

CRADLEPOINT ARC CBA850

PRODUCT MANUAL

Cellular Broadband Adapter



for additional information, visit:
knowledgebase.cradlepoint.com



PREFACE

Cradlepoint reserves the right to revise this publication and to make changes in the content thereof without obligation to notify any person or organization of any revisions or changes.

MANUAL REVISIONS

Revision	Date	Description	Author
1.0	Apr. 28, 2015	Initial release for Firmware version 5.4.0	Pat Burroughs

TRADEMARKS

Cradlepoint and the Cradlepoint logo are registered trademarks of Cradlepoint, Inc. in the United States and other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

Copyright © 2015 by Cradlepoint, Inc. All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written consent by Cradlepoint, Inc.



TABLE OF CONTENTS

PREFACE.....	I	5 STATUS.....	32
MANUAL REVISIONS.....	I	5.1 CLIENT LIST.....	33
TRADEMARKS.....	I	5.2 DASHBOARD	34
TABLE OF CONTENTS	II	5.3 GPS.....	37
1 INTRODUCTION	3	5.4 INTERNET CONNECTIONS	38
1.1 PACKAGE CONTENTS	3	5.5 LLDP	44
1.2 SYSTEM REQUIREMENTS.....	3	5.6 ROUTING.....	45
1.3 CBA850 OVERVIEW	4	5.7 STATISTICS.....	46
1.4 CRADLEPOINT ARC CBA850 SERIES	6	5.8 SYSTEM LOGS.....	48
2 HARDWARE OVERVIEW	12	6 NETWORK SETTINGS	49
2.1 PORTS, BUTTONS, AND SWITCHES.....	13	6.1 CONTENT FILTERING	50
2.2 LEDs.....	15	6.2 DHCP SERVER	54
3 QUICK START	16	6.3 DNS	55
3.1 BASIC SETUP	16	6.4 FIREWALL	58
3.2 ACCESSING THE ADMINISTRATION PAGES	17	6.5 LOCAL NETWORKS	65
3.3 COMMON PROBLEMS	18	6.6 MAC FILTER/LOGGING.....	79
4 WEB INTERFACE -- ESSENTIALS.....	20	6.7 ROUTING.....	81
4.1 ADMINISTRATOR LOGIN	21	7 INTERNET.....	82
4.2 GETTING STARTED – FIRST TIME SETUP.....	23	7.1 CONNECTION MANAGER	83
4.3 QUICK LINKS	28	7.2 DATA USAGE	104
4.4 CONFIGURATION PAGES	29	7.3 WAN AFFINITY AND LOAD BALANCING.....	108
4.5 ENTERPRISE CLOUD MANAGER REGISTRATION.....	31	8 SYSTEM SETTINGS	112
4.6 IP PASSTHROUGH SETUP	31	8.1 ADMINISTRATION.....	113
		8.2 DEVICE ALERTS.....	130



8.3	ENTERPRISE CLOUD MANAGER	133	10	APPENDIX	155
8.4	SERIAL REDIRECTOR.....	135	10.1	REGULATORY AND SAFETY INFORMATION	155
8.5	SNMP CONFIGURATION	138	10.2	WARRANTY, LIABILITY, PRIVACY, ETC.....	157
8.6	SYSTEM CONTROL.....	141	10.3	SPECIFICATIONS.....	158
8.7	SYSTEM SOFTWARE	142			
9	GLOSSARY.....	144			

1 INTRODUCTION

1.1 Package Contents

- CBA850 with integrated MC400 Multi-Carrier Software-Defined Radio modem
- Universal 3G/4G/LTE antennas with dedicated active GPS antenna port
- AC power adapter (12V, 1A, 1.5 meter cord) **WARNING:** using a power adapter other than the one provided may damage the CBA850 and will void the warranty
- Ethernet cable
- Quick Start Guide
- Mounting hardware
- Warranty and regulatory information

- ARC Series includes integrated 3G/4G business-grade modem with modem antennas
 - o ARC CBA850LPE-VZ – 4G LTE/HSPA+/EVDO for Verizon
 - o ARC CBA850LPE-AT – 4G LTE/HSPA+/EVDO for AT&T
 - o ARC CBA850LPE-SP – 4G LTE/HSPA+/EVDO for Sprint
 - o ARC CBA850LP3-EU – 4G LTE/HSPA+ for Europe
 - o ARC CBA850LPE-GN – 4G LTE/HSPA+/EVDO for T-Mobile in US and Rogers, Bell, and TELUS in Canada

1.2 System Requirements

- An Internet source: a Cradlepoint 3G/4G business-grade modem or USB broadband data modem with active subscription
- Windows 2000/XP/7, Mac OS X, or Linux computer
- Internet Explorer v8.0 or higher (standards mode only), Chrome, Firefox v2.0 or higher (PC and Mac), Safari v6.0 or higher (PC and Mac), Opera



1.3 CBA850 Overview

WIRELESS WAN CONNECTIVITY

The Cradlepoint CBA850 mobile broadband series adapters enable easy-to-install wireless WAN connectivity in fixed-business locations. For distributed enterprises like branch offices, retail stores, restaurants, and small businesses, the CBA850 provides 3G/4G wireless network connectivity to keep your business up and running.

