CGNM/ CGNM-3552
D3 WiFi MoCA Gateway

User's Guide

Version 2.0 - 2015

hitron

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the CGNM/ CGNM-3552's features via its Graphical User Interface (GUI).

How to Use this User's Guide

This manual contains information on each the CGNM/ CGNM-3552's GUI screens, and describes how to use its various features.

- Use the CGNM Overview on page 13 to see an overview of the topics covered in this manual.
- Use the Table of Contents (page 1), List of Figures (page 1) and List of Tables (page 1) to quickly find information about a particular GUI screen or topic.
- Use the Index (page 1) to find information on a specific keyword.
- Use the rest of this User's Guide to see in-depth descriptions of the CGNM/ CGNM-3552's features.

Related Documentation

- **Quick Installation Guide**: see this for information on getting your CGNM/ CGNM-3552 up and running right away. It includes information on system requirements, package contents, the installation procedure, and basic troubleshooting tips.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

- **Online Help**: each screen in the CGNM/ CGNM-3552'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 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Customer Support

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

Default Login Details

The CGNM/ CGNM-3552's default IP address and login credentials are as follows. For more information, see Login into the CGNM on page 22.

Table 1: Default Credentials

IP Address	192.168.0.1
Username	cusadmin
Password	password

Copyright © 2013-2014 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

About This User's Guide 2

Table of Contents 5

List of Figures 9

List of Tables 11

Introduction 13

1.1 CGNM Overview 13
1.1.1 Key Features 14
1.2 Hardware Connections 14
1.3 LEDs 17
1.4 IP Address Setup 21
1.4.1 Manual IP Address Setup 21
1.5 Login into the CGNM 22
1.6 GUI Overview 23
1.7 Factory Default Resetting the CGNM 24

Setup Wizard 26

2.1 Setup Wizard Overview 26
2.2 The Setup Wizard Screen 26
2.3 The Welcome Screen 27
2.4 The Setting Password Screen 28
2.5 The Wireless Settings Screen 29
2.6 The Summary Screen 30

Status 32

3.1 Status Overview 32
3.1.1 DOCSIS 32

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

3.1.2 IP Addresses and Subnets 33
3.1.2.1 IP Address Format 33
3.1.2.2 IP Address Assignment 33
3.1.2.3 Subnets 34
3.1.3 DHCP 35
3.1.4 DHCP Lease 36
3.1.5 MAC Addresses 36
3.1.6 Routing Mode 37
3.1.7 Configuration Files 37
3.1.8 Downstream and Upstream Transmissions 37
3.1.9 Cable Frequencies 37
3.1.10 Modulation 38
3.1.11 TDMA, FDMA and SCDMA 38
3.1.12 The Multimedia over Coax Alliance 39
3.2 The Overview Screen 40
3.3 The System Information Screen 44
3.4 The DOCSIS Provisioning Screen 46
3.5 The DOCSIS WAN Screen 47
3.6 The DOCSIS Event Screen 49
3.7 The Wireless Screen 51
3.8 The MoCA Screen 54

Basic 56

4.1 Basic Overview 56
4.1.1 WAN and LAN 56
4.1.2 LAN IP Addresses and Subnets 57
4.1.3 DNS and Domain Suffix 57
4.1.4 Debugging (Ping and Traceroute) 57
4.1.5 Port Forwarding 58
4.1.6 Port Triggering 58
4.1.7 DMZ 58
4.2 The LAN Setup Screen 58
4.3 The Gateway Function Screen 61
4.4 The Port Forwarding Screen 62
4.4.1 Adding or Editing a Port Forwarding Rule 63
4.5 The Port Triggering Screen 66

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

4.5.1 Adding or Editing a Port Triggering Rule 67
4.6 The DMZ Screen 69
4.7 The DNS Screen 71
4.8 The MoCA Screen 72

Wireless 77

5.1 Wireless Overview 77
5.1.1 Wireless Networking Basics 77
5.1.2 Architecture 77
5.1.3 Wireless Standards 78
5.1.4 Service Sets and SSIDs 78
5.1.5 Wireless Security 78
5.1.5.1 WPS 79
5.1.6 WMM 80
5.2 The Basic Settings Screen 80
5.2.1 2.4G Settings 80
5.2.2 5G Settings 84
5.2.3 WPS 88
5.3 The Access Control Screen 90
5.3.1 Adding or Editing a Managed Device 92

Admin 93

6.1 Admin Overview 93
6.1.1 Debugging (Ping and Traceroute) 93
6.2 The Management Screen 94
6.3 The Remote Management Screen 95
6.4 The Diagnostics Screen 97
6.5 The Backup Screen 98
6.6 The USB Storage Screen 99
6.7 The Device Reset Screen 100

Security 102

7.1 Security Overview 102
7.1.1 Firewall 102

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

7.1.2 Device Filtering 103
7.1.3 Service Filtering 103
7.2 The Firewall Screen 103
7.3 The Service Filter Screen 106
7.3.1 Adding or Editing a Service Filter Rule 108
7.3.2 Adding or Editing a Trust PC List 110
7.4 The Device Filter Screen 111
7.4.1 Adding or Editing a Managed Device 113
7.5 The Keyword Filter Screen 115
7.5.1 Adding or Editing a Trust PC List 117

Advanced 119

8.1 The Switch Setup Screen 119
8.2 The DDNS Screen 121

Troubleshooting 123

Index 127

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

List of Figures

Figure 1: Application Overview 13
Figure 2: Hardware Connections 15
Figure 3: Power Adaptor 17
Figure 4: LEDs 18
Figure 5: Login 23
Figure 6: GUI Overview 24
Figure 7: The Setup Wizard Screen 27
Figure 8: The Quick Wizard: Welcome Screen 28
Figure 9: The Quick Wizard: Setting Password Screen 28
Figure 10: The Quick Wizard: Wireless Settings Screen 29
Figure 11: The Setup Wizard: Summary Screen 31
Figure 12: The Setup Wizard: Summary Screen 31
Figure 13: Bridging the Gap Between IP and Coaxial Networks 39
Figure 14: The Status: Overview Screen 41
Figure 15: The Status: System Information Screen 45
Figure 16: The Status: DOCSIS Provisioning Status Screen 46
Figure 17: The Status: DOCSIS WAN Screen 47
Figure 18: The Status: DOCSIS Event Screen 50
Figure 19: The Status: Wireless Screen 51
Figure 20: Wireless Client List 53
Figure 21: The Status: MoCA Information Screen 54
Figure 22: The Basic: LAN Setup Screen 59
Figure 23: The Basic: Gateway Function Screen 61
Figure 24: The Basic: Port Forwarding Screen 62
Figure 25: The Basic: Port Forwarding Add/Edit Screen 64
Figure 26: The Basic: Port Triggering Screen 66
Figure 27: The Basic: Port Triggering Add/Edit Screen 68
Figure 28: The Basic: DMZ Screen 70
Figure 29: Connected Device Info 70
Figure 30: The Basic: DNS Screen 71
Figure 31: The Basic: MoCA Screen 73
Figure 32: Bridge Name Options 74

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Figure 33: Channel Plan 74
Figure 34: Channel 75
Figure 35: The Wireless: Basic Settings Screen (2.4G) 81
Figure 36: The Wireless: Basic Settings Screen (5G) 85
Figure 37: The Wireless: Basic Settings Screen (WPS) 89
Figure 38: The Wireless: Access Control Screen 90
Figure 39: The Wireless: Access Control Add/Edit Screen 92
Figure 40: The Admin: Management Screen 94
Figure 41: The Admin: Remote Management Screen 96
Figure 42: The Admin: Diagnostics Screen 97
Figure 43: The Admin: Backup Screen 98
Figure 44: The Admin: USB Storage Screen 99
Figure 45: The Admin: Device Reset Screen 101
Figure 46: The Security: Firewall Screen 104
Figure 47: The Security: Service Filter Screen 106
Figure 48: The Security: Service Filter Add/Edit Screen 108
Figure 49: Additional Service Filtering Options 110
Figure 50: The Security: Service Filter > Trust PC List Add/Edit Screen 111
Figure 51: The Security: Device Filter Screen 112
Figure 52: The Security: Device Filter Add/Edit Screen 114
Figure 53: Additional Service Filtering Options 115
Figure 54: The Security: Keyword Filter Screen 116
Figure 55: Keyword Filter > Trust PC List Add/Edit Screen 118
Figure 56: The Advanced > Switch Setup Screen 120
Figure 57: The Advanced > DDNS Screen 121

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

List of Tables

Table 1: Default Credentials 4
Table 2: Hardware Connections 16
Table 3: LEDs 18
Table 4: GUI Overview 24
Table 5: The Setup Wizard Screen 27
Table 6: The Setup Wizard: Setting Password Screen 29
Table 7: The Setup Wizard: Wireless Settings Screen 30
Table 8: Private IP Address Ranges 34
Table 9: IP Address: Decimal and Binary 34
Table 10: Subnet Mask: Decimal and Binary 35
Table 11: The Status: Overview Screen 42
Table 12: The Status: System Information Screen 45
Table 13: The Status: DOCSIS WAN Screen 48
Table 14: The Status: DOCSIS Event Screen 50
Table 15: The Status: Wireless Status Screen 52
Table 16: The Status: MoCA Information Screen 54
Table 17: The Basic: LAN Setup Screen 60
Table 18: The Basic: Gateway Function Screen 61
Table 19: The Basic: Port Forwarding Screen 62
Table 20: The Basic: Port Forwarding Add/Edit Screen 64
Table 21: The Basic: Port Triggering Screen 66
Table 22: The Basic: Port Triggering Add/Edit Screen 68
Table 23: The Basic: DMZ Screen 70
Table 24: The Basic: DNS Screen 71
Table 25: The Basic: MoCA Screen 74
Table 26: The Wireless: Basic Settings Screen (2.4G) 81
Table 27: The Wireless: Basic Settings Screen (5G) 85
Table 28: The Wireless: Basic Settings Screen (WPS) 89
Table 29: The Wireless: Access Control Screen 90
Table 30: The Wireless: Access Control Add/Edit Screen 92
Table 31: The Admin: Management Screen 95
Table 32: The Admin: Remote Management Screen 96

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 33: The Admin: Diagnostics Screen 97
Table 34: The Admin: Backup Screen 99
Table 35: The Admin: USB Storage Screen 100
Table 36: The Admin: Device Reset Screen 101
Table 37: The Security: Firewall Screen 105
Table 38: The Security: Service Filter Screen 106
Table 39: The Security: Service Filter Add/Edit Screen 109
Table 40: The Security: Service Filter Add/Edit Trust Manage Device Screen 111
Table 41: The Security: Device Filter Screen 112
Table 42: The Security: Device Filter Add/Edit Screen 114
Table 43: The Security: Keyword Filter Screen 116
Table 44: The Security: Keyword Filter Add/Edit Trust Manage Device Screen 118
Table 45: The Advanced > Switch Setup Screen 120
Table 46: The Advanced > DDNS Screen 121

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

1

Introduction

This chapter introduces the CGNM/ CGNM-3552 and its GUI (Graphical User Interface).

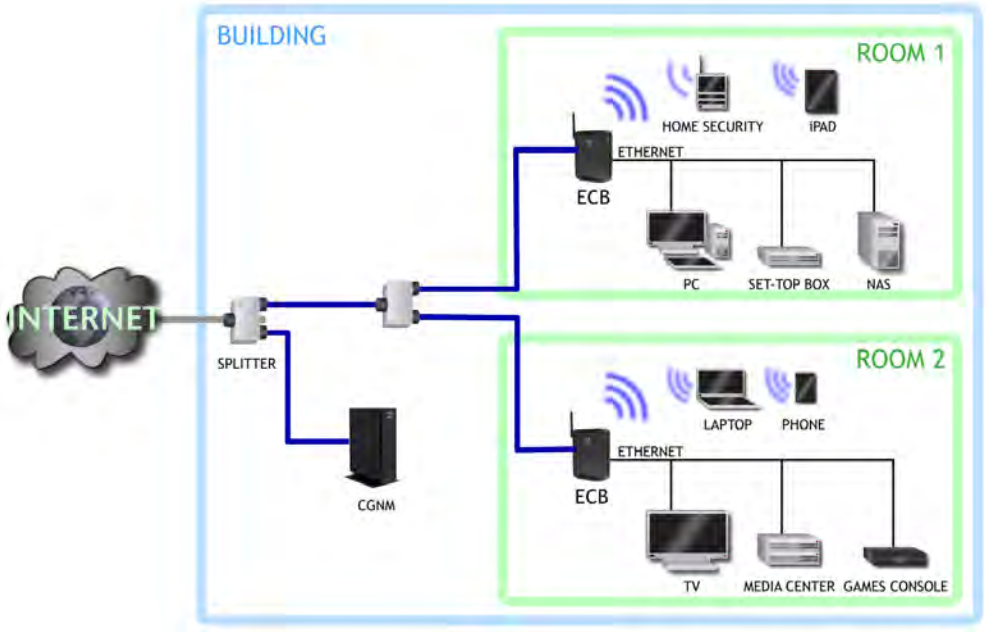
1.1 CGNM/ CGNM-3552 Overview

Your CGNM/ CGNM-3552 is a NAT-capable cable modem and wireless access point that allows you to connect your computers, wireless devices, and other network devices to one another, and to the Internet via the cable connection.

The CGNM/ CGNM-3552 must be placed vertically on its stand, should not be positioned in either wall-mount or horizontal.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Figure 1: Application Overview



1.1.1 Key Features

The CGNM/ CGNM-3552 provides:

- MoCA 2.0 high-performance entertainment networking providing real throughput of 480Mbps in baseline mode
- High-performance Internet connection via the CATV port (F-type RF connector). For 24x8 models (DOCSIS 3.0 24-channel downstream, 8-channel upstream), the download speed can be up to 960 Mbps (megabits per second). For 32x8 models (DOCSIS 3.0 32-channel downstream, 8-channel upstream) such as CGNM-3552 and CGNM-3550, the download speed can be up to 1200Mbps.
- Full dual-stack IPv4/IPv6 support for routing and firewall (DSLite and 6RD)
- Local Area Network connection via four 10/100/1000 Mbps Ethernet ports
- Dynamic Host Configuration Protocol (DHCP) for devices on the LAN
- LAN troubleshooting tools (Ping and Traceroute)
- IEEE 802.11a/b/g/n/ac concurrent dual band (2.4GHz and 5GHz) wireless MIMO (Multiple-In, Multiple-Out) networking, allowing speeds of up to 450Mbps+1300Mbps PHY data rate.

- Wireless security: WEP, WPA-PSK and WPA2-PSK encryption, WiFi Protected Setup (WPS) push-button and PIN configuration, MAC filtering,
- Wired security: stateful inspection firewall with intrusion detection system, IP and MAC filtering, port forwarding and port triggering, De-Militarized Zone (DMZ)
- Settings backup and restore
- Secure configuration interface, accessible by Web browser

1.2 Hardware Connections

This section describes the CGNM/ CGNM-3552's physical ports and buttons.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Figure 2: Hardware Connections

Version 2.0, 07/2015. Copyright © 2015 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. See WPS on page 79 for more information.
USB	The CGNM/ CGNM-3552 provides two USB 2.0 host ports on the rear, allowing you to plug in USB flash disks for mounting and sharing through the LAN interfaces via the Samba protocol (network neighborhood). The CGNM/ CGNM-3552 supports the following Windows file systems: ▸ FAT16 ▸ FAT32 ▸ NTFS **USB devices must not drain more than 500mA from the USB port. USB devices requiring more than 500mA should be provided with their own power source(s).**
Reset	Use this button to reboot or reset your CGNM/ CGNM-3552. ▸ Press the button and hold it for less than five seconds to reboot the CGNM/ CGNM-3552. The CGNM/ CGNM-3552 restarts, using your existing settings. ▸ Press the button and hold it for more than five seconds to delete all user-configured settings and restart the CGNM/ CGNM-3552 using its factory default settings. See Factory Default Resetting the CGNM/ CGNM-3552 on page 14 for more information on resetting the CGNM/ CGNM-3552. NOTE: Unless you previously backed-up the CGNM/ CGNM-3552's configuration settings prior to resetting the CGNM/ CGNM-3552, the settings cannot be recovered.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 2: Hardware Connections

LAN1	Use these ports to connect your computers and other network devices, using Category 5 or 6 Ethernet cables with RJ45 connectors.
LAN2	
LAN3	
LAN4	
CABLE	Use this to connect to the Internet and coax network via an F-type RF cable.
POWER	Use this to connect to the 12v/2.5A power adapter that came with your CGNM/ CGNM-3552. **NEVER use another power adapter with your CGNM/ CGNM-3552. Doing so could harm your CGNM/ CGNM-3552.** Figure 3: Power Adaptor

1.3 LEDs

This section describes the CGNM/ CGNM-3552's LEDs (lights).

Figure 4: LEDs

Table 3: LEDs

LED	STATUS	**DESCRIPTION**
POWER	Off	The CGNM/ CGNM-3552 is not receiving power.
	On	The CGNM/ CGNM-3552 is receiving power.

Table 3: LEDs

DS	Green, blinking	The CGNM/ CGNM-3552 is searching for a downstream frequency on the **CABLE** connection.
	Green, steady	The CGNM/ CGNM-3552 has successfully located and locked onto a downstream frequency on the **CABLE** connection.
	Blue, blinking	The CGNM/ CGNM-3552 is ranging on the downstream frequency.
	Blue, steady	Downstream frequency is locked or online with channel bonding.
	Off	There is no downstream activity on the **CABLE** connection.
US	Green, blinking	The CGNM/ CGNM-3552 is searching for an upstream frequency on the **CABLE** connection.
	Green, steady	The CGNM/ CGNM-3552 has successfully located and locked onto an upstream frequency on the **CABLE** connection.
	Blue, blinking	The CGNM/ CGNM-3552 is ranging on the upstream frequency.
	Blue, steady	Upstream frequency is locked or online with channel bonding.
	Off	There is no upstream activity on the **CABLE** connection.
STATUS	Blinking	The CGNM/ CGNM-3552's cable modem is registering with the service provider's CMTS.
	On	The CGNM/ CGNM-3552's cable modem has successfully registered with the service provider and is ready for data transfer.
LAN	Off	No device is connected to one of the **LAN** ports.
	Green, blinking	A device is connected to one of the **LAN** ports and is transmitting or receiving data.
	Green, steady	A device is connected to one of the **LAN** ports but is not transmitting or receiving data.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 3: LEDs

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.
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.
MoCA	Off	The CABLE port is not connected to a coax socket, or the CABLE port is connected to a coax socket, but no other MoCA device has been detected on the coax network.
	Green, steady	Another MoCA device has been detected on the coax network, and the CGNM/ CGNM-3552 has successfully made a connection.
	Green, blinking	Data is being transferred to or from the CGNM/ CGNM-3552 over the coax network.

When you turn on the CGNM/ CGNM-3552, the LEDs light up in the following order:

1 POWER

2 DS

3 US

4 STATUS

5 The **LAN** LED lights up as soon as there is activity on the LAN ports, the **WIRELESS** LEDs light up once the wireless network is ready, and the **MoCA** LED lights up once a connected device is detected.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

1.4 IP Address Setup

Before you log into the CGNM/ CGNM-3552's GUI, your computer's IP address must be in the same subnet as the CGNM/ CGNM-3552. This allows your computer to communicate with the CGNM/ CGNM-3552.

NOTE: See IP Addresses and Subnets on page 33 for background information.

The CGNM/ CGNM-3552 has a built-in DHCP server that, when active, assigns IP addresses to computers on the LAN. When the DHCP server is active, you can get an IP address automatically. The DHCP server is active by default.

If your computer is configured to get an IP address automatically, or if you are not sure, try to log in to the CGNM/ CGNM-3552 (see GUI Overview on page 12).

- If the login screen displays, your computer is already configured correctly.
- If the login screen does not display, either the CGNM/ CGNM-3552's DHCP server is not active or your computer is not configured correctly. Follow the procedure in Manual IP Address Setup on page 10 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 CGNM/ CGNM-3552's IP settings may have been changed from their defaults. If you do not know the CGNM/ CGNM-3552's new address, you should return it to its factory defaults. See Factory Default Resetting the CGNM/ CGNM-3552 on page 14. Bear in mind that ALL user-configured settings are lost.

1.4.1 Manual IP Address Setup

By default, your CGNM/ CGNM-3552's local IP address is **192.168.0.1**. If your CGNM/ CGNM-3552 is using the default IP address, you should set your computer's IP address to be between **192.168.0.2** and **192.168.0.254**.

NOTE: If your CGNM/ CGNM-3552 DHCP server is active, set your computer to get an IP address automatically in step 5. The CGNM/ CGNM-3552 assigns an IP address to your computer. The DHCP server is active by default.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Take the following steps to manually set up your computer's IP address to connect to the CGNM/ CGNM-3552:

NOTE: This example uses Windows XP; the procedure for your operating system may be different.

1. Click **Start**, then click **Control Panel**.
2. In the window that displays, double-click **Network Connections**.
3. Right-click your network connection (usually **Local Area Connection**) and click **Properties**.
4. In the **General** tab's **This connection uses the following items** list, scroll down and select **Internet Protocol (TCP/IP)**. Click **Properties**.
5. You can get an IP address automatically, or specify one manually:
   - If your CGNM/ CGNM-3552's DHCP server is active, select **Get an IP address automatically**.
   - If your CGNM/ CGNM-3552's DHCP server is active, select **Use the following IP address**. In the **IP address** field, enter a value between **192.168.0.2** and **192.168.0.254** (default). In the **Subnet mask** field, enter **255.255.255.0** (default).

NOTE: If your CGNM/ CGNM-3552 is not using the default IP address, enter an IP address and subnet mask that places your computer in the same subnet as the CGNM/ CGNM-3552.

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 CGNM/ CGNM-3552, or uses the IP address that you specified, and can communicate with the CGNM/ CGNM-3552.

1.5 Login into the CGNM/ CGNM-3552

Take the following steps to login into the CGNM/ CGNM-3552's GUI.

