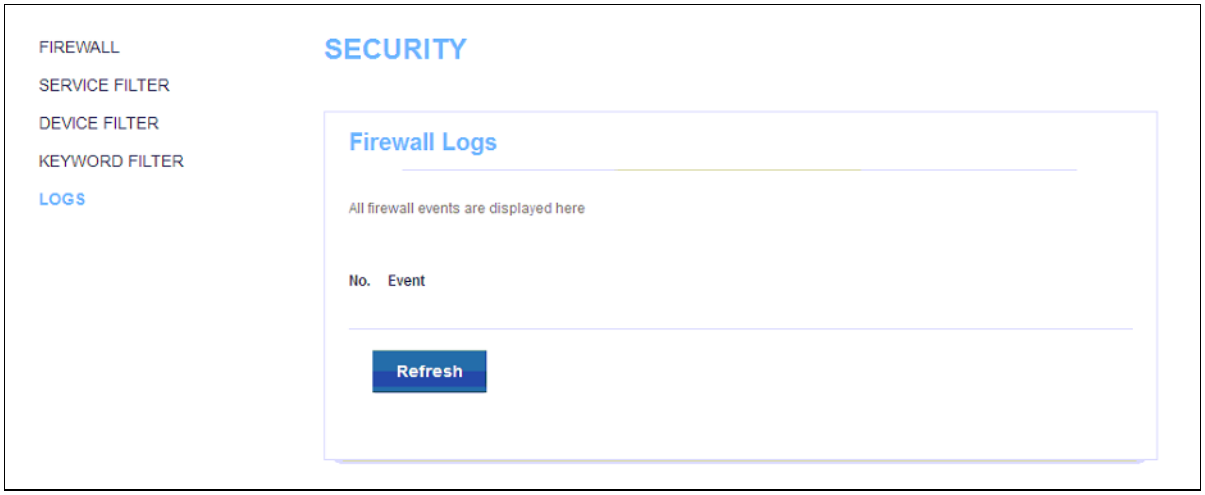
Host Name	Enter a name to identify the device.
MAC Address	Enter the Media Access Control (MAC) address of the device.
Rule Status	Use this field to define whether the trusted device rule should be active or not. - Select **Enabled** to activate the trusted device rule. - Select **Disabled** to deactivate the trusted device rule.
Apply	Click this to save your changes to the fields in this screen.
Close	Click this to return to the **Keyword Filter** screen without saving your changes to the rule.

6.6 The Logs Screen

Use this screen to view information about local firewall activity events.

Click **Security** > **Logs**. The following screen displays.

Figure 42: The Security: Logs Screen



All firewall events are displayed here

No. Event

The following table describes the labels in this screen.

Table 40: The Security: Logs Screen

No.	This displays the arbitrary, incremental index number assigned to the firewall event.
Event	This displays a description of the firewall event.

7

Troubleshooting

Use this section to solve common problems with the CGNV4 and your network. It contains the following sections:

Problem: None of the LEDs Turn On

The CGNV4 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 CGNV4 can damage the CGNV4.

2. Ensure that the power adaptor is connected to the CGNV4 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 CGNV4.

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 CGNV4's hardware is connected correctly; see the Quick Installation Guide.

3 Disconnect and re-connect the power adaptor to the CGNV4.

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

Problem: I Forgot the CGNV4's IP Address

1 The CGNV4's default LAN IP address is **192.168.0.1**.

2 Depending on your operating system and your network, you may be able to find the CGNV4'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.

Problem: I Forgot the CGNV4's Admin Username or Password

The default username is **admin**, and the default password is **admin**.

Problem: I Cannot Access the CGNV4 or the Internet

1 Ensure that you are using the correct IP address for the CGNV4.

2 Check your network's hardware connections, and that the CGNV4's LEDs display correctly (see LEDs on page 18).

3 Make sure that your computer is on the same subnet as the CGNV4; see IP Address Setup on page 21.

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 CGNV4. See Resetting the CGNV4 on page 25. All user-configured data is lost, and the CGNV4 is returned to its default settings. If you previously backed-up a more recent version your CGNV4's settings, you can now upload them to the CGNV4; see The Backup Screen on page 82.

6 If the problem persists, contact your vendor.

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 CGNV4'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 CGNV4's signal quality and coverage area.

3 Ensure that the CGNV4 and the wireless client are set to use the same wireless mode, SSID and security settings (see The Wireless Basic Settings Screen on page 64 and The WPS & Security Screen on page 71).

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 CGNV4 and the button on the wireless client within 2 minutes of one another.

Index