CGNVM DOCSIS 3.0 eMTA WiFi Gateway

User's Guide

Version 1.0 - 02/2015
SW Version CGNVM_4.5.10.10T3-MGCP-150429

hitron

About This User's Guide

Intended Audience

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

How to Use this User's Guide

This manual contains information on each the CGNVM'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 124) to find information on a specific keyword.
- Use the rest of this User's Guide to see in-depth descriptions of the CGNVM's features.

Related Documentation

- **Quick Installation Guide**: see this for information on getting your CGNVM up and running right away. It includes information on system requirements, package contents, the installation procedure, and basic troubleshooting tips.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

- **Online Help**: each screen in the CGNVM'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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Customer Support

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

Default Login Details

The CGNVM's default IP address and login credentials are as follows. For more information, see Login to the CGNVM on page 25.

Table 1: Default Credentials

IP Address	192.168.0.1
Username	cusadmin
Password	password

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Copyright © 2014 Hitron Technologies. All rights reserved. All trademarks and registered trademarks used are the properties of their respective owners.

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

Table of Contents

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

List of Figures

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

List of Tables

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

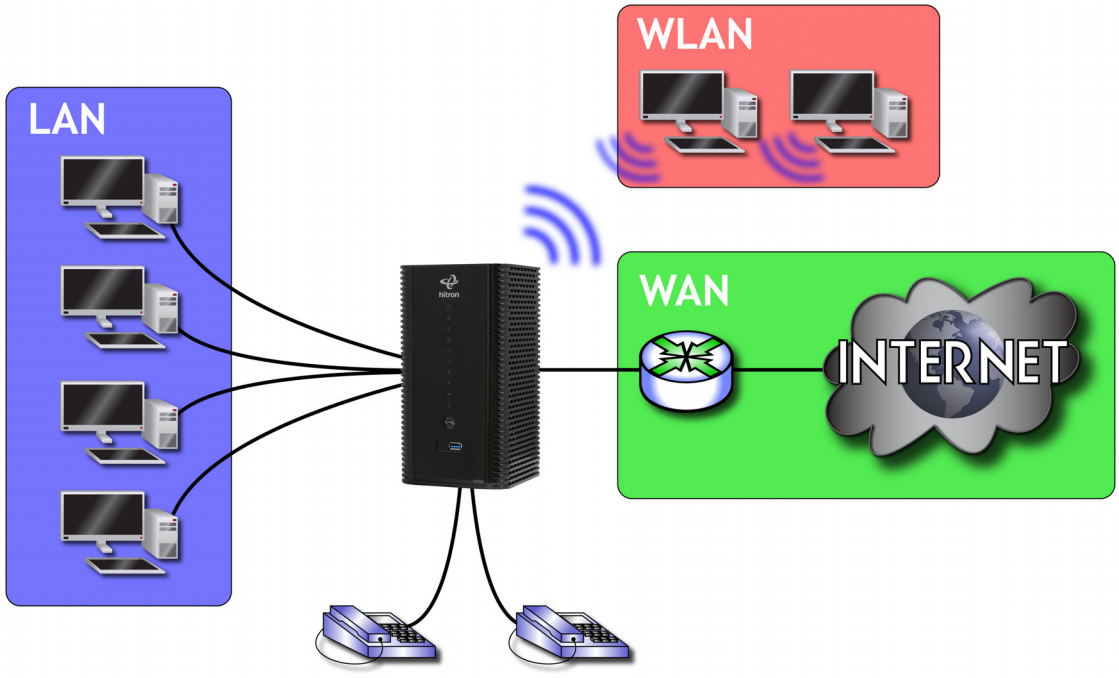
1 Introduction

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

1.1 CGNVM Overview

Your CGNVM 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 another and to the Internet via your building's cable connection.

Figure 1: Application Overview



Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

1.1.1 Key Features

The CGNVM provides:

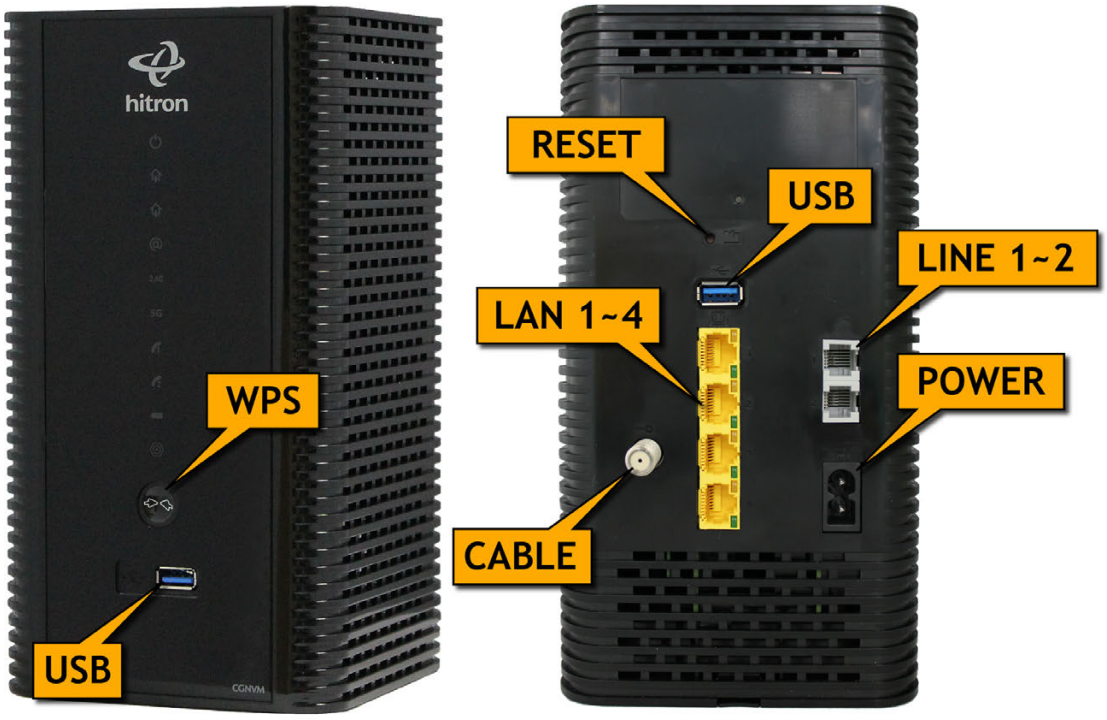
- DOCSIS/EuroDOCSIS 3.0 compliance and DOCSIS 3.0 certification.
- Two USB 2.0 hosts, supporting Network Attached Storage (NAS) functionality.
- WiFi 2.4GHz 802.11n and 5GHz 802.11ac dual-band MIMO internal antennas.
- 16 wireless Service Set IDentifiers (SSIDS); 8 SSIDs per radio.
- Individual configuration for each SSID, including security, bridging, routing, firewall and WiFi parameters.
- Integrated DLNA media server with support for video, audio and image serving.
- Well-defined LEDs that clearly display device and network status.
- Enhanced management and stability for low total cost of ownership.
- 2 FXS ports for telephony using SIP or MGCP.
- MoCA 2.0 connectivity for highest performance.
- Full operator control via configuration file and SNMP
- TR-069 and HNAP ready for easy setup and remote management

1.2 Hardware Connections

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 2: Hardware Connections



Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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. The **WPS** LED displays WiFi Protected Setup connection status as follows: ▸ **Bi-color, blinking**: the WPS connection is processing. ▸ **Green, steady**: the WPS connection has been successful. ▸ **Red, steady**: the WPS connection has failed, or an error has occurred. ▸ **Off**: WPS is not active. See WPS on page 78 for more information.
USB	The CGNVM provides two USB 2.0 host ports, allowing you to plug in USB flash disks for mounting and sharing through the LAN interfaces via the Samba protocol (network neighborhood). The CGNVM supports the following Windows file systems: ▸ FAT16 ▸ FAT32 **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).**

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 2: Hardware Connections

RESET	Use this button to reboot or reset your CGNVM to its factory default settings. To reboot the CGNVM, press the button and hold it for less than five seconds. The CGNVM restarts, using your existing settings. To reset the CGNVM, press the button and hold it for five or more seconds. All user-configured settings are deleted, and the CGNVM restarts using its factory default settings.
LINE 1 LINE 2	Use these ports to connect your analog phones for VoIP services, using cables with RJ11 connectors.
LAN1 LAN2 LAN3 LAN4	Use these ports to connect your computers and other network devices, using Category 5 or 6 Ethernet cables with RJ45 connectors.
CABLE	Use this to connect to the Internet via an F-type RF cable.
POWER	Use the **POWER** port to connect to the 100~125VAC power cable that came with your CGNVM. NOTE: Additionally to the POWER connection, you can also use a battery to power the CGNVM in the event of a power outage; see Battery Installation (optional) on page 19. Figure 3: Power Cable 

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

1.3 Battery Installation (optional)

Depends on your multiple system operator (MSO), the CGNVM may be equipped with a lithium-ion battery backup that can provide emergency power to the device in the event of a power outage.

You can install and replace the CGNVM's battery without disconnecting the power cable.

NOTE: The CGNVM battery is intended for use as a backup to the main power source, not as a replacement for it. For optimal power performance you should use the battery in conjunction with the main power source.

For safety and regulatory reasons, batteries are shipped separately to the CGNVM, and must be manually installed. To install the battery:

1. The battery compartment is located on the underside of the CGNVM. Place the CGNVM on a table and remove the battery compartment door.

Figure 4: Battery Compartment (optional)

2. Remove the battery from its packaging.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 5: Battery (optional)

NOTE: Your battery may look somewhat different from the battery depicted, depending on the number of cells it contains.

3 Insert the battery into the battery compartment.

4 Replace the battery compartment door and return the CGNVM to an upright position.

1.4 LEDs

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 6: LEDs

Table 3: LEDs

LED	STATUS	DESCRIPTION

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 3: LEDs

POWER 	Green, steady	The CGNVM is running on AC power via the power cord.
	Green, blinking (optional)	The CGNVM is running on battery power when AC power is disconnected.
	Off	The CGNVM is not running on AC power via the power cord.
DS 	Green, blinking	The CGNVM is searching for a downstream frequency on the **CABLE** connection.
	Green, steady	The CGNVM has successfully located and locked onto a single downstream frequency on the **CABLE** connection.
	Blue, steady	The CGNVM is successfully engaged in channel bonding on the downstream connection.
	Off	There is no downstream activity on the **CABLE** connection.
US 	Green, blinking	The CGNVM is searching for an upstream frequency on the **CABLE** connection.
	Green, steady	The CGNVM has successfully located and locked onto a single upstream frequency on the **CABLE** connection.
	Blue, steady	The CGNVM is successfully engaged in channel bonding on the upstream connection.
	Off	There is no upstream activity on the **CABLE** connection.
Online 	Green, blinking	The CGNVM's cable modem is registering with the service provider's CMTS.
	Green, steady	The CGNVM's cable modem has successfully registered with the service provider and is ready for data transfer.
	Off	The CGNVM's cable modem is offline.
WIRELESS (2.4GHZ) 	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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 3: LEDs

WIRELESS (5GHZ) 	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.
Line 1 Line 2  	Off	No telephone is connected to the relevant **Line** port.
	Green, blinking	A telephone is connected to the relevant **Line** port, and is off-hook.
	Green, steady	A telephone is connected to the relevant **Line** port, and is on-hook.
BATTERY (optional) 	Off	The CGNVM is running on battery power.
	Amber, steady	The CGNVM is not running on battery power.
	Amber, blinking	The CGNVM's battery power is low.
MoCA 	Off	The CGNVM's MoCA functionality is not enabled.
	Green, blinking	The CGNVM is searching for MoCA devices on the cable network.
	Green, steady	The CGNVM has detected a MoCA device on the cable network, and has successfully made a connection to it.

NOTE: For information on the behavior of the **WPS** button LED, see Table 2 on page 17.

1.5 IP Address Setup

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

NOTE: See IP Addresses and Subnets on page 30 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 CGNVM (see GUI Overview on page 26).

- 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 24 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 CGNVM's IP settings may have been changed from their defaults. If you do not know the CGNVM's new address, you should return it to its factory defaults. See Resetting the CGNVM on page 28. Bear in mind that ALL user-configured settings are lost.

1.5.1 Manual IP Address Setup

By default, your CGNVM's local IP address is **192.168.0.1**. If your CGNVM 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 CGNVM:

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:

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

- 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 CGNVM is not using the default IP address, enter an IP address and subnet mask that places your computer in the same subnet as the CGNVM.

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

1.6 Login to the CGNVM

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

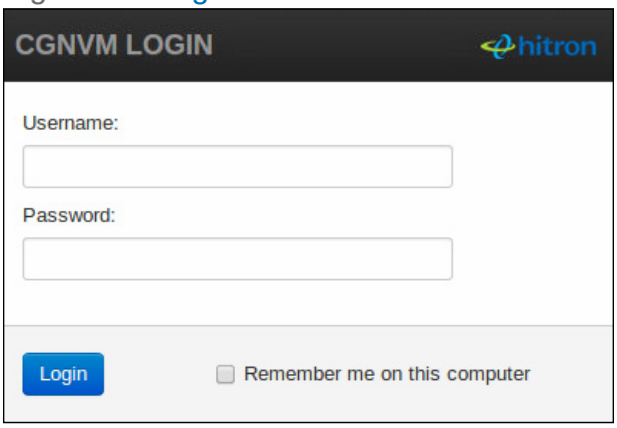
NOTE: You can login to the CGNVM's GUI via the wireless interface. However, it is strongly recommended that you configure the CGNVM via a wired connection on the LAN.

1 Open a browser window.

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 7: Login



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

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

4 Click **Login**. The **Status Overview** screen displays (see Status Overview on page 29).

1.7 GUI Overview

This section describes the CGNVM's GUI.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 8: GUI Overview

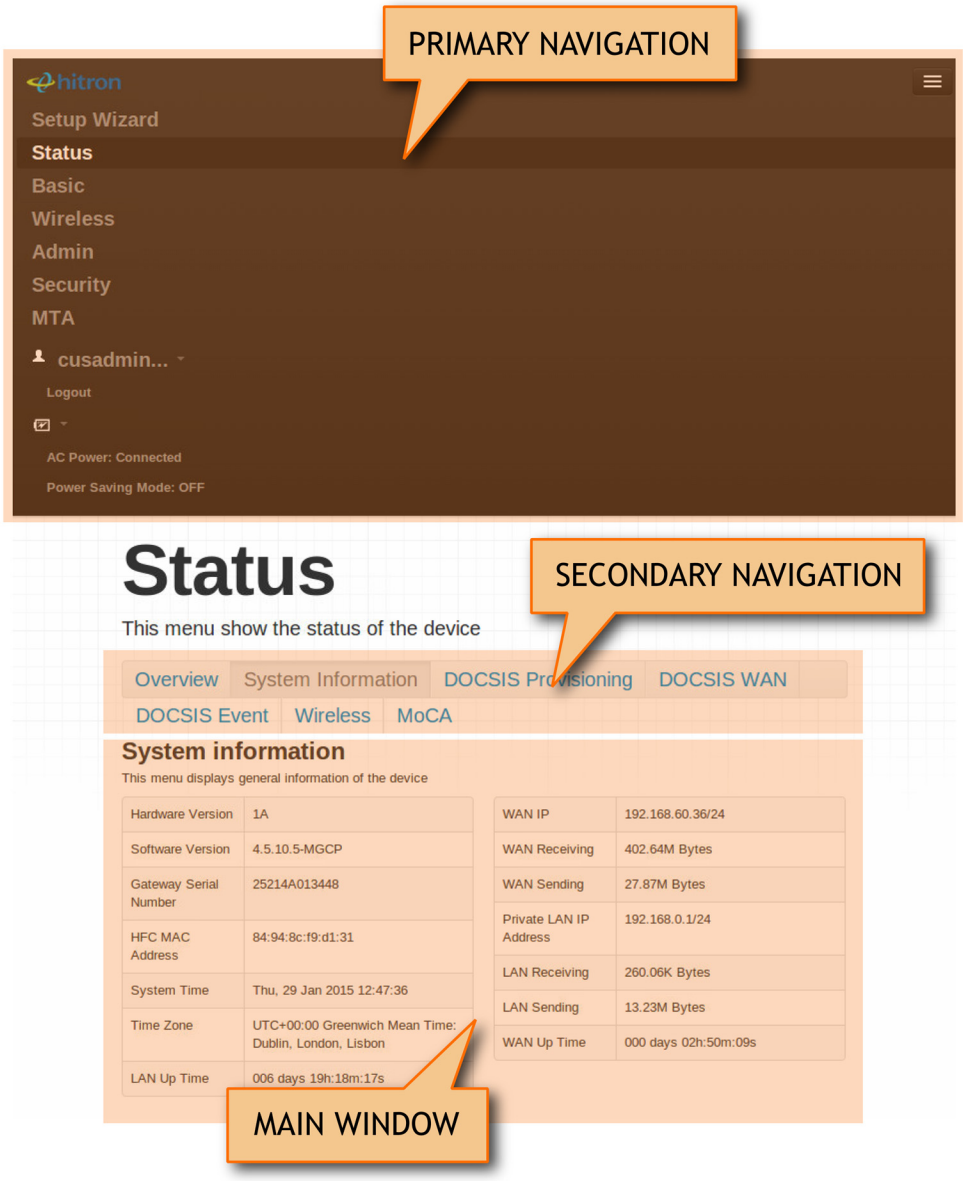


Table 4: GUI Overview

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

1.8 Resetting the CGNVM

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

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

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

NOTE: Depending on your CGNVM's previous configuration, you may need to re-configure your computer's IP settings; see IP Address Setup on page 23.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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 CGNVM supports DOCSIS version 3.0.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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 CGNVM:

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

- 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 CGNVM 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 CGNVM'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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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 23 for more information.

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

2.1.6 Routing Mode

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

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

2.1.7 Configuration Files

The CGNVM's configuration (or config) file is a document that the CGNVM obtains automatically over the Internet from the service provider's server, which specifies the settings that the CGNVM 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 CGNVM, and "upstream" refers to traffic from the CGNVM 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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

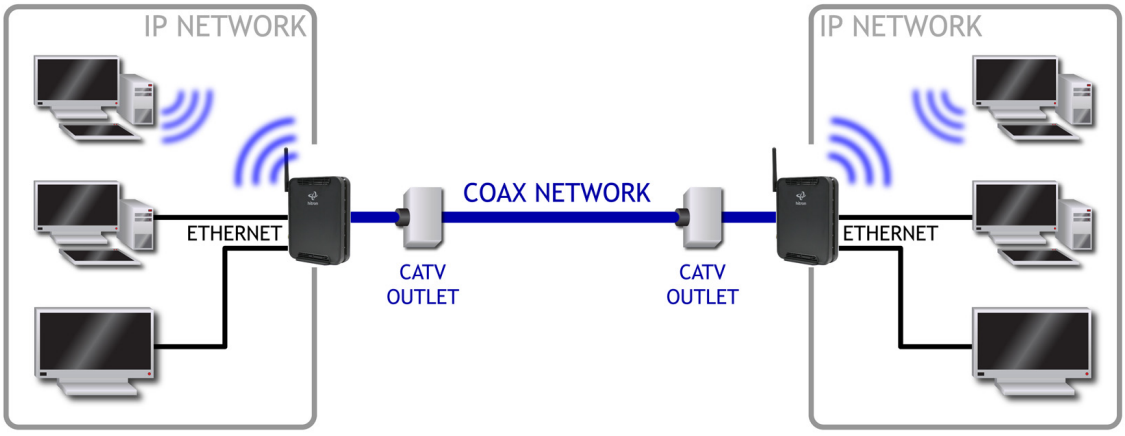
- SCDMA allows multiple users to share the same frequency channel by assigning a unique orthogonal code to each user.