FAILOVER MADE SIMPLE

The Cradlepoint CBA850 3G/4G cellular broadband adapter provides IP passthrough capabilities for any device that requires wireless broadband access. For most applications, simply connect the CBA850 to an existing CPE router configured for WAN failover, and it's ready to go. The CBA850 handles the wireless WAN connection through a 3G/4G modem (included with ARC models) when failover occurs.

PRIMARY CONNECT IS EASY TOO

For temporary networks – or when wired connections are impractical – the CBA850 can serve as a primary-connect device, converting mobile broadband to Ethernet for point-of-sale tools, digital signs, and kiosks.

KEY FEATURES

- 3G/4G mobile broadband connectivity
- Drop into existing network for a turnkey failover solution
- Remote management capabilities
- Power-over-Ethernet (PoE)

1.3.1 Cradlepoint Enterprise Cloud Manager

Rapidly deploy and dynamically manage networks at geographically distributed stores and branch locations with Enterprise Cloud Manager, Cradlepoint's next generation management and application platform. Enterprise Cloud Manager integrates cloud management with your Cradlepoint devices to improve productivity, increase reliability, reduce costs, and enhance the intelligence of your network and business operations. Learn more at <http://Cradlepoint.com/ecm>.



1.3.2 CradleCare – Access the Experts 24/7

Cradlepoint understands how important and critical network uptime is to your business. We have a knowledgeable enterprise technical support staff that is available anytime via phone, chat, or email to protect your investment. Our experts will expedite issue resolution and provide flexible device-by-device solutions to help maximize operational efficiency. This allows you to dedicate more time to what's important: your business.

SUPPORT

- **CradleCare Support Agreement:** 24/7 technical support, software upgrades, and advanced hardware exchange – 1-, 3-, and 5-year options
- **CradleCare Extended Warranty:** extends the standard warranty to 3 or 5 years

ON-SITE SERVICES

- **CradleCare Standard 3G/4G Site Survey:** Comprehensive carrier analysis for optimal performance
- **CradleCare Standard Installation:** Deploy the experts to ensure a successful installation

Learn more at <http://www.Cradlepoint.com/products/cradlecare>.

1.4 Cradlepoint ARC CBA850 Series

ARC Series includes a Cradlepoint 3G/4G business-grade modem with the CBA850 and creates an effortless instant network from high-speed wireless broadband.

Cradlepoint integrated business-grade modems are specifically designed to provide the highest level of performance, reliability, and security for 24x7 business-critical applications. Modems can be located and antennas oriented to receive the highest signal strength.

Choose from the following ARC CBA850 Products:

- **ARC CBA850LPE-VZ – 4G LTE/HSPA+/EVDO for Verizon**
- **ARC CBA850LPE-AT – 4G LTE/HSPA+/EVDO for AT&T**
- **ARC CBA850LPE-SP – 4G LTE/HSPA+/EVDO for Sprint**
- **ARC CBA850LP3-EU – 4G LTE/HSPA+ for Europe**
- **ARC CBA850LPE-GN – 4G LTE/HSPA+/EVDO for T-Mobile in US and Rogers, Bell, and TELUS in Canada**



ARC CBA850LPE-VZ – 4G LTE/HSPA+/EVDO for Verizon
Technology: LTE, HSPA+, EVDO Rev A
Downlink Rates: LTE: 100 Mbps; HSPA+: 21.1 Mbps; EVDO: 3.1 Mbps (theoretical)
Uplink Rates: LTE: 50 Mbps; HSPA+: 5.76 Mbps; EVDO: 1.8 Mbps (theoretical)
Frequency Bands: • LTE: Band 2 (1900 MHz), Band 4 – AWS (1700/2100 MHz), Band 5 (850 MHz), Band 13 (700 MHz), Band 17 (700 MHz), Band 25 (1900 MHz) • HSPA+/UMTS: (850/900/1900/2100 MHz, AWS) • GSM/GPRS/EDGE: (850/900/1800/1900 MHz) • CDMA EVDO: Rev A/1xRTT (800/1900 MHz) <i>NOTE: LPE models are flexible and support bands for multiple cellular providers; however, only the frequency bands in bold above are supported by the listed provider.</i>
Power: LTE: 23 dBm +/- 1; HSPA+: 23 dBm +/- 1; EVDO: 24 +0.5/- 1 dBm (typical conducted)
Antennas: two SMA male (plug), 1 dBi (LTE), 2 dBi (Cellular/PCS) gain; finger tighten only (maximum torque spec is 7 kgf-cm)
GPS: active GPS support
Industry Standards & Certs: FCC, Verizon
Modem Part Number: MC400LPE
SIM: two 2FF SIM slots