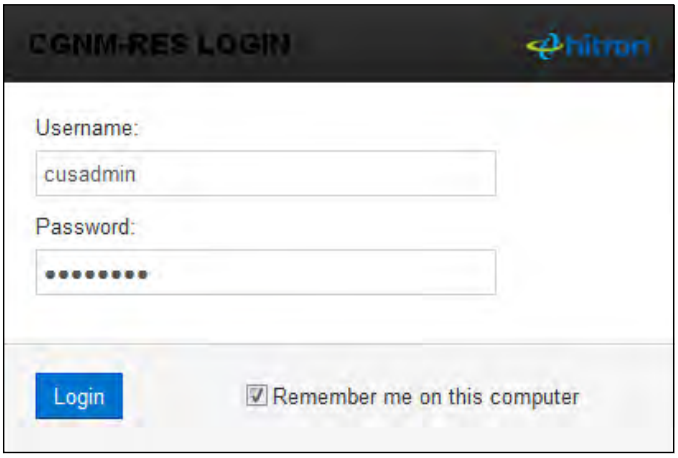
Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

NOTE: You can login into the CGNM/ CGNM-3552's GUI via the wireless interface. However, it is strongly recommended that you configure the CGNM/ CGNM-3552 via a wired connection on the LAN.

1 Open a browser window.

2 Enter the CGNM/ CGNM-3552's IP address (default **192.168.0.1**) in the URL bar. The **Login** screen displays.

Figure 5: Login



3 Enter the **Username** and **Password**. The default login username is **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 **Overview** screen displays (see The Overview Screen on page 40).

1.6 GUI Overview

This section describes the CGNM/ CGNM-3552's GUI.

Figure 6: GUI Overview

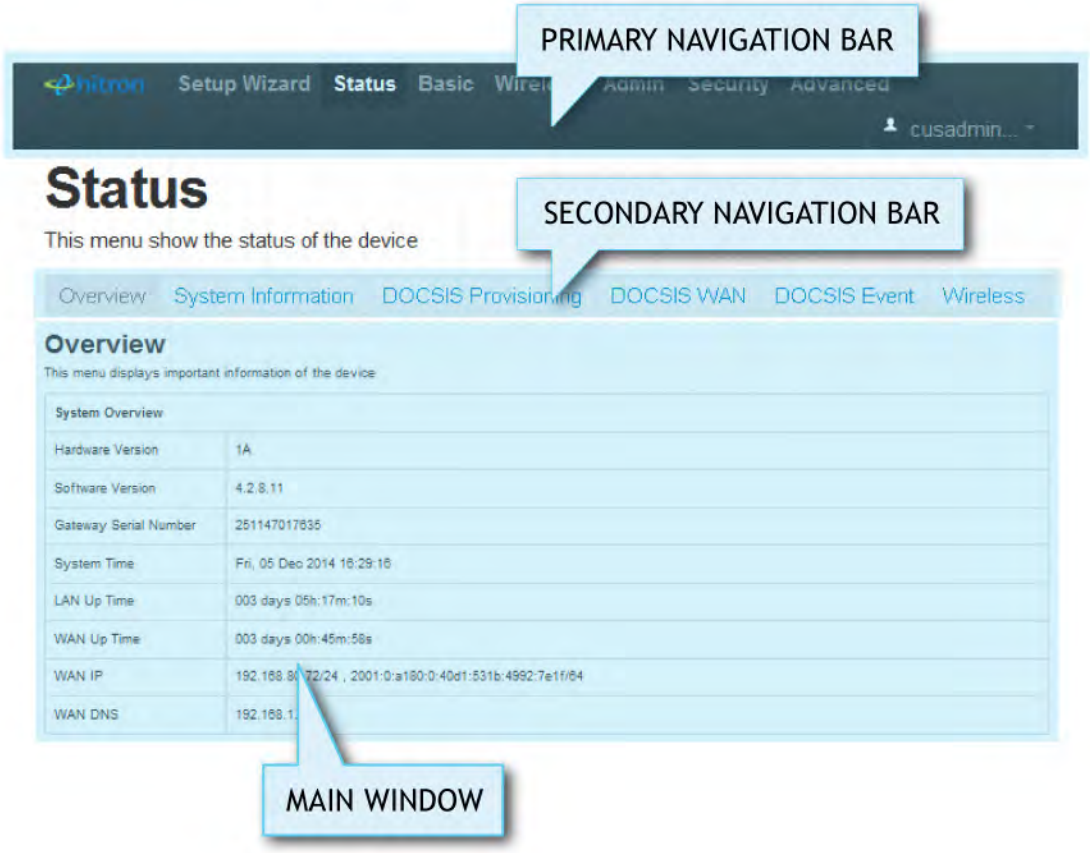


Table 4: GUI Overview

Primary Navigation Bar	Use this section to move from one part of the GUI to another, select the language and your login account.
Secondary Navigation Bar	Use this section to move from one related screen to another.
Main Window	Use this section to read information about your CGNM/ CGNM-3552's configuration, and make configuration changes.

1.7 Factory Default Resetting the CGNM/ CGNM-3552

When you reset the CGNM/ CGNM-3552 to its factory defaults, all user-configured settings are lost, and the CGNM/ CGNM-3552 is returned to its initial configuration state.

There are two ways to reset the CGNM/ CGNM-3552:

- Press the **RESET** button on the CGNM/ CGNM-3552, and hold it in for 5 seconds or longer.
- Click **Admin** > **Device Reset**. In the screen that displays, click the **Factory Reset** button.

After the operation, the CGNM/ CGNM-3552 turns off and on again, using its factory default settings.

NOTE: Depending on your CGNM/ CGNM-3552's previous configuration, you may need to re-configure your computer's IP settings; see IP Address Setup on page 10.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

2

Setup Wizard

This chapter describes the CGNM/ CGNM-3552's setup wizard, which displays when you click **Setup Wizard** in the toolbar. It contains the following sections:

- Setup Wizard Overview on page 1
- The Setup Wizard Screen on page 1
- The Welcome Screen on page 2
- The Setting Password Screen on page 3
- The Wireless Settings Screen on page 4
- The Summary Screen on page 5

2.1 Setup Wizard Overview

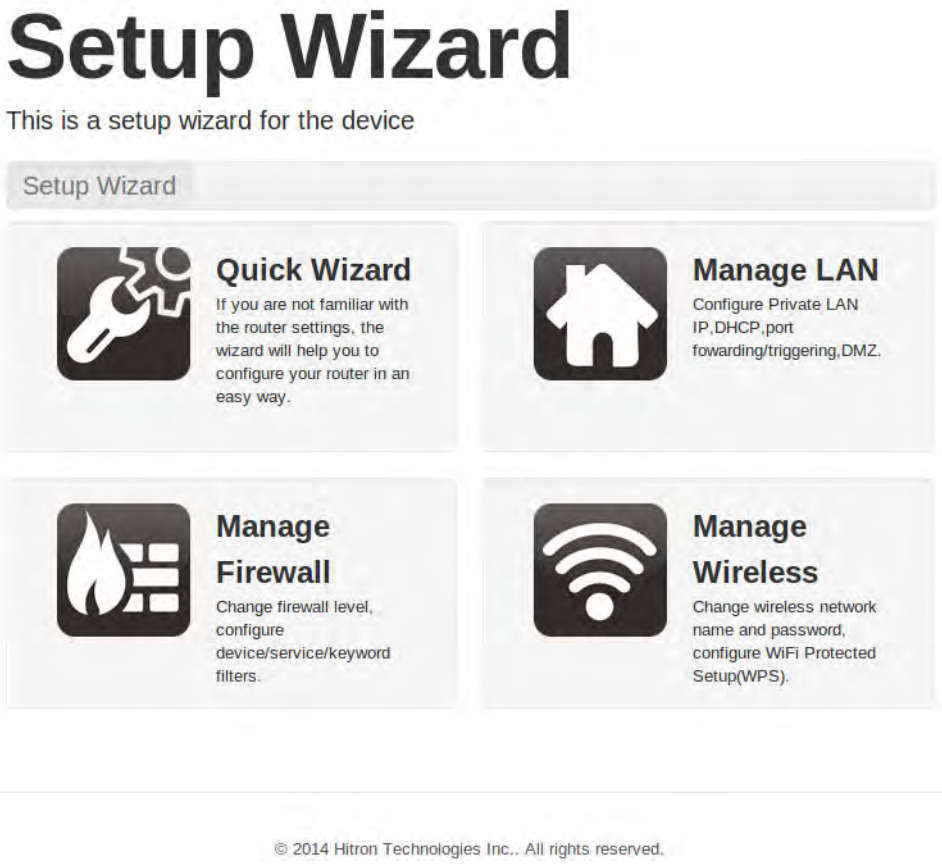
Your CGNM/ CGNM-3552 possess a setup wizard that allows you to rapidly configure its most important settings, including password and wireless settings.

2.2 The Setup Wizard Screen

This section describes the CGNM/ CGNM-3552's Setup Wizard Screen.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Figure 7: The Setup Wizard Screen



The following table describes the labels in this screen.

Table 5: The Setup Wizard Screen

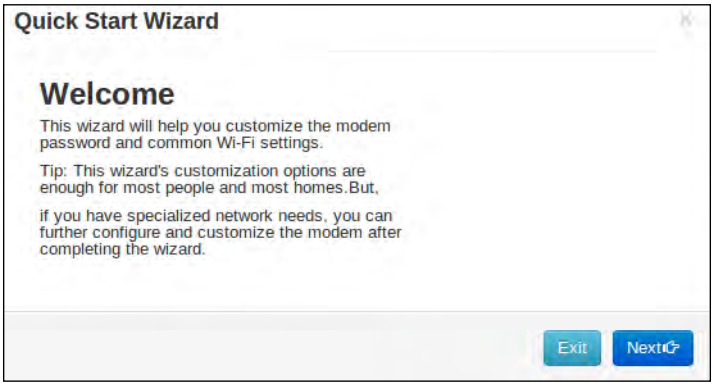
Quick Wizard	Click to customize the CGNM/ CGNM-3552's password and common Wi-Fi settings.
Manage LAN	Click to manage the CGNM/ CGNM-3552's firewall settings. See The LAN Setup Screen on page 58.
Manage Firewall	Click to manage the CGNM/ CGNM-3552's firewall settings. See The Firewall Screen on page 103.
Manage Wireless	Click to manage the CGNM/ CGNM-3552's wireless settings. See The Basic Settings Screen on page 80.

2.3 The Welcome Screen

This screen displays the welcome message of the Quick Wizard.

Click **Quick Wizard**. The following screen displays.

Figure 8: The Quick Wizard: Welcome Screen



2.4 The Setting Password Screen

Use this screen to customize the CGNM/ CGNM-3552's password settings.

Click **Next** in the **Quick Wizard: Welcome Screen**. The following screen displays.

NOTE: It is strongly recommended that you change the CGNM/ CGNM-3552's password from its factory default.

Figure 9: The Quick Wizard: Setting Password Screen

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

The following table describes the labels in this screen.

Table 6: The Setup Wizard: Setting Password Screen

Old Password	Enter the password with which you currently log into the CGNM/ CGNM-3552 for this account.
New Password	Enter and re-enter the password you want to use to log into the CGNM/ CGNM-3552 for this account.
Confirm New Password	
Exit	Click this to return the fields in this screen to their last-saved values without saving your changes.
Prev	Click this to return to the previous screen.
Next	Click this to continue to the next screen.

2.5 The Wireless Settings Screen

Use this screen to configure the CGNM/ CGNM-3552's wireless settings.

Click **Next** in the **Quick Wizard: Setting Password** screen. The following screen displays.

Figure 10: The Quick Wizard: Wireless Settings Screen

The following table describes the labels in this screen.

Table 7: The Setup Wizard: Wireless Settings Screen

Primary SSID	Enter the name that you want to use for your CGNM/ CGNM-3552's wireless network. This is the name that identifies your network, and to which wireless clients connect.
Security Type	Use this field to apply security encryption to your wireless network. ▸ Select **Open** to use no wireless security. Anyone can join the network. ▸ Select **Encrypted** to require people who want to access your wireless network to use a password. Then, enter the password you want to use in the **Security Key** field that displays.
Exit	Click this to return the fields in this screen to their last-saved values without saving your changes.
Prev	Click this to return to the previous screen.
Next	Click this to continue to the next screen.

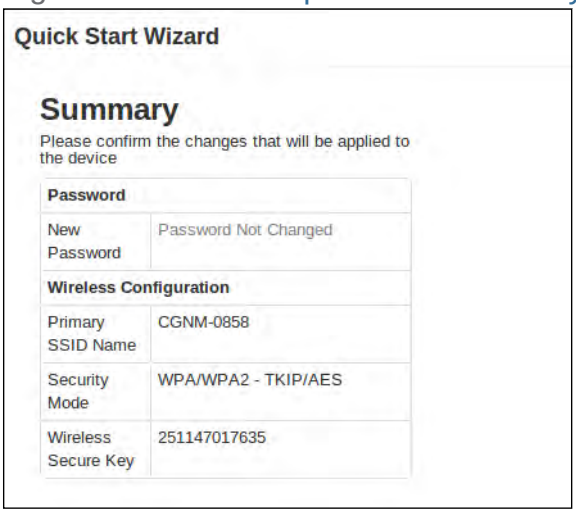
2.6 The Summary Screen

Use this screen to view the CGNM/ CGNM-3552's settings.

Click **Next** in the **Quick Wizard: Wireless Settings** screen. The following screen displays.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Figure 11: The Setup Wizard: Summary Screen



If you are happy with the settings, click **Finish**. The following confirmation message displays.

Figure 12: The Setup Wizard: Summary Screen

NOTE: If you changed the **Primary SSID Name** or **Wireless Secure Key**, make sure you keep a note of the new details.

Alternatively, click **Prev** to make further changes to the wizard's fields.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

3

Status

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

- Status Overview on page 1
- The Overview Screen on page 9
- The System Information Screen on page 13
- The DOCSIS Provisioning Screen on page 15
- The DOCSIS WAN Screen on page 16
- The DOCSIS Event Screen on page 19
- The Wireless Screen on page 21
- The MoCA Screen on page 24

3.1 Status Overview

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

3.1.1 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 CGNM/ CGNM-3552 supports DOCSIS version 3.0.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

3.1.2 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.

3.1.2.1 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).

3.1.2.2 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 CGNM/ CGNM-3552:

- The public network (Wide Area Network or WAN) is the link between the cable connector and your Internet Service Provider. Your CGNM/ CGNM-3552's IP address on this network is assigned by your service provider.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

- The private network (in routing mode - see Routing Mode on page 6) 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 CGNM/ CGNM-3552 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 8: 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 CGNM/ CGNM-3552's LAN subnet.

3.1.2.3 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 9: IP Address: Decimal and Binary

192	168	0	1
11000000	10101000	00000000	00000001

Version 2.0, 07/2015. Copyright © 2015 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 10: 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**.

3.1.3 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 10 for more information.

By default, the CGNM/ CGNM-3552 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 CGNM/ CGNM-3552 is a DHCP server on the LAN; it provides IP addresses to computers on the LAN which request them.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

3.1.4 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.

3.1.5 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 CGNM/ CGNM-3552 via one of the **LAN** ports) and also has a wireless card (to connect to your CGNM/ CGNM-3552 over the wireless interface) the MAC addresses of the two cards will be different. In the case of the CGNM/ CGNM-3552, each internal module (cable modem module, Ethernet module, wireless module, etc.) possesses its own MAC address.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

3.1.6 Routing Mode

When your CGNM/ CGNM-3552 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 CGNM/ CGNM-3552 on the WAN, and all traffic for LAN computers is sent to that IP address. The CGNM/ CGNM-3552 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 CGNM/ CGNM-3552 in routing mode, each computer on the LAN must be assigned an IP address in the CGNM/ CGNM-3552's subnet manually.

When the CGNM/ CGNM-3552 is not in routing mode, the service provider assigns an IP address to each computer connected to the CGNM/ CGNM-3552 directly. The CGNM/ CGNM-3552 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 CGNM/ CGNM-3552's configuration file.

3.1.7 Configuration Files

The CGNM/ CGNM-3552's configuration (or config) file is a document that the CGNM/ CGNM-3552 obtains automatically over the Internet from the service provider's server, which specifies the settings that the CGNM/ CGNM-3552 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.

3.1.8 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 CGNM/ CGNM-3552, and "upstream" refers to traffic from the CGNM/ CGNM-3552 to the service provider.

3.1.9 Cable Frequencies

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

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

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

3.1.10 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.

3.1.11 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.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

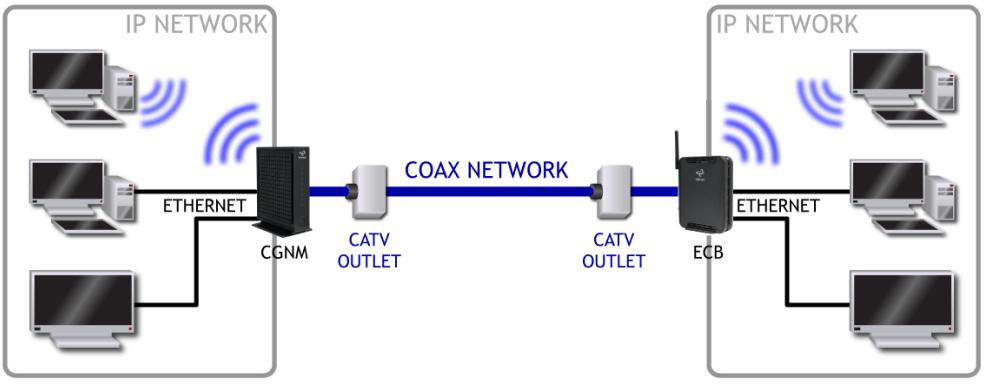
- FDMA allows multiple users to share the same frequency channel by assigning a frequency band within the existing channel to each user.
- SCDMA allows multiple users to share the same frequency channel by assigning a unique orthogonal code to each user.

3.1.12 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 13: 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)

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

3.2 The Overview Screen

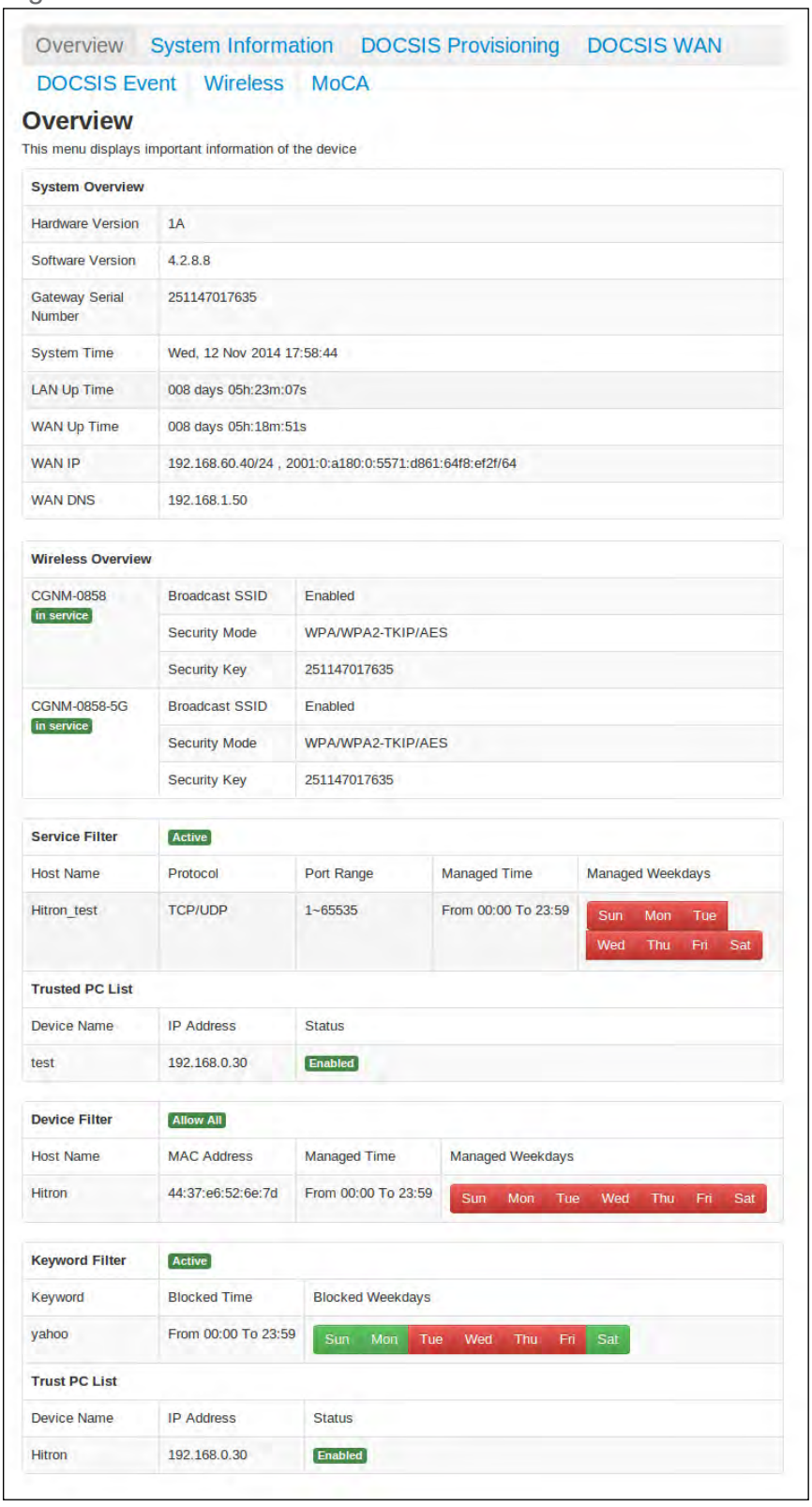
Use this screen to see general information about your CGNM/ CGNM-3552's hardware, its software, and its connection to the Internet.

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

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

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Figure 14: The Status: Overview Screen



The following table describes the labels in this screen.

Table 11: The Status: Overview Screen

System Overview	
Hardware Version	This displays the version number of the CGNM/ CGNM-3552's physical hardware.
Software Version	This displays the version number of the software that controls the CGNM/ CGNM-3552.
Gateway Serial Number	This displays a number that uniquely identifies the device.
System Time	This displays the current date and time.
LAN Up Time	This displays the time the LAN has been online.
WAN Up Time	This displays the time the WAN has been online.
WAN IP	This field displays the CGNM/ CGNM-3552's IP address on the WAN (Wide Area Network) interface.
WAN DNS	This field displays the DNS server IP used by the WAN side.
Wireless Overview	
(SSID)	This displays the 2.4 GHz wireless network's Service Set Identifier. This is the name of the wireless network, to which wireless clients connect.
Broadcast SSID	This field displays **Enabled** when the 2.4 GHz wireless network's SSID is being broadcast, and displays **Disabled** when it is not.
Security Mode	This displays the type of security the CGNM/ CGNM-3552's 2.4 GHz wireless network is currently using.
Security Key	This displays the password for the CGNM/ CGNM-3552's 2.4 GHz wireless network.
(SSID 5 GHz)	This displays the 5 GHz wireless network's Service Set Identifier. This is the name of the wireless network, to which wireless clients connect.
Broadcast SSID	This field displays **Enabled** when the 5 GHz wireless network's SSID is being broadcast, and displays **Disabled** when it is not.
Security Mode	This displays the type of security the CGNM/ CGNM-3552's 5 GHz wireless network is currently using.
Security Key	This displays the password for the CGNM/ CGNM-3552's 5 GHz wireless network.