2.1.12 The Multimedia over Coax Alliance

The Multimedia over Coax Alliance (MoCA) is a non-profit technology alliance, which defines a set of specifications for the delivery of high-speed data, such as HD video, over your building's existing co-axial cabling network. Co-axial, or coax (pronounced "ko-axe") cable is already incorporated into most buildings for the transmission of RF signals, traditionally for relaying television broadcasts from a TV antenna, satellite or cable box to individual televisions around the building.

MoCA devices allow you use the coax cable network as an extension of your building's existing IP network, which includes both wired (Ethernet) and wireless (WiFi) traffic. Because they bridge the two networks, they are known as Ethernet-to-Coax Bridges, or ECBs.

Figure 9: Bridging the Gap Between IP and Coaxial Networks



MoCA traffic on the coax network does not interfere with existing broadcasts from cable, telco, IPTV or satellite service providers, as it makes use of a previously-unused segment of the RF spectrum. The medium is ideal for real-time applications, providing high data throughput (100Mbps~1Gbps) with low latency, jitter or data loss. Also, coax cabling is generally better-shielded than IP networking media, especially wireless.

Applications to which MoCA networking is well-suited include:

- Video on Demand (VoD)

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

- Multi-room, multi-camera Digital Video Recording (DVR)
- Gaming (LAN or online multiplayer)
- Internet video
- Home automation
- Video conferencing

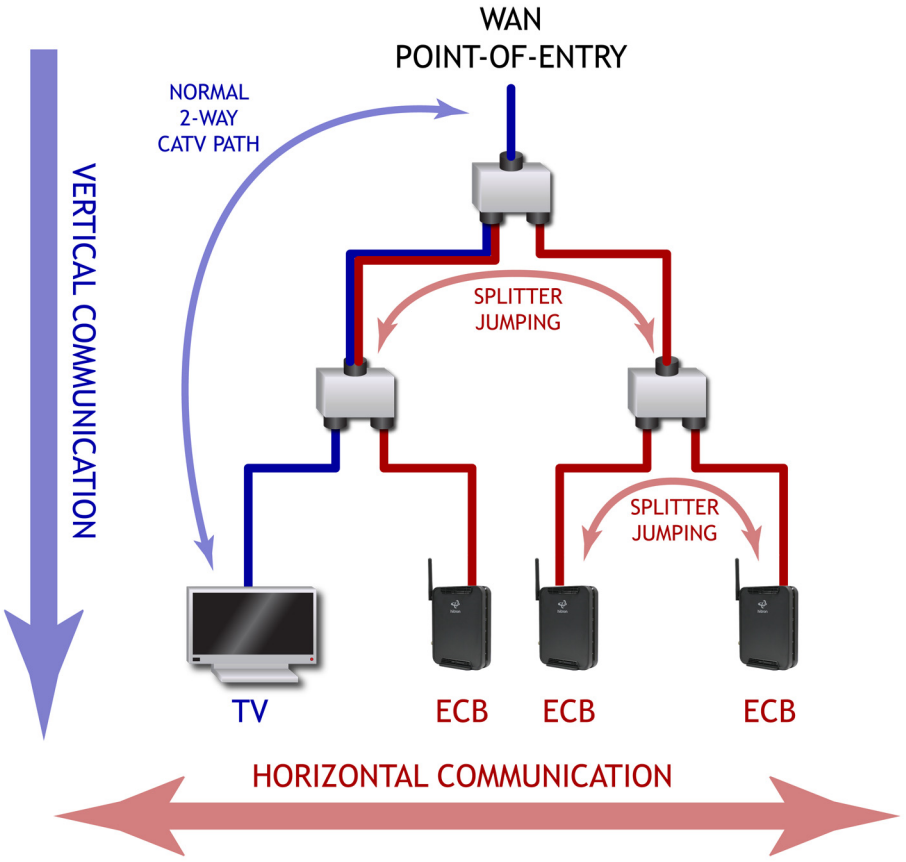
2.1.12.1 Horizontal vs. Vertical Communications

Unlike traditional coax networking (TV, satellite, IPTV, etc.) MoCA devices do not need to receive data from a single source. It is "outlet-to-outlet". Each MoCA network uses a Network Controller (NC) to manage the network's communications, but any ECB on the network is capable of acting as the NC. By default, the NC is chosen by negotiation between all ECBs on the network, based on factors such as signal strength.

"Outlet-to-outlet" communications are also known as "splitter jumping". Traditional cable networking commonly utilized splitters to split a single incoming signal into two outgoing signals. With MoCA, communications between devices connected to each splitter output are possible. For this reason, MoCA communications can be considered "horizontal", as opposed to traditional "vertical" cable communications.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 10: Traditional Vertical CATV vs. Horizontal MoCA Networking

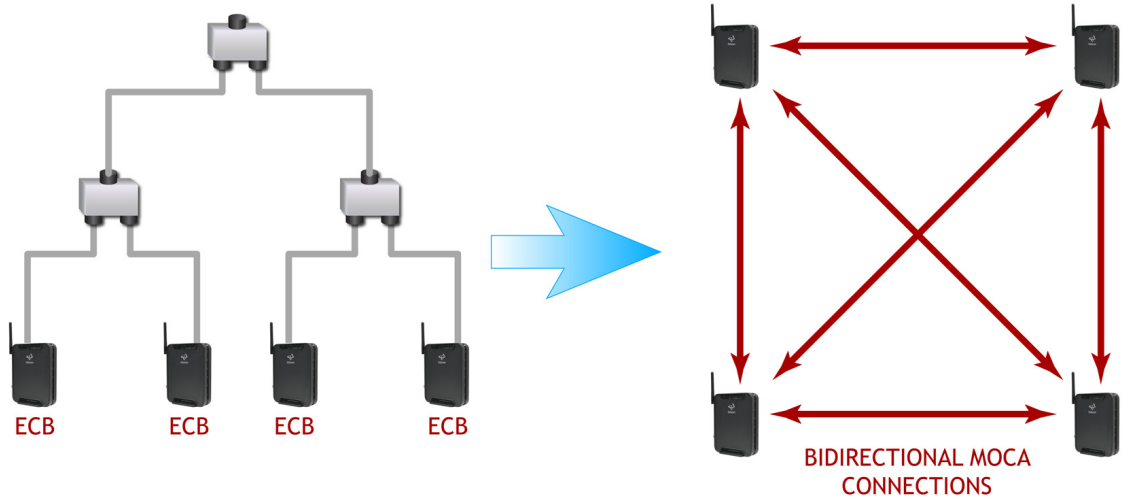


2.1.12.2 Example MoCA Mesh Network

MoCA devices form a full "mesh", or peer-to-peer network (where all devices communicate directly with one another). In the following example, four MoCA devices connect directly to and from one another, via ECBs, forming 12 unique MoCA links (or 6 bidirectional links).

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 11: Example MoCA Peer-to-Peer Network



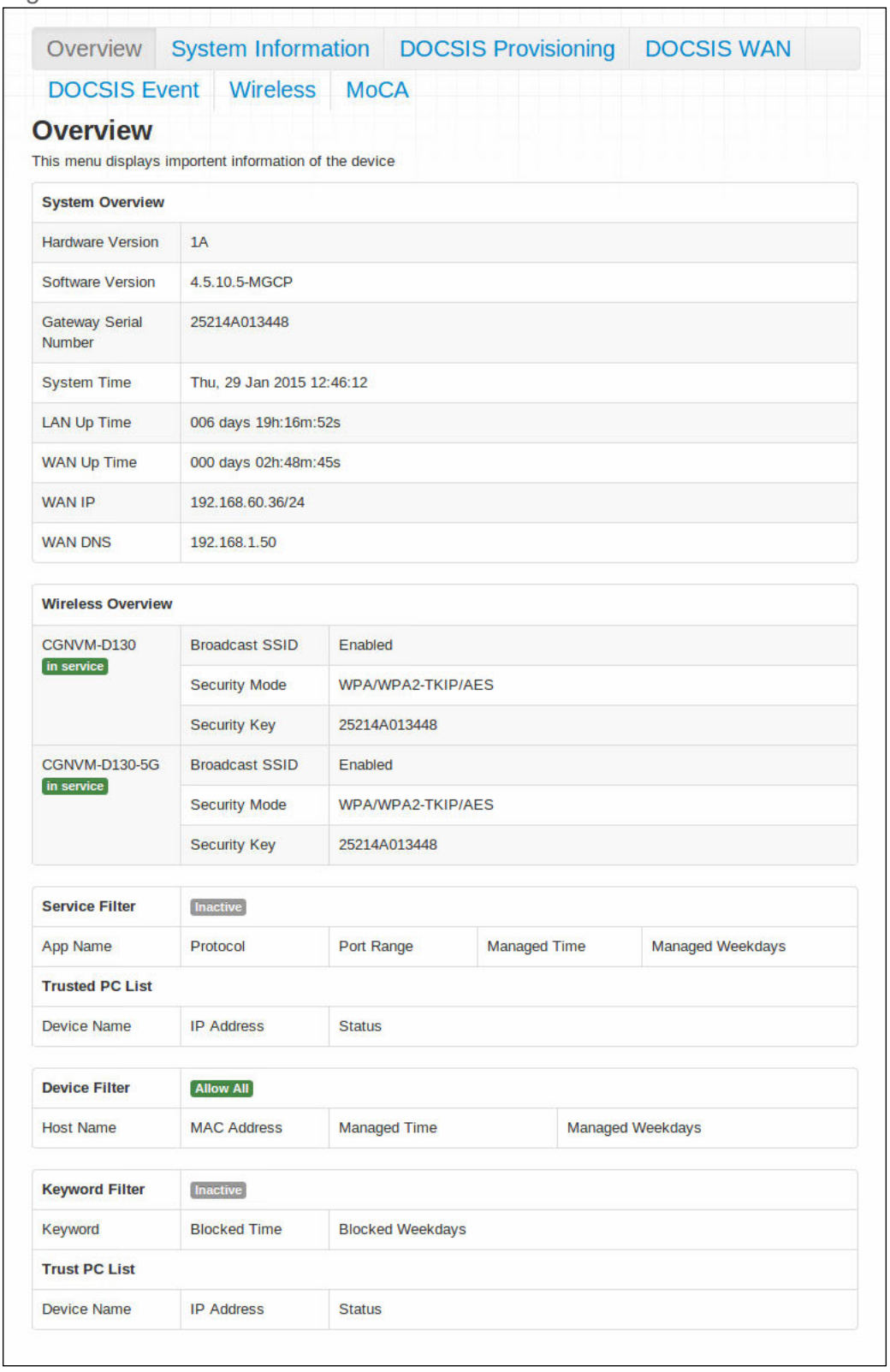
2.2 The Status: Overview Screen

Use this screen to

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 12: The Status: Overview Screen



Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

The following table describes the labels in this screen.

Table 8: The Status: Overview Screen

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.

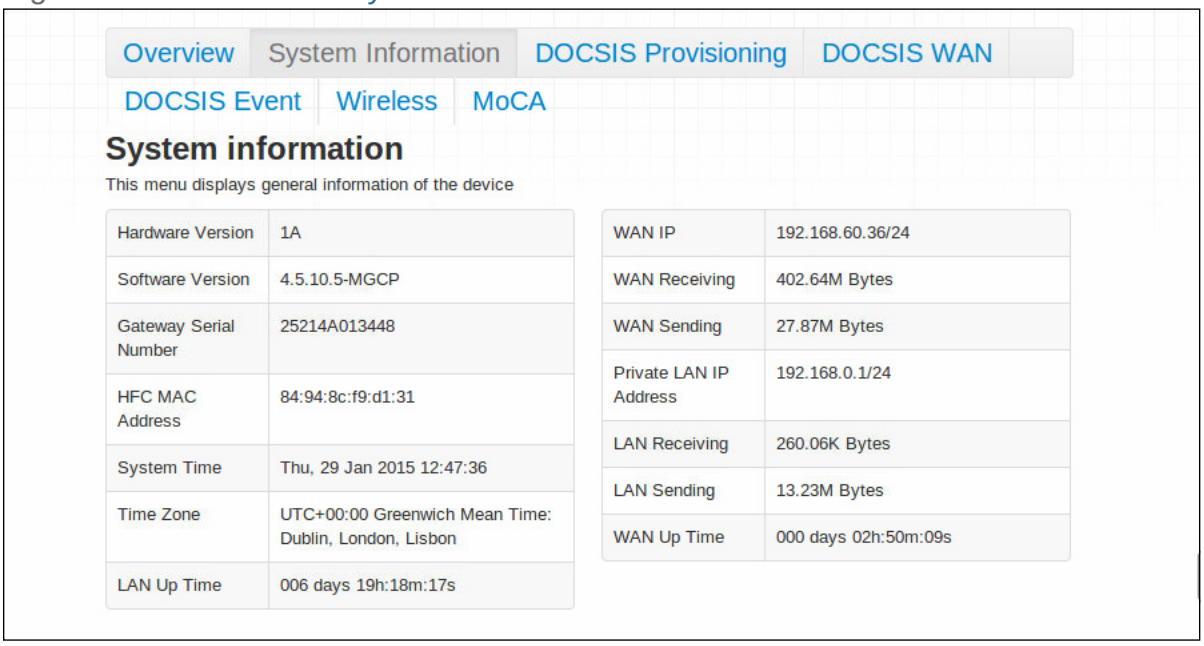
2.3 The Status: System Information Screen

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

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 13: The Status: System Information Screen



The following table describes the labels in this screen.

Table 9: The Status: System Information Screen

Hardware Version	This displays the version number of the CGNVM's physical hardware.
Software Version	This displays the version number of the software that controls the CGNVM.
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 CGNVM'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.
Time Zone	This displays the time zone in which the CGNVM is located.
LAN Up Time	This displays the amount of time that has elapsed since the CGNVM's Local Area Network connection was last restarted.
WAN IP	This displays the CGNVM's WAN IP address. This IP address is automatically assigned to the CGNVM
WAN Receiving	This displays the amount of data received over the WAN connection since the device was last started.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 9: The Status: System Information Screen (continued)

WAN Sending	This displays the amount of data transmitted over the WAN connection since the device was last started.
Private LAN IP Address	This displays the CGNVM's LAN subnet's IP information.
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.
WAN Up Time	This displays the amount of time that has elapsed since the CGNVM's Wide Area Network connection was last restarted.

2.4 The Status: DOCSIS Provisioning Screen

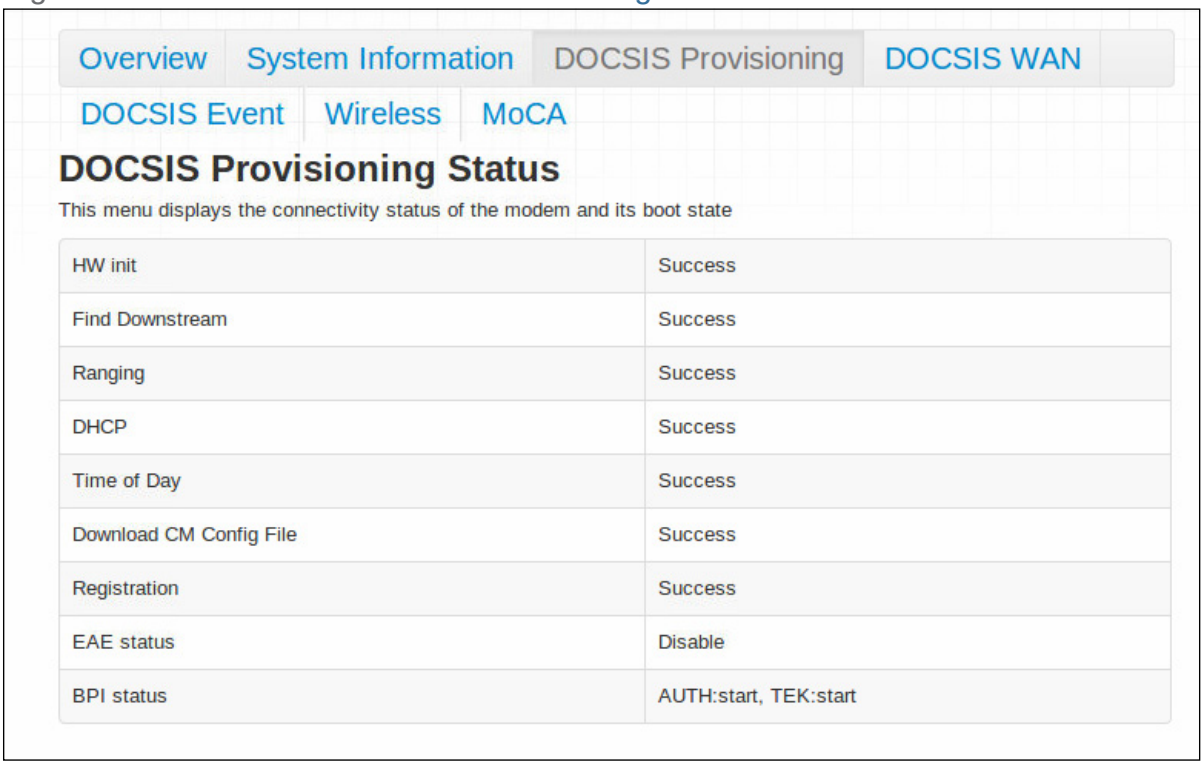
This screen displays the steps successfully taken to connect to the Internet over the **Cable** connection.

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

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 14: The Status: DOCSIS Provisioning Screen



For each step:

- **Process** displays when the CGNVM is attempting to complete a connection step.
- **Success** displays when the CGNVM has completed a connection step.
- **Disable** displays when the relevant feature has been turned off.