ARC CBA850LPE-AT – 4G LTE/HSPA+/EVDO for AT&T
Technology: LTE, HSPA+, EVDO Rev A
Downlink Rates: LTE: 100 Mbps; HSPA+: 21.1 Mbps; EVDO: 3.1 Mbps (theoretical)
Uplink Rates: LTE: 50 Mbps; HSPA+: 5.76 Mbps; EVDO: 1.8 Mbps (theoretical)
Frequency Bands: • LTE: Band 2 (1900 MHz), Band 4 – AWS (1700/2100 MHz), Band 5 (850 MHz), Band 13 (700 MHz), Band 17 (700MHz), Band 25 (1900 MHz) • HSPA+/UMTS: (850/900/1900/2100 MHz, AWS) • GSM/GPRS/EDGE: (850/900/1800/1900 MHz) • CDMA EVDO: Rev A/1xRTT (800/1900 MHz) <i>NOTE: LPE models are flexible and support bands for multiple cellular providers; however, only the frequency bands in bold above are supported by the listed provider.</i>
Power: LTE: 23 dBm +/- 1; HSPA+: 23 dBm +/- 1; EVDO: 24 dBm +0.5/-1 (typical conducted)
Antennas: two SMA male (plug), 1 dBi (LTE), 2 dBi (Cellular/PCS) gain; finger tighten only (maximum torque spec is 7 kgf-cm)
GPS: active GPS support
Industry Standards & Certs: PTCRB, FCC, IC, AT&T
Modem Part Number: MC400LPE
SIM: two 2FF SIM slots



ARC CBA850LPE-SP – 4G LTE/HSPA+/EVDO for Sprint	
Technology:	LTE, HSPA+, EVDO Rev A
Downlink Rates:	LTE: 100 Mbps; HSPA+: 21.1 Mbps; EVDO: 3.1 Mbps (theoretical)
Uplink Rates:	LTE: 50 Mbps; HSPA+: 5.76 Mbps; EVDO: 1.8 Mbps (theoretical)
Frequency Bands:	• LTE: Band 2 (1900 MHz), Band 4 – AWS (1700/2100 MHz), Band 5 (850 MHz), Band 13 (700 MHz), Band 17 (700 MHz), Band 25 (1900 MHz) • HSPA+/UMTS: (850/900/1900/2100 MHz, AWS) • GSM/GPRS/EDGE: (850/900/1800/1900 MHz) • CDMA EVDO: Rev A/1xRTT (800/1900 MHz) <i>NOTE: LPE models are flexible and support bands for multiple cellular providers; however, only the frequency bands in bold above are supported by the listed provider.</i>
Power:	LTE: 23 dBm +/-1; HSPA+: 23 dBm +/-1 dBm; EVDO: 24 dBm +0.5/-1 (typical conducted)
Antennas:	two SMA male (plug), 1 dBi (LTE), 2 dBi (Cellular/PCS) gain; finger tighten only (maximum torque spec is 7 kgf-cm)
GPS:	active GPS support
Industry Standards & Certs:	FCC, Sprint
Modem Part Number:	MC400LPE
SIM:	two 2FF SIM slots

ARC CBA850LP3-EU – 4G LTE/HSPA+ for Europe
Technology: LTE, HSPA+
Downlink Rates: LTE: 100 Mbps; HSPA+: 21.1 Mbps (theoretical)
Uplink Rates: LTE: 50 Mbps; HSPA+: 5.76 Mbps (theoretical)
Frequency Bands: • LTE: Band 1 (2100 MHz), Band 3 (1800 MHz), Band 7 (2600 MHz), Band 8 (900 MHz), Band 20 (800 MHz) • HSPA+/UMTS: (800/850/900/1900/2100 MHz) • GSM/GPRS/EDGE: Quad-Band (850/900/1800/1900 MHz) <i>NOTE: LPE models are flexible and support bands for multiple cellular providers; however, only the frequency bands in bold above are supported by the listed provider.</i>
Power: LTE Band 1/3/8/20: 23 +/-1 dBm, Band 7: 22 dBm +/-1; HSPA+: 23 dBm +/-1 (typical conducted)
Antennas: two SMA male (plug), 1 dBi (LTE), 2 dBi (Cellular/PCS) gain; finger tighten only (maximum torque spec is 7 kgf-cm)
GPS: active GPS support
Industry Standards & Certs: CE, GCF-CC
Modem Part Number: MC400LP3
SIM: two 2FF SIM slots