Table 11: The Status: Overview Screen (continued)

Service Filter	
Filter Status	This displays **Active** when a Service Filter is Enabled.
Host Name	This displays the name for the application for which you want to create the rule.
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 Time	This displays the start (**From**) and end (**To**) of the time period during which this rule applies, on the specified **Managed Weekdays**.
Managed Weekdays	This displays the days of the week on which this rule applies.
Trusted PC List	
Device Name	This displays the name of the trust device connected.
IP Address	This displays the IP address of the trust network device connected.
Status	This displays whether or not the service filter rule is enabled to the trust device connected.
Device Filter	
Block Rules Status	This displays the status of the devices listed. ▸ **Allow All:** ignore the **Managed Devices** list and let all devices connect to the CGNM/ CGNM-3552. ▸ **Allow**: permit only devices you added to the **Managed Devices** list to access the CGNM/ CGNM-3552 and the network. All other devices are denied access. ▸ **Deny**: permit all devices except those you added to the **Managed Devices** list to access the CGNM/ CGNM-3552 and the network. The specified devices are denied access.
Host Name	This displays the name of each network device in the list.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 11: The Status: Overview Screen (continued)

MAC Address	This displays the Media Access Control (MAC) address of each network device in the list.
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**.
Managed Weekdays	This displays the days of the week on which the device is managed.
Keyword Filter	
Keywords Status	This displays **Active** when a Keyword Filter is Enabled.
Keyword	Enter the keyword that you want to block. The CGNM/ CGNM-3552 examines both the page's URL (Internet address) and its page content (text).
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.
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.
Trusted PC List	
Device Name	This displays the name of each network device connected.
IP Address	This displays the IP address of each network device connected.
Rule Status	This displays whether or not the keyword filter rule is enabled to the trust device connected.

3.3 The System Information Screen

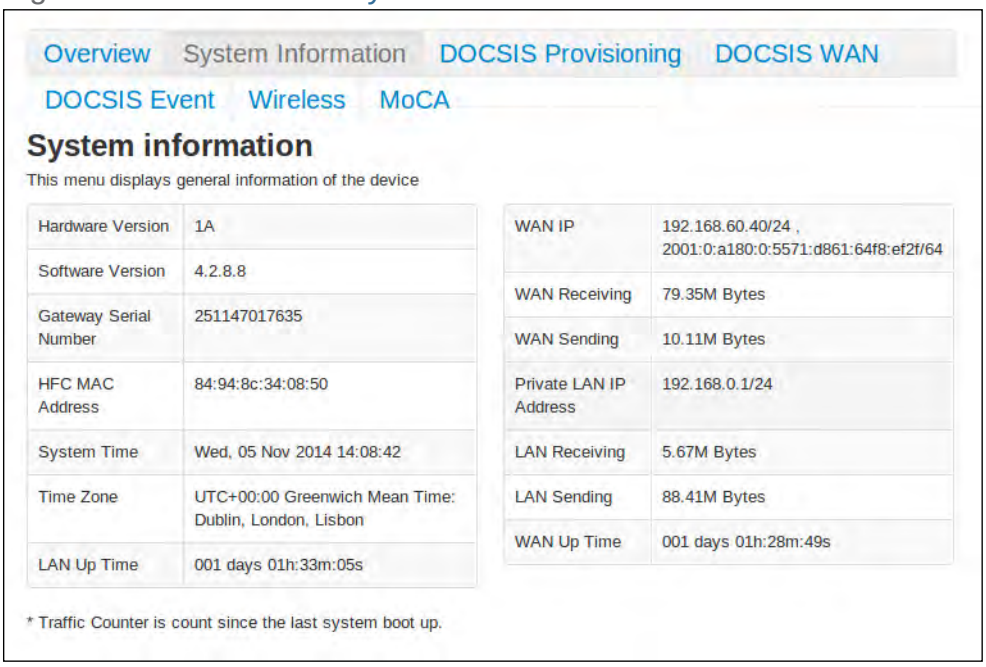
Use this screen to see general information about your CGNM/ CGNM-3552's hardware, its software, and its connection to the Internet.

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

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

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

Figure 15: The Status: System Information Screen



The following table describes the labels in this screen.

Table 12: The Status: System Information Screen

Hardware Version	This displays the version number of the CGNM/ CGNM-3552's physical hardware.
Software Version	This displays the version number of the software that controls the CGNM/ CGNM-3552.
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 CGNM/ CGNM-3552's RF module. This is the module that connects to the Internet through the **Cable** connection.
System Time	This displays the current date and time.
Time Zone	Use display the time zone when the ToD Function enabled.
LAN Up Time	This displays the time the LAN has been online.
WAN IP	This field displays the CGNM/ CGNM-3552's IP address on the WAN (Wide Area Network) interface.

Table 12: The Status: System Information Screen (continued)

WAN Receiving	This displays the number of bytes that the WAN is receiving.
WAN Sending	This displays the number of bytes that the WAN is sending.
Private LAN IP Address	Use this field to define the IP address of the CGNM/ CGNM-3552 on the LAN.
LAN Receiving	This displays the number of bytes that the LAN is receiving.
LAN Sending	This displays the number of bytes that the LAN is sending.
WAN Up Time	This displays the time the WAN has been online.

3.4 The DOCSIS Provisioning Screen

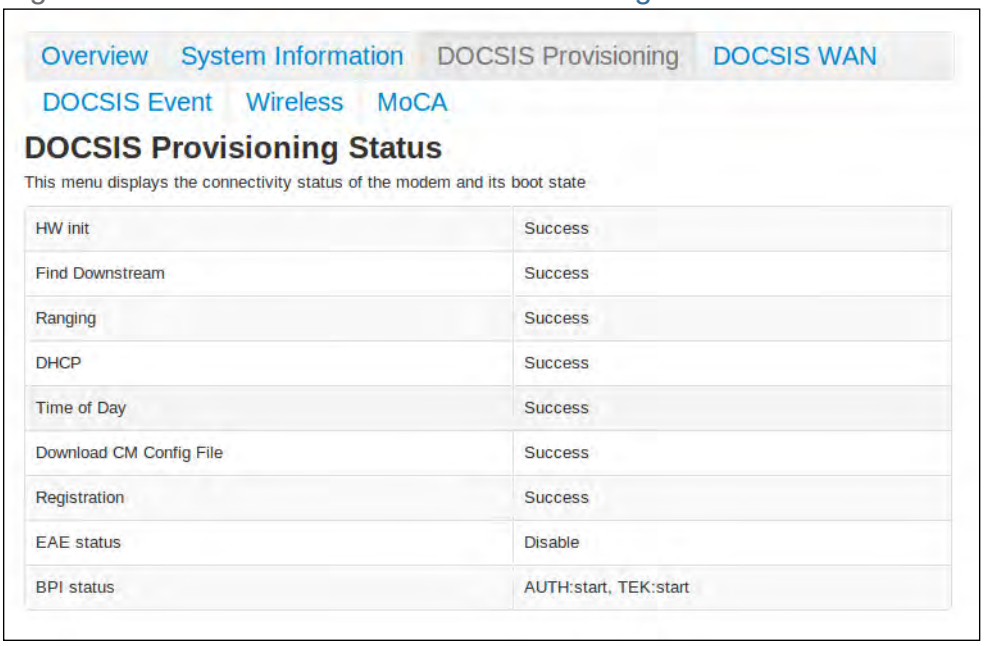
This screen displays the steps successfully taken to connect to the Internet over the **Cable** connection.

Use this screen for troubleshooting purposes to ensure that the CGNM/ CGNM-3552 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.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Figure 16: The Status: DOCSIS Provisioning Status Screen



For each step:

- **Process** displays when the CGNM/ CGNM-3552 is attempting to complete a connection step.
- **Success** displays when the CGNM/ CGNM-3552 has completed a connection step.

3.5 The DOCSIS WAN Screen

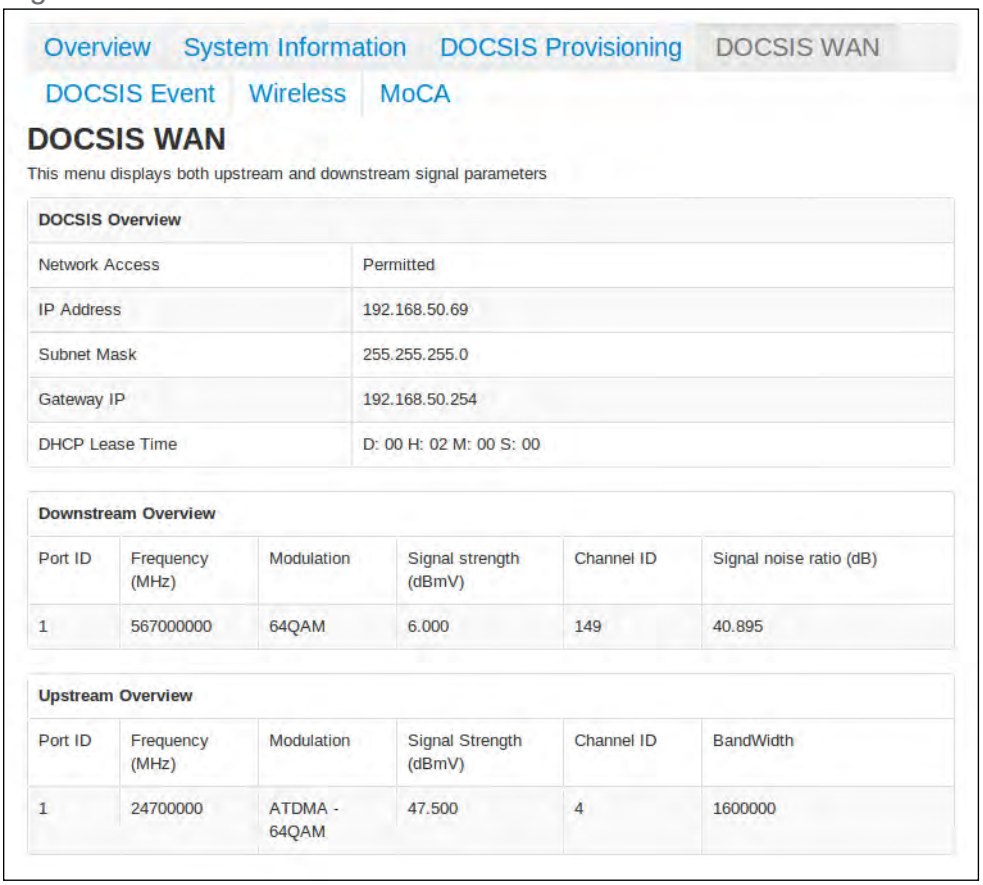
Use this screen to discover information about:

- The nature of the upstream and downstream connection between the CGNM/ CGNM-3552 and the device to which it is connected through the **CABLE** interface.
- IP details of the CGNM/ CGNM-3552's WAN connection.

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

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Figure 17: The Status: DOCSIS WAN Screen



The following table describes the labels in this screen.

Table 13: 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 CGNM/ CGNM-3552's WAN IP address. This IP address is automatically assigned to the CGNM/ CGNM-3552.
Subnet Mask	This displays the CGNM/ CGNM-3552's WAN subnet mask.
Gateway IP	This displays the IP address of the device to which the CGNM/ CGNM-3552 is connected over the **CABLE** interface.

Table 13: The Status: DOCSIS WAN Screen (continued)

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 CGNM/ CGNM-3552.	
Port ID	This displays the ID number of the downstream connection's port.
Frequency (MHz)	This displays the actual frequency in Megahertz (MHz) of each downstream data channel to which the CGNM/ CGNM-3552 is connected.
Modulation	This displays the type of modulation that each downstream channel uses.
Signal Strength (dBmV)	This displays the power of the signal of each downstream data channel to which the CGNM/ CGNM-3552 is connected, in dBmV (decibels above/below 1 millivolt).
Channel ID	This displays the ID number of each channel on which the downstream signal is transmitted.
Signal Noise Ratio (dB)	This displays the Signal to Noise Ratio (SNR) of each downstream data channel to which the CGNM/ CGNM-3552 is connected, in dB (decibels).
Upstream Overview NOTE: The upstream signal is the signal transmitted from the CGNM/ CGNM-3552.	
Port ID	This displays the ID number of the upstream connection's port.
Frequency (MHz)	This displays the actual frequency in Megahertz (MHz) of each upstream data channel to which the CGNM/ CGNM-3552 is connected.
Modulation	This displays the type of modulation that each upstream channel uses.
Signal Strength (dBmV)	This displays the power of the signal of each upstream data channel to which the CGNM/ CGNM-3552 is connected, in dBmV (decibels above/below 1 millivolt).

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 13: The Status: DOCSIS WAN Screen (continued)

Channel ID	This displays the ID number of each channel on which the upstream signal is transmitted.
BandWidth	This displays the BandWidth of each upstream channel to which the CGNM/ CGNM-3552 is connected.

3.6 The DOCSIS Event Screen

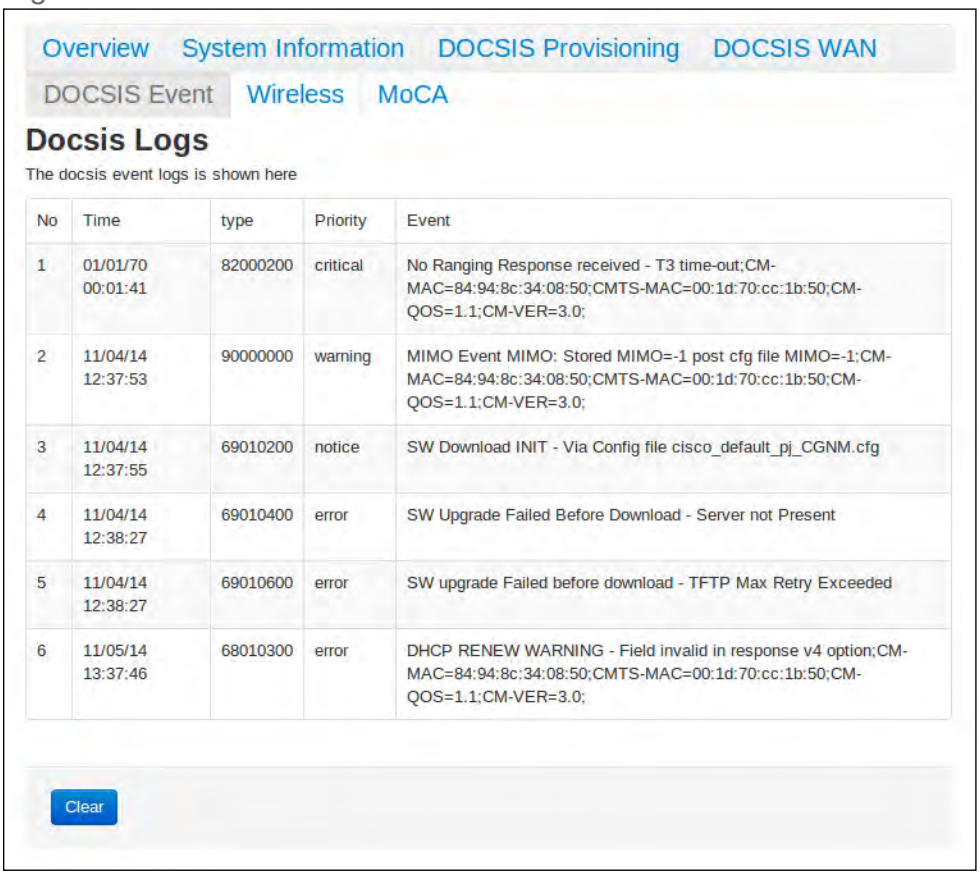
Use this screen to discover information about:

- The nature of the upstream and downstream connection between the CGNM/ CGNM-3552 and the device to which it is connected through the **CABLE** interface.
- IP details of the CGNM/ CGNM-3552's WAN connection.

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

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Figure 18: The Status: DOCSIS Event Screen



The following table describes the labels in this screen.

Table 14: The Status: DOCSIS Event Screen

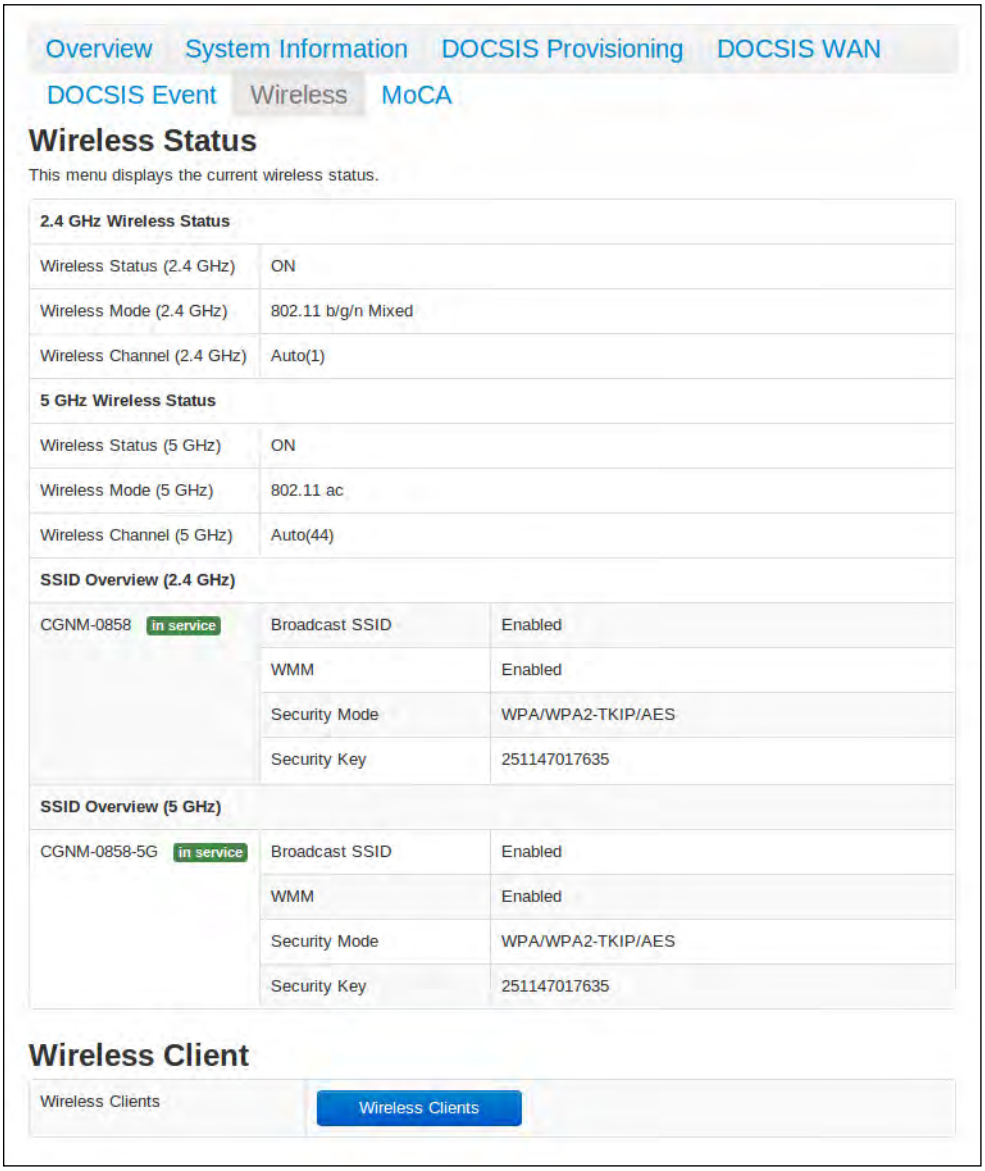
No.	This displays the arbitrary, incremental index number assigned to the DOCSIS event.
Time	This displays the time and date of the DOCSIS event.
Type	This displays the type of the DOCSIS event. NOTE: The definitions of the type of DOCSIS event follow DOCSIS's specification accordingly.
Priority	This displays the priority of the DOCSIS event. NOTE: The definitions of the priority of DOCSIS event follow DOCSIS's specification accordingly.
Event	This displays a description of the DOCSIS event.

3.7 The Wireless Screen

Use this screen to view general information about the CGNM/ CGNM-3552's WiFi-related settings. You can modify many of the fields in this screen using the **Wireless** > **Basic Setting** screen; see The Basic Settings Screen on page 80

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

Figure 19: The Status: Wireless Screen



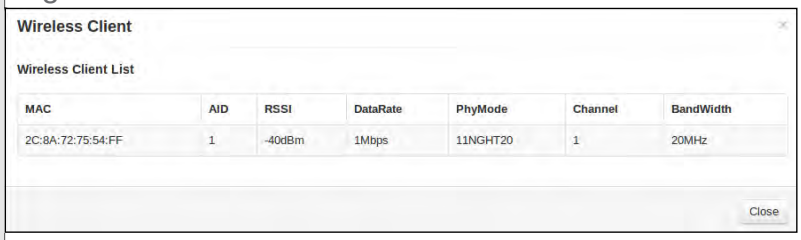
Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

The following table describes the labels in this screen.

Table 15: The Status: Wireless Status Screen

2.4GHz Wireless Status	
Wireless Status	This field displays **ON** when the CGNM/ CGNM-3552's 2.4 GHz wireless network is active, and displays **OFF** when it is inactive.
Wireless Mode	This displays the type of 2.4 GHz wireless network that the CGNM/ CGNM-3552 is using.
Wireless Channel	This displays the wireless channel on which the CGNM/ CGNM-3552's 2.4 GHz wireless network is transmitting and receiving.
5GHz Wireless Status	
Wireless Status (5GHz)	This field displays **ON** when the CGNM/ CGNM-3552's 5 GHz wireless network is active, and displays **OFF** when it is inactive.
Wireless Mode (5GHz)	This displays the type of 5 GHz wireless network that the CGNM/ CGNM-3552 is using.
Wireless Channel (5GHz)	This displays the wireless channel on which the CGNM/ CGNM-3552's 5 GHz wireless network is transmitting and receiving.
SSID Overview (2.4GHz)	
(SSID)	This displays the 2.4 GHz wireless network's Service Set Identifier. This is the name of the wireless network, to which wireless clients connect.
Broadcast SSID	This field displays **Enabled** when the 2.4 GHz wireless network's SSID is being broadcast, and displays **Disabled** when it is not.
WMM	This field displays **Enabled** when the 2.4 GHz wireless network, and displays **Disabled** when it is not.
Security Mode	This displays the type of security the CGNM/ CGNM-3552's 2.4 GHz wireless network is currently using.
Security Key	This displays the password for the CGNM/ CGNM-3552's 2.4 GHz wireless network.
SSID Overview (5GHz)	
(SSID)	This displays the 5 GHz wireless network's Service Set Identifier. This is the name of the wireless network, to which wireless clients connect.