2.5 The Status: DOCSIS WAN Screen

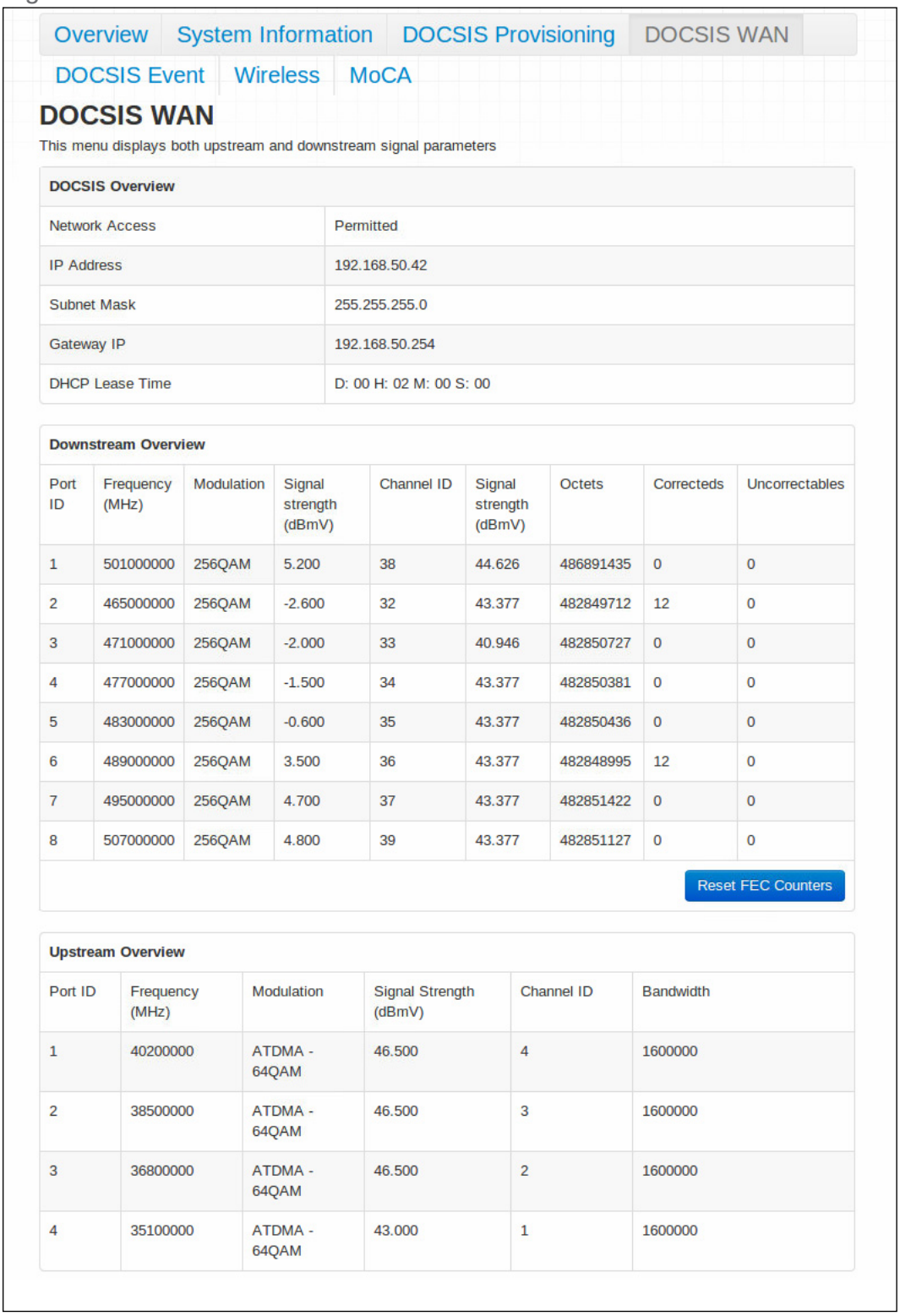
Use this screen to discover information about:

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

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 15: The Status: DOCSIS WAN Screen



Overview | System Information | DOCSIS Provisioning | DOCSIS WAN | DOCSIS Event | Wireless | MoCA

DOCSIS WAN

This menu displays both upstream and downstream signal parameters

DOCSIS Overview

Network Access	Permitted
IP Address	192.168.50.42
Subnet Mask	255.255.255.0
Gateway IP	192.168.50.254
DHCP Lease Time	D: 00 H: 02 M: 00 S: 00

Downstream Overview

Port ID	Frequency (MHz)	Modulation	Signal strength (dBmV)	Channel ID	Signal strength (dBmV)	Octets	Correcteds	Uncorrectables
1	501000000	256QAM	5.200	38	44.626	486891435	0	0
2	465000000	256QAM	-2.600	32	43.377	482849712	12	0
3	471000000	256QAM	-2.000	33	40.946	482850727	0	0
4	477000000	256QAM	-1.500	34	43.377	482850381	0	0
5	483000000	256QAM	-0.600	35	43.377	482850436	0	0
6	489000000	256QAM	3.500	36	43.377	482848995	12	0
7	495000000	256QAM	4.700	37	43.377	482851422	0	0
8	507000000	256QAM	4.800	39	43.377	482851127	0	0

Reset FEC Counters

Upstream Overview

Port ID	Frequency (MHz)	Modulation	Signal Strength (dBmV)	Channel ID	Bandwidth
1	40200000	ATDMA - 64QAM	46.500	4	1600000
2	38500000	ATDMA - 64QAM	46.500	3	1600000
3	36800000	ATDMA - 64QAM	46.500	2	1600000
4	35100000	ATDMA - 64QAM	43.000	1	1600000

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

The following table describes the labels in this screen.

Table 10: 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 CGNVM's WAN IP address. This IP address is automatically assigned to the CGNVM
Subnet Mask	This displays the CGNVM's WAN subnet mask.
Gateway IP	This displays the IP address of the device to which the CGNVM is connected on the WAN.
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 CGNVM.	
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 CGNVM is connected.
Modulation	This displays the type of modulation that each downstream channel uses.
Channel ID	This displays the ID number of each channel on which the downstream signal is transmitted.
SNR (dB)	This displays the Signal to Noise Ratio (SNR) of each downstream data channel to which the CGNVM is connected, in dB (decibels).
Octets	This displays the total number of octets received.
Correcteds	This displays the number of blocks received that required correction due to corruption, and were corrected.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 10: The Status: DOCSIS WAN Screen (continued)

Uncorrectables	This displays the number of blocks received that required correction due to corruption, but were unable to be connected.
Reset FEC Counters	Click this to return the Forward Error Connection (FEC) columns (**Correcteds** and **Uncorrectables**).
Upstream Overview NOTE: The upstream signal is the signal transmitted from the CGNVM.	
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 CGNVM is connected.
Modulation	This displays the type of modulation that each upstream channel uses.
SNR (dB)	This displays the Signal to Noise Ratio (SNR) of each upstream data channel to which the CGNVM is connected, in dB (decibels).
Channel ID	This displays the ID number of each channel on which the upstream signal is transmitted.
Bandwidth	This displays the maximum available bandwidth on the relevant channel.

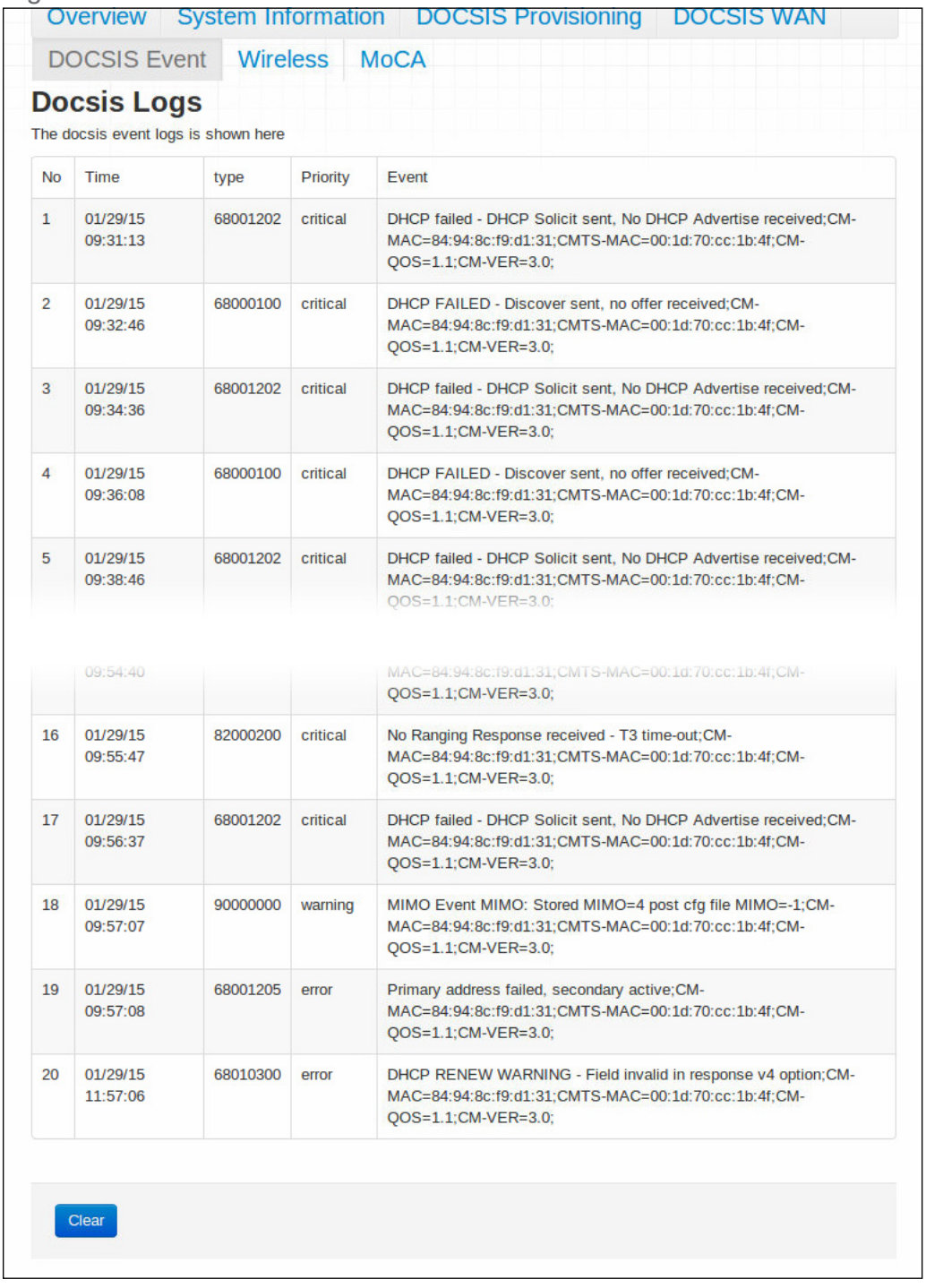
2.6 The Status: DOCSIS Event Screen

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

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 16: The Status: DOCSIS Event Screen



No	Time	type	Priority	Event
1	01/29/15 09:31:13	68001202	critical	DHCP failed - DHCP Solicit sent, No DHCP Advertise received;CM-MAC=84:94:8c:f9:d1:31;CMTS-MAC=00:1d:70:cc:1b:4f;CM-QOS=1.1;CM-VER=3.0;
2	01/29/15 09:32:46	68000100	critical	DHCP FAILED - Discover sent, no offer received;CM-MAC=84:94:8c:f9:d1:31;CMTS-MAC=00:1d:70:cc:1b:4f;CM-QOS=1.1;CM-VER=3.0;
3	01/29/15 09:34:36	68001202	critical	DHCP failed - DHCP Solicit sent, No DHCP Advertise received;CM-MAC=84:94:8c:f9:d1:31;CMTS-MAC=00:1d:70:cc:1b:4f;CM-QOS=1.1;CM-VER=3.0;
4	01/29/15 09:36:08	68000100	critical	DHCP FAILED - Discover sent, no offer received;CM-MAC=84:94:8c:f9:d1:31;CMTS-MAC=00:1d:70:cc:1b:4f;CM-QOS=1.1;CM-VER=3.0;
5	01/29/15 09:38:46	68001202	critical	DHCP failed - DHCP Solicit sent, No DHCP Advertise received;CM-MAC=84:94:8c:f9:d1:31;CMTS-MAC=00:1d:70:cc:1b:4f;CM-QOS=1.1;CM-VER=3.0;
	09:54:40			MAC=84:94:8c:f9:d1:31;CMTS-MAC=00:1d:70:cc:1b:4f;CM-QOS=1.1;CM-VER=3.0;
16	01/29/15 09:55:47	82000200	critical	No Ranging Response received - T3 time-out;CM-MAC=84:94:8c:f9:d1:31;CMTS-MAC=00:1d:70:cc:1b:4f;CM-QOS=1.1;CM-VER=3.0;
17	01/29/15 09:56:37	68001202	critical	DHCP failed - DHCP Solicit sent, No DHCP Advertise received;CM-MAC=84:94:8c:f9:d1:31;CMTS-MAC=00:1d:70:cc:1b:4f;CM-QOS=1.1;CM-VER=3.0;
18	01/29/15 09:57:07	90000000	warning	MIMO Event MIMO: Stored MIMO=4 post cfg file MIMO=-1;CM-MAC=84:94:8c:f9:d1:31;CMTS-MAC=00:1d:70:cc:1b:4f;CM-QOS=1.1;CM-VER=3.0;
19	01/29/15 09:57:08	68001205	error	Primary address failed, secondary active;CM-MAC=84:94:8c:f9:d1:31;CMTS-MAC=00:1d:70:cc:1b:4f;CM-QOS=1.1;CM-VER=3.0;
20	01/29/15 11:57:06	68010300	error	DHCP RENEW WARNING - Field invalid in response v4 option;CM-MAC=84:94:8c:f9:d1:31;CMTS-MAC=00:1d:70:cc:1b:4f;CM-QOS=1.1;CM-VER=3.0;

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

The following table describes the labels in this screen.

Table 11: 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.
Clear	Click this to remove all DOCSIS event logs from the system.

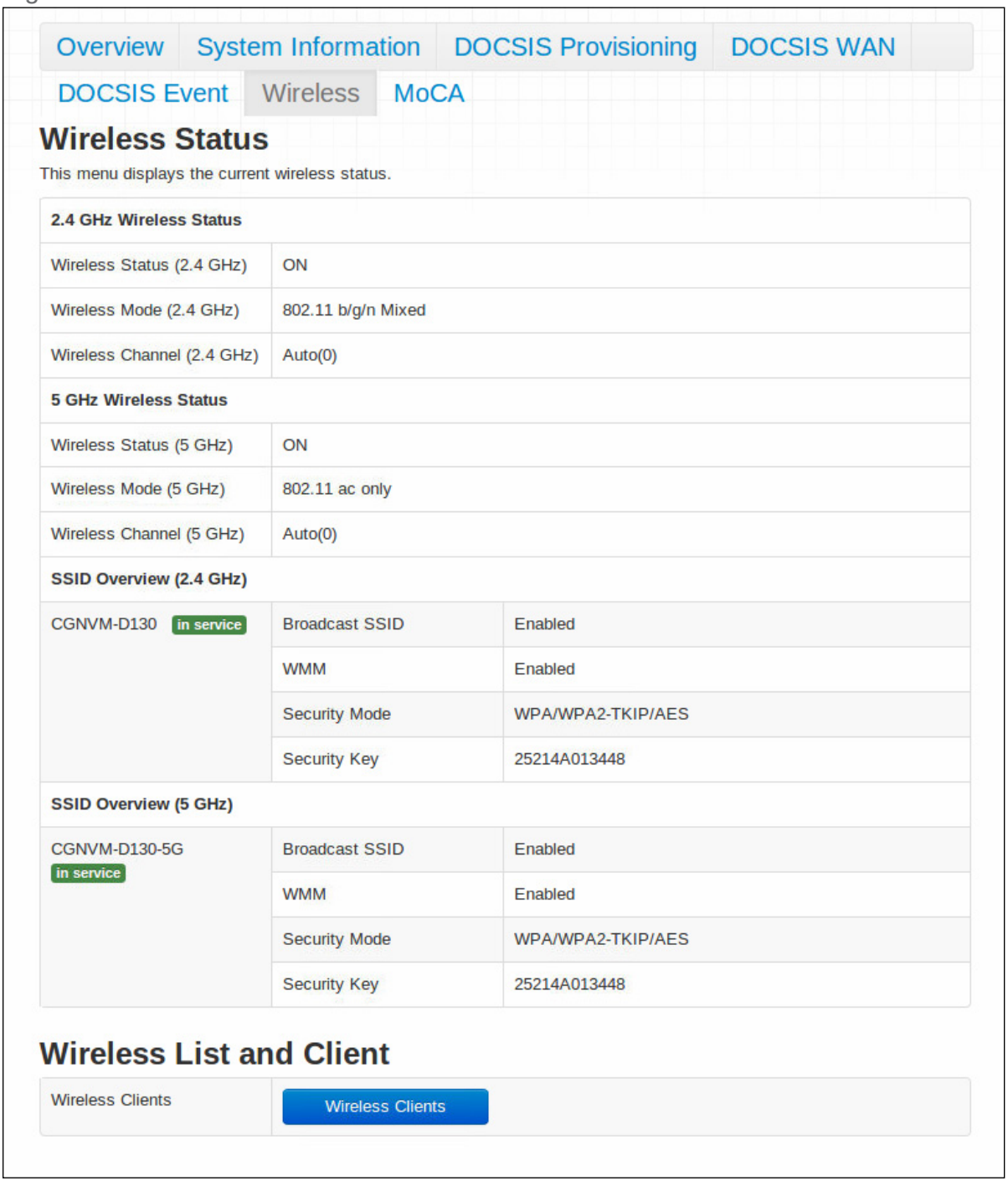
2.7 The Status: Wireless Screen

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

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 17: The Status: Wireless Screen



Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

The following table describes the labels in this screen.

Table 12: The Status: Wireless Screen

2.4G Wireless Status	
Wireless Status (2.4GHz)	This displays whether or not the CGNVM's 2.4GHz wireless network is active.
Wireless Mode (2.4GHz)	This displays the type of wireless network that the CGNVM's 2.4GHz network is using.
Wireless Channel (2.4GHz)	This displays the wireless channel on which the CGNVM's 2.4GHz wireless network is transmitting and receiving.
5G Wireless Status	
Wireless Status (5GHz)	This displays whether or not the CGNVM's 5GHz wireless network is active.
Wireless Mode (5GHz)	This displays the type of wireless network that the CGNVM's 5GHz network is using.
Wireless Channel (5GHz)	This displays the wireless channel on which the CGNVM's 5GHz wireless network is transmitting and receiving.
SSID Overview (2.4GHz)	
(SSID)	This displays the SSID (Service Set IDentifier) of the CGNVM's 2.4GHz wireless network, and whether or not it is currently active.
Broadcast SSID	This displays whether the CGNVM's 2.4GHz wireless network SSID is visible to client devices (**Enabled**) or not (**Disabled**).
WMM	This displays whether Wi-Fi Multimedia is active (**Enabled**) or inactive (**Disabled**) on the CGNVM's 2.4GHz wireless network.
Security Mode	This displays the type of security and encryption method currently enabled on the CGNVM's 2.4GHz wireless network.
Security Key	This displays the wireless security password for the CGNVM's 2.4GHz wireless network.
SSID Overview (5GHz)	
(SSID)	This displays the SSID (Service Set IDentifier) of the CGNVM's 5GHz wireless network, and whether or not it is currently active.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 12: The Status: Wireless Screen (continued)

Broadcast SSID	This displays whether the CGNVM's 5GHz wireless network SSID is visible to client devices (**Enabled**) or not (**Disabled**).
WMM	This displays whether Wi-Fi Multimedia is active (**Enabled**) or inactive (**Disabled**) on the CGNVM's 5GHz wireless network.
Security Mode	This displays the type of security and encryption method currently enabled on the CGNVM's 5GHz wireless network.
Security Key	This displays the wireless security password for the CGNVM's 5GHz wireless network.
Wireless List and Clients	
Wireless Clients	Click this to display a list of the wireless devices currently connected to the CGNVM.