ARC CBA850LPE-GN – 4G LTE/HSPA+/EVDO for T-Mobile in US and Rogers, Bell, and TELUS in Canada

Technology: LTE, HSPA+, EVDO Rev A

Downlink Rates: LTE: 100 Mbps; HSPA+: 21.1 Mbps; EVDO: 3.1 Mbps (theoretical)

Uplink Rates: LTE: 50 Mbps; HSPA+: 5.76 Mbps; EVDO: 1.8 Mbps (theoretical)

Frequency Bands:

- **LTE: Band 2 (1900 MHz), Band 4 – AWS (1700/2100 MHz), Band 5 (850 MHz), Band 13 (700 MHz), Band 17 (700 MHz), Band 25 (1900 MHz)**
- **HSPA+/UMTS: (850/900/1900/2100 MHz, AWS)**
- **GSM/GPRS/EDGE: (850/900/1800/1900 MHz)**
- **CDMA EVDO: Rev A/1xRTT (800/1900 MHz)**

*NOTE: LPE models are flexible and support bands for multiple cellular providers; however, only the frequency bands in **bold** above are supported by the listed provider.*

Power: LTE: 23 dBm +/-1; HSPA+: 23 dBm +/-1 dBm; EVDO: 24 dBm +0.5/-1 (typical conducted)

Antennas: two SMA male (plug), 1 dBi (LTE), 2 dBi (Cellular/PCS) gain; finger tighten only (maximum torque spec is 7 kgf-cm)

GPS: active GPS support

Industry Standards & Certs: PTCRB, FCC, IC

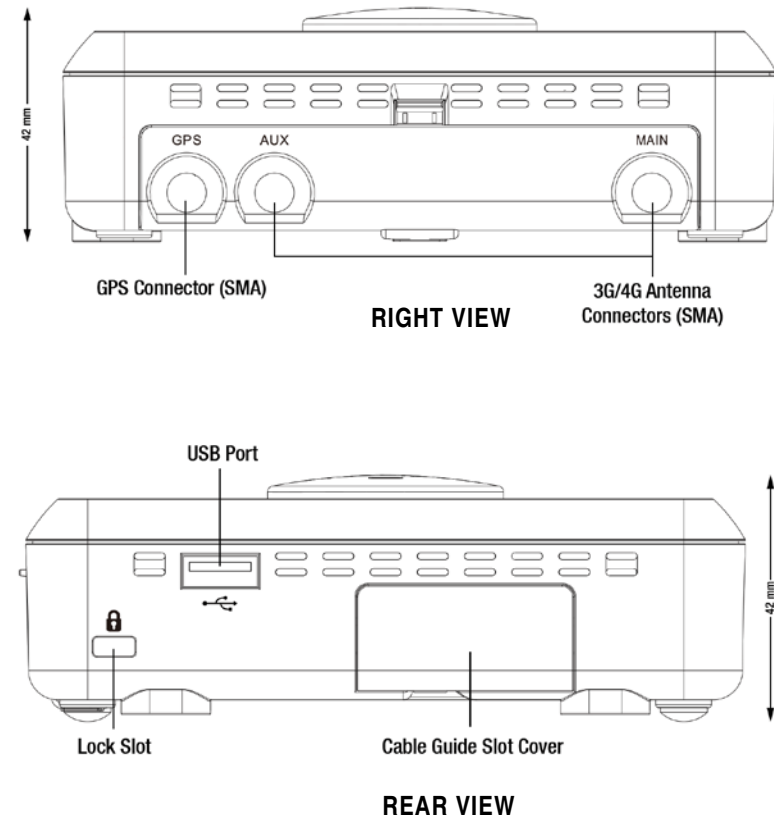
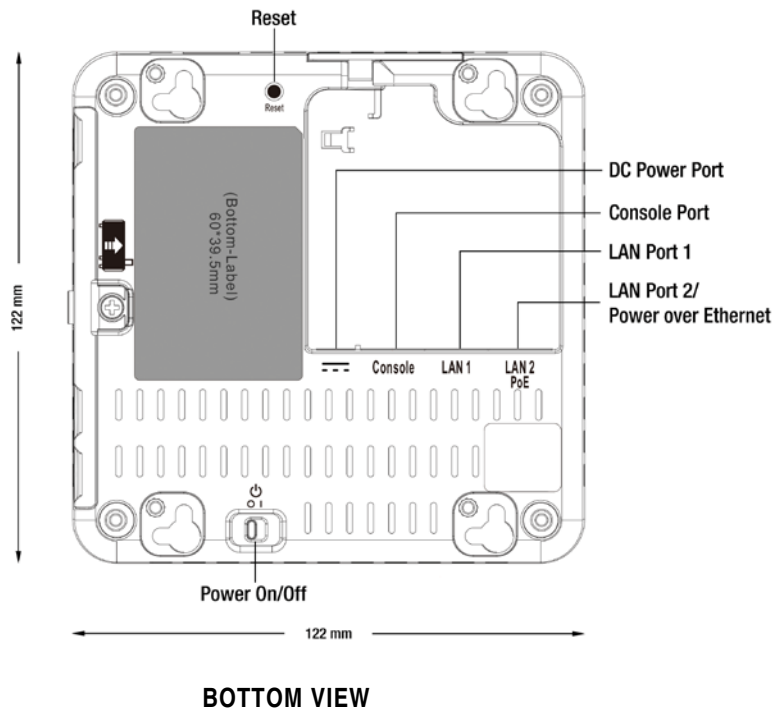
Modem Part Number: MC400LPE