Table 15: The Status: Wireless Status Screen (continued)

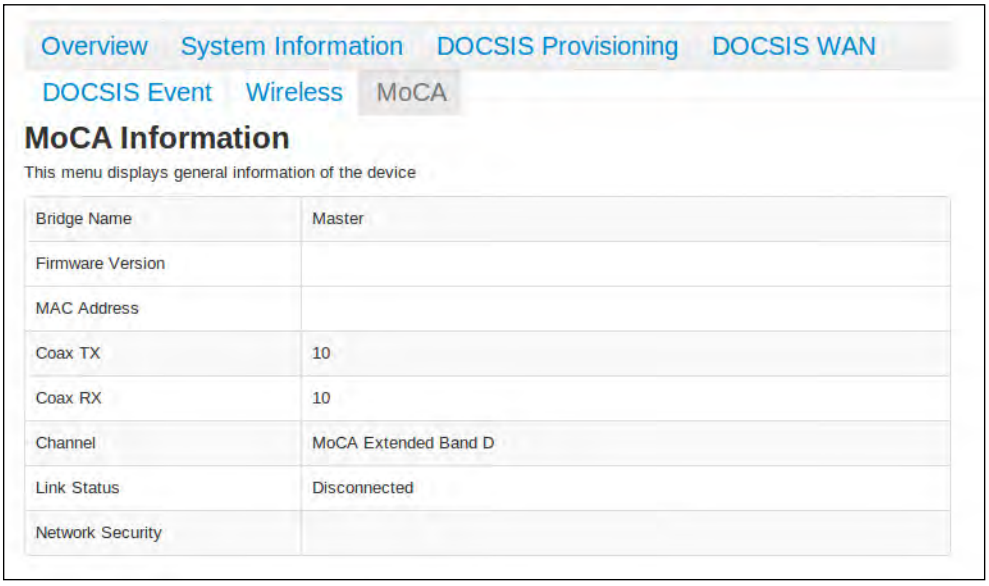
Broadcast SSID	This field displays **Enabled** when the 5 GHz wireless network's SSID is being broadcast, and displays **Disabled** when it is not.
WMM	This field displays **Enabled** when the 5 GHz wireless network, and displays **Disabled** when it is not.
Security Mode	This displays the type of security the CGNM/ CGNM-3552's 5 GHz wireless network is currently using.
Security Key	This displays the password for the CGNM/ CGNM-3552's 5 GHz wireless network.
Wireless Client	This displays the wireless client of the CGNM/ CGNM-3552's wireless network. Figure 20: Wireless Client List 
MAC	This displays the MAC (Media Access Control) address of each wireless client connected to the device's wireless network.
AID	This displays the AID (Association ID) of each wireless client connected to the device's wireless network.
RSSI	This field display the Received Signal Strength Indication from each wireless client connected to the device's wireless network.
DateRate	This displays the transfer speed of each wireless client connected to the device's wireless network.
PhyMode	This displays the Physical Mode (IEEE 802.11a,b,g or n) of each wireless client connected to the device's wireless network.
Channel	This displays the wireless channel on which the device is connected.
BandWidth	This displays the bandwidth (20/40MHz) of each wireless client connected to the device's wireless network.

3.8 The MoCA Screen

Use this screen to view general information about the CGNM/ CGNM-3552's MoCA-related settings. You can modify many of the fields in this screen using the **Basic** > **MoCA** screen; see The MoCA Screen on page 72

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

Figure 21: The Status: MoCA Information Screen



The following table describes the labels in this screen.

Table 16: The Status: MoCA Information Screen

Bridge Name	This displays the name of this CGNM/ CGNM-3552 in your MoCA network. Each CGNM/ CGNM-3552 receives an individual, unique bridge name.
Firmware Version	This displays the version number of the firmware currently running on your CGNM/ CGNM-3552's MoCA module
IP Address	This displays the IP address of the CGNM/ CGNM-3552's MoCA module, which is visible to devices accessing the CGNM/ CGNM-3552 via the Ethernet ports.

MAC Address	This displays the MAC address of the CGNM/ CGNM-3552's MoCA module, which is visible to devices accessing the CGNM/ CGNM-3552 via the Ethernet ports.
Coax TX	This displays the transmission (TX) power of the CGNM/ CGNM-3552 on the cable network, from **0** (extremely weak) to **10** (extremely strong).
Coax RX	This displays the strength of the signal that the CGNM/ CGNM-3552 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 CGNM/ CGNM-3552 is transmitting and receiving over the cable network. The channel number displays, followed by the channel's frequency in MHz.
Link Status	This displays whether or not the CGNM/ CGNM-3552 is connected over the cable network.
Network Security	This displays the type of security that the cable network is using (56-bit DES or 128-bit AES).

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

4

Basic

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

- Basic Overview on page 1
- The LAN Setup Screen on page 3
- The Gateway Function Screen on page 6
- The Port Forwarding Screen on page 7
- The Port Triggering Screen on page 11
- The DMZ Screen on page 14
- The DNS Screen on page 16
- The MoCA Screen on page 17

4.1 Basic Overview

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

4.1.1 WAN and LAN

A Local Area Network (LAN) is a network of computers and other devices that usually occupies a small physical area (a single building, for example). Your CGNM/ CGNM-3552's LAN consists of all the computers and other networking devices connected to the **LAN 1~4** ports. This is your private network (in routing mode - see Routing Mode on page 6).

The LAN is a separate network from the Wide Area Network (WAN). In the case of the CGNM/ CGNM-3552, the WAN refers to all computers and other devices available on the cable connection.

By default, computers on the WAN cannot identify individual computers on the LAN; they can see only the CGNM/ CGNM-3552. The CGNM/ CGNM-3552 handles routing to and from individual computers on the LAN.

4.1.2 LAN IP Addresses and Subnets

IP addresses on the LAN are controlled either by the CGNM/ CGNM-3552's built-in DHCP server (see The LAN Setup Screen on page 51), or by you (when you manually assign IP addresses to your computers).

For more information about IP addresses and subnets in general, see The LAN Setup Screen on page 51.

4.1.3 DNS and Domain Suffix

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

Similarly, the CGNM/ CGNM-3552 allows you to define a **Domain Suffix** to the LAN. When you enter the domain suffix into your browser, you can reach the CGNM/ CGNM-3552 no matter what IP address it has on the LAN.

4.1.4 Debugging (Ping and Traceroute)

The CGNM/ CGNM-3552 provides a couple of tools to allow you to perform network diagnostics on the LAN:

- Ping: this tool allows you to enter an IP address and see if a computer (or other network device) responds with that address on the network. The name comes from the pulse that submarine SONAR emits when scanning for underwater objects, since the process is rather similar. You can use this tool to see if an IP address is in use, or to discover if a device (whose IP address you know) is working properly.

- Traceroute: this tool allows you to see the route taken by data packets to get from the CGNM/ CGNM-3552 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.

4.1.5 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 CGNM/ CGNM-3552 receives incoming traffic from the WAN with a destination port that matches a port forwarding rule, it forwards the traffic to the LAN IP address and port number specified in the port forwarding rule.

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

4.1.6 Port Triggering

Port triggering is a means of automating port forwarding. The CGNM/ CGNM-3552 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 CGNM/ CGNM-3552 automatically opens the incoming ports specified in the rule, in anticipation of incoming traffic.

4.1.7 DMZ

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

4.2 The LAN Setup Screen

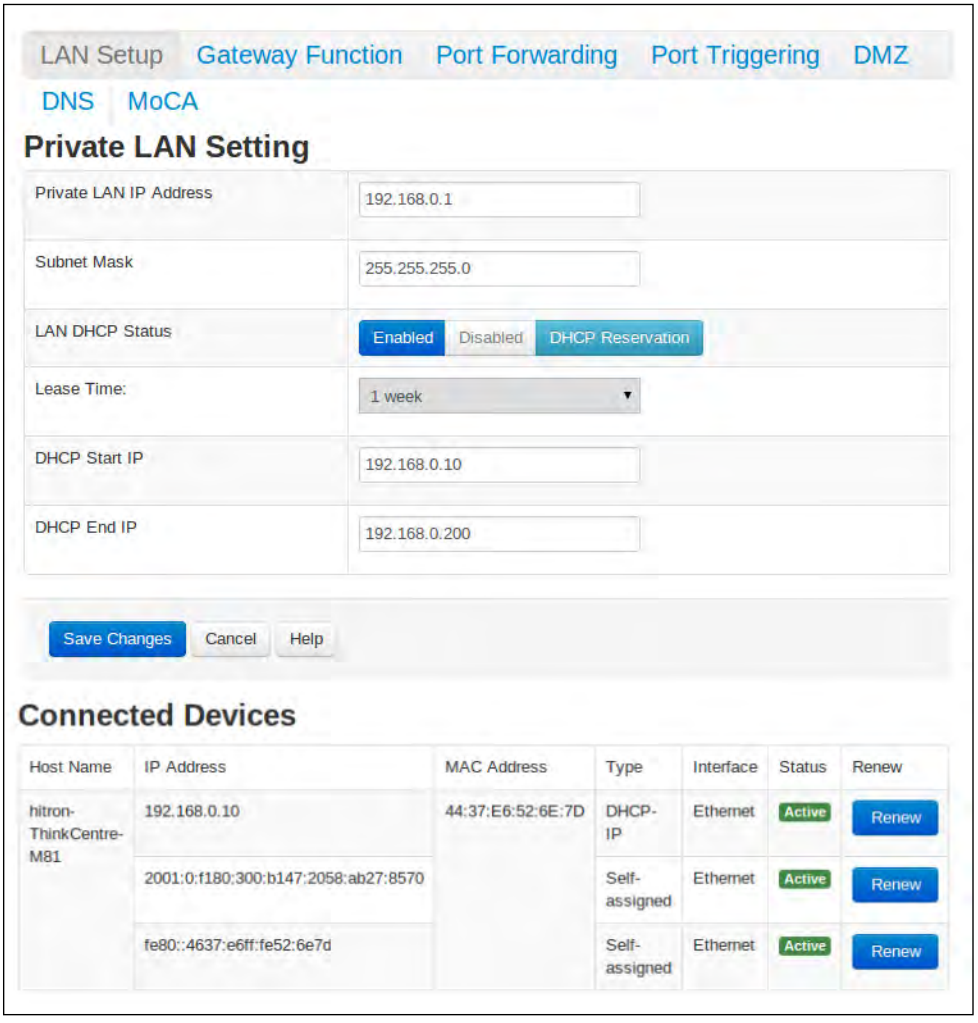
Use this screen to:

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

- View information about the CGNM/ CGNM-3552's connection to the WAN
- Configure the CGNM/ CGNM-3552's LAN IP address, subnet mask and domain suffix
- Configure the CGNM/ CGNM-3552's internal DHCP server
- Define how the CGNM/ CGNM-3552 assigns IP addresses on the LAN
- See information about the network devices connected to the CGNM/ CGNM-3552 on the LAN.

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

Figure 22: The Basic: LAN Setup Screen



The following table describes the labels in this screen.

Table 17: The Basic: LAN Setup Screen

Private LAN Setting	
Private LAN IP Address	Use this field to define the IP address of the CGNM/ CGNM-3552 on the LAN.
Subnet Mask	Use this field to define the LAN subnet. Use dotted decimal notation (for example, **255.255.255.0**).
LAN DHCP Status	Use this field to configure whether or not the CGNM/ CGNM-3552's DHCP server is active. ▸ To turn the DHCP server on, click **Enabled**. ▸ To turn the DHCP server off, click **Disabled**.
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.
DHCP Start IP	Use this field to specify the IP address at which the CGNM/ CGNM-3552 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 CGNM/ CGNM-3552 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 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 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 17: The Basic: LAN Setup Screen (continued)

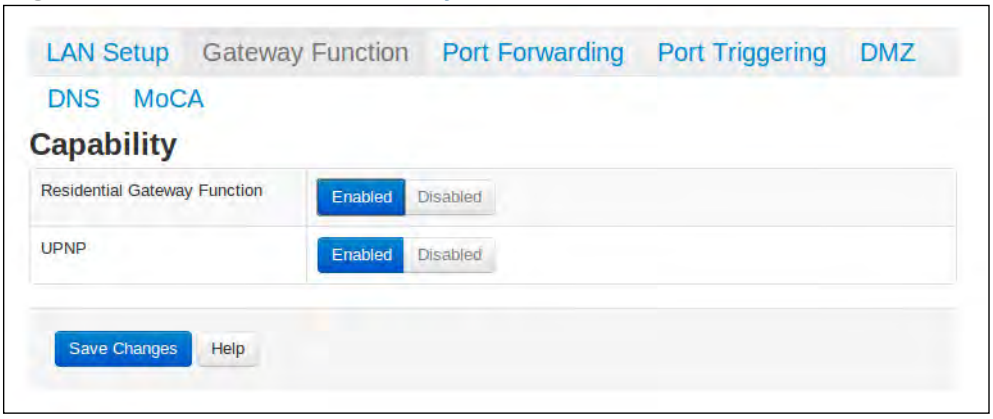
Type	This displays whether the device's IP address was assigned by DHCP (**DHCP-IP**), or **self-assigned**.
Interface	This displays whether the device is connected on the LAN (**Ethernet**) or the WLAN (**Wireless(x)**, where **x** denotes the wireless mode; **b**, **g** or **n**).
Status	This displays Active when a device is connected.
Renew	Click this to obtain the connected device's information again.

4.3 The Gateway Function Screen

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

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

Figure 23: The Basic: Gateway Function Screen



The following table describes the labels in this screen.

Table 18: The Basic: Gateway Function Screen

Residential Gateway Function	Use this field to turn gateway function on or off. ▸ Select **Enabled** to turn gateway function on. ▸ Select **Disabled** to turn gateway function off.
UPNP	Use this field to turn UPNP on or off. ▸ Select **Enabled** to turn UPNP on. ▸ Select **Disabled** to turn UPNP off.

Table 18: The Basic: Gateway Function Screen (continued)

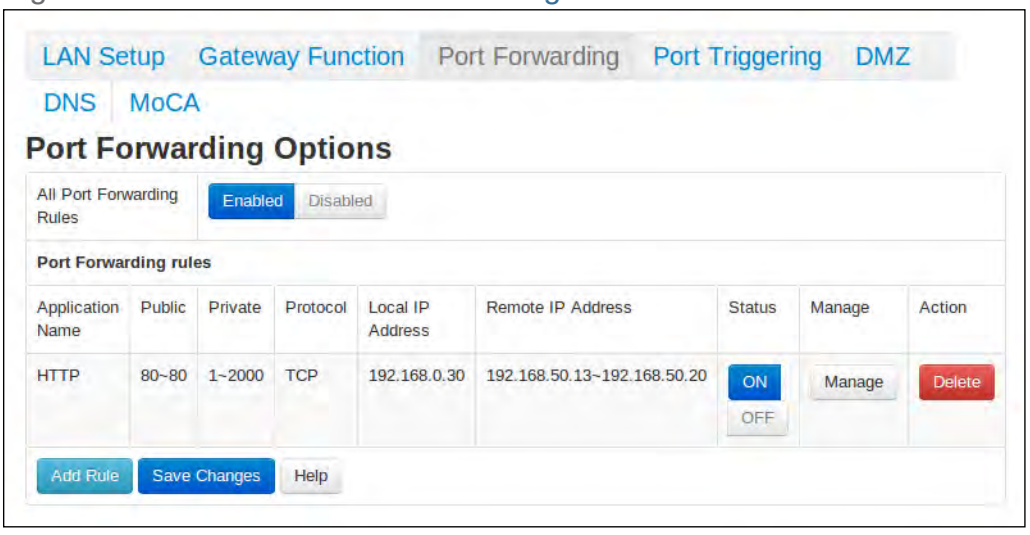
Save Changes	Click this to save your changes to the fields in this screen.
Help	Click this to see information about the fields in this screen.

4.4 The Port Forwarding 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 Forwarding**. The following screen displays.

Figure 24: The Basic: Port Forwarding Screen



The following table describes the labels in this screen.

Table 19: The Basic: Port Forwarding Screen

All Port Forwarding Rules	Use this field to turn port forwarding on or off. ▸ Select **Enabled** to turn all port forwarding rules on. ▸ Select **Disabled** to turn all port forwarding rules off.
Port Forwarding Rules	
Application Name	This displays the name you assigned to the rule when you created it.
Public	This field displays the incoming port range. These are the ports on which the CGNM/ CGNM-3552 received traffic from the originating host on the WAN.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 19: The Basic: Port Forwarding Screen (continued)

Private	This field displays the port range to which the CGNM/ CGNM-3552 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 rule's conditions is forwarded.
Remote IP Address	This displays the IP address range on the WAN from which traffic is forwarded (if configured).
Status	Use this field to turn port forwarding rule on or off.
Manage	Use this field to **Edit** a port forwarding rule. Port forwarding must first be set to **Enabled**. See Adding or Editing a Port Forwarding Rule on page 8 for information on the screen that displays.
Action	Use this field to **Delete** a port forwarding rule. The deleted rule's information cannot be retrieved.
Add Rule	Click this to define a new port forwarding rule. Port forwarding must first be set to **Enabled**. See Adding or Editing a Port Forwarding Rule on page 8 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.

4.4.1 Adding or Editing a Port Forwarding Rule

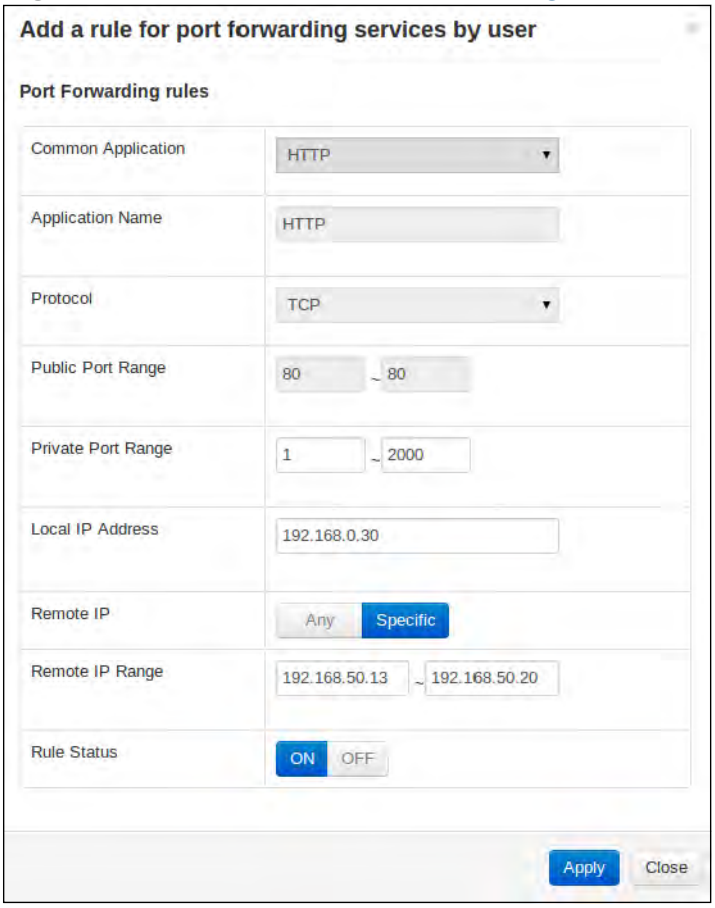
- To add a new port forwarding rule, click **Add Rule** in the **Basic** > **Port Forwarding** screen.
- To edit an existing port forwarding rule, click **Manage** in the **Basic** > **Port Forwarding** screen.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

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 25: The Basic: Port Forwarding Add/Edit Screen



The following table describes the labels in this screen.

Table 20: 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 20: The Basic: Port Forwarding Add/Edit Screen

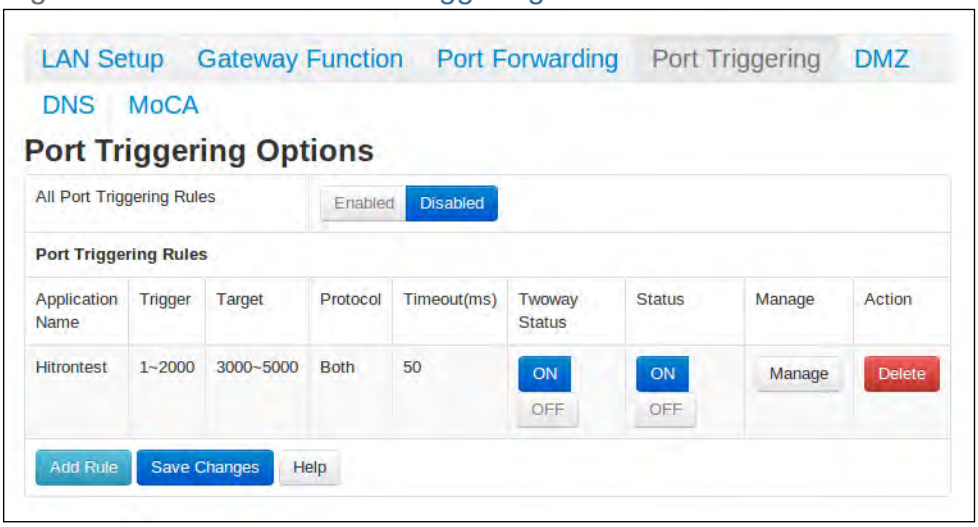
Protocol	Use this field to specify whether the CGNM/ CGNM-3552 should forward traffic via: ▸ Transmission Control Protocol (**TCP**) ▸ User Datagram Protocol (**UDP**) ▸ Transmission Control Protocol and User Datagram Protocol (**TCP/UDP**) ▸ Generic Routing Encapsulation (**GRE**) ▸ Encapsulating Security 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 CGNM/ CGNM-3552 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 CGNM/ CGNM-3552 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	Use this field to configure the IP address range on the WAN from which traffic is forwarded.
Remote IP Range	
Rule Status	Use this field to turn port forwarding rule on or off.
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 port forwarding rule.