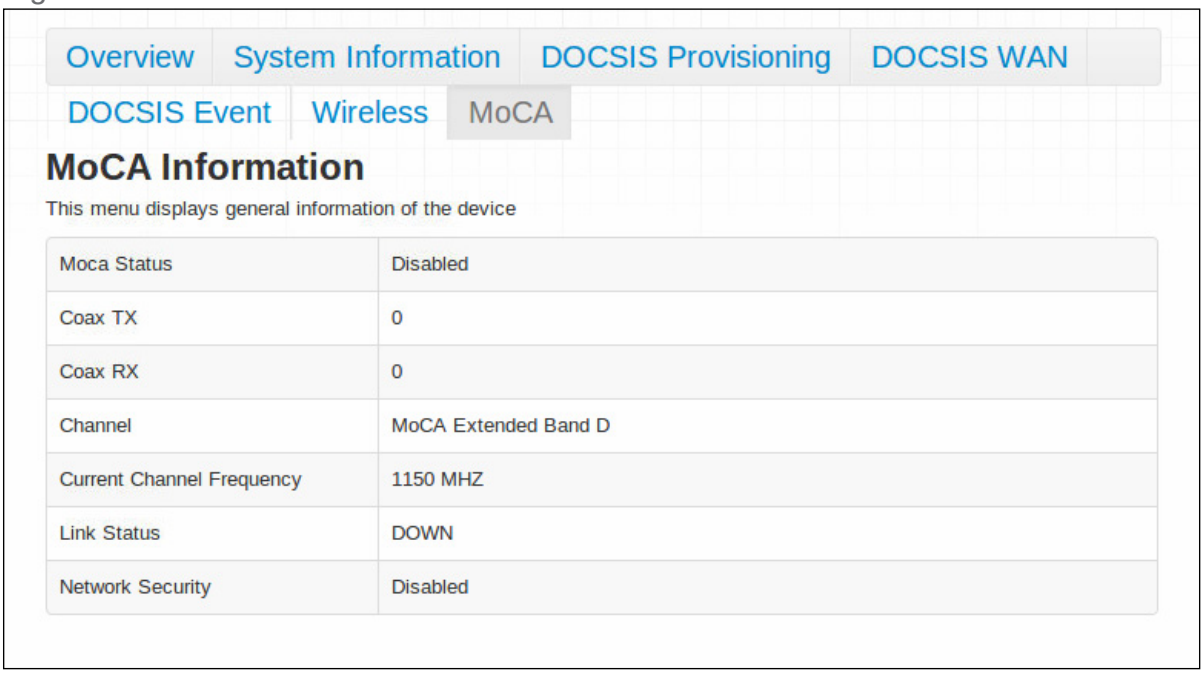
2.8 The Status: MoCA Screen

Use this screen to view general information about the CGNVM's MoCA-related settings.

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 18: The Status: MoCA Screen



The following table describes the labels in this screen.

Table 13: The Status: MoCA Screen

Coax TX	This displays the transmission (TX) power of the CGNVM on the cable network, from **0** (extremely weak) to **10** (extremely strong), or **Disabled**.
Coax RX	This displays the strength of the signal that the CGNVM is receiving (RX) on the cable network, from **0** (extremely weak) to **10** (extremely strong).
Channel	This displays the radio frequency (RF) channel on which the CGNVM is transmitting and receiving over the cable network.
Current Channel Frequency	This displays the frequency in megahertz of the the radio frequency (RF) channel on which the CGNVM is transmitting and receiving over the cable network.
Link Status	This displays whether or not the CGNVM is connected over the cable network.
Network Security	This displays the type of security that the cable network is using (56-bit DES, 128-bit AES or **Disabled**).

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

3

Basic

This chapter describes the screens that display when you click **1** in the toolbar. It contains the following sections:

3.1 Basic Overview

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

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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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

3.2 The Basic: LAN Setup Screen

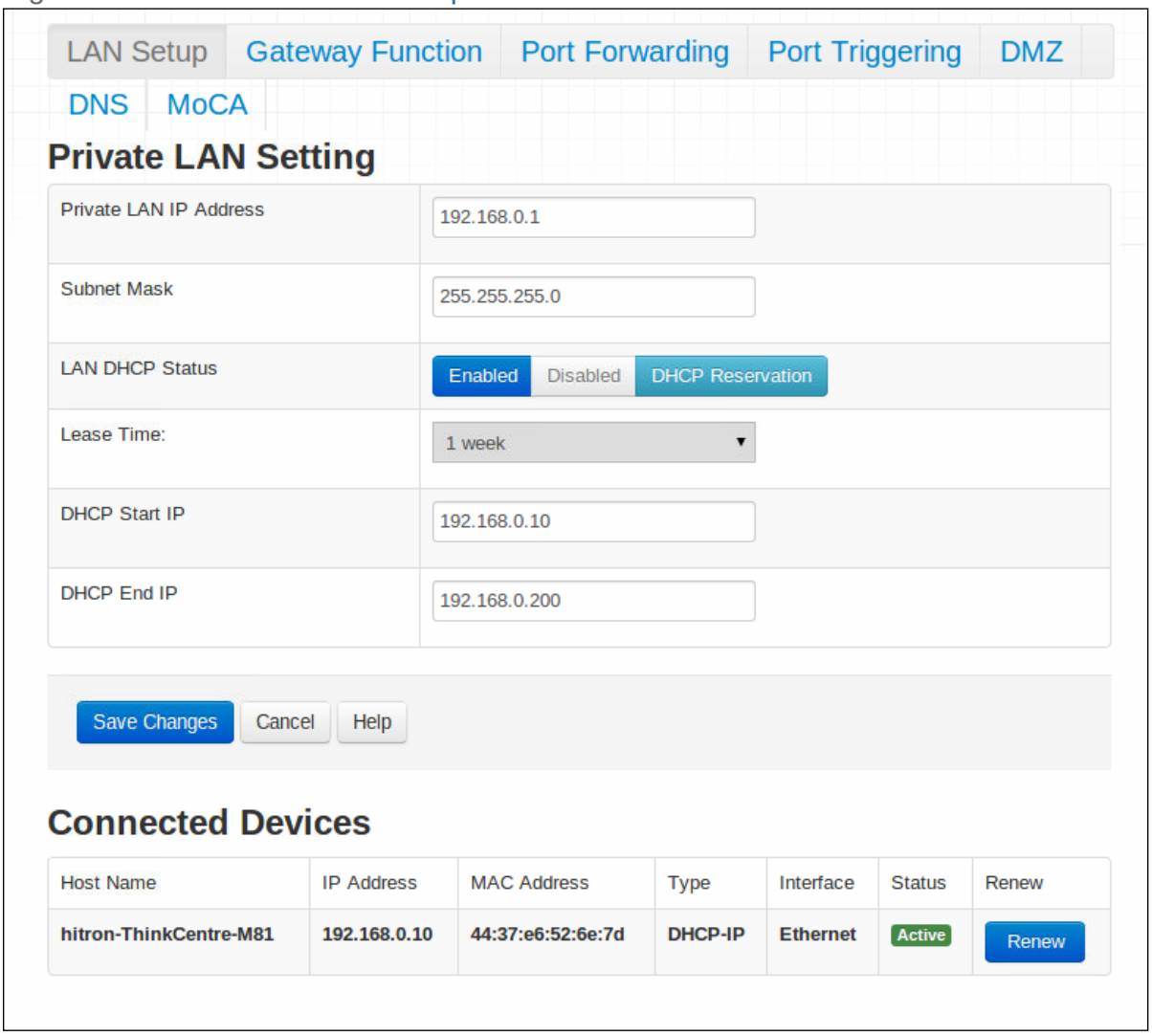
Use this screen to:

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

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 19: The Basic: LAN Setup Screen



The following table describes the labels in this screen.

Table 14: The Basic: LAN Setup Screen

Private LAN Setting	
Private LAN IP Address	Use this field to define the IP address of the CGNVM on the LAN.
Subnet Mask	Use this field to define the LAN subnet. Use dotted decimal notation (for example, **255.255.255.0**).

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 14: The Basic: LAN Setup Screen (continued)

LAN DHCP Status	Use this field to configure whether or not the CGNVM'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.
DHCP Start IP	Use this field to specify the IP address at which the CGNVM 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 CGNVM 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 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.
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**).

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 14: The Basic: LAN Setup Screen (continued)

Status	This displays **Active** when the connected computer is online, and **Inactive** when the connected computer is offline.
Renew	Click this to refresh the information in this section.

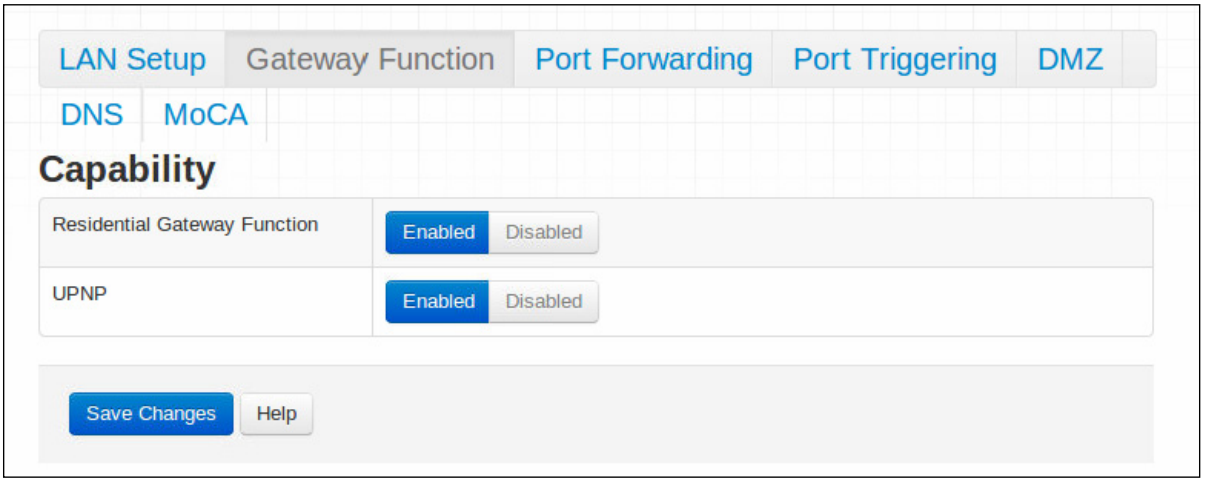
3.3 The Basic: Gateway Function Screen

Use this screen to enable or disable the CGNVM'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 20: The Basic: Gateway Function Screen



The following table describes the labels in this screen.

Table 15: The Basic: Gateway Function Screen

Residential Gateway function	Select **Enabled** to enable the CGNVM's residential gateway features, or select **Disabled** to disable them.
UPnP	Select **Enabled** to enable the CGNVM's Universal Plug n Play features, or select **Disabled** to disable them.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 15: The Basic: Gateway Function Screen (continued)

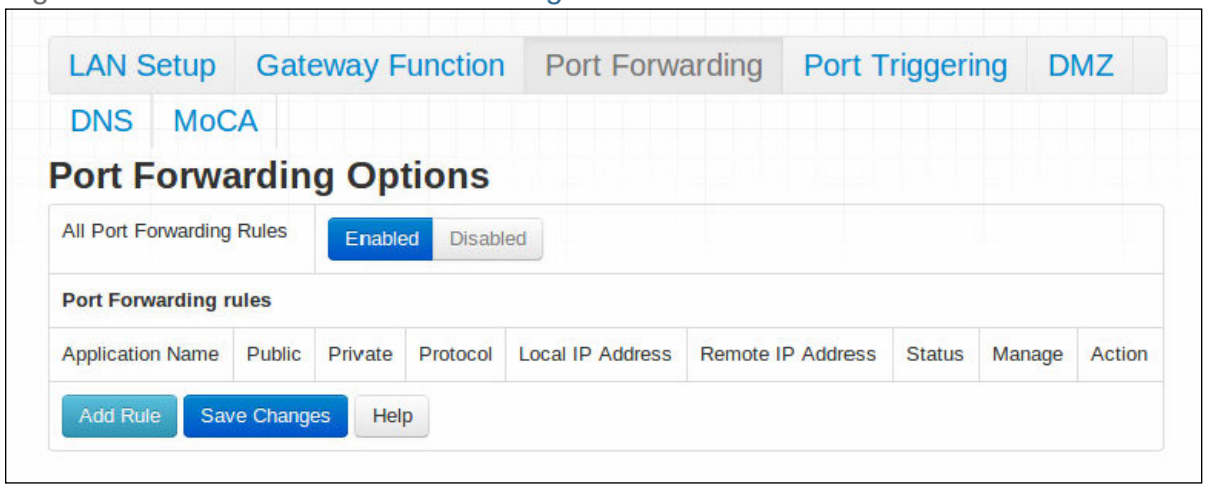
Save Changes	Click this to save your changes to the fields in this screen.
Help	Click this to see information about the fields in this screen.

3.4 The Basic: 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 21: The Basic: Port Forwarding Screen



The following table describes the labels in this screen.

Table 16: 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	
Application Name	This displays the arbitrary name you assigned to the rule when you created it.

Table 16: The Basic: Port Forwarding Screen (continued)

Public Private	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 CGNVM received traffic from the originating host on the WAN. ▸ The **Private** field displays the port range to which the CGNVM forwards traffic to the device on the LAN.
Protocol	This field displays the protocol or protocols to which this rule applies: ▸ Transmission Control Protocol (**TCP**) ▸ User Datagram Protocol (**UDP**) ▸ Transmission Control Protocol and User Datagram Protocol (**TCP/UDP**) ▸ Generic Routing Encapsulation (**GRE**) ▸ Encapsulating Security Protocol (**ESP**)
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.
Remote IP Address	This displays the IP address of the computer on the WAN from which traffic conforming to the **Public Port Range** and **Protocol** conditions is forwarded to the **Local IP Address**.
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.
Manage	Click this to make changes to the rule.
Action	Use this to delete the rule.
Add Rule	Click this to define a new port forwarding rule. See Adding or Editing a Port Forwarding Rule on page 62 for information on the screen that displays.
Save Changes	Click this to save your changes to the fields in this screen.
Help	Click this to see information about the fields in this screen.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

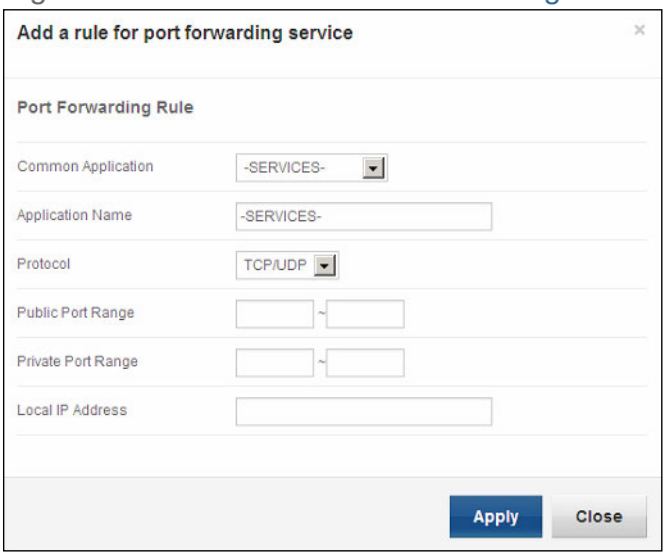
3.4.1 Adding or Editing a Port Forwarding Rule

- 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 22: The Basic: Port Forwarding Add/Edit Screen



The following table describes the labels in this screen.

Table 17: 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.

Table 17: The Basic: Port Forwarding Add/Edit Screen

Protocol	Use this field to specify whether the CGNVM 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**).
Public Port Range	Use these fields to specify the incoming port range. These are the ports on which the CGNVM 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 CGNVM 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.
Remote IP Address	Use this field to enter the IP address of the computer on the WAN from 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.

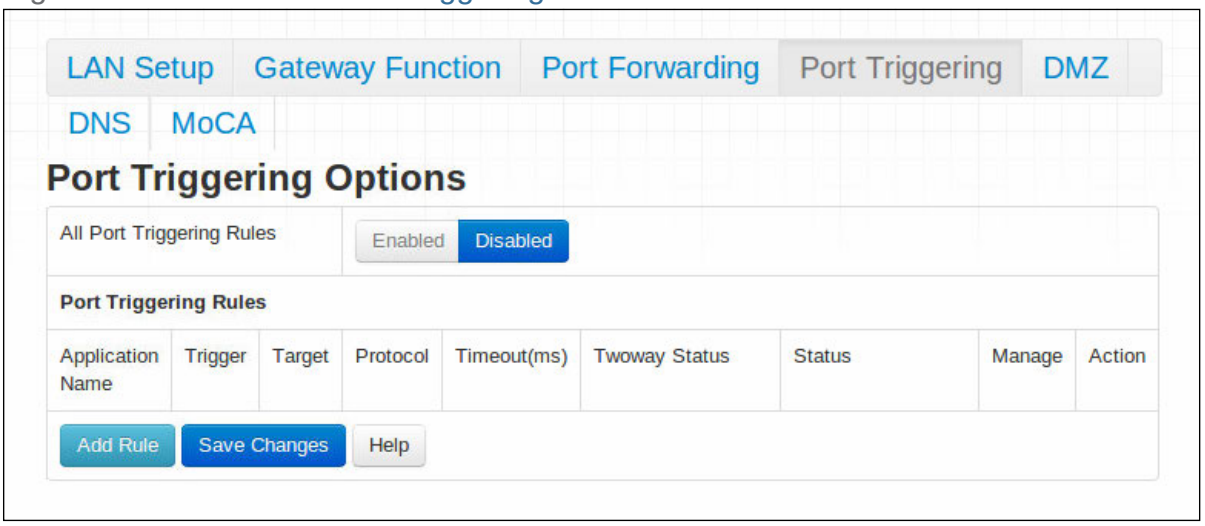
Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

3.5 The Basic: 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 23: The Basic: Port Triggering Screen



The following table describes the labels in this screen.

Table 18: 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	
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 CGNVM 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 CGNVM detects activity on the **Trigger** ports from computers on the LAN.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 18: The Basic: Port Triggering Screen (continued)

Protocol	This displays the protocol of the port triggering rule (**TCP**, **UDP** or **Both**).
Timeout (ms)	This displays the time (in milliseconds) after the CGNVM 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**.
Manage	Click this to make changes to the rule.
Action	Use this to delete the rule.
Add Rule	Click this to define a new port forwarding rule. See Adding or Editing a Port Forwarding Rule on page 62 for information on the screen that displays.
Save Changes	Click this to save your changes to the fields in this screen.
Help	Click this to see information about the fields in this screen.