SIM: two 2FF SIM slots

2 HARDWARE OVERVIEW



2.1 Ports, Buttons, and Switches



LAN Port: The CBA850 has two Ethernet ports for local network connections. LAN2 can also be used for PoE (optional). *NOTE: USB port may not be used for external modem if router is being run using PoE.*

Power On/Off:

- I = On
- O = Off



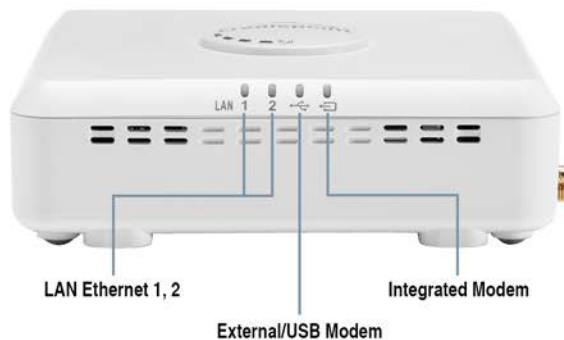
DC Power Port: Attach the included power supply.

Reset: Return your CBA850 to factory default settings by pressing and holding the **Reset** button. This button is recessed, so it requires a pointed object such as a paper clip to press. Press and hold for 10 seconds to initiate reset. This erases configuration changes and resets the administrator password to the **Default Password** found on the product label.

USB Modem Port: The CBA850 has one USB 3.0 port.

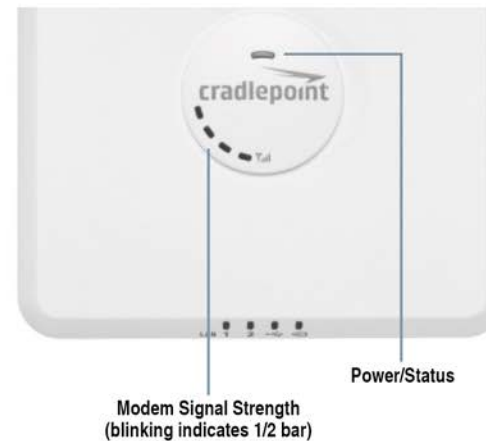
Console Port: Used for Out-of-Band Management (OOBM) when connected to console port of connected device.

2.2 LEDs



INTEGRATED MODEM KEY:

- Connected
- (blinking) Connecting
- Not active / may be engaged in failover process
- (blinking) Connection error
- (blinking) Modem resetting



MODEM SIGNAL STRENGTH KEY:

Blinking indicates 1/2 bar

POWER/STATUS COLOR CODE:

● 4G ● 3G ● Attention

Modem Signal Strength: The bar LEDs indicate the signal strength from the active 3G/4G modem (Cradlepoint business-grade modem or USB modem). A blinking LED indicates ½ bar.