4.5 The Port Triggering Screen

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

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

Figure 26: The Basic: Port Triggering Screen



The following table describes the labels in this screen.

Table 21: The Basic: Port Triggering Screen

All Port Triggering Rules	Use this field to turn all port triggering rules on or off. ▸ Select **Enabled** to turn all port triggering rules on. ▸ Select **Disabled** to turn all port triggering rules off.
Port Triggering Rules	
Application Name	This displays the arbitrary name you assigned to the rule when you created it.
Trigger	This displays the range of outgoing ports. When the CGNM/ CGNM-3552 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 CGNM/ CGNM-3552 detects activity on the **Trigger** ports from computers on the LAN.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 21: 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 CGNM/ CGNM-3552 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	Use this field to **Edit** a port triggering rule.
Action	Use this field to **Delete** a port triggering rule.
Add Rule	Click this to define a new port triggering rule. Port triggering must first be set to **Enabled**. See Adding or Editing a Port Triggering Rule on page 12 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.

4.5.1 Adding or Editing a Port Triggering Rule

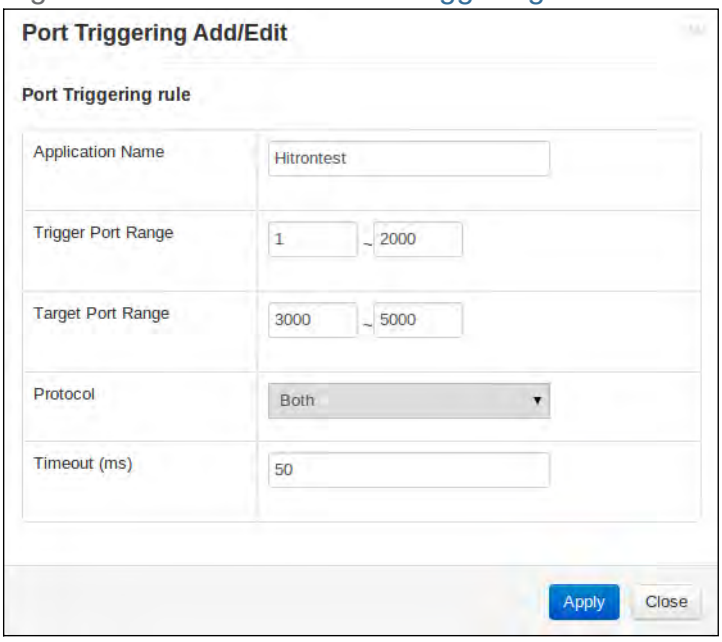
- To add a new port triggering rule, click **Add Rule** in the **Basic** > **Port Triggering** screen.
- To edit an existing port triggering rule, click **Manage** in the **Basic** > **Port Triggering** screen.

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 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Figure 27: The Basic: Port Triggering Add/Edit Screen



The following table describes the labels in this screen.

Table 22: 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 CGNM/ CGNM-3552 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.

Table 22: The Basic: Port Triggering Add/Edit Screen

Target Port Range	Use these fields to specify the target ports. The CGNM/ CGNM-3552 opens these ports in expectation of incoming traffic whenever it detects activity on any of the **Trigger** ports. The incoming traffic is forwarded to these ports on the computer connected to the LAN. Enter the start port number in the first field, and the end port number in the second field. To specify only a single port, enter its number in both fields.
Protocol	Use this field to specify whether the CGNM/ CGNM-3552 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 CGNM/ CGNM-3552 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 screen without saving your changes to the port forwarding rule.

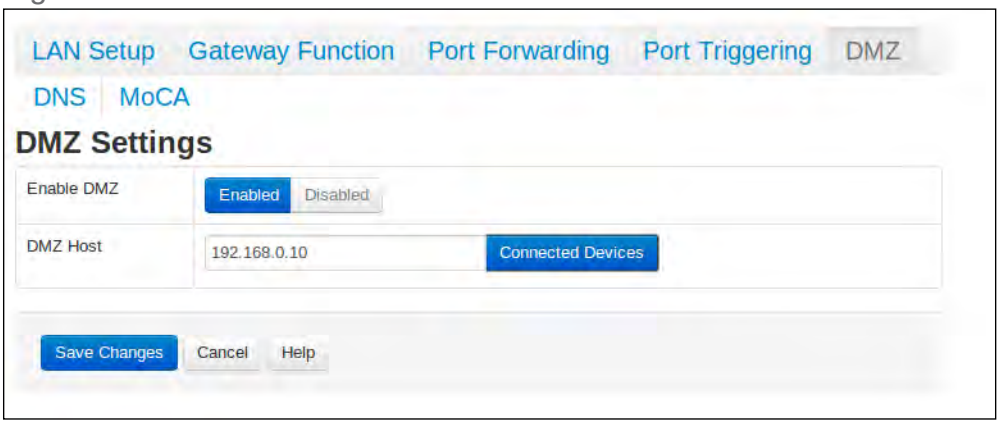
4.6 The DMZ Screen

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

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

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

Figure 28: The Basic: DMZ Screen



The following table describes the labels in this screen.

Table 23: 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 CGNM/ CGNM-3552 on the LAN. Figure 29: Connected Device Info
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.

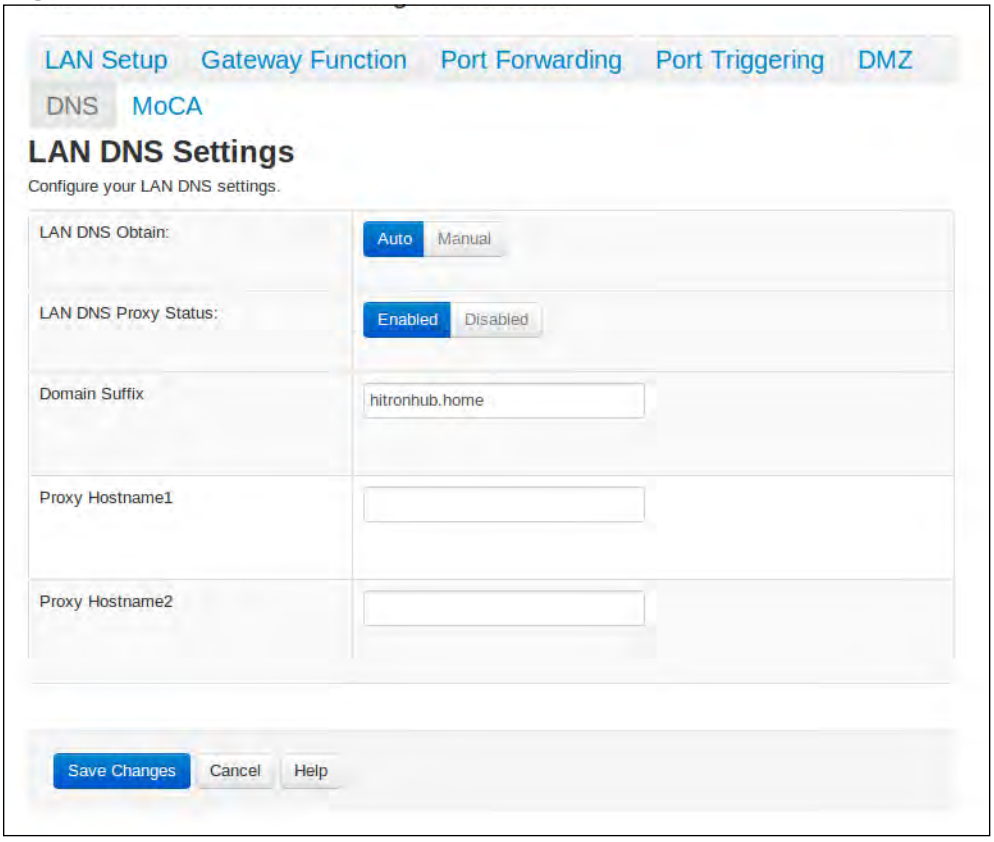
Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

4.7 The DNS Screen

Use this screen to configure your LAN DNS settings.

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

Figure 30: The Basic: DNS Screen



The following table describes the labels in this screen.

Table 24: The Basic: DNS Screen

LAN DNS Obtain	Use this field to obtain the DNS automatically or manually. ▸ Select **Auto** to obtain the DNS automatically. ▸ Select **Manual** to obtain the DNS manually.
LAN DNS Proxy Status	Use this field to turn the DNS Proxy on or off. ▸ Select **Enabled** to turn the DNS Proxy on. ▸ Select **Disabled** to turn the DNS Proxy off.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 24: 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 CGNM/ CGNM-3552 on the LAN.
Proxy Hostname1	Enter the Hostname of the computer that you want to add to the DNS manually.
Proxy Hostname2	Enter the Hostname of the computer that you want to add to the DNS manually.
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.

4.8 The MoCA Screen

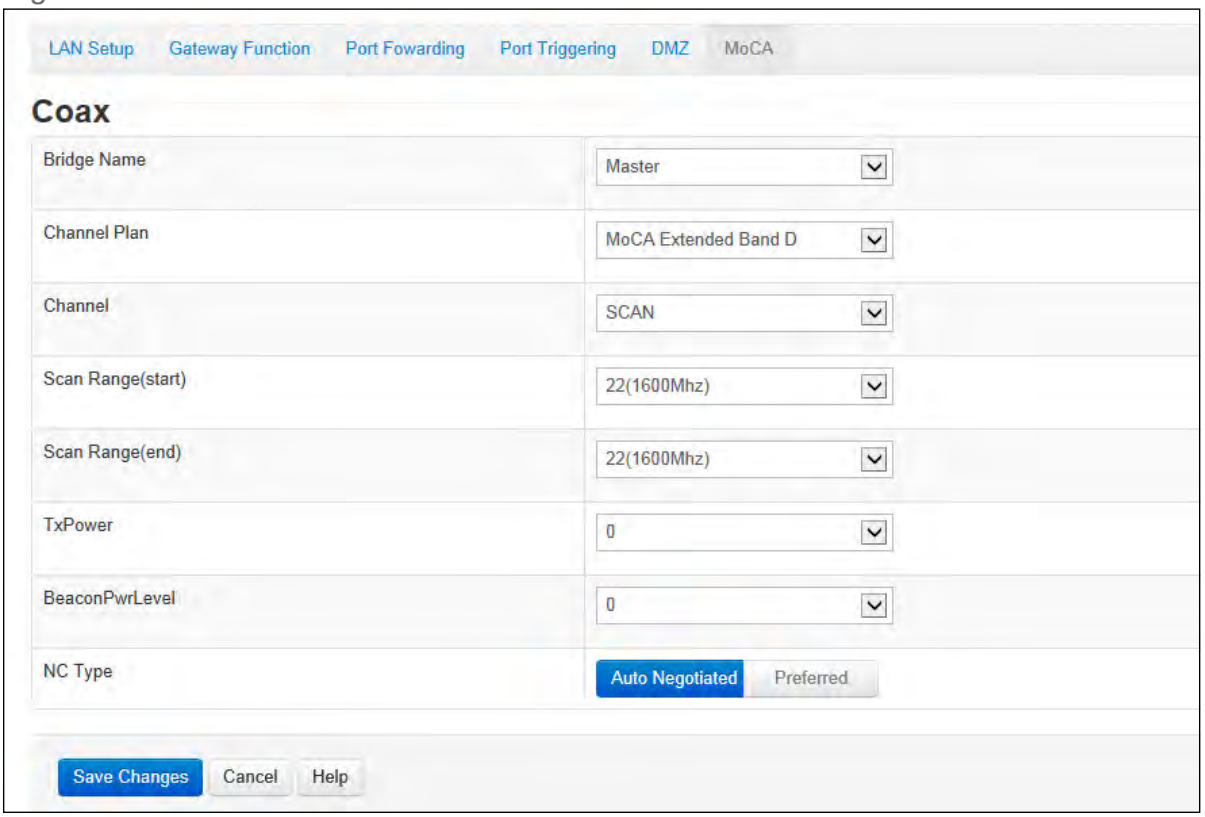
Use this screen to view and make changes to the CGNM/ CGNM-3552's cable network settings.

NOTE: Do not change any of the settings in this screen unless you have a good reason to do so!

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

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

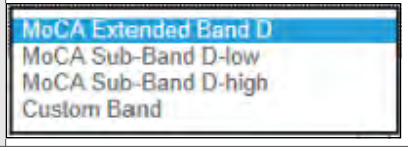
Figure 31: The Basic: MoCA Screen



Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

The following table describes the labels in this screen.

Table 25: The Basic: MoCA Screen

Bridge Name	Use this field to modify the name of the CGNM/ CGNM-3552 on the network. This allows you to identify the specific device by the room in which it is installed when you assign a unique Bridge Name to each device on the MoCA network. Select the room type from the drop-down list. Figure 32: Bridge Name Options
Channel Plan	The MoCA specification defines several channel plans for communication on the cable network (see The Multimedia over Coax Alliance on page 8). This field allows you to select the channel plan that you want the CGNM/ CGNM-3552 to use. Select the channel plan that you wish to use from the dropdown list. Figure 33: Channel Plan 

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 25: The Basic: MoCA Screen (continued)

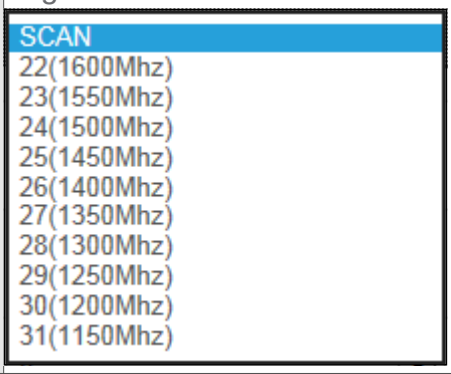
Channel	Use this field to define the channel on which you want the CGNM/ CGNM-3552 to communicate on the cable network, dependent on the **Channel Plan** that you selected. Select the channel plan that you wish to use from the dropdown list. If you select SCAN, ensure that you also configure the **Scan Range (Start)** and **Scan Range (End)** fields. Figure 34: Channel 
Scan Range (Start)	If you selected **SCAN** in the **Channel** field, use this field to select a channel at which the CGNM/ CGNM-3552 should start scanning for a connection on the cable network.
Scan Range (End)	If you selected **SCAN** in the **Channel** field, use this field to select a channel at which the CGNM/ CGNM-3552 should stop scanning for a connection on the cable network.
TxPower	Use this field to set the power at which the CGNM/ CGNM-3552 transmits (TX) over the cable network, from **0** to **10**.

Table 25: The Basic: MoCA Screen (continued)

BeaconPwLevel	Use this field to set the CGNM/ CGNM-3552's beacon power on the cable network, from **0** to **10**. The MoCA beacon allows other devices on the cable network to detect the CGNM/ CGNM-3552.
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 CGNM/ CGNM-3552 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 CGNM/ CGNM-3552 to the preferred group.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

5

Wireless

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

- Wireless Overview on page 1
- The Basic Settings Screen on page 4
- The Access Control Screen on page 15

5.1 Wireless Overview

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

5.1.1 Wireless Networking Basics

Your CGNM/ CGNM-3552'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 CGNM/ CGNM-3552 and the other computers and devices that connect to it.

5.1.2 Architecture

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

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

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

The CGNM/ CGNM-3552 is the access point, and the computers you connect to the CGNM/ CGNM-3552 are the wireless clients.

5.1.3 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 CGNM/ CGNM-3552 supports the following (in order of adoption - old to new - and data transfer speeds - low to high):

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

5.1.4 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 CGNM/ CGNM-3552 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 2.0, 07/2015. Copyright © 2015 Hitron Technologies

5.1.5 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 CGNM/ CGNM-3552 supports the following wireless security protocols (in order of effectiveness):

- **WEP** (the Wired Equivalency Protocol): this protocol uses a series of "keys" or data strings to authenticate the wireless client with the AP, and to encrypt data sent over the wireless link. WEP is a deprecated protocol, and should only be used when it is the only security standard supported by the wireless clients. WEP provides only a nominal level of security, since widely-available software exists that can break it in a matter of minutes.
- **WPA-PSK** (WiFi Protected Access - Pre-Shared Key): WPA was created to solve the inadequacies of WEP. There are two types of WPA: the "enterprise" version (known simply as WPA) requires the use of a central authentication database server, whereas the "personal" version (supported by the CGNM/ CGNM-3552) 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.

5.1.5.1 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 CGNM/ CGNM-3552 provides two methods of WPS authentication:

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

- **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.

5.1.6 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.

5.2 The Basic Settings Screen

Use this screen to configure your CGNM/ CGNM-3552's basic 2.4GHz and 5GHz wireless settings. You can turn the wireless modules on or off, select the wireless mode and channel, and configure the wireless networks' SSID settings.

The CGNM/ CGNM-3552 has separate concurrent dual band 2.4GHz and 5GHz wireless networks:

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

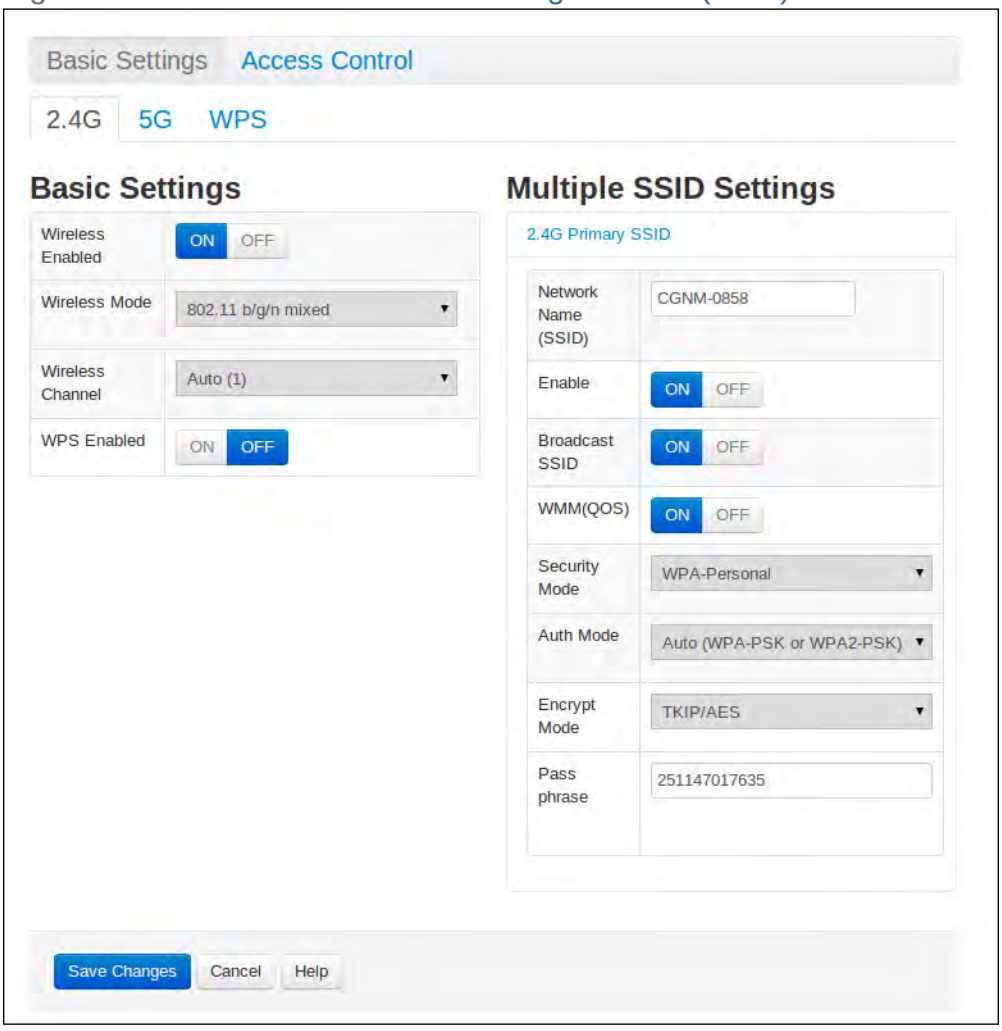
- To configure the CGNM/ CGNM-3552's 2.4GHz wireless network, click **Wireless** > **Basic Settings**, then click the **2.4G** tab. See 2.4G Settings on page 5 for information on the screen that displays.
- To configure the CGNM/ CGNM-3552's 5GHz wireless network, click **Wireless** > **Basic Settings**, then click the **5G** tab. See 5G Settings on page 9 for information on the screen that displays.

5.2.1 2.4G Settings

Use this screen to configure the CGNM/ CGNM-3552's 2.4GHz wireless network.

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

Figure 35: The Wireless: Basic Settings Screen (2.4G)



Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

The following table describes the labels in this screen.

Table 26: The Wireless: Basic Settings Screen (2.4G)

Basic Settings	
Wireless Enabled	Use this field to turn the 2.4GHz wireless network on or off. ▸ Select **ON** to enable the wireless network. ▸ Select **OFF** to disable the wireless network.
Wireless Mode	Select the type of 2.4GHz wireless network that you want to use: ▸ **802.11 B/G Mixed**: use IEEE 802.11b and 802.11n ▸ **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** (default).
Wireless Channel	Select the 2.4GHz wireless channel that you want to use, or select **Auto** to have the CGNM/ CGNM-3552 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. ▸ Deselect **OFF** to disable WPS.
Multiple SSID Settings	
Primary SSID	Click this to view settings for the main 2.4GHz SSID.
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.

Table 26: The Wireless: Basic Settings Screen (2.4G) (continued)

Enable	Use this field to enable or disable the SSID. ▸ Select **ON** to enable the SSID. ▸ Deselect **OFF** to disable the SSID.
Broadcast SSID	Use this field to make this SSID visible or invisible to other wireless devices. ▸ Select **ON** if you want your network name (SSID) to be public. Anyone with a wireless device in the coverage area can discover the SSID, and attempt to connect to the network. ▸ Select **OFF** if you do not want the CGNM/ CGNM-3552 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)	Use this field to apply WiFi MultiMedia (WMM) Quality of Service (QoS) settings to this SSID. ▸ Select **ON** to enable WMM QoS on this SSID. ▸ Select **OFF** to disable WMM QoS on this SSID.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 26: The Wireless: Basic Settings Screen (2.4G) (continued)

Security Mode	Select the type of security that you want to use. ▸ Select **Open** 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** to use the WiFi Protected Access (Personal) security protocol. ▸ Select **WPA2** to use the WiFi Protected Access 2 (Personal) security protocol. ▸ Select **WPA/WPA2** 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. 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 one of the **WPA** options.
Auth Mode	Select the type of security authentication the device should use.
Encryption Mode	Select the type of encryption you want to use. The options that display depend on the **Security Mode** you selected. **WEP**: ▸ Select **WEP64** to use a ten-digit security key. ▸ Select **WEP128** to use a twenty-six-digit security key. **WPA**, **WPA2** and **WPA/WPA2**: ▸ 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 CGNM/ CGNM-3552.