3.5.1 Adding or Editing a Port Triggering Rule

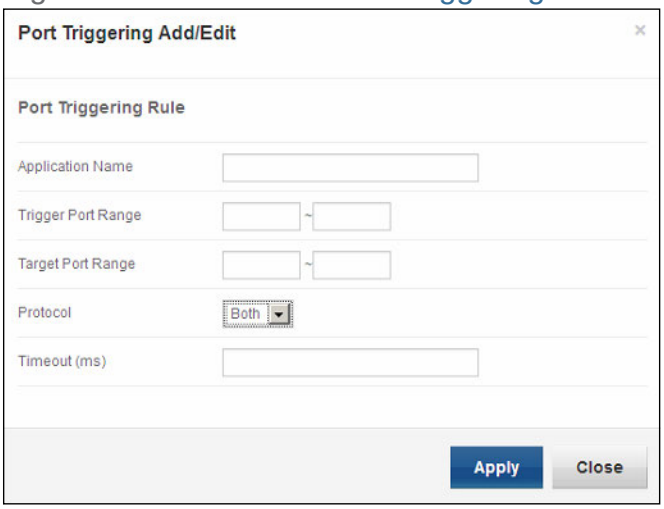
- To add a new port triggering rule, click **Add** in the **Basic** > **Port Triggering** screen.
- To edit an existing port triggering rule, select the rule's radio button in the **Basic** > **Port Triggering** screen and click the **Edit** button.

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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 24: The Basic: Port Triggering Add/Edit Screen



The following table describes the labels in this screen.

Table 19: 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 CGNVM 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 CGNVM 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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 19: The Basic: Port Triggering Add/Edit Screen

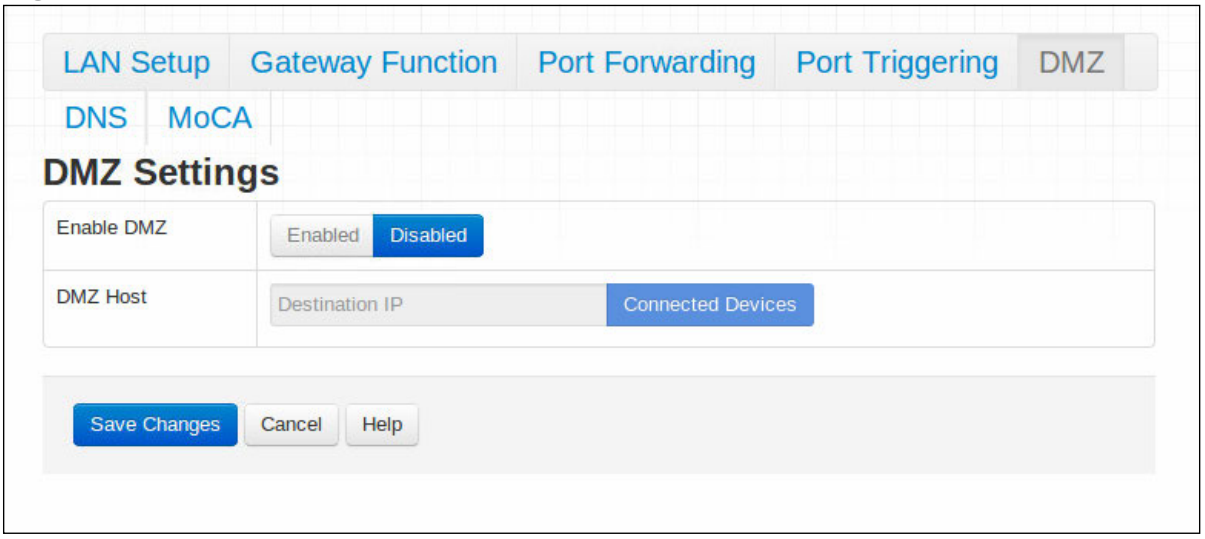
Protocol	Use this field to specify whether the CGNVM should activate this trigger when it detects activity via: ▸ Transmission Control Protocol (**TCP**) ▸ User Datagram Protocol (**UDP**) ▸ Transmission Control Protocol and User Datagram Protocol (**Both**) NOTE: If in doubt, leave this field at its default (**Both**).
Timeout (ms)	Enter the time (in milliseconds) after the CGNVM 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 Basic: DMZ Screen

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

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

Figure 25: The Basic: DMZ Screen



Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

The following table describes the labels in this screen.

Table 20: 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 CGNVM 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.

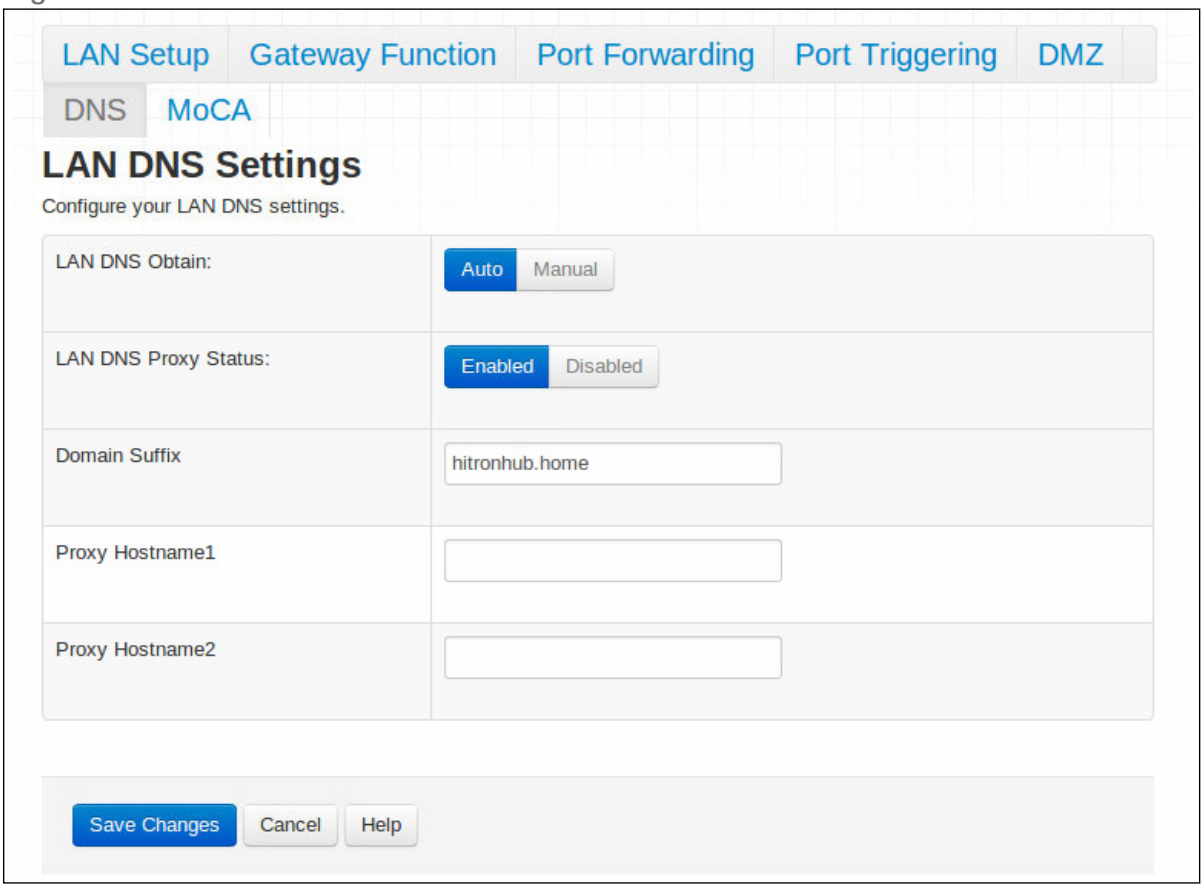
3.7 The Basic: DNS Screen

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

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 26: The Basic: DNS Screen



The following table describes the labels in this screen.

Table 21: 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 CGNVM'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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 21: The Basic: DNS Screen (continued)

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 CGNVM 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 CGNVM's GUI without knowledge of its IP address.
Proxy Hostname 1	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.
Proxy Hostname 2	
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.

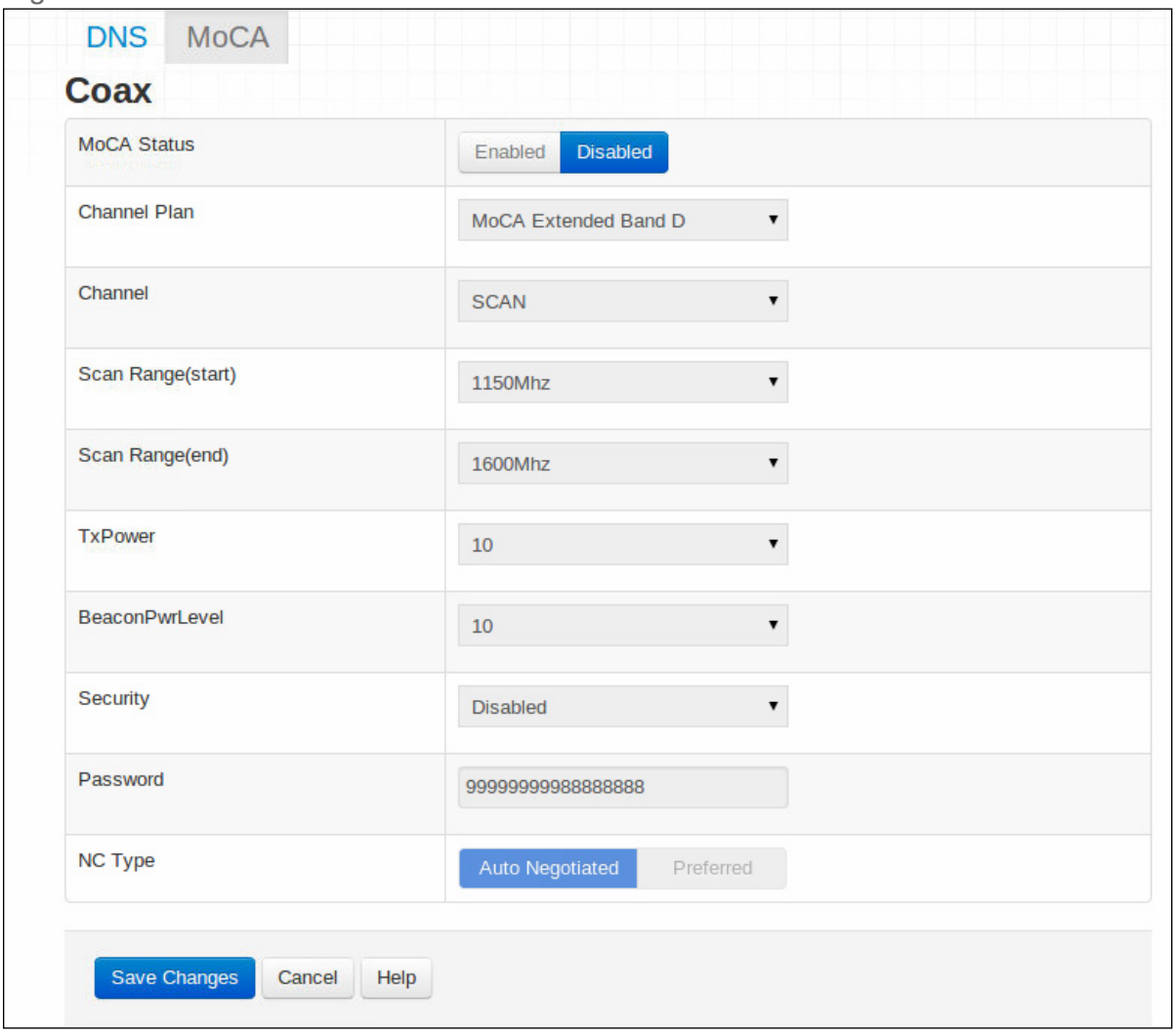
3.8 The Basic: MoCA Screen

Use this screen to

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

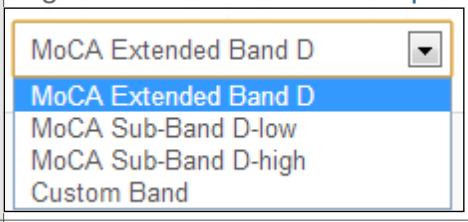
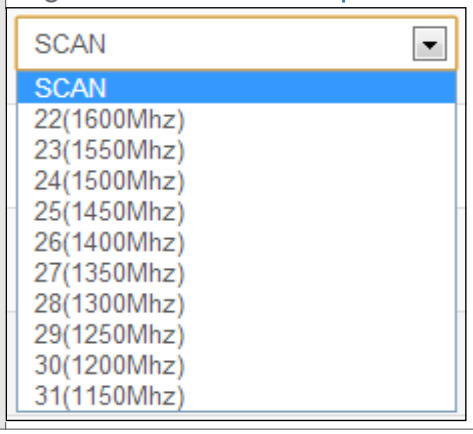
Figure 27: The Basic: MoCA Screen



Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

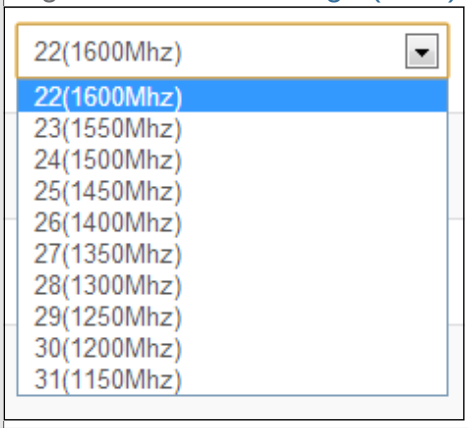
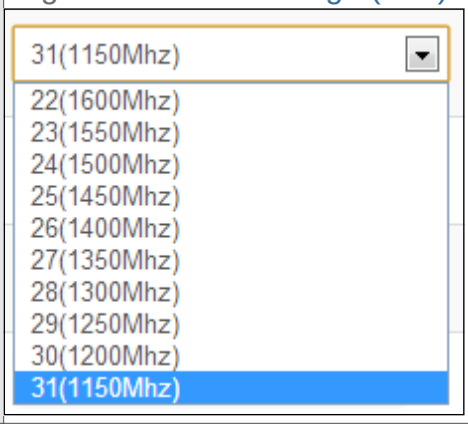
The following table describes the labels in this screen.

Table 22: The Basic: MoCA Screen

MoCA Status	▸ Select **Enabled** to turn the MoCA network off. ▸ Select **Disabled** to turn the MoCA network connection off.
Channel Plan	The MoCA specification defines several channel plans for communication on the cable network (see The Multimedia over Coax Alliance on page 36). This field allows you to select the channel plan that you want the CGNVM to use. Select the channel plan that you wish to use from the dropdown list. Figure 28: Channel Plan Options 
Channel	Use this field to define the channel on which you want the CGNVM to communicate on the cable network, dependent on the **Channel Plan** that you selected. Select the channel plan that you wish to use from the dropdown list. If you select SCAN, ensure that you also configure the **Scan Range (Start)** and **Scan Range (End)** fields. Figure 29: Channel Options 

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 22: The Basic: MoCA Screen (continued)

Scan Range (Start)	If you selected **SCAN** in the **Channel** field, use this field to select a channel at which the CGNVM should start scanning for a connection on the cable network. Figure 30: Scan Range (Start) 
Scan Range (End)	If you selected **SCAN** in the **Channel** field, use this field to select a channel at which the CGNVM should stop scanning for a connection on the cable network. Figure 31: Scan Range (End) 
TxPower	Use this field to set the power at which the CGNVM transmits (TX) over the cable network, from **0** to **10**.
Beacon Pwr Level	Use this field to set the CGNVM's beacon power on the cable network, from **0** to **10**. The MoCA beacon allows other devices on the cable network to detect the CGNVM.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 22: The Basic: MoCA Screen (continued)

NC Type	Each MoCA network has a Network Coordinator (NC) which acts as a manager for all the other devices on the cable network. ▸ By default, the NC is chosen from the pool of MoCA devices based on its suitability (signal strength, etc.) To base NC status on merit, or if you have specified another device as "preferred" and do not want the CGNVM to compete with it, select **Auto-negotiated**. ▸ When one device is set to be the "preferred" NC, it will be the NC whenever it is available on the network (if multiple devices are "preferred", the most suitable one will be chosen). Select **Preferred** to add the CGNVM to the preferred group.
Security	▸ Select **Enabled** to turn MoCA security on. Only MoCA devices configured to use the **Password** you define can access the network. ▸ Select **Disabled** to turn MoCA security off. Any MoCA device can access the network.
Password	When MoCA **Security** is **Enabled**, enter the password you want to use on the MoCA in this field. Only MoCA devices configured to use this password can access the network.
Save Changes	Click this to save your changes to the fields in this screen.
Help	Click this to see information about the fields in this screen.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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 CGNVM'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 CGNVM 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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

The CGNVM is the access point, and the computers you connect to the CGNVM 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 CGNVM supports the following (in order of adoption - old to new - and data transfer speeds - low to high):

- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n
- IEEE 802.11ac

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 CGNVM 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).

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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 CGNVM 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. Additionally, use of WEP limits the wireless network speed to a speed of 54MBps (802.11g speed).
- **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 CGNVM) 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.

NOTE: The CGNVM can be configured to use the TKIP encryption standard; however, this limits the wireless network speed to 54Mbps (802.11g speed).

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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 CGNVM 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 CGNVM's 2.4GHz, 5GHz, Wifi Protected Setup (WPS) and guest network wireless settings.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

- Use the 2.4GHz network screen to enable 2.4GHz wireless clients to connect to the CGNVM. See The Wireless: Basic Settings: 2.4G Screen on page 79.
- Use the 5GHz network screen to enable 5GHz wireless clients to connect to the CGNVM. See The Wireless: Basic Settings: 5G Screen on page 84.
- Use the WPS screen to enable WPS-capable wireless clients to connect to the CGNVM via a simple push-button, or by entering a password. See The Wireless: Basic Settings: WPS Screen on page 88.
- Use the Guest Network screen to enable wireless clients to connect to the CGNVM with reduced privileges. See The Wireless: Basic Settings: Guest Screen on page 90.