3 QUICK START

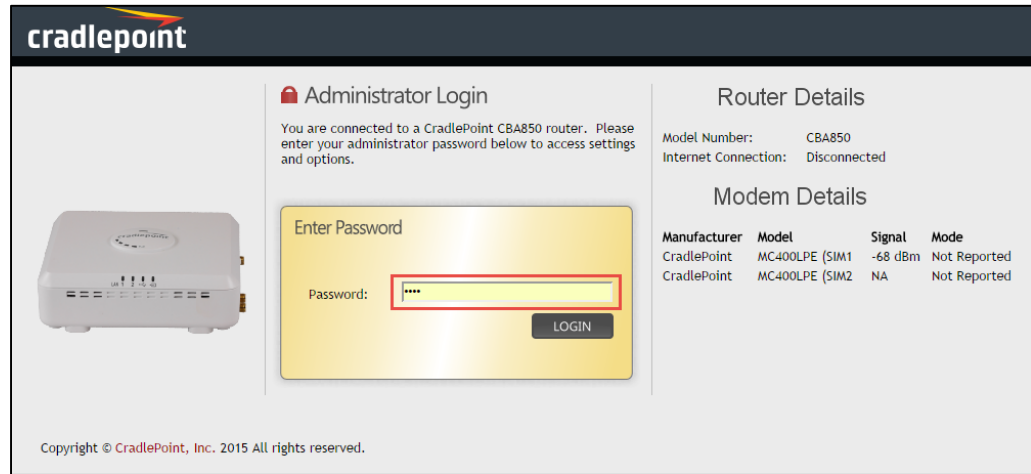
3.1 Basic Setup

1. Insert an activated SIM into the integrated modem.
2. Reinsert the integrated modem.
3. Attach modem cover and insert screw if desired.
4. Attach included modem antennas.
5. Connect to a power source.
6. Connect to a computer or other network equipment.

3.2 Accessing the Administration Pages

The CBA850 can be used immediately without any configuration changes, but to configure any of the advanced features of the CBA850, you need to log into the administration pages:

- Access your router's **Administrator Login** screen by opening a web browser window and typing "[cp/](#)" (your router's default hostname) or the IP address "[192.168.0.1](#)" into the address bar.
- Enter your **Default Password**. This password can be found on the bottom of the CBA850. Then click the **LOGIN** button.
- When you log in for the first time, you will be automatically directed to the **First Time Setup Wizard**. Follow the instructions given with the Wizard or see [Getting Started – First Time Setup](#) for more information about using the **First Time Setup Wizard**.



Administrator Login

You are connected to a CradlePoint CBA850 router. Please enter your administrator password below to access settings and options.

Enter Password

Password:

LOGIN

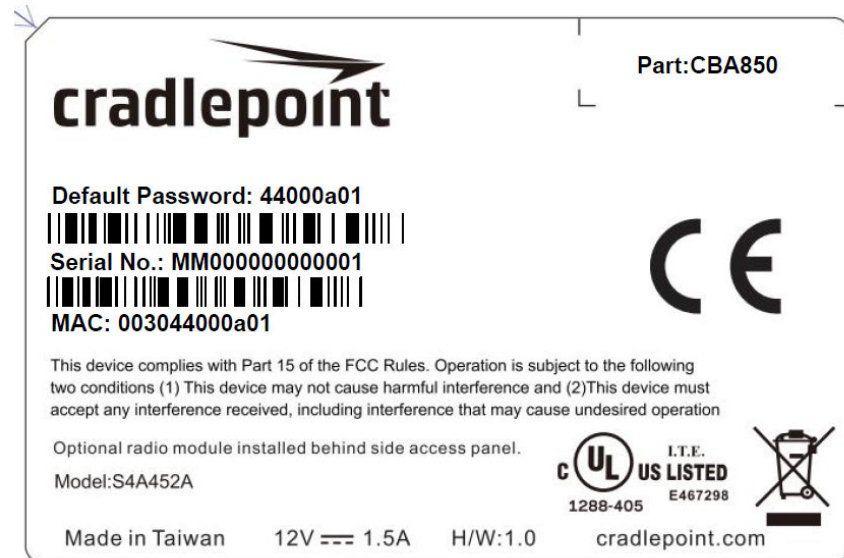
Router Details

Model Number: CBA850
Internet Connection: Disconnected

Modem Details

Manufacturer	Model	Signal	Mode
CradlePoint	MC400LPE (SIM1)	-68 dBm	Not Reported
CradlePoint	MC400LPE (SIM2)	NA	Not Reported

Copyright © CradlePoint, Inc. 2015 All rights reserved.





3.3 Common Problems

This section contains some of the most common issues faced by users of the CBA850. Please visit Cradlepoint Knowledge Base at <http://knowledgebase.Cradlepoint.com/> for more help and answers to your other questions.

3.3.1 You Cannot Connect to the Internet with a Cradlepoint Business-grade Modem

Make sure that you have an active data plan and that your modem has been activated. A wireless broadband data plan must be added to your business-grade modem. Wireless broadband data plans are available from wireless carriers such as Verizon, AT&T, and Sprint. A new line of service can be added or a data plan can be transferred from an existing account. You will need the ESN number (or SIM/IMEI number depending on your carrier plan) from the product label on your modem to add or transfer a line of service.

After adding a data plan to the modem, you may need to activate the modem:

1. Log in to the CBA850 administration pages (see [Accessing the Administration Pages](#)).
2. Select **Internet** from the top navigation bar and **Modem Settings** from the dropdown menu (**Internet** → **Modem Settings**).
3. Find and select the Cradlepoint modem.
4. Click Update/Activate.
5. Click Activate in the popup.

Finally, if you have an active data plan and you have already activated your modem, you may be out of range of your service provider. Check your signal strength in the Internet section of the **Dashboard** (**Status** → **Dashboard**). If you have a weak signal in your location, contact your service provider.

If you are still not online after activating the modem, call Cradlepoint Technical Support for further assistance.



3.3.2 Your USB Modem Does Not Work With the Router

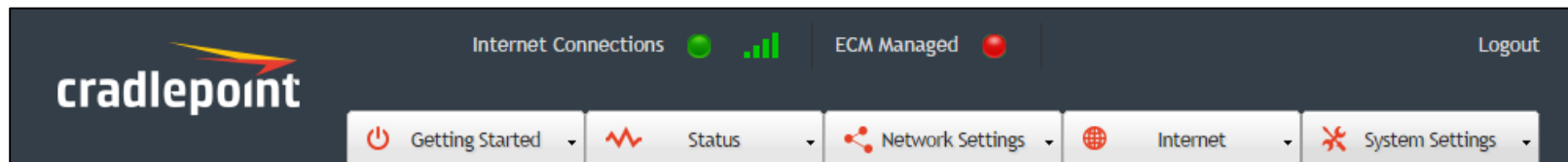
- If your USB modem is not working with the router, check the list of supported devices at <http://www.Cradlepoint.com/modems> to ensure you are using a supported device and carrier. The device you are using must be supported on the carrier network providing your cellular service or it's considered an unsupported device, even if it is supported on another carrier's network.
- Sometimes a USB data modem needs to be updated or have other configurations set correctly in order to make a connection through the router. If your USB Modem has not been updated recently, it is recommended that you do so if it is having trouble connecting to the CBA850. Insert your USB data modem into your PC and access the Internet using the software provided by your cellular carrier. Follow the directions provided to complete the update. Once you have updated your USB data modem, reconnect the cellular device to your Cradlepoint router and connect to the Internet.
- Some wireless carriers provide more than one Access Point Name (APN) that a modem can connect to. If you wish to specify the APN, this can be done on the administration pages. Log in using the hostname "[cp/](#)" or IP address "<http://192.168.0.1>" in your browser. Go to **Internet → Connection Manager**. In the **WAN Interfaces** section, select your modem and click "Edit." Select the **SIM/APN Settings** tab. There is an Access Point Name field: Set the APN and click **Submit**. Some APN examples are **isp.cingular**, **ecp.tmobile.com**, and **vpn.com**. The modem must be removed and reinserted (or the router must be rebooted) for this change to take effect.
- If the above issues have been resolved and you can connect to the router but you cannot get Internet through it using your modem, you may need to upgrade the router firmware. Use your computer (you may need to plug your modem directly into your computer if you don't have another way to access the Internet) to download the latest firmware for the router at <http://www.Cradlepoint.com/firmware/CBA850>. Then log into the router administration pages and manually upload the firmware. Go to **System Settings → System Software** and click on "Manual Firmware Upload."

If you are still unable to access the Internet after following the above directions, contact Cradlepoint Technical Support for further assistance.

4 WEB INTERFACE -- ESSENTIALS

The CBA850 has a Web interface for configuration and administration of all features. The interface is organized with five tabs at the top of the screen:

- Getting Started
- Status
- Network Settings
- Internet
- System Settings

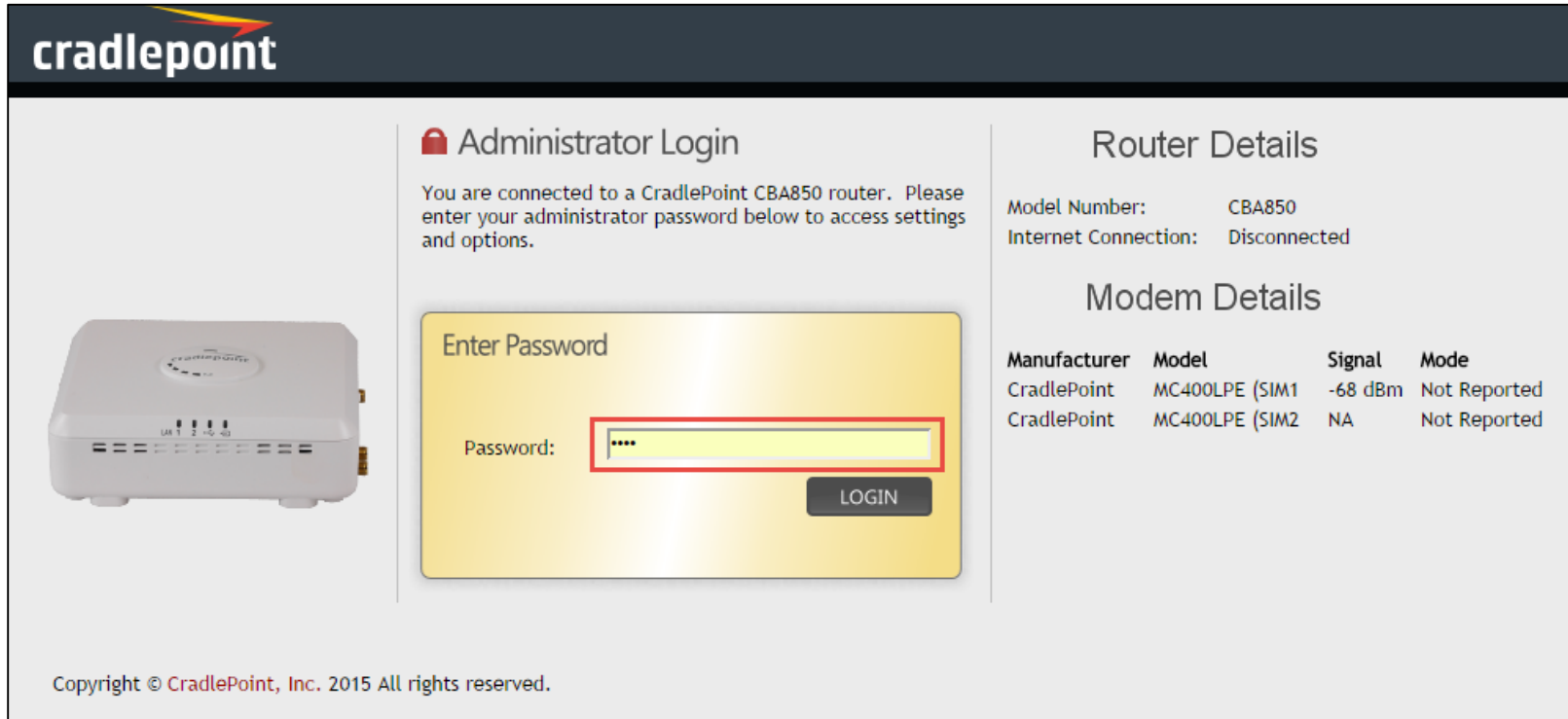


Web Interface – Essentials contains the following sections to help you more quickly and easy navigate these administration pages:

- 4.1 Administrator Login
- 4.2 Getting Started – First Time Setup
- 4.3 Quick Links
- 4.4 Configuration Pages
- 4.5 IP Passthrough Setup

4.1 Administrator Login

To access the administration pages, open a Web browser and type the hostname “[cp/](#)” or IP address “[http://192.168.0.1](#)” into the address bar. The Administrator Login page will appear.



Administrator Login

You are connected to a CradlePoint CBA850 router. Please enter your administrator password below to access settings and options.

Enter Password

Password:

LOGIN

Router Details

Model Number: CBA850
Internet Connection: Disconnected

Modem Details

Manufacturer	Model	Signal	Mode
CradlePoint	MC400LPE (SIM1)	-68 dBm	Not Reported
CradlePoint	MC400LPE (SIM2)	NA	Not Reported

Copyright © CradlePoint, Inc. 2015 All rights reserved.

Log in using your administrator password. Initially, this password can be found on the bottom of the CBA850 unit as the **Default Password**. This password is also the last eight digits of the unit’s MAC address. You may have changed the administrator password during initial setup using the First Time Setup Wizard. Log in using your personalized administrator password.



If you have forgotten your personalized password, you can reset the CBA850 to factory defaults. When you reset the router, the administrator password will revert back to the **Default Password**. Press and hold the **reset button** on the router unit until the lights flash (approximately 10-15 seconds). You can then log in using the **Default Password**.

4.1.1 Router Details

The Administrator Login page includes a quick-reference section that shows the following information:

ROUTER DETAILS

- **Model Number:** CBA850
- **Internet Connection:** Connected/Disconnected