Table 26: The Wireless: Basic Settings Screen (2.4G) (continued)

Pass Phrase	Enter the security key or password that you want to use for your wireless network. You will need to enter this key into your wireless clients in order to allow them to connect to the network.
Save Changes	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

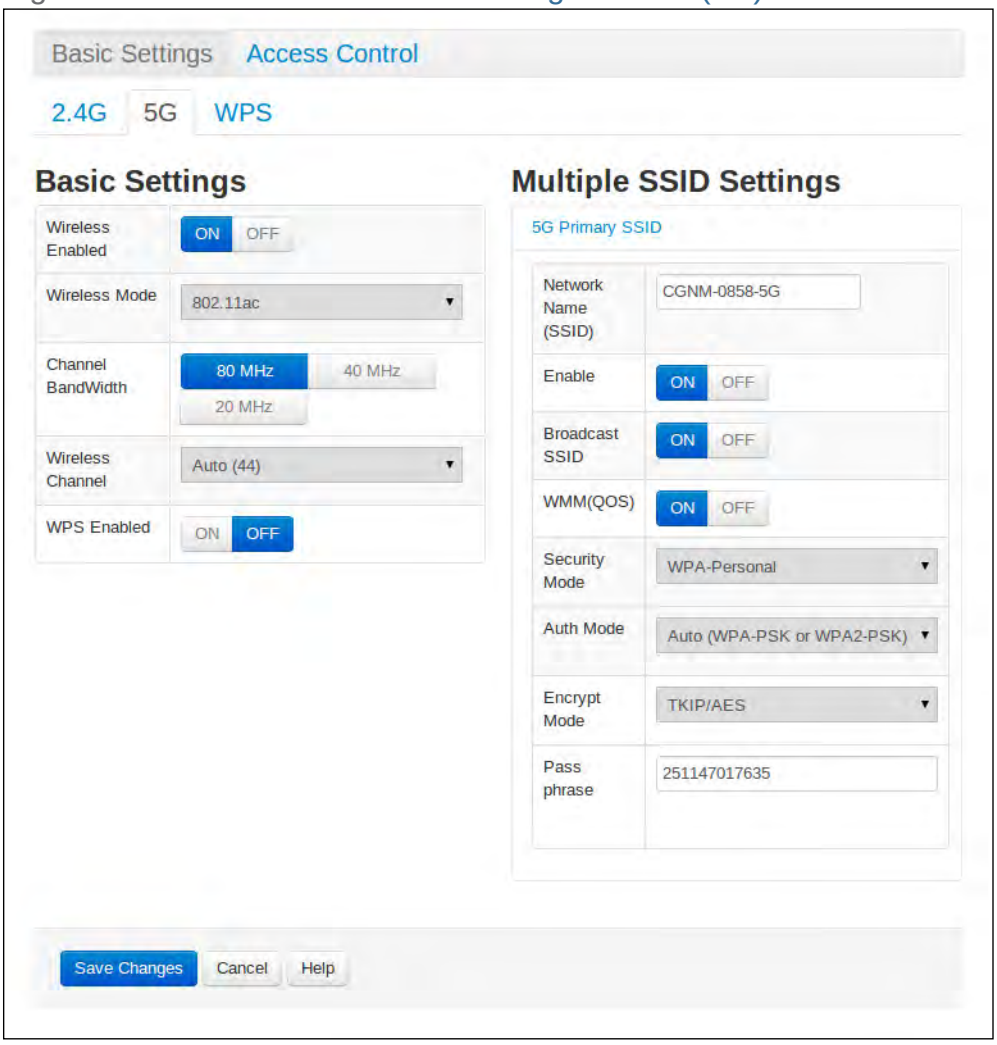
5.2.2 5G Settings

Use this screen to configure the CGNM/ CGNM-3552's 5GHz wireless network.

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

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Figure 36: The Wireless: Basic Settings Screen (5G)



The following table describes the labels in this screen.

Table 27: The Wireless: Basic Settings Screen (5G)

Basic Settings	
Wireless Enabled	Use this field to turn the 5GHz wireless network on or off. ▸ Select **ON** to enable the wireless network. ▸ Select **OFF** to disable the wireless network.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 27: The Wireless: Basic Settings Screen (5G) (continued)

Wireless Mode	Select the type of 5GHz wireless network that you want to use: ▸ **802.11n 5g**: use IEEE 802.11n 5GHz. NOTE: At the time of writing IEEE 802.11n is the only 5GHz network type available. NOTE: Only wireless clients that support the network protocol you select can connect to the wireless network.
Channel Bandwidth	Select the 5GHz wireless channel bandwidth that you want to use.
Wireless Channel	Select the 5GHz wireless channel that you want to use, or select **Auto** to have the CGNM/ CGNM-3552 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. ▸ Deselect **OFF** to disable WPS.
Multiple SSID Settings	
Multiple SSID	Click this to view settings for the main 5GHz SSID.
Network Name (SSID)	Enter the name that you want to use for this SSID. This is the name that identifies your network, and to which wireless clients connect. NOTE: It is suggested that you change the SSID from its default, for security reasons.
Enable	Use this field to enable or disable the SSID. ▸ Select **ON** to enable the SSID. ▸ Deselect **OFF** to disable the SSID.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 27: The Wireless: Basic Settings Screen (5G) (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 CGNM/ CGNM-3552 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)	Use this field to apply WiFi MultiMedia (WMM) Quality of Service (QoS) settings to this SSID. ▸ Select **ON** to enable WMM QoS on this SSID. ▸ Select **OFF** to disable WMM QoS on this SSID.
Security Mode	Select the type of security that you want to use. ▸ Select **Open** 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** to use the WiFi Protected Access (Personal) security protocol. ▸ Select **WPA2** to use the WiFi Protected Access 2 (Personal) security protocol. ▸ Select **WPA/WPA2** 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. 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 one of the **WPA** options.
Auth Mode	Select the type of security authentication the device should use.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 27: The Wireless: Basic Settings Screen (5G) (continued)

Encryption Mode	Select the type of encryption you want to use. The options that display depend on the **Security Mode** you selected. **WEP**: ▸ Select **WEP64** to use a ten-digit security key. ▸ Select **WEP128** to use a twenty-six-digit security key. **WPA**, **WPA2** and **WPA/WPA2**: ▸ 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 CGNM/ CGNM-3552.
Pass Phrase	Enter the security key or password that you want to use for your wireless network. You will need to enter this key into your wireless clients in order to allow them to connect to the network.
Save Changes	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

5.2.3 WPS

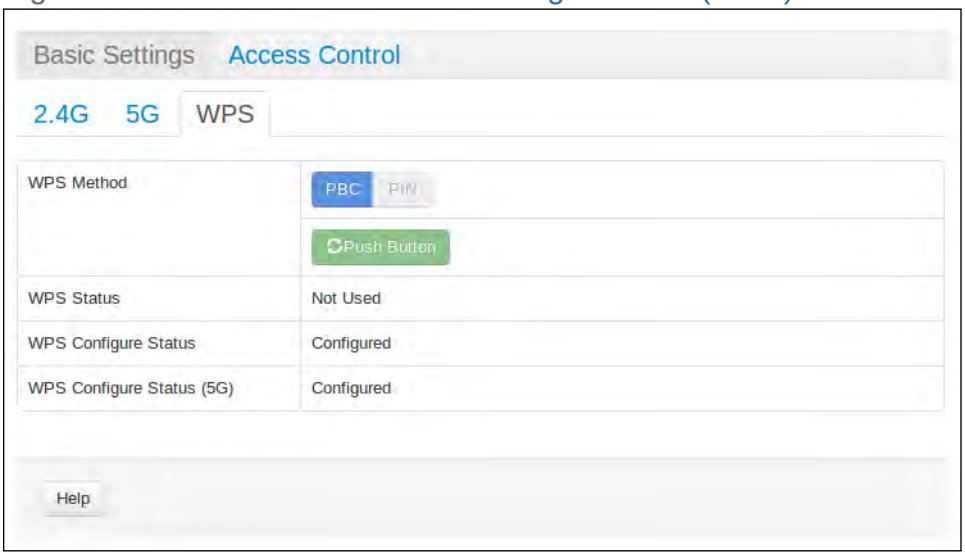
Use this screen to manage WiFi Protected Setup (WPS).

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

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

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Figure 37: The Wireless: Basic Settings Screen (WPS)



The following table describes the labels in this screen.

Table 28: The Wireless: Basic Settings Screen (WPS)

WPS Settings	
WPS Method	Use these buttons to run WiFi Protected Setup (WPS): ▸ Click the **PBC** button and then **Push Button** to begin the Push-Button Configuration process. You must then press the PBC button on your client wireless devices within two minutes in order to register them on your wireless network. ▸ Click the **PIN** button to begin the PIN configuration process. In the screen that displays, enter the WPS PIN that you want to use for the CGNM/ CGNM-3552, or the WPS PIN of the client device you want to add to the network.
WPS Status	This displays whether or not the CGNM/ CGNM-3552 is using WiFi Protected Setup.
WPS Configure Status	This displays the WiFi Protected Setup configuration for the wireless network.
WPS Configure Status (5G)	This displays the WiFi Protected Setup configuration for the 5G wireless network.
Help	Click this to see information about the fields in this screen.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

5.3 The Access Control Screen

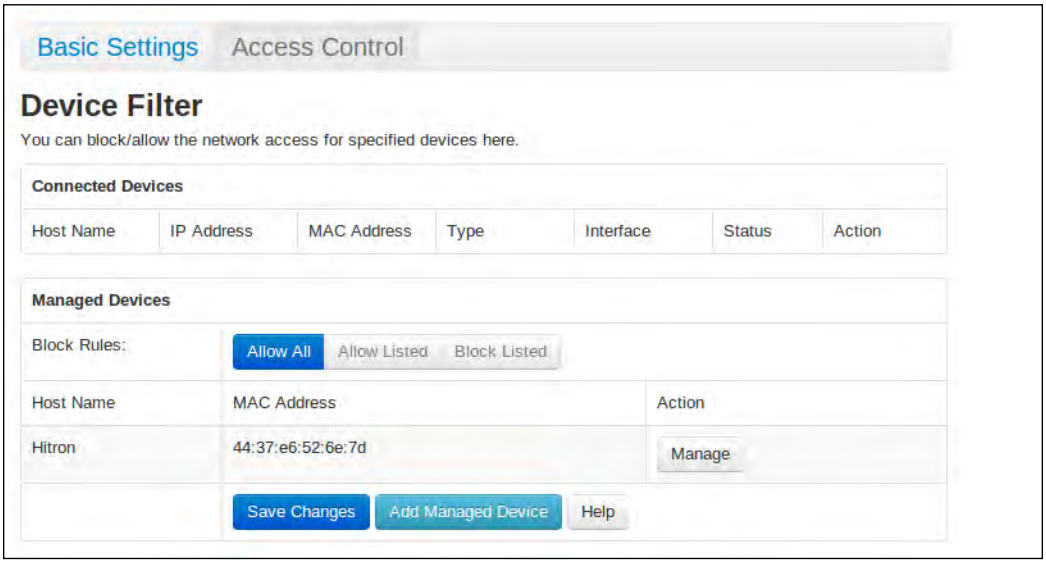
Use this screen to configure Media Access Control (MAC) address filtering on the wireless network.

NOTE: To configure MAC address filtering on the wired LAN, see The Device Filter Screen on page 100.

You can set the CGNM/ CGNM-3552 to allow only certain devices to access the CGNM/ CGNM-3552 and the network wirelessly, or to deny certain devices access.

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

Figure 38: The Wireless: Access Control Screen



The following table describes the labels in this screen.

Table 29: The Wireless: Access Control Screen

Connected Devices	
Host Name	This displays the name of each network device that has connected to the CGNM/ CGNM-3552 on the wireless network.
IP Address	This displays the IP address of each network device that has connected to the CGNM/ CGNM-3552 on the wireless network.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 29: The Wireless: Access Control Screen (continued)

MAC Address	This displays the MAC address of each network device that has connected to the CGNM/ CGNM-3552 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 if the device filter is active or not.
Action	Click **Manage** to make changes to the device's filtering status; see Adding or Editing a Managed Device on page 17 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 **Devices** list and let all devices connect wirelessly to the CGNM/ CGNM-3552. ▸ Select **Allow** to permit only devices you added to the **Devices** list to access the CGNM/ CGNM-3552 and the network wirelessly. All other devices are denied access. ▸ Select **Deny** to permit all devices except those you added to the **Devices** list to access the CGNM/ CGNM-3552 and the network wirelessly. The specified devices are denied access.
Host Name	This field displays the name of the wireless device.
MAC Address	This field displays the device's MAC (Media Access Control) address.
Action	Click **Manage** to make changes to the device's filtering status; see Adding or Editing a Managed Device on page 17 for information on the screen that displays.
Save Changes	Click this to save your changes to the fields in this screen.
Add Managed Device	Click this to add a new service filtering rule (see Adding or Editing a Managed Device on page 17).
Help	Click this to see information about the fields in this screen.

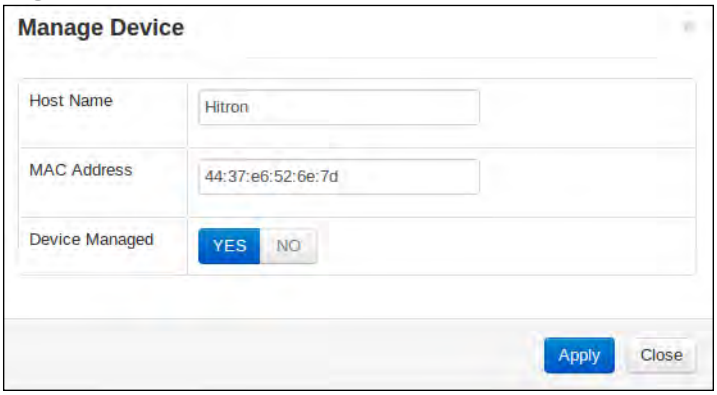
Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

5.3.1 Adding or Editing a Managed Device

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

The following screen displays.

Figure 39: The Wireless: Access Control Add/Edit Screen



The following table describes the labels in this screen.

Table 30: The Wireless: Access Control Add/Edit Screen

Host Name	Enter the name of the wireless device.
MAC Address	Enter the device's MAC (Media Access Control) address.
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.
Apply	Click this to save your changes to the fields in this screen.
Close	Click this to return to the **Wireless Access Control** screen without saving your changes to the rule.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

6

Admin

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

- Admin Overview on page 1
- The Management Screen on page 2
- The Remote Management Screen on page 3
- The Diagnostics Screen on page 5
- The Backup Screen on page 6
- The USB Storage Screen on page 7
- The Device Reset Screen on page 8

6.1 Admin Overview

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

6.1.1 Debugging (Ping and Traceroute)

The CGNM/ CGNM-3552 provides a couple of tools to allow you to perform network diagnostics on the LAN:

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

- Ping: this tool allows you to enter an IP address and see if a computer (or other network device) responds with that address on the network. The name comes from the pulse that submarine SONAR emits when scanning for underwater objects, since the process is rather similar. You can use this tool to see if an IP address is in use, or to discover if a device (whose IP address you know) is working properly.
- Traceroute: this tool allows you to see the route taken by data packets to get from the CGNM/ CGNM-3552 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.

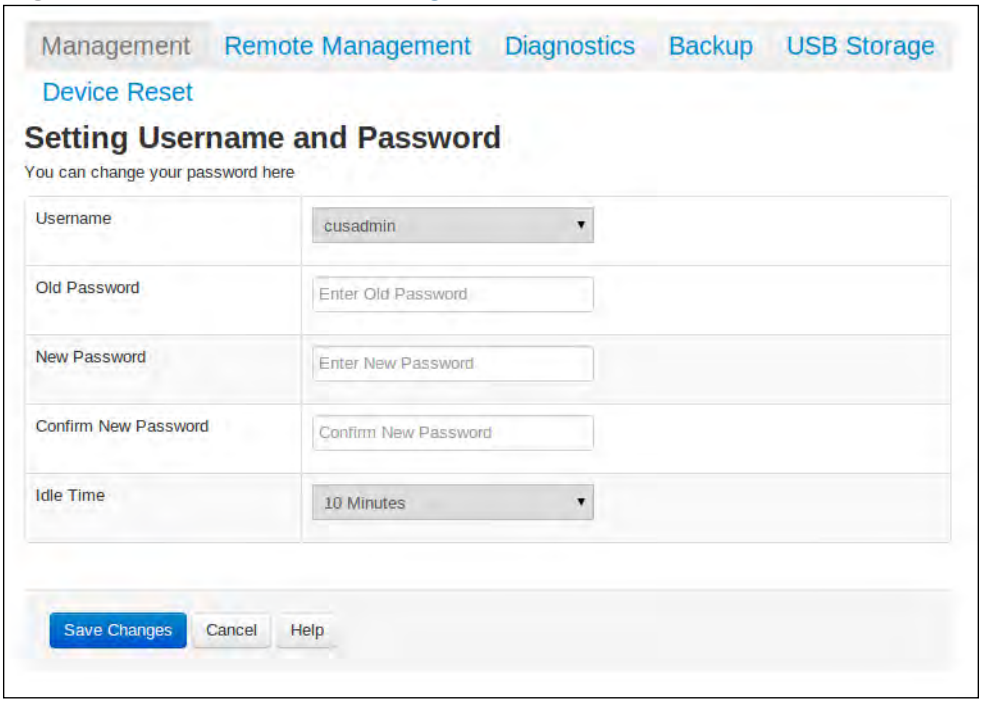
6.2 The Management Screen

Use this screen to make changes to the CGNM/ CGNM-3552's login credentials (username and password).

NOTE: If you forget your password, you will need to reset the CGNM/ CGNM-3552 to its factory defaults.

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

Figure 40: The Admin: Management Screen



The following table describes the labels in this screen.

Table 31: The Admin: Management Screen

Username	If your CGNM/ CGNM-3552 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 CGNM/ CGNM-3552 for this account.
New Password	Enter and re-enter the password you want to use to log into the CGNM/ CGNM-3552 for this account.
Confirm New Password	
Idle Time	Use this to set your CGNM/ CGNM-3552's idle time
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.

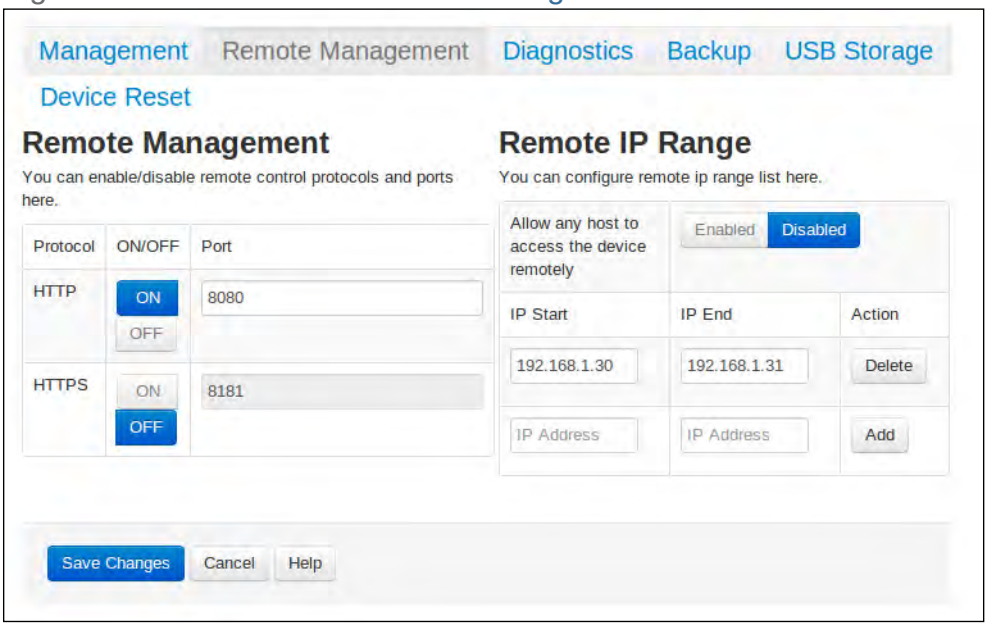
6.3 The Remote Management Screen

Use this screen to back up your CGNM/ CGNM-3552's settings to your computer, to load settings from a backup you created earlier, to reboot your CGNM/ CGNM-3552, or to return it to its factory default settings.

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

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Figure 41: The Admin: Remote Management Screen



The following table describes the labels in this screen.

Table 32: The Admin: Remote Management Screen

Remote Management	
Protocol	Use this field to enable/disable remote control protocols and ports on CGNM. ▸ HyperText Transfer Protocol (**HTTP**) ▸ HyperText Transfer Protocol Secure (**HTTPS**) ▸ **Telnet**
ON/OFF	Use this field to enable/disable each protocol.
Port	Use this field to specify which port to use with each protocol.
Remote IP Range	
Remote Range Allow All	This function allows you to grant access to a certain range of IP addresses or all IP addresses.
IP Start	Use this field to enter the start IP.
IP End	Use this field to enter the end IP.
Action	Use this field to **Delete** a port forwarding rule. The deleted rule's information cannot be retrieved.
Save Changes	Click this to save your changes to the fields in this screen.