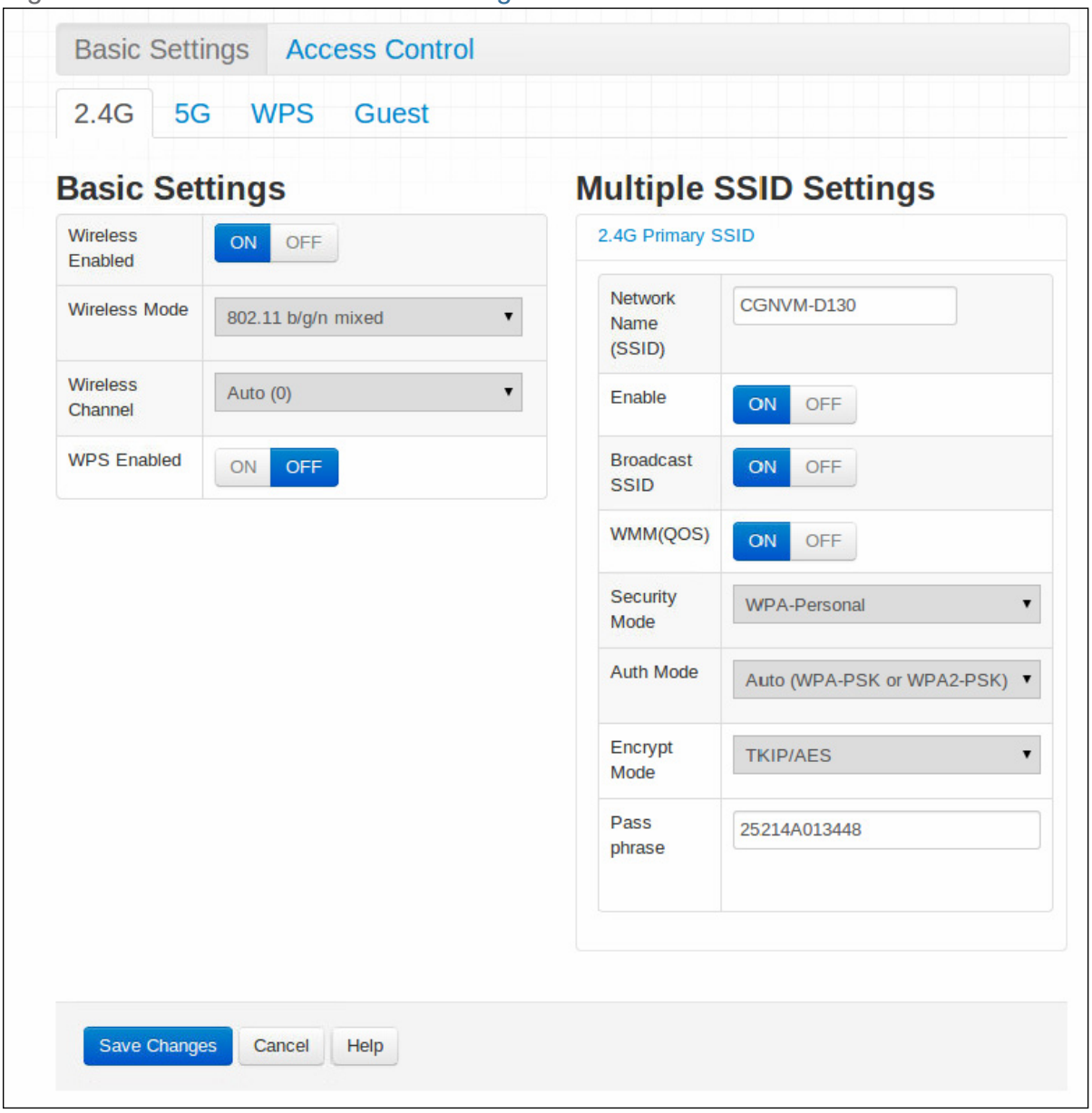
4.2.1 The Wireless: Basic Settings: 2.4G Screen

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

Click **Wireless** > **Basic Settings** > **2.4G**. The following screen displays.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 32: The Wireless: Basic Settings: 2.4G Screen



The following table describes the labels in this screen.

Table 23: The Wireless: Basic Settings: 2.4G Screen

Basic Settings	
Wireless Enabled	▸ Select **On** to enable the 2.4GHz wireless network. ▸ Select **Off** to disable the 2.4GHz wireless network.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 23: The Wireless: Basic Settings: 2.4G Screen (continued)

Wireless Mode	Select the mode 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).
Wireless Channel	Select the 2.4GHz wireless channel that you want to use, or select **Auto** to have the CGNVM select the optimum channel to use. NOTE: Use the **Auto** setting unless you have a specific reason to do otherwise.
WPS Enabled	Use this field to turn Wifi Protected Setup (WPS) on or off on the 2.4GHz network. ▸ Select **ON** to enable WPS. ▸ Select **OFF** to disable WPS.
Multiple 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. ▸ Select **OFF** to disable the SSID.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 23: The Wireless: Basic Settings: 2.4G Screen (continued)

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 CGNVM 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.
Security Mode	Select the mode of security that you want to use on the 2.4GHz network. ▸ 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. Additionally, use of **WEP** limits the wireless network speed to 54Mbps (802.11g speed).

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 23: The Wireless: Basic Settings: 2.4G Screen (continued)

Auth Mode	Select the mode 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 mode of encryption you want to use on the 2.4GHz network. 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 CGNVM. NOTE: Use of the TKIP encryption standard limits the wireless network speed to 54Mbps (802.11g speed).
Passphrase	Enter the security key or password that you want to use for the 2.4GHz 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.

Table 23: The Wireless: Basic Settings: 2.4G Screen (continued)

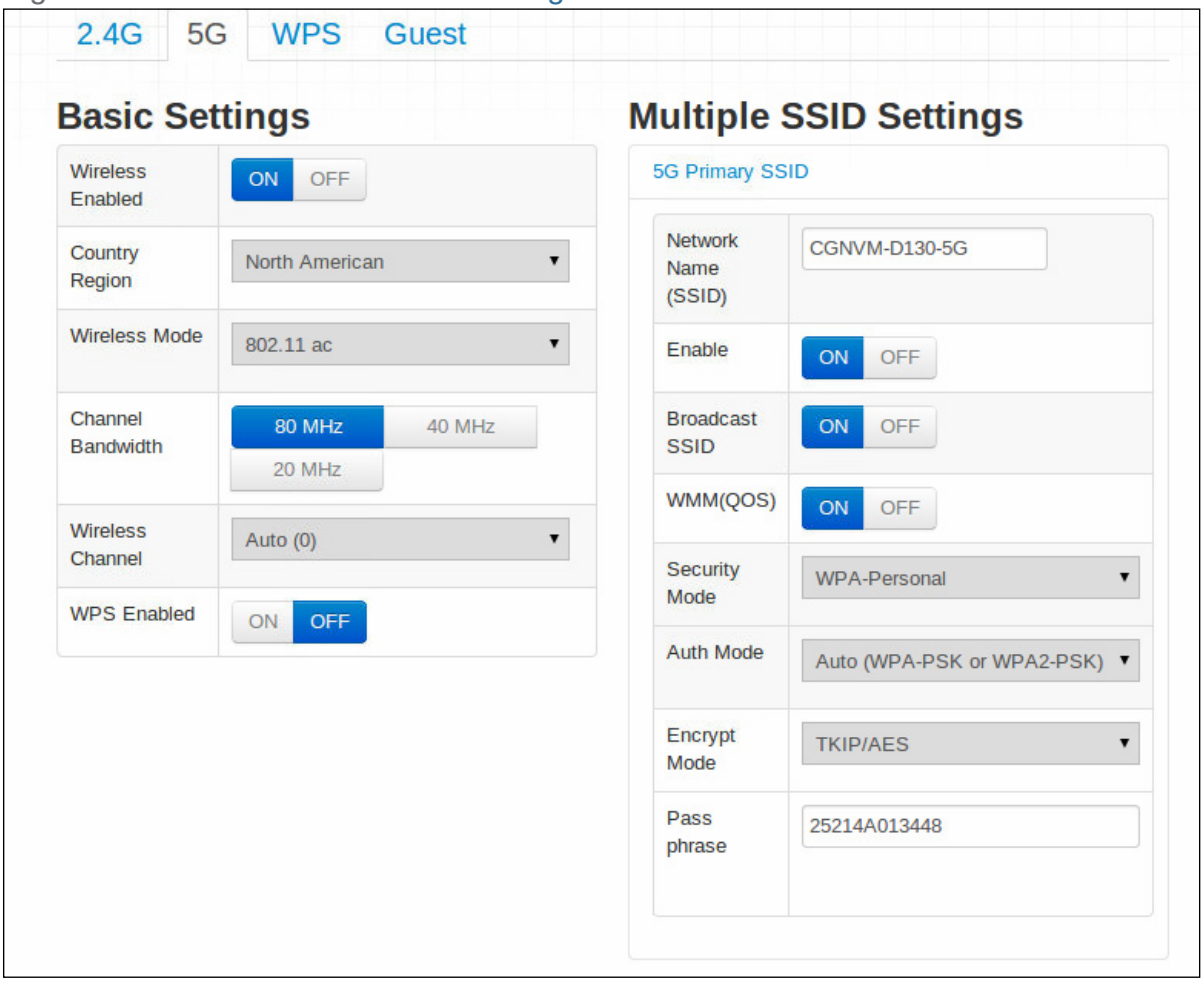
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.2.2 The Wireless: Basic Settings: 5G Screen

Use the 5GHz network screen to enable 5GHz wireless clients to connect to the CGNVM.

Click **Wireless** > **Basic Settings** > **5G**. The following screen displays.

Figure 33: The Wireless: Basic Settings: 5G Screen



The following table describes the labels in this screen.

Table 24: The Wireless: Basic Settings: 5G Screen

Basic Settings	
Wireless Enabled	▸ Select **On** to enable the 5GHz wireless network. ▸ Select **Off** to disable the 5GHz wireless network.
Country Region	Select your region. 5GHz networking regulations differ from one country to another.
Wireless Mode	Select the mode of 5GHz wireless network that you want to use: ▸ **802.11a**: use IEEE 802.11a. ▸ **802.11n Only**: use IEEE 802.11n. ▸ **802.11a/n Mixed**: allow clients using both IEEE 802.11a and IEEE 802.11n to access the network. ▸ **802.11ac**: use IEEE 802.11ac. ▸ **802.11n/ac Mixed** (default): allow clients using both IEEE 802.11n and IEEE 802.11ac to access the network. NOTE: Only wireless clients that support the network protocol you select can connect to the wireless network. If in doubt, use **802.11n/ac Mixed** (default).
Wireless Channel	Select the 5GHz wireless channel that you want to use, or select **Auto** to have the CGNVM select the optimum channel to use. NOTE: Use the **Auto** setting unless you have a specific reason to do otherwise.
WPS Enabled	Use this field to turn Wifi Protected Setup (WPS) on or off on the 5GHz network. ▸ Select **ON** to enable WPS. ▸ Select **OFF** to disable WPS.
Multiple SSID Settings	
(SSID)	Your CGNVM has multiple SSIDs. Click the SSID you wish to configure to see its security fields.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 24: The Wireless: Basic Settings: 5G Screen (continued)

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. ▸ Select **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 CGNVM 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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 24: The Wireless: Basic Settings: 5G Screen (continued)

Security Mode	Select the mode of security that you want to use on the 5GHz network. ▸ 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. Additionally, use of **WEP** limits the wireless network speed to 54Mbps (802.11a speed).
Auth Mode	Select the mode 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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 24: The Wireless: Basic Settings: 5G Screen (continued)

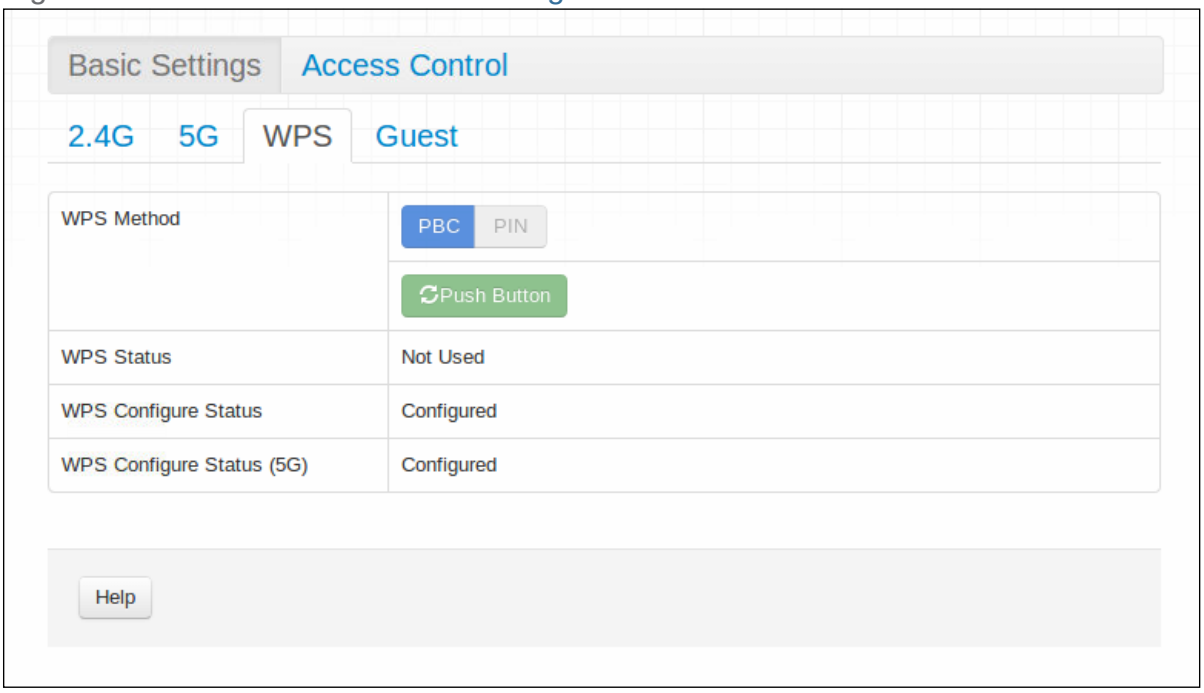
Encrypt Mode	Select the mode of encryption you want to use on the 5GHz network. The options that display depend on the options you selected in the other fields in this screen. **WEP**: ▸ Select **WEP64** to use a ten-digit security key. ▸ Select **WEP128** to use a twenty-six-digit security key. **WPA-PSK**, **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 CGNVM. NOTE: Use of the TKIP encryption standard limits the wireless network speed to 54Mbps (802.11a speed).
Passphrase	Enter the security key or password that you want to use for the 5GHz 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.

4.2.3 The Wireless: Basic Settings: WPS Screen

Use the WPS screen to enable WPS-capable wireless clients to connect to the CGNVM via a simple push-button, or by entering a password. See The Wireless: Basic Settings: WPS Screen on page 88.

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

Figure 34: The Wireless: Basic Settings: WPS Screen



The following table describes the labels in this screen.

Table 25: The Wireless: Basic Settings: WPS Screen

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 CGNVM, or the WPS PIN of the client device you want to add to the network.
WPS Status	This displays whether or not the CGNVM is using Wifi Protected Setup.
WPS Configure Status	This displays the Wifi Protected Setup configuration.
Help	Click this to see information about the fields in this screen.

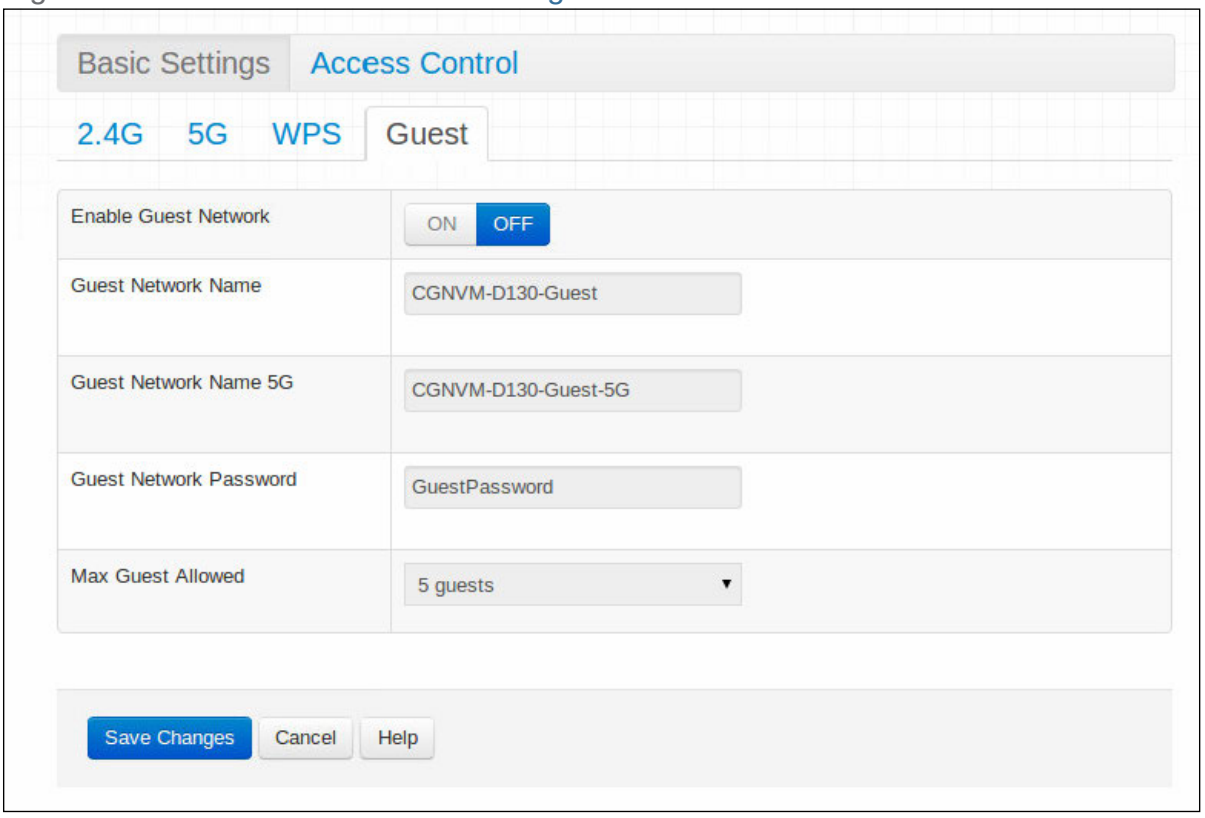
Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

4.2.4 The Wireless: Basic Settings: Guest Screen

Use the Guest Network screen to enable wireless clients to connect to the CGNVM with reduced privileges. See The Wireless: Basic Settings: Guest Screen on page 90.

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

Figure 35: The Wireless: Basic Settings: Guest Screen



The following table describes the labels in this screen.

Table 26: The Wireless: Basic Settings: Guest Screen

Enable Guest Network	Use this field to enable or disable the guest network. ▸ Select **ON** to enable the guest network. ▸ Select **OFF** to disable the guest network.
Guest Network Name	Enter the SSID to use on the 2.4GHz wireless guest network.
Guest Network Name 5G	Enter the SSID to use on the 5GHz wireless guest network.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 26: The Wireless: Basic Settings: Guest Screen (continued)

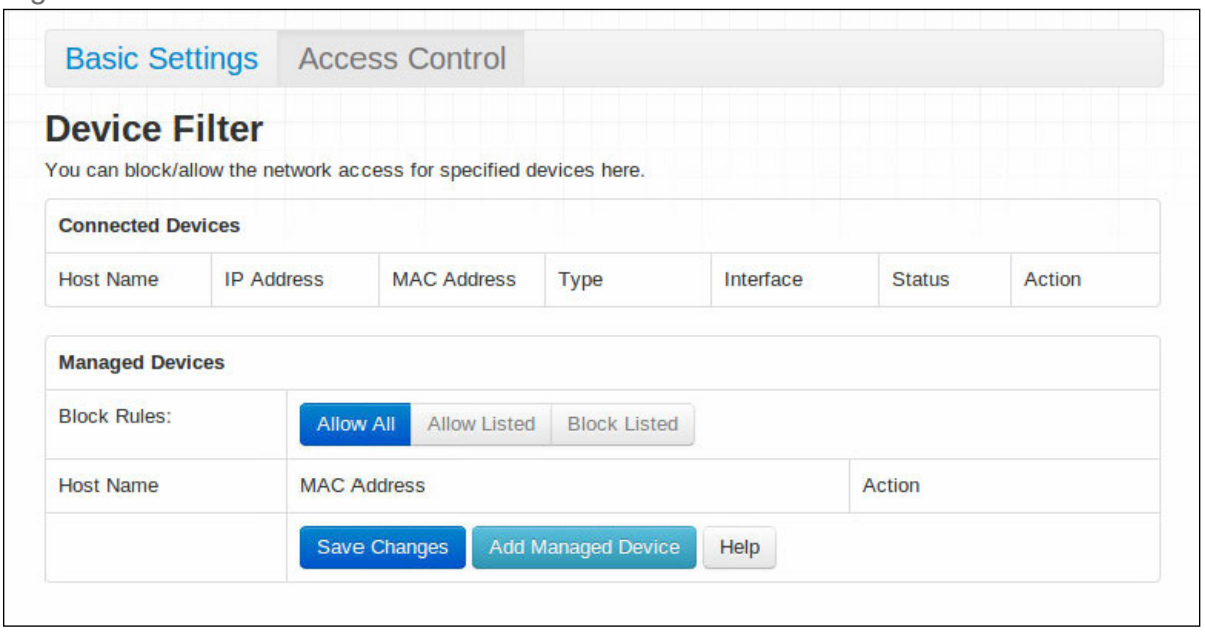
Guest Network Password	Enter the password that wireless clients must be configured to use to connect to either the 2.4GHz or the 5GHz wireless guest network.
Max Guest Allowed	Select the maximum number of wireless clients that may concurrently connect to the wireless guest network.
Save Changes	Click 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.

4.3 The Wireless: Access Control Screen

Use this screen to modify the CGNVM's wireless networks' Service Set Identifiers (SSIDs) and manage the devices that connect to the wireless network.

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

Figure 36: The Wireless: Access Control Screen



Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

The following table describes the labels in this screen.

Table 27: The Wireless: Access Control Screen

Connected Devices	
Host Name	This displays the name of each network device connected on the wireless network.
IP Address	This displays the IP address of each network device connected on the wireless network.
MAC Address	This displays the Media Access Control (MAC) address of each network device connected on the wireless network.
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 113 for information on the screen that displays.
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 CGNVM. ▸ Select **Allow Listed** to permit only devices you added to the **Managed Devices** list to access the CGNVM 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 CGNVM 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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 27: The Wireless: Access Control Screen (continued)

Action	Click **Manage** to make changes to a managed device rule (see Adding or Editing a Managed Device on page 113).
Add Managed Device	Click this to add a new managed device rule (see Adding or Editing a Managed Device on page 113).
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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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 CGNVM 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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

- Traceroute: this tool allows you to see the route taken by data packets to get from the CGNVM 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.

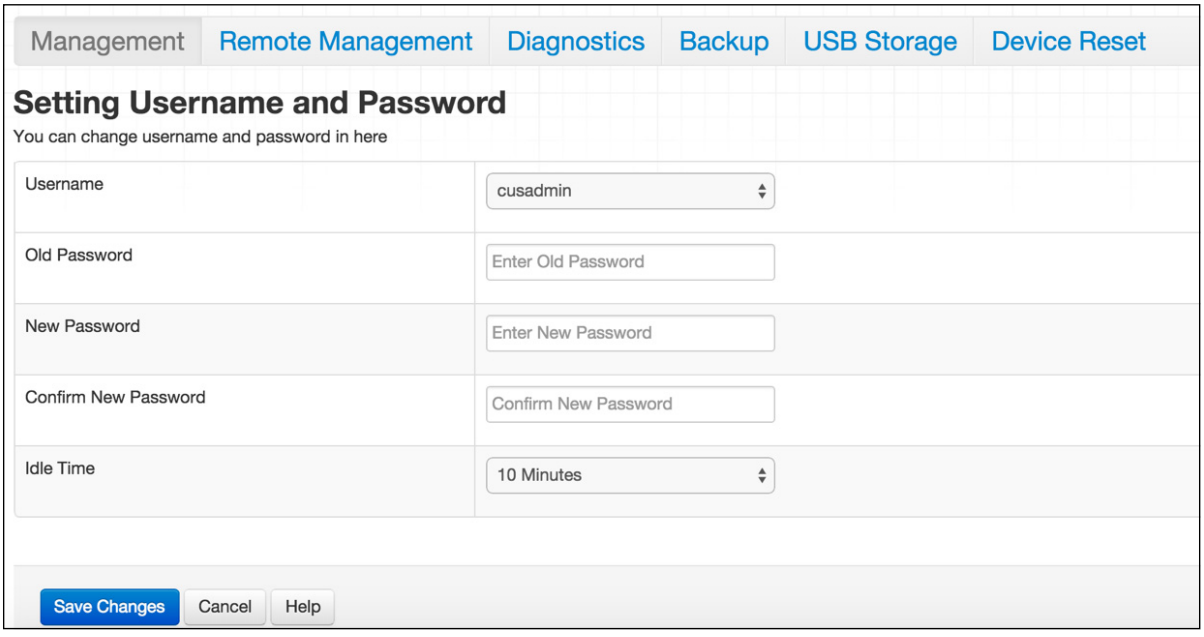
5.2 The Admin: Management Screen

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

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

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

Figure 37: The Admin: Management Screen



The following table describes the labels in this screen.

Table 28: The Admin: Management Screen

Username	If your CGNVM 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 CGNVM for this account.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 28: The Admin: Management Screen (continued)

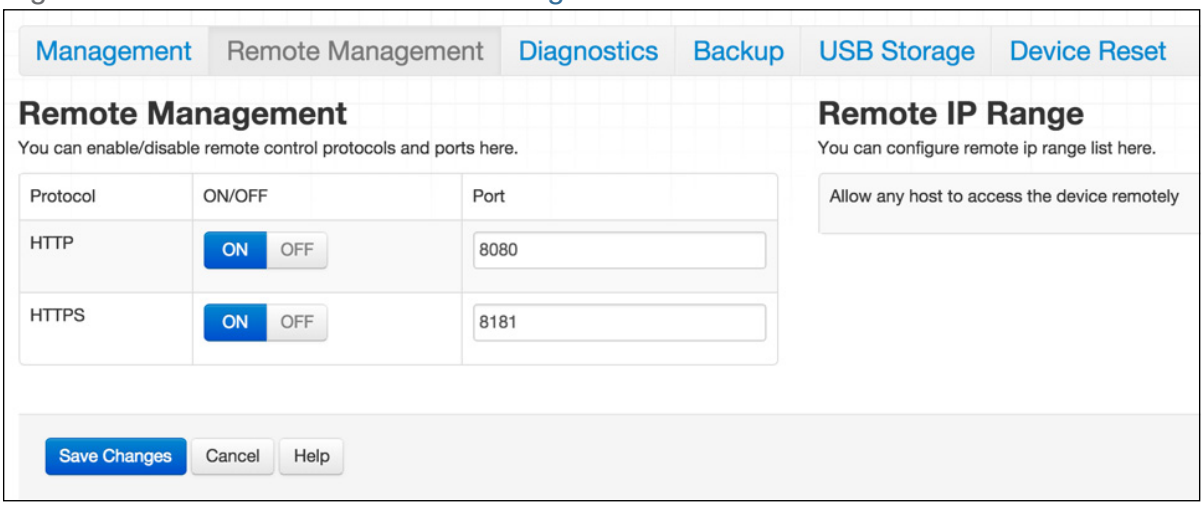
New Password	Enter and re-enter the password you want to use to log into the CGNVM for this account.
Confirm New Password	
Idle Time	Select the time interval after which an inactive user should be logged out of the CGNVM's admin interface.
Save Changes	Click this to save your changes to the fields in 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 Admin: Remote Management Screen

Use this screen to configure remote management of the CGNVM via HTTP and/or HTTPS.

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

Figure 38: The Admin: Remote Management Screen



Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

The following table describes the labels in this screen.

Table 29: The Admin: Remote Management Screen

Protocol	Use the relevant row to permit or forbid remote management via the relevant protocol.
ON/OFF	▸ Select **On** to permit remote management via the ▸ Select **Off** to forbid remote management via the relevant protocol.
Remote IP Range	▸ Select **Enabled** to permit remote management, for all protocols, from computers with IP addresses in the range specified. ▸ Select **Disabled** to allow computers with any IP address to manage the CGNVM remotely.
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.

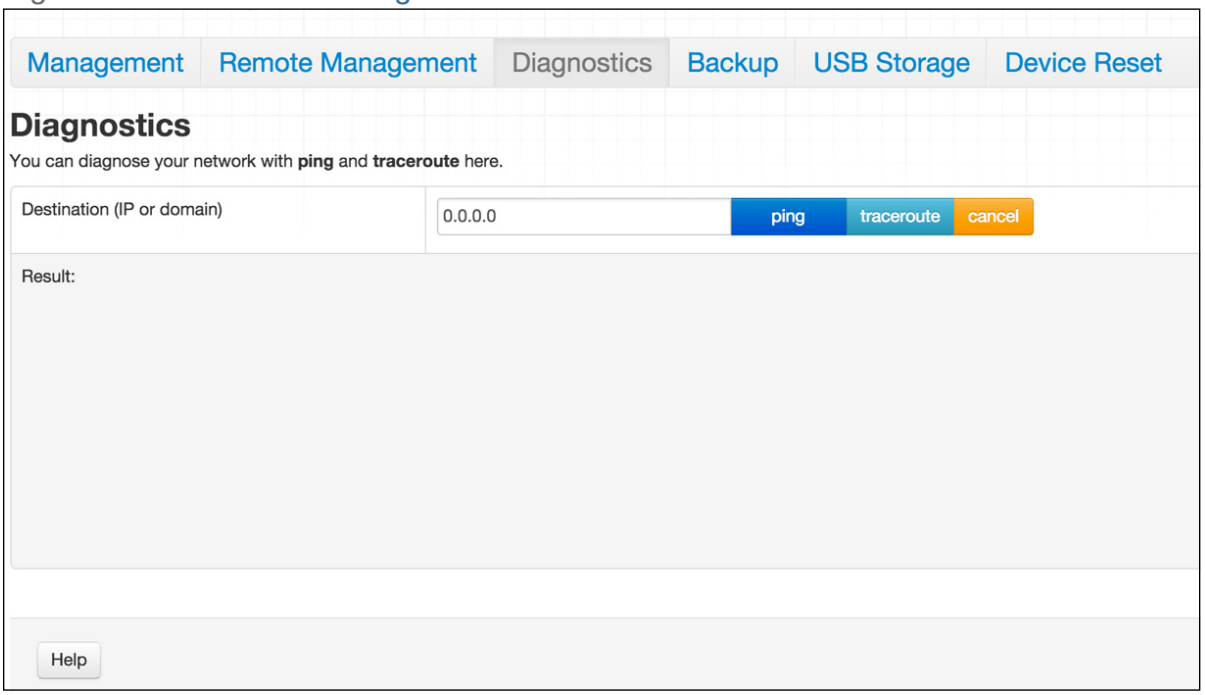
5.4 The Admin: Diagnostics Screen

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

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 39: The Admin: Diagnostics Screen



The following table describes the labels in this screen.

Table 30: 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.

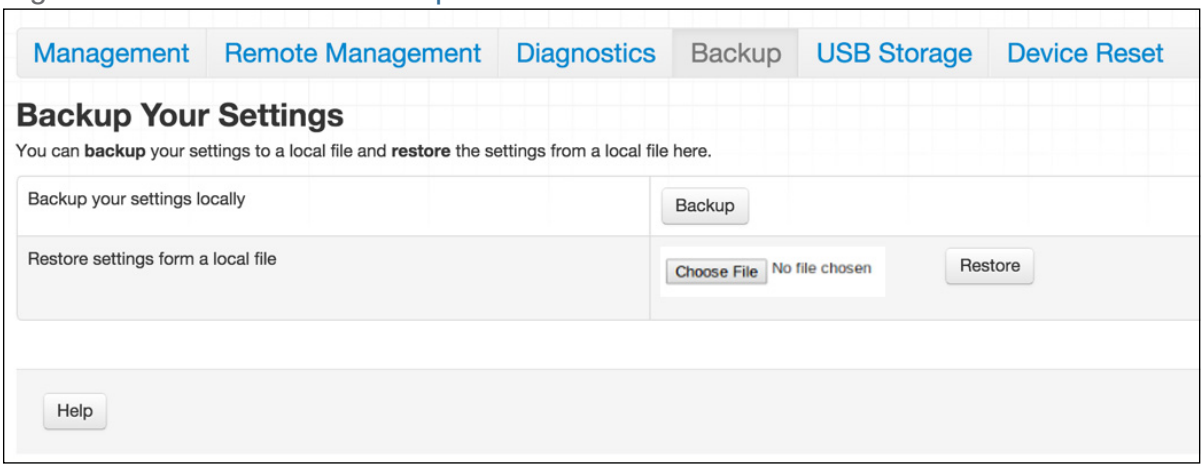
5.5 The Admin: Backup Screen

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

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 40: The Admin: Backup Screen



The following table describes the labels in this screen.

Table 31: The Admin: Backup Screen

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

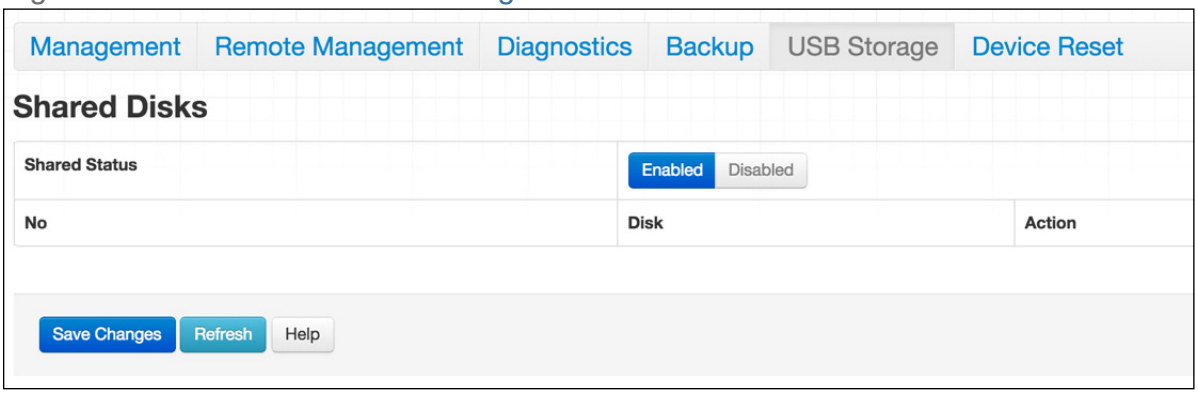
5.6 The USB Storage Screen

Use this screen to configure your CGNVM's USB settings.

Click **Admin** >**USB Storage**. The following screen displays.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 41: The Admin: USB Storage Screen



The following table describes the labels in this screen.

Table 32: The Admin: USB Storage Screen

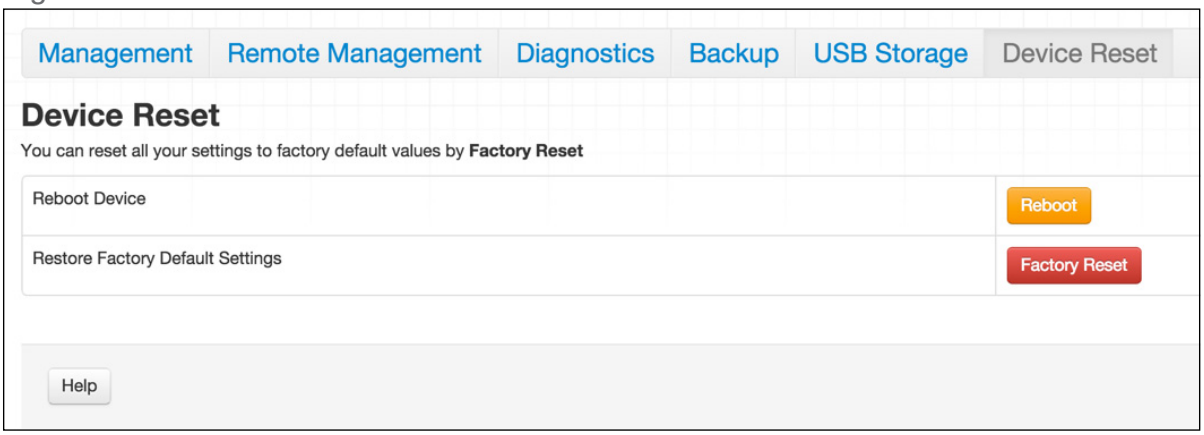
Shared Status	Use this field to select whether the shared status of USB be active or not. ▸ Select **Enabled** to activate the shared status. ▸ Select **Disabled** to deactivate the shared status.
No	This displays the arbitrary identification number assigned to the shared disk.
Disk	This displays the network path of the shared disk.
Action	Click **Eject** to remove the shared disk.
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.

5.7 The Admin: Device Reset Screen

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

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

Figure 42: The Admin: Device Reset Screen



The following table describes the labels in this screen.

Table 33: The Admin: Device Reset Screen

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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 CGNVM'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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

6.1.2 Intrusion detection system

An intrusion detection system monitors network activity, looking for policy violations, and malicious or suspicious activity. The CGNVM'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 CGNVM'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 CGNVM 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.

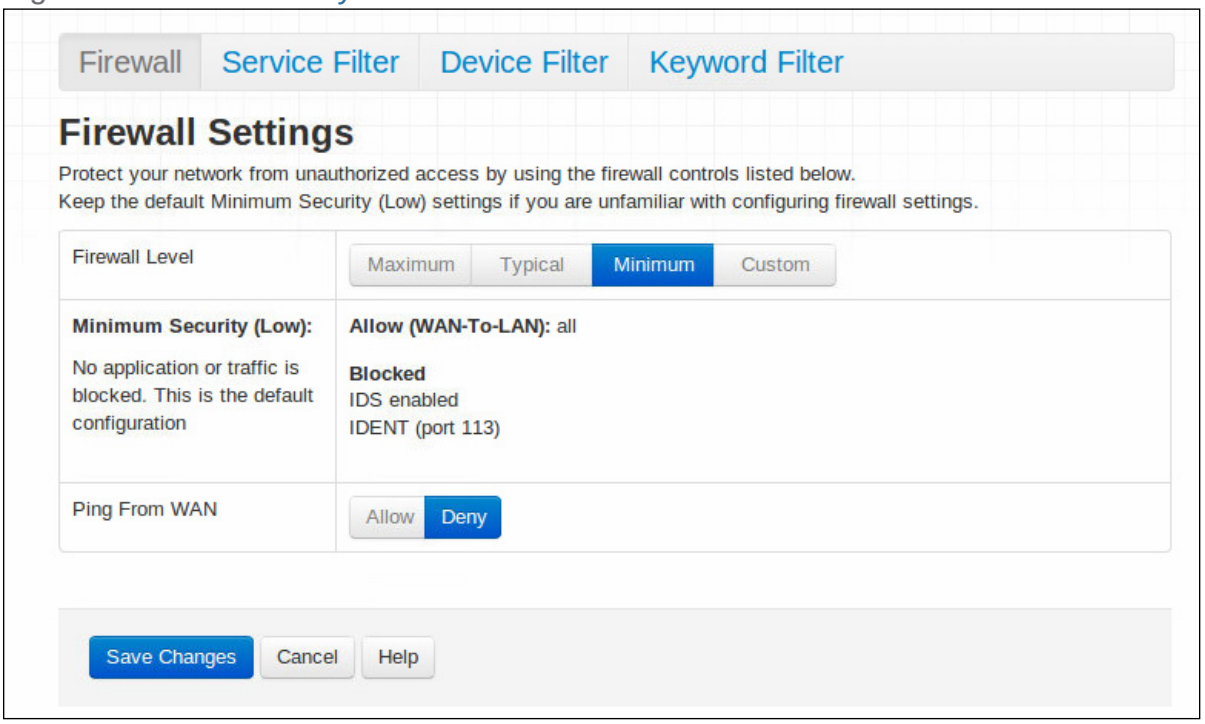
6.2 The Security: Firewall Screen

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.