Table 32: The Admin: Remote Management Screen (continued)

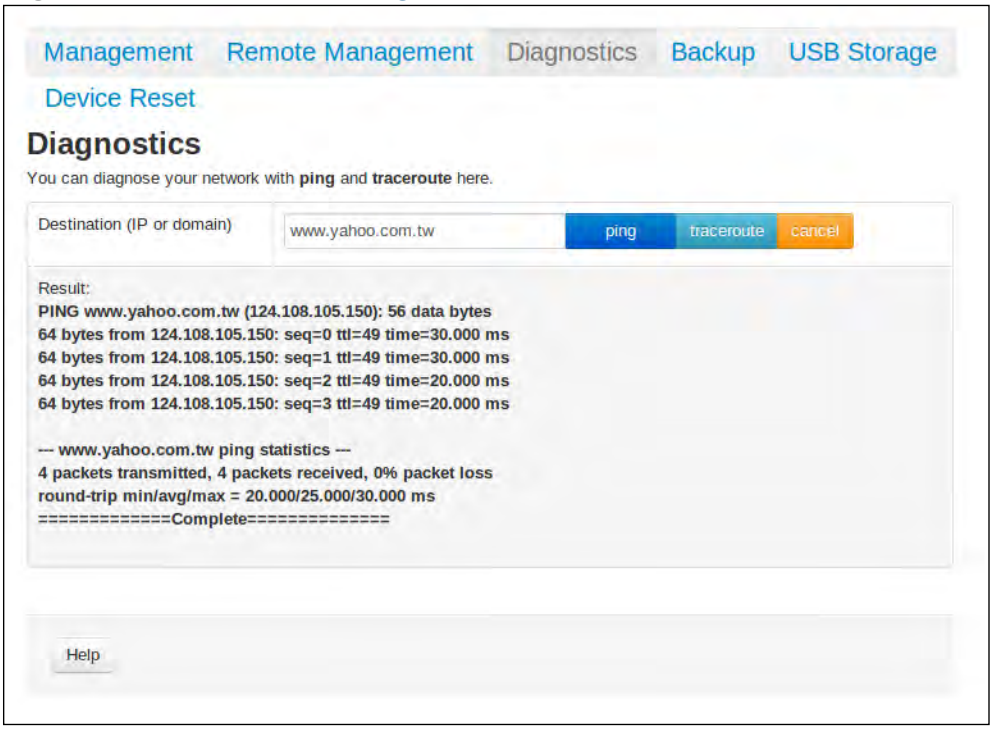
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

6.4 The Diagnostics Screen

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

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

Figure 42: The Admin: Diagnostics Screen



The following table describes the labels in this screen.

Table 33: 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	

Table 33: The Admin: Diagnostics Screen (continued)

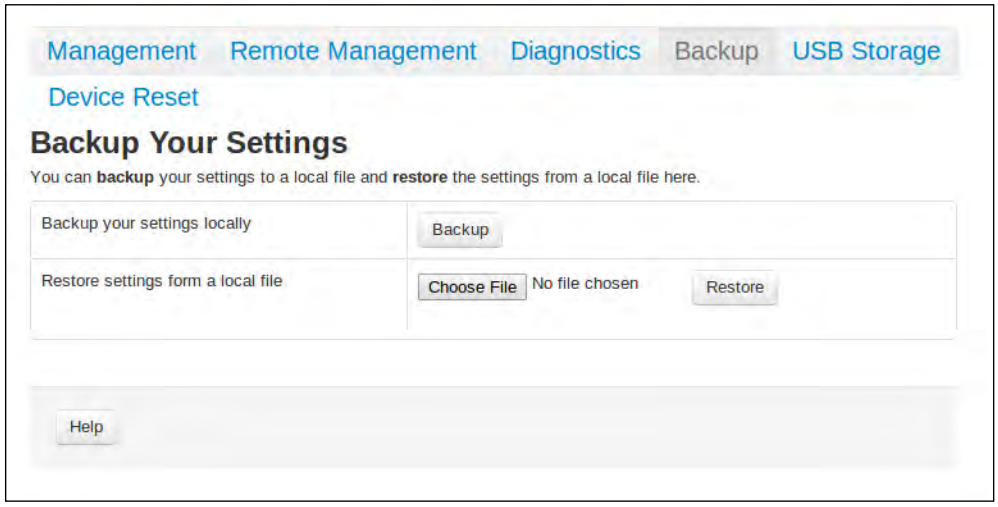
Result	This field displays a report of the test most recently performed.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

6.5 The Backup Screen

Use this screen to back up your CGNM/ CGNM-3552's settings to your computer, to load settings from a backup you created earlier, to reboot your CGNM/ CGNM-3552, or to return it to its factory default settings.

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

Figure 43: The Admin: Backup Screen



The following table describes the labels in this screen.

Table 34: The Admin: Backup Screen

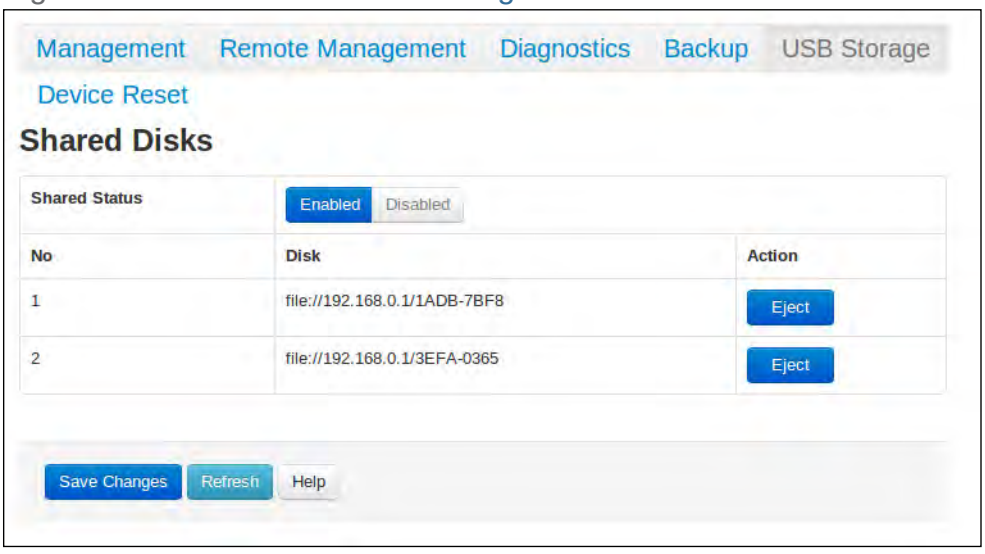
Back Up Your Settings Locally	Click this to create a backup of all your CGNM/ CGNM-3552's settings on your computer.
Restore Settings From a Local File	Use these fields to return your CGNM/ CGNM-3552's settings to those specified in a backup that you created earlier. Click **Browse** to select a backup, then click **Restore** to return your CGNM/ CGNM-3552's settings to those specified in the backup.
Reboot Device	Click **Reboot** to restart your CGNM/ CGNM-3552.
Restore Factory Default Settings	Click **Factory** to return your CGNM/ CGNM-3552 to its factory default settings. When you do this, all your user-configured settings are lost, and cannot be retrieved.

6.6 The USB Storage Screen

Use this screen to configure your CGNM/ CGNM-3552's USB settings.

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

Figure 44: The Admin: USB Storage Screen



Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

The following table describes the labels in this screen.

Table 35: 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.

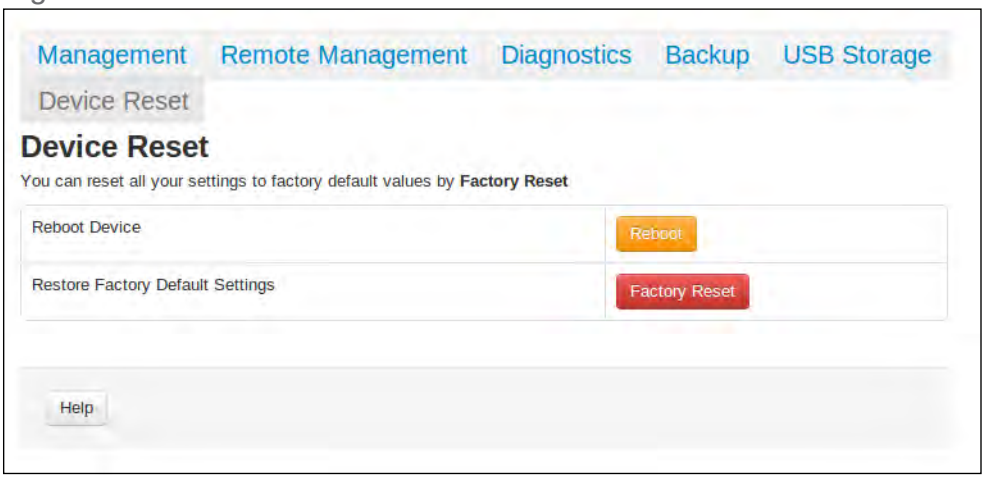
6.7 The Device Reset Screen

Use this screen to back up your CGNM/ CGNM-3552's settings to your computer, to load settings from a backup you created earlier, to reboot your CGNM/ CGNM-3552, or to return it to its factory default settings.

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

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Figure 45: The Admin: Device Reset Screen



The following table describes the labels in this screen.

Table 36: The Admin: Device Reset Screen

Reboot Device	Click **Reboot** to restart your CGNM/ CGNM-3552.
Restore Factory Default Settings	Click **Factory Reset** to return your CGNM/ CGNM-3552 to its factory default settings. When you do this, all your user-configured settings are lost, and cannot be retrieved.
Help	Click this to see information about the fields in this screen.

7

Security

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

- Security Overview on page 1
- The Firewall Screen on page 2
- The Service Filter Screen on page 5
- The Device Filter Screen on page 10
- The Keyword Filter Screen on page 14

7.1 Security Overview

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

7.1.1 Firewall

The term "firewall" comes from a construction technique designed to prevent the spread of fire from one room to another. Similarly, your CGNM/ CGNM-3552'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 2.0, 07/2015. Copyright © 2015 Hitron Technologies

7.1.2 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 CGNM/ CGNM-3552'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 CGNM/ CGNM-3552 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).

7.1.3 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.

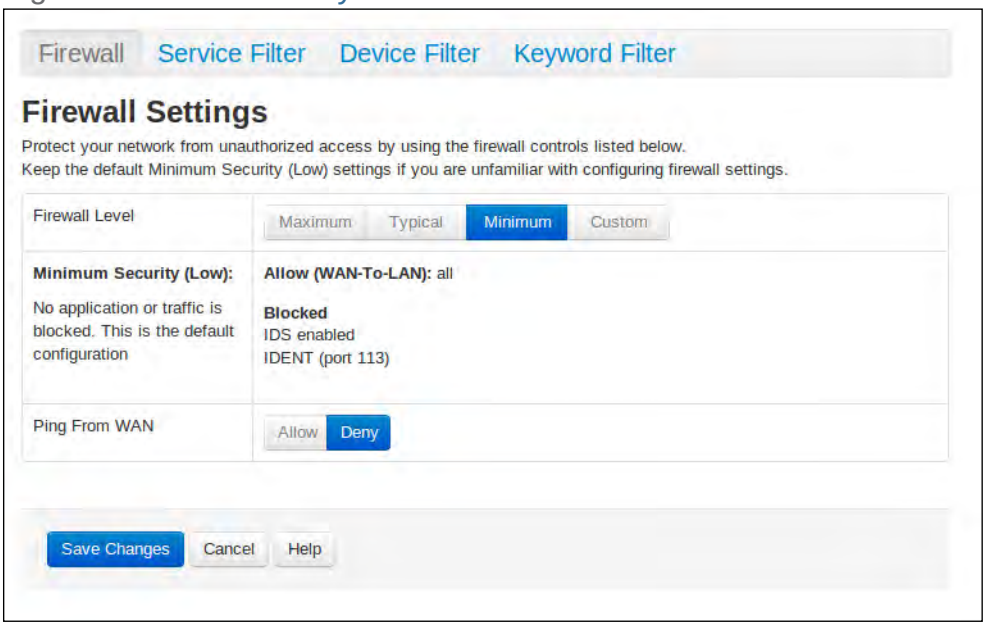
7.2 The Firewall Screen

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

NOTE: To block specific ports, use the Service Filter screen (see The Service Filter Screen on page 5).

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

Figure 46: The Security: Firewall Screen



Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

The following table describes the labels in this screen.

Table 37: The Security: Firewall Screen

Firewall Level	Select the level of firewall protection that you want to apply to your LAN. Details about the protection level display beneath the buttons.
(Security Level)	These fields describe the specific protocols and applications that are permitted or denied by the firewall security level you select. When you select **Custom** in the **Firewall Level** field, additional fields display that allow you to toggle specific features on or off: ▸ **Entire Firewall**: select **ON** to enable firewall security protection, or select **OFF** to disable it (not recommended). ▸ **HTTP**: use this field to **Allow** or **Deny** HyperText Transfer Protocol traffic. ▸ **ICMP**: use this field to **Allow** or **Deny** Internet Control Message Protocol traffic. ▸ **Multicast**: use this field to **Allow** or **Deny** multicast traffic (sent to multiple devices at once). ▸ **P2P**: use this field to **Allow** or **Deny** peer-to-peer traffic (such as BitTorrent). ▸ **Ident**: use this field to **Allow** or **Deny** Identification protocol traffic. The Identification protocol allows remote hosts to request identifying information about users of a device.
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.

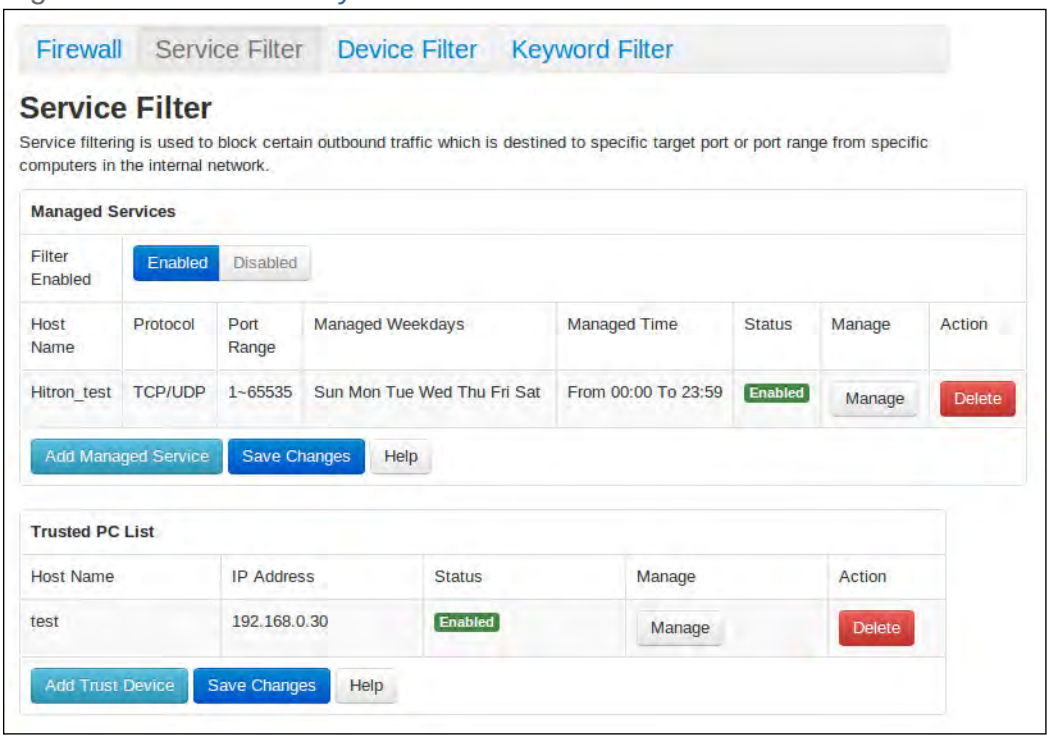
Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

7.3 The Service Filter Screen

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

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

Figure 47: The Security: Service Filter Screen



The following table describes the labels in this screen.

Table 38: 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.
Host Name	This displays the name you assigned to the filtering rule when you created it.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

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

Protocol	This field displays the protocol or protocols to which this filtering rule applies: ▸ Transmission Control Protocol (**TCP**) ▸ User Datagram Protocol (**UDP**)
Port Range	This displays the start and end port for which this filtering rule applies.
Managed Weekdays	This displays the days of the week on which this rule applies.
Managed Time	This displays the start (**From**) and end (**To**) of the time period during which this rule applies, on the specified **Managed Weekdays**.
Status	This displays the status of a service filter rule.
Manage	Click **Manage** to make changes to a port blocking rule (see Adding or Editing a Service Filter Rule on page 7).
Action	Click **Delete** to remove the existing service filter from the list. NOTE: The deleted rule's information cannot be retrieved.
Add Managed Service	Click this to add a new service filtering rule (see Adding or Editing a Service Filter Rule on page 7).
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.
Trust PC List	
Host Name	This displays the name of the trust device connected.
IP Address	This displays the IP address of the trust network device connected.
Status	This displays whether or not the service filter rule is enabled to the trust device connected.
Manage	Click **Manage** to make changes to the trust device's service filter status (see Adding or Editing a Trust PC List on page 9).
Action	Click **Delete** to remove the existing trust device from the list.

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

Add Trust Device	Click this to add a new Trust Device. (see Adding or Editing a Trust PC List on page 9).
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.

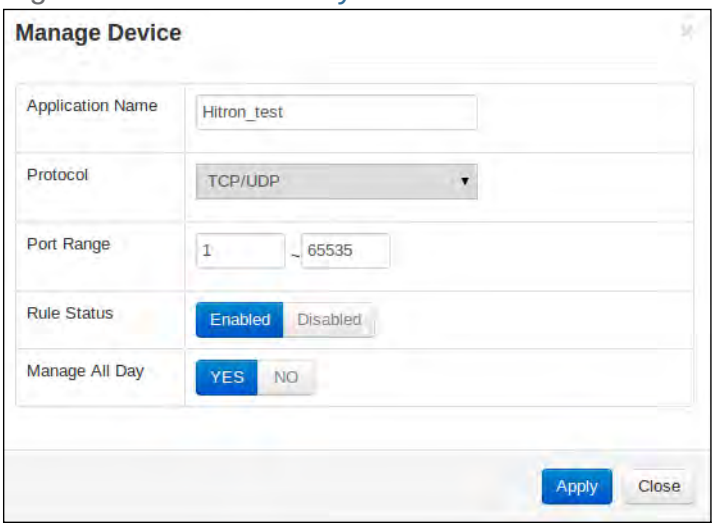
7.3.1 Adding or Editing a Service Filter Rule

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

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

The following screen displays.

Figure 48: The Security: Service Filter Add/Edit Screen



Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

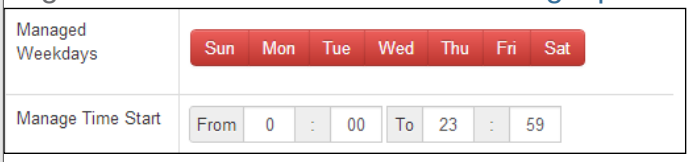
The following table describes the labels in this screen.

Table 39: 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 CGNM/ CGNM-3552 should filter via: ▸ Transmission Control Protocol (**TCP**) ▸ User Datagram Protocol (**UDP**) NOTE: If in doubt, leave this field at its default (**TCP**).
Port Range	Use these fields to specify the start and end port for which this filtering rule applies. These are the ports to which traffic will be blocked. Enter the start port number in the first field, and the end port number in the second field. To specify only a single port, enter its number in both fields.
Rule Status	Use this field to select whether the filtering rule should be active or not. ▸ Select **Enabled** to activate the rule. Matching traffic will be blocked. ▸ Select **Disabled** to deactivate the rule. Matching traffic will not be blocked.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 39: The Security: Service Filter Add/Edit Screen

Manage All Day	Use this field to specify whether the filtering rule should apply on all days of the week, at all times, or whether the rule should be applied only at certain times. ▸ Select **YES** to apply the rule at all times. ▸ Select **NO** to apply the rule only at certain times. Additional fields display, allowing you to specify the times at which the rule should be applied. Figure 49: 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.

7.3.2 Adding or Editing a Trust PC List

- To add a new trust PC to the list, click **Add Trust Device** in the **Security** > **Service Filter** screen.
- To edit an existing trust PC in the list, locate the device in the **Security** > **Service Filter** screen and click its **Manage** button.

NOTE: NOTE: Ensure that **Enabled** is selected in the **Security** > **Service Filter** screen in order to add or edit a trust PC.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

The following screen displays.

Figure 50: The Security: Service Filter > Trust PC List Add/Edit Screen

The following table describes the labels in this screen.

Table 40: The Security: Service Filter Add/Edit Trust Manage Device Screen

Host Name	This displays the name of each network device connected.
IP Address	This displays the IP address of each network device connected.
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.
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 trust PC list.

7.4 The Device Filter Screen

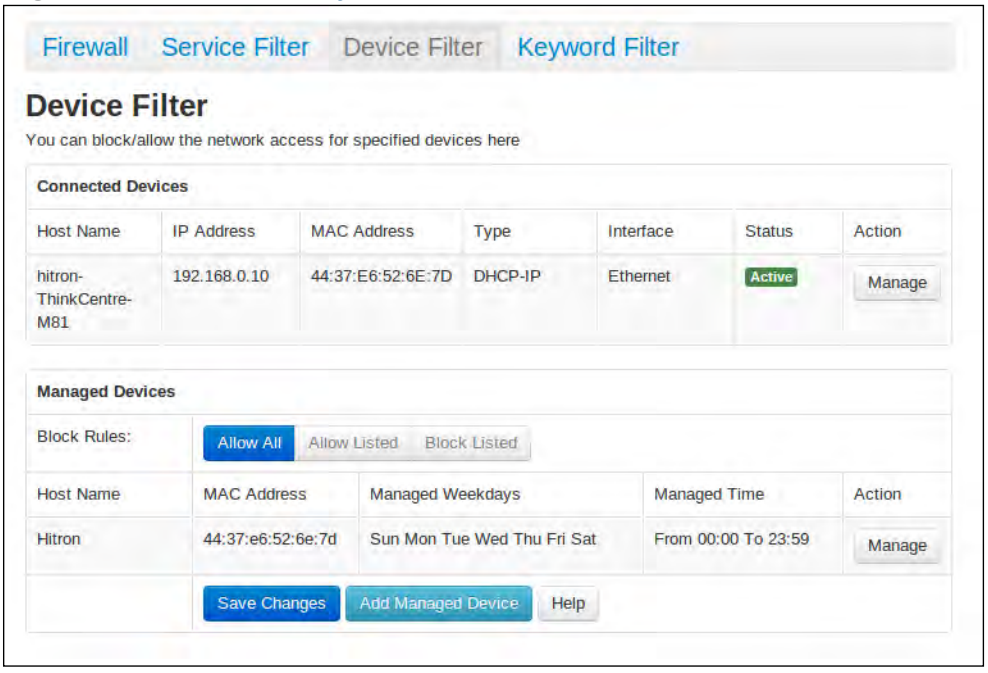
Use this screen to configure Media Access Control (MAC) address filtering on the LAN, and to configure IP filtering.

You can set the CGNM/ CGNM-3552 to allow only certain devices to access the CGNM/ CGNM-3552 and the network, or to deny certain devices access.

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

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

Figure 51: The Security: Device Filter Screen



The following table describes the labels in this screen.

Table 41: The Security: Device Filter Screen

Connected Devices	
Host Name	This displays the name of each network device connected on the LAN.
IP Address	This displays the IP address of each network device connected on the LAN.
MAC Address	This displays the Media Access Control (MAC) address of each network device connected on the LAN.
Type	This displays whether the device's IP address was assigned by DHCP (**DHCP-IP**), or **self-assigned**.
Interface	This displays the name of the interface on which the relevant device is connected.
Status	This displays if the device filter is active or not.
Action	Click **Manage** to make changes to the device's filtering status; see Adding or Editing a Managed Device on page 12 for information on the screen that displays.

Table 41: The Security: Device Filter Screen (continued)

Managed Devices	
Block Rules	Use these buttons to control the action to be taken for the devices listed: ▸ Select **Allow All** to ignore the **Managed Devices** list and let all devices connect to the CGNM/ CGNM-3552. ▸ Select **Allow** to permit only devices you added to the **Managed Devices** list to access the CGNM/ CGNM-3552 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 CGNM/ CGNM-3552 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 filtering rule (see Adding or Editing a Managed Device on page 12).
Save Changes	Click this to save your changes to the fields in this screen.
Add Managed Device	Click this to add a new service filtering rule (see Adding or Editing a Managed Device on page 12).
Help	Click this to see information about the fields in this screen.

7.4.1 Adding or Editing a Managed Device

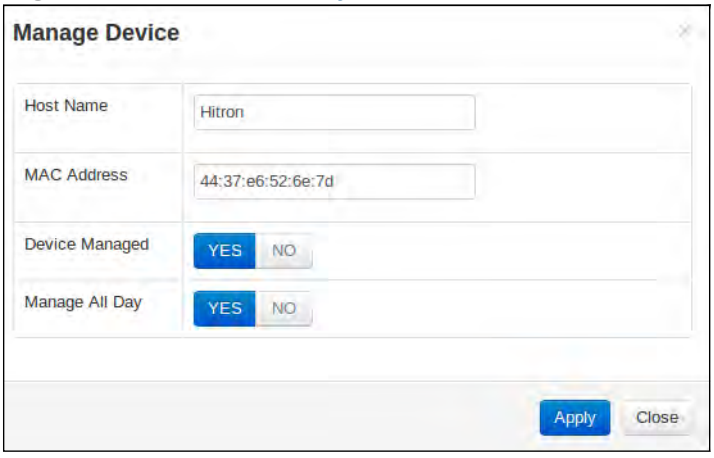
- To add a new managed device, click **Add Managed Device** in the **Security** > **Device Filter** screen.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

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

The following screen displays.

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

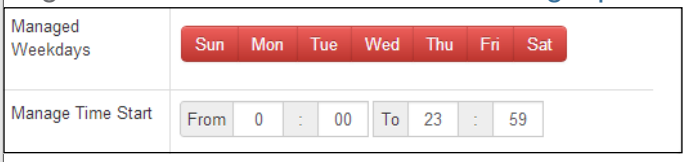


The following table describes the labels in this screen.

Table 42: The Security: Device Filter Add/Edit Screen

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

Table 42: The Security: Device Filter Add/Edit Screen

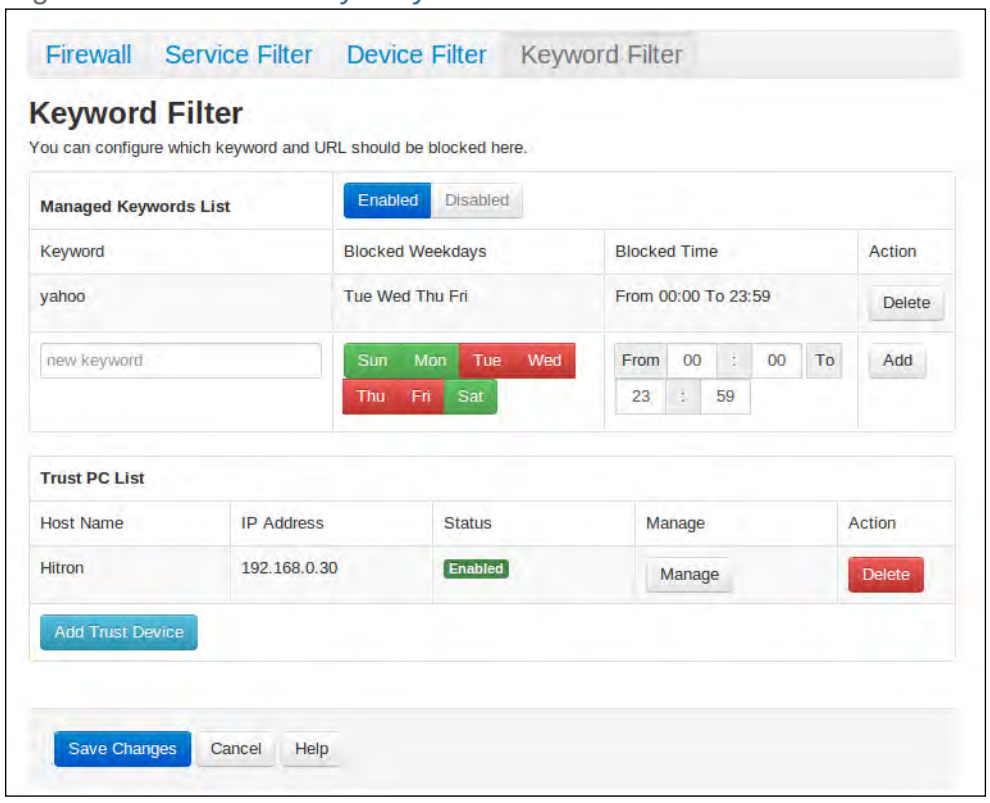
Manage All Day	Use this field to specify whether the device should be managed on all days of the week, at all times, or whether the device should be managed only at certain times. ▸ Select **YES** to managed the device at all times. ▸ Select **NO** to managed the device only at certain times. Additional fields display, allowing you to specify the times at which the device should be managed. Figure 53: 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.

7.5 The Keyword Filter Screen

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

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

Figure 54: The Security: Keyword Filter Screen



The following table describes the labels in this screen.

Table 43: 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 CGNM/ CGNM-3552 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.
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.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 43: The Security: Keyword Filter Screen (continued)

Action	Click **Add** to create a new keyword blocking rule; a new row of fields display. Click **Delete** to remove a existing keyword blocking rule.
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.
Trust PC List	
Host Name	This displays the name of the trust device connected.
IP Address	This displays the IP address of the trust network device connected.
Status	This displays whether or not the keyword filter rule is enabled of the trust device connected.
Manage	Click **Manage** to make changes to the trust device's keyword filter status; see Adding or Editing a Trust PC List on page 16.
Action	Click to delete the existing trust device from the list.
Add Trust Device	Click this to add a new Trust Device. (see Adding or Editing a Trust PC List on page 16).
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.

7.5.1 Adding or Editing a Trust PC List

- To add a new trust PC to the list, click **Add Trust Device** in the **Security** > **Keyword Filter** screen.
- To edit an existing trust PC in the list, locate the device in the **Security** > **Keyword Filter** screen and click its **Manage** button.

NOTE: Ensure that **Enabled** is selected in the **Security** > **Keyword Filter** screen in order to add or edit a trust PC.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

The following screen displays.

Figure 55: Keyword Filter > Trust PC List Add/Edit Screen

The following table describes the labels in this screen.

Table 44: The Security: Keyword Filter Add/Edit Trust Manage Device Screen

Host Name	This displays the name of each network device connected.
IP Address	This displays the IP address of each network device connected.
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.
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 trust PC list.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

8

Advanced

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

- The Switch Setup Screen on page 1
- The DDNS Screen on page 3

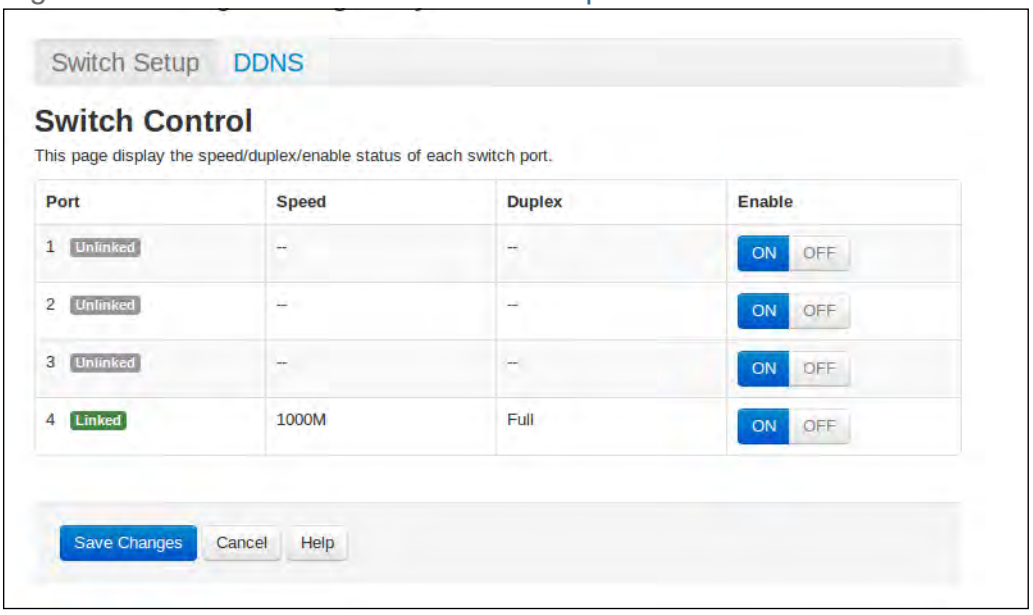
8.1 The Switch Setup Screen

Use this screen to view the speed and duplex status of each of the CGNM/ CGNM-3552's LAN ports, and enable or disable them.

Click **Advanced** > **Switch Setup**. The following screen displays.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Figure 56: The Advanced > Switch Setup Screen



The following table describes the labels in this screen.

Table 45: The Advanced > Switch Setup Screen

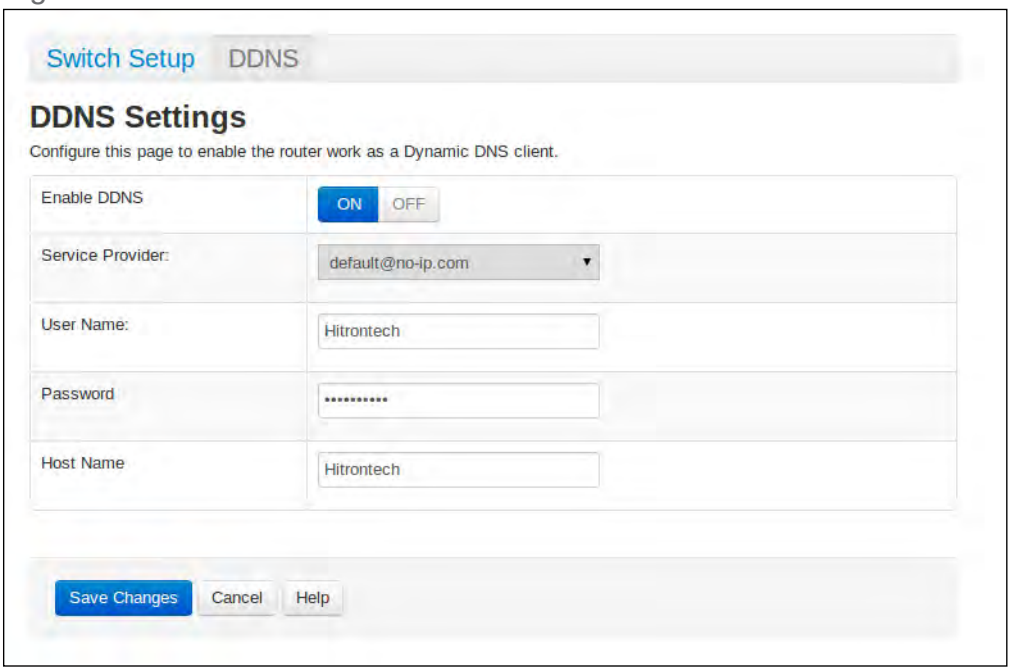
Port	This displays the number of each LAN port. ▸ When no device is connected to the LAN port, **Unlinked** displays. ▸ When a device is connected to the LAN port, **Linked** displays.
Speed	This displays the speed of the data link to the device connected to the LAN port, in kilobits per second (kbps).
Duplex	This displays the duplex status of the data link to the device connected to the LAN port.
Enable	Use this to turn the LAN port on or off. ▸ Click a disabled LAN port's **On** button to enable the port. Data can be exchanged with the device connected to this port. ▸ Click an enabled LAN port's **Off** button to disable the port. Data cannot be exchanged with the device connected to this port.
Save Changes	Click this to save your changes to the settings in this screen.
Cancel	Click this to discard your changes to the settings in this screen.

8.2 The DDNS Screen

Use this screen to configure the CGNM/ CGNM-3552's Dynamic Domain Name System (DDNS) settings.

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

Figure 57: The Advanced > DDNS Screen



The following table describes the labels in this screen.

Table 46: The Advanced > DDNS Screen

Enable DDNS	Use this to configure the CGNM/ CGNM-3552's DDNS function. ▸ Click **On** to have the CGNM/ CGNM-3552 work as a DDNS client. The CGNM/ CGNM-3552 receives DDNS information from the **Service Provider** you specify. ▸ Click **Off** to have the CGNM/ CGNM-3552 not work as a DDNS client.
Service Provider	Select the organization from which you wish to receive DDNS information.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Table 46: The Advanced > DDNS Screen (continued)

User Name	Enter the credentials assigned to you by the selected **Service Provider**.
Password	
Host Name	
Save Changes	Click this to save your changes to the settings in this screen.
Cancel	Click this to discard your changes to the settings in this screen.
Help	Click this to see more information about the items in this screen.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

9

Troubleshooting

Use this section to solve common problems with the CGNM/ CGNM-3552 and your network. It contains the following sections:

- None of the LEDs Turn On on page 1
- One of the LEDs does not Display as Expected on page 2
- I Forgot the CGNM/ CGNM-3552's IP Address on page 2
- I Forgot the CGNM/ CGNM-3552's Admin Username or Password on page 3
- I Cannot Access the CGNM/ CGNM-3552 or the Internet on page 3
- I Cannot Access the Internet and the DS and US LEDs Keep Blinking on page 3
- I Cannot Connect My Wireless Device on page 4

Problem: None of the LEDs Turn On

The CGNM/ CGNM-3552 is not receiving power, or there is a fault with the device.

1 Ensure that you are using the correct power adaptor.

Using a power adaptor other than the one that came with your CGNM/ CGNM-3552 can damage the CGNM/ CGNM-3552.

2 Ensure that the power adaptor is connected to the CGNM/ CGNM-3552 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.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

4 Disconnect and re-connect the power adaptor to the power source and the CGNM/ CGNM-3552.

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 6).

2 Ensure that the CGNM/ CGNM-3552's hardware is connected correctly; see the Quick Installation Guide.

3 Disconnect and re-connect the power adaptor to the CGNM/ CGNM-3552.

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

Problem: I Forgot the CGNM/ CGNM-3552's IP Address

1 The CGNM/ CGNM-3552's default LAN IP address is **192.168.0.1**.

2 You can locate the CGNM/ CGNM-3552's GUI by entering the LAN domain suffix into your browser's address bar (on a computer connected to the LAN). The default LAN domain suffix is displayed in the **Basic** > **LAN Setup** screen's **Domain Suffix** field. See The LAN Setup Screen on page 3 for more information.

3 Depending on your operating system and your network, you may be able to find the CGNM/ CGNM-3552's IP address by looking up your computer's default gateway. To do this on (most) Windows machines, click **Start** > **Run**, enter "cmd", and then enter "ipconfig". Get the IP address of the **Default Gateway**, and enter it in your browser's address bar.

4 If you still cannot access the CGNM/ CGNM-3552, you need to reset the CGNM/ CGNM-3552. See Factory Default Resetting the CGNM/ CGNM-3552 on page 14. All user-configured data is lost, and the CGNM/ CGNM-3552 is returned to its default settings. If you previously backed-up a more recent version your CGNM/ CGNM-3552's settings, you can now upload them to the CGNM/ CGNM-3552; see The Backup Screen on page 6.

Problem: I Forgot the CGNM/ CGNM-3552's Admin Username or Password

1. The default username is **cusadmin**, and the default password is **password**.
2. If the default username and password do not work, you need to reset the CGNM/ CGNM-3552. See Factory Default Resetting the CGNM/ CGNM-3552 on page 14. All user-configured data is lost, and the CGNM/ CGNM-3552 is returned to its default settings. If you previously backed-up a more recent version your CGNM/ CGNM-3552's settings, you can now upload them to the CGNM/ CGNM-3552; see The Backup Screen on page 6.

Problem: I Cannot Access the CGNM/ CGNM-3552 or the Internet

1. Ensure that you are using the correct IP address for the CGNM/ CGNM-3552.
2. Check your network's hardware connections, and that the CGNM/ CGNM-3552's LEDs display correctly (see LEDs on page 6).
3. Make sure that your computer is on the same subnet as the CGNM/ CGNM-3552; see IP Address Setup on page 10.
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 CGNM/ CGNM-3552. See Factory Default Resetting the CGNM/ CGNM-3552 on page 14. All user-configured data is lost, and the CGNM/ CGNM-3552 is returned to its default settings. If you previously backed-up a more recent version your CGNM/ CGNM-3552's settings, you can now upload them to the CGNM/ CGNM-3552; see The Backup Screen on page 6.
6. If the problem persists, contact your vendor.

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

Your service provider may have disabled your Internet access; check the **Status** > **DOCSIS WAN** screen's **Network Access** field (see The DOCSIS WAN Screen on page 16).

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 CGNM/ CGNM-3552'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 CGNM/ CGNM-3552's signal quality and coverage area.

3. Ensure that the CGNM/ CGNM-3552 and the wireless client are set to use the same wireless mode and SSID (see The Basic Settings Screen on page 4) and security settings (see The Access Control Screen on page 15).

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 CGNM/ CGNM-3552 and the button on the wireless client within 2 minutes of one another.

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Index

Numbers

802.11a/b/g/n/ac 14, 78

A

access 14
access point 13, 26, 58, 77, 93
accounts, login 23
address, IP 21
address, IP, local 21
admin management 94
AP 13, 26, 58, 77, 93
attached network devices 47, 49

B

backup 98, 100
backup and restore 14
bar, navigation 24
bridge 74
buttons 14

C

cable connection 13, 26, 58, 77, 93
cable connection status 46
cable modem 13, 26, 58, 77, 93
CATV 14, 32, 33
channel 74, 75
channel plan 74
clients, wireless 77
configuration file 37
connection status, cable 46
conventions, document 3
customer support 4

D

debugging 57, 93, 97
default 98, 100
default IP address 21
default username and password 23
defaults 98, 100
De-Militarized Zone 58
DHCP 14, 21, 35
DHCP lease 36
diagnostics 57, 93, 97
DMZ 58
DMZ De-Militarized Zone 14
DNS 57
document conventions 3
Domain Name System 57
domain suffix 57
downstream transmission 37
DS 19

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

E

ETH 19
Ethernet 14
Ethernet cables 17
Ethernet port 21

F

factory defaults 98, 100
factory reset 16, 24
fast Ethernet 14
FDMA 38
forwarding, port 14, 58
frequencies, cable 37
F-type RF connector 14

G

graphical user interface 13, 26, 32, 77, 93, 102
GUI 13, 23, 26, 32, 77, 93, 102
GUI overview 23, 26

H

hardware 14
host ID 33

I

IANA 33
IEEE 802.11a/b/g/n/ac 14, 78
interface, user 13, 26, 32, 77, 93, 102
intrusion detection 14
IP address 21, 33, 57, 124
IP address lease 36
IP address renewal 36
IP address setup 21, 22
IP address, default 21
IP address, format 33
IP address, local 21
IP filtering 14
ISP 33

L

LAN 56, 77
LAN 1~4 17
LAN setup 59
LEDs 17, 123, 125
lights 17
local IP address 21
logging in 23
login accounts 23
login screen 21

M

MAC address 36
MAC filtering 14, 103
main window 24, 27
Media Access Control address 36
MIMO 14
modem 13, 26, 58, 77, 93
modem status 46

modulation 38
Multiple-In, Multiple-Out 14

N

navigation 24
navigation bar 24
network devices, attached 47, 49
network diagnostics 57, 93
network number 33

O

overview, GUI 23, 26

P

password 124
password and username 23
PBC configuration 79
PIN configuration 14, 79
ping 14, 57, 93, 97
port forwarding 14, 58, 61, 62
port triggering 14, 66
port, Ethernet 21
ports 14
private IP address 34
push-button configuration 14

Q

QAM 38
QAM TCM 38
QoS 80
QPSK 38

R

radio coverage 88
radio links 77
reboot 98, 100
reset 16, 24
restore and backup 14
RF connector 14
RJ45 connectors 17
routing mode 34, 37, 56
rule, port forwarding 63

S

scan range 75
SCDMA 38
scheduled website blocking 14
security, wireless 14
service filter 106
service set 78
settings backup and restore 14
SSID 78, 80
Status 19
status 47, 49
status, cable connection 46
subnet 21, 33, 57
subnet, IP 21
support, customer 4

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

T

TCP/IP 22
TDMA 38
traceroute 14, 57, 93, 97
transmission power 75
triggering, port 14, 66

U

upstream transmission 37
US 19
user interface 13, 26, 32, 77, 93, 102
username 124
username and password 23

V

Video conferencing 40
Video on Demand (VoD) 39

W

WAN 33
WAN connection 47, 49
website blocking, scheduled 14
WEP 14, 78
WiFi MultiMedia 80
WiFi Protected Setup 14, 79
window, main 24, 27
Windows XP 22
wired security 14
wireless access point 13, 26, 58, 77, 93
wireless clients 77

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

wireless connection 125
wireless networking standards 78
wireless security 14, 78
wireless security settings 88
wireless settings 29
wireless settings, basic 80
wireless status 51, 54
WLAN 77
WMM 80
WPA2 80
WPA2-PSK 14, 78
WPA-PSK 14, 78
WPS 14, 79, 80
WPS PBC 16

X

XP, Windows 22

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies

Version 2.0, 07/2015. Copyright © 2015 Hitron Technologies