To block specific ports, use the Service Filter screen (see The Security: Service Filter Screen on page 105).Click **Security** > **Firewall**. The following screen displays.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 43: The Security: Firewall Screen



The following table describes the labels in this screen.

Table 34: 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).

Table 34: The Security: Firewall Screen (continued)

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.
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 Security: Service Filter Screen

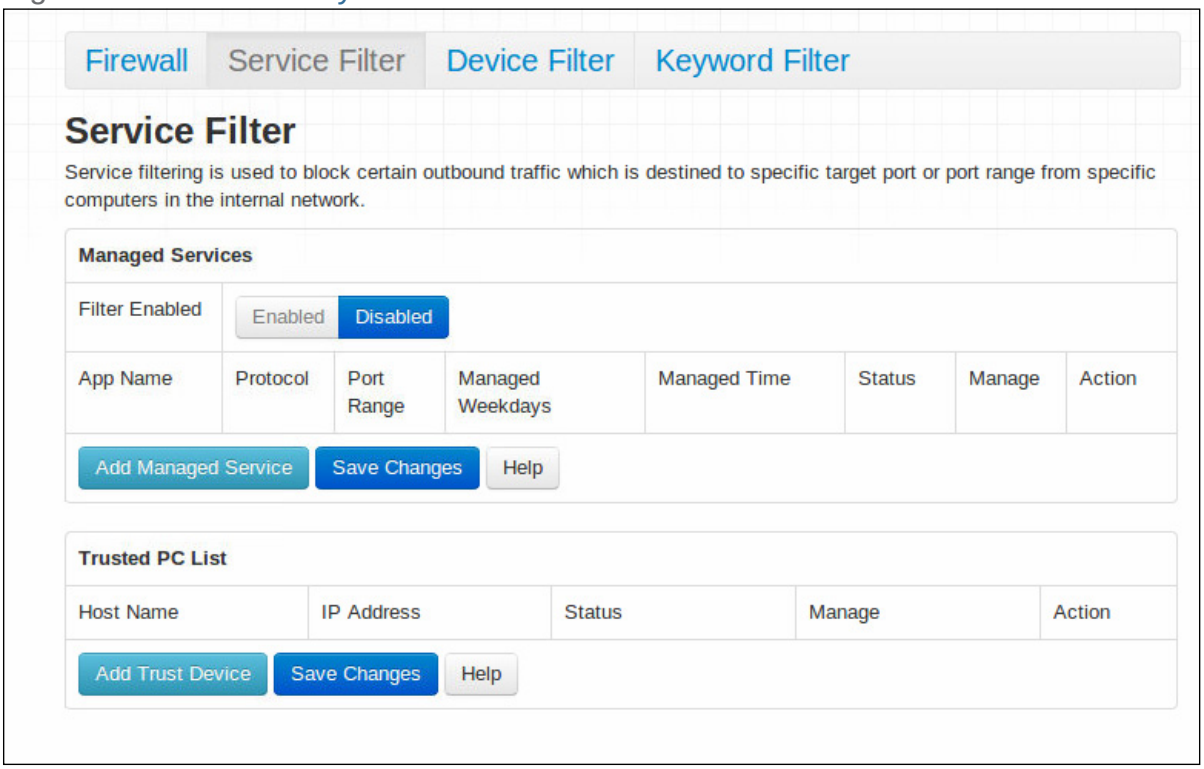
Use this screen to configure service filtering. You can turn service filtering on or off and configure new and existing service filtering rules.

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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 44: The Security: Service Filter Screen



The following table describes the labels in this screen.

Table 35: 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.

Table 35: The Security: Service Filter Screen (continued)

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 107).
Add Managed Service	Click this to add a new service filtering rule (see Adding or Editing a Service Filter Rule on page 107).
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 110 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 Service Filter Trusted Device Rule on page 110 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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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 45: The Security: Service Filter Add/Edit Screen

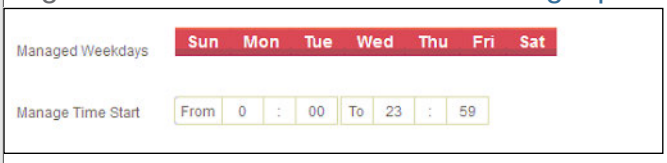
The following table describes the labels in this screen.

Table 36: 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 CGNVM 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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 36: The Security: Service Filter Add/Edit Screen

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.
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 46: Additional Service Filtering Options  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.

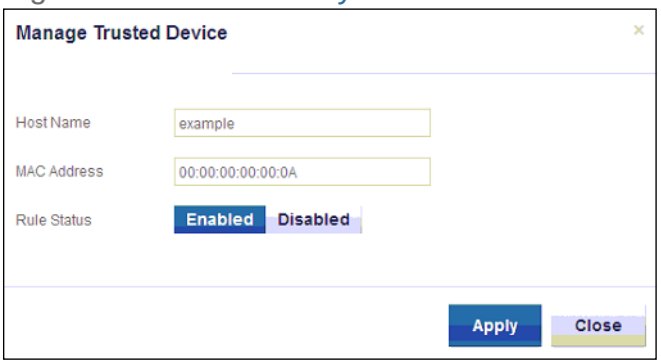
Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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 47: The Security: Service Filter Trusted Device Add/Edit Screen



The following table describes the labels in this screen.

Table 37: 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.

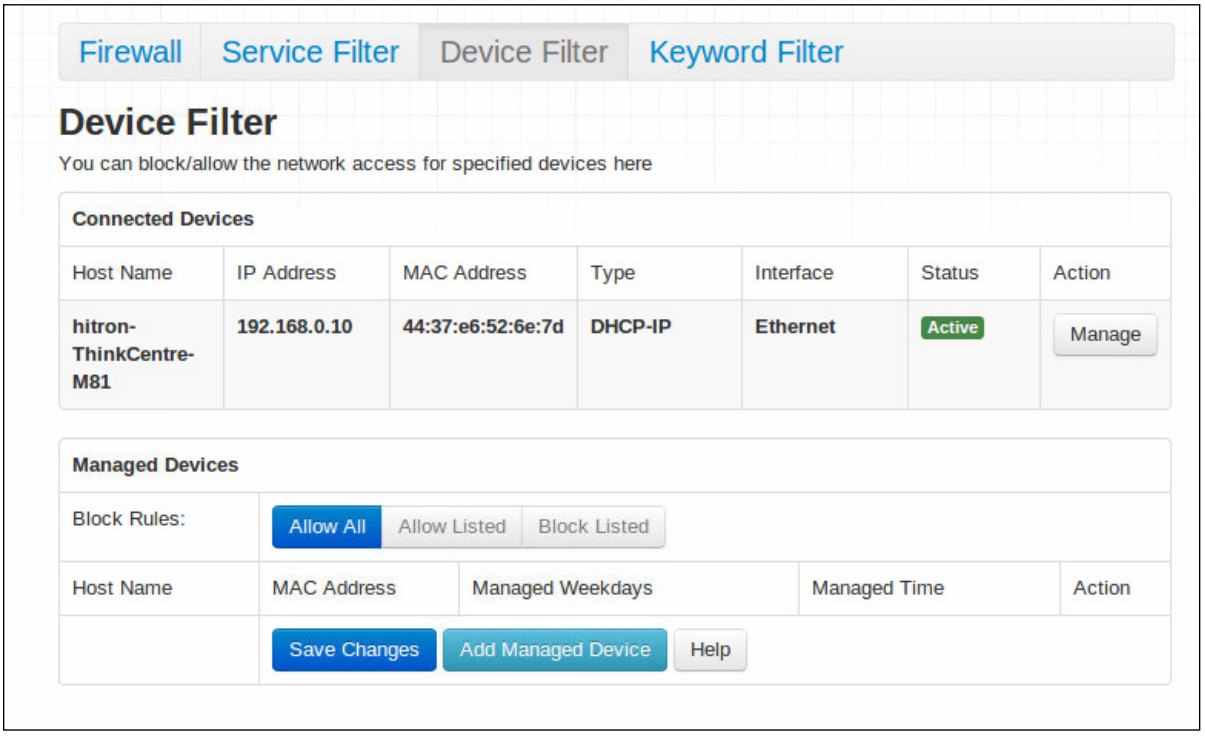
6.4 The Security: Device Filter Screen

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 91.

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

Figure 48: The Security: Device Filter Screen



The following table describes the labels in this screen.

Table 38: 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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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

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 113 for information on the screen that displays.
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 CGNVM. ▸ Select **Allow Listed** to permit only devices you added to the **Managed Devices** list to access the CGNVM 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 CGNVM 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 113).
Save Changes	Click this to save your changes to the fields in this screen.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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

Add Managed Device	Click this to add a new managed device rule (see Adding or Editing a Managed Device on page 113).
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 LAN device, click **Add Managed Device** in the **Security** > **Device Filter** screen.
- To edit an existing managed LAN device, locate the device in the **Security** > **Device Filter** screen and click its **Manage** button.
- To add a new managed wireless network device, click **Add Managed Device** in the **Wireless** > **Access Control** screen.
- To edit an existing managed wireless network device, locate the device in the **Wireless** > **Access Control** screen and click its **Manage** button.

The following screen displays.

Figure 49: The Security: Device Filter Add/Edit Screen

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

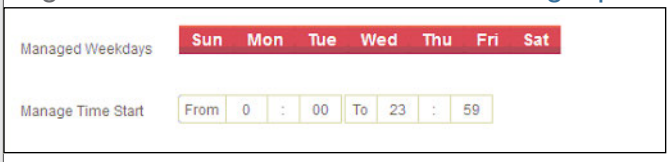
The following table describes the labels in this screen.

Table 39: 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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 39: 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 50: Additional Service Filtering Options  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 Security: Keyword Filter Screen

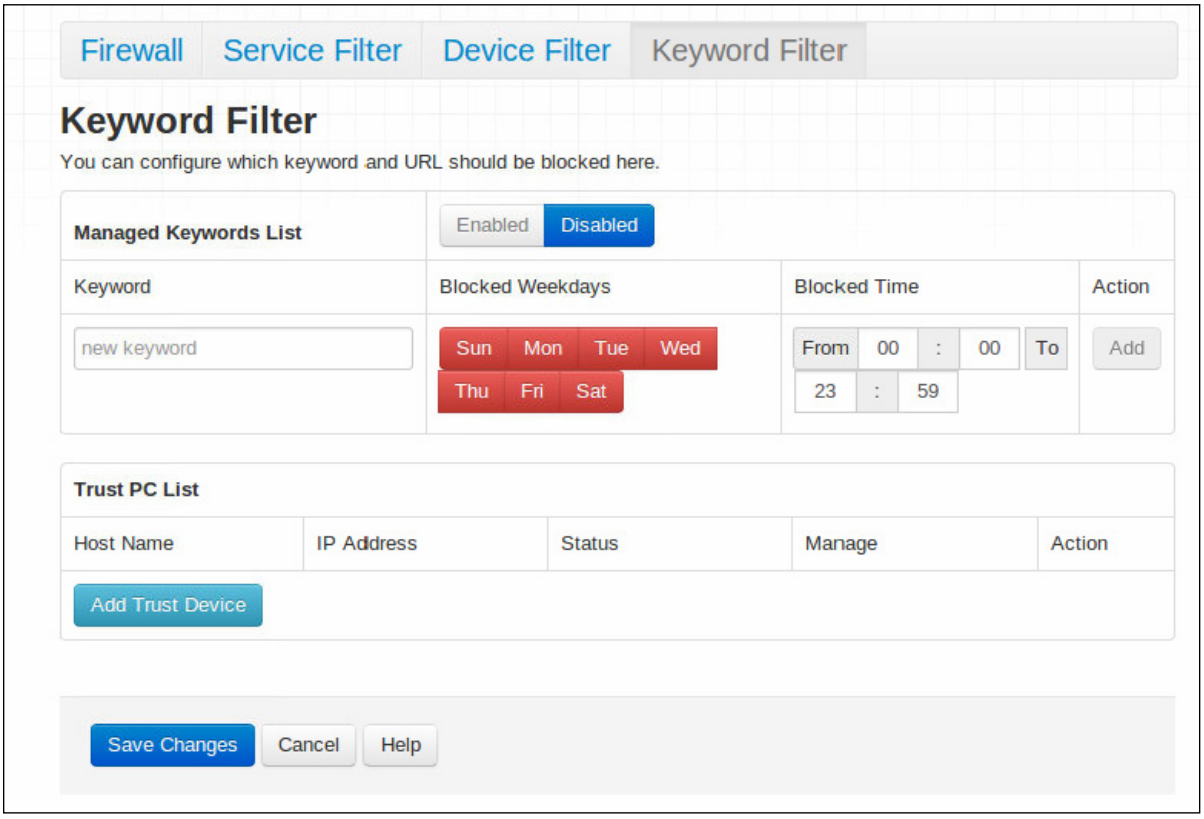
Use this screen to block access from the LAN to websites whose URLs (Web addresses) and page content (text) contain certain keywords. You can create multiple keyword blocking rules, and set them to apply on certain days and at certain times.

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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

Figure 51: The Security: Keyword Filter Screen



The following table describes the labels in this screen.

Table 40: 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 CGNVM 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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Table 40: 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.
Trust 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 117 for information on the screen that displays.
Action	Click **Delete** to remove the trusted device rule.
Add Trust Device	Click this to create a new trusted device rule. See Adding or Editing a Keyword Filter Trusted Device Rule on page 117 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.

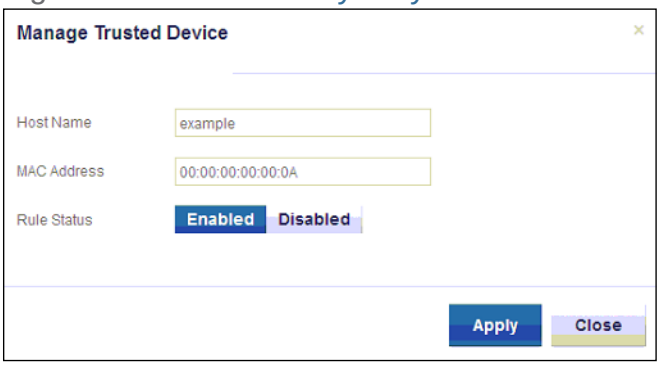
6.5.1 Adding or Editing a Keyword Filter Trusted Device Rule

- 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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Figure 52: The Security: Keyword Filter Trusted Device Add/Edit Screen



The following table describes the labels in this screen.

Table 41: 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.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

7

MTA

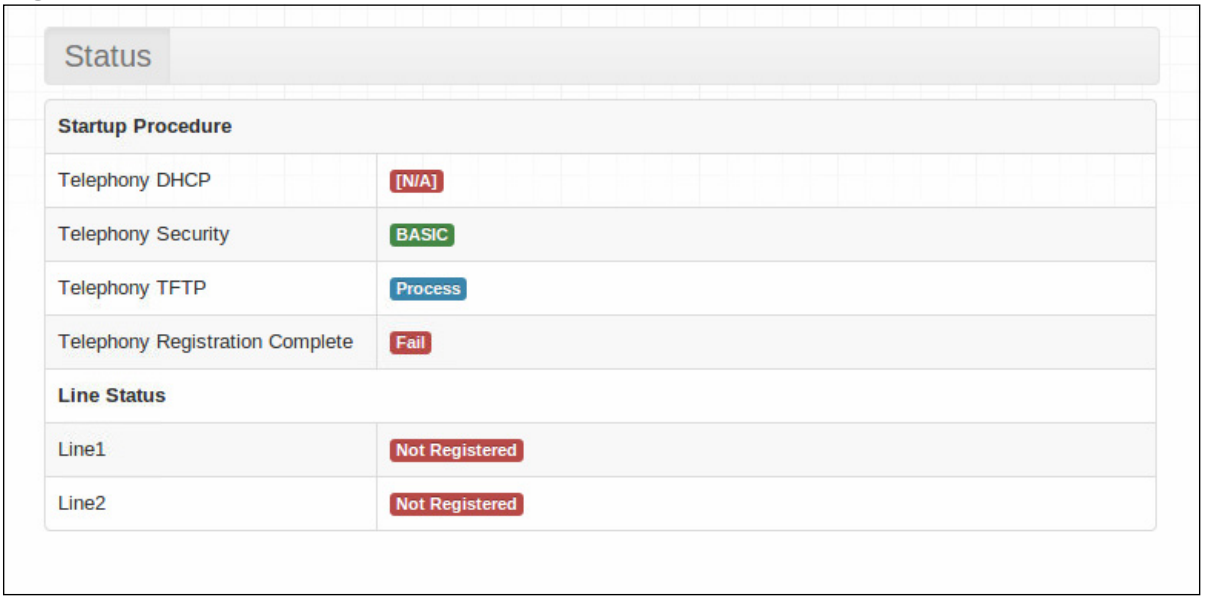
This chapter describes the screens that display when you click **MTA** in the toolbar. It contains the following sections:

7.1 The MTA: Status Screen

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

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

Figure 53: The MTA: Status Screen



Version 1.2, 10/2014. Copyright © 2014 Hitron Technologies

The following table describes the labels in this screen.

Table 42: The MTA: Status 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	

Version 1.2, 10/2014. Copyright © 2014 Hitron Technologies

8

Troubleshooting

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

Problem: None of the LEDs Turn On

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

1. Ensure that you are using the correct power cable/battery.

Using a power source other than the one that came with your CGNVM can damage the CGNVM.

2. If using the power cable, ensure that it is connected to the CGNVM 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 cable to the power source and the CGNVM.

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

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 20).

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

3 Disconnect and re-connect the power cable to the CGNVM.

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

Problem: I Forgot the CGNVM's IP Address

1 The CGNVM'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 CGNVM'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 CGNVM's Admin Username or Password

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

Problem: I Cannot Access the CGNVM or the Internet

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

2 Check your network's hardware connections, and that the CGNVM's LEDs display correctly (see LEDs on page 20).

3 Make sure that your computer is on the same subnet as the CGNVM; see IP Address Setup on page 23.

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 CGNVM. See Resetting the CGNVM on page 28. All user-configured data is lost, and the CGNVM is returned to its default settings. If you previously backed-up a more recent version your CGNVM's settings, you can now upload them to the CGNVM; see The Admin: Backup Screen on page 98.

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 CGNVM'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 CGNVM's signal quality and coverage area.

3 Ensure that the CGNVM and the wireless client are set to use the same wireless mode, SSID and security settings (see The Wireless: Basic Settings Screen on page 78).

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

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

Index

Numbers

A

B

C

D

E

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

F

G

H

I

L

M

N

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

O

P

Q

R

S

T

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

U

V

W

Version 1.0, 02/2015. Copyright © 2014 Hitron Technologies

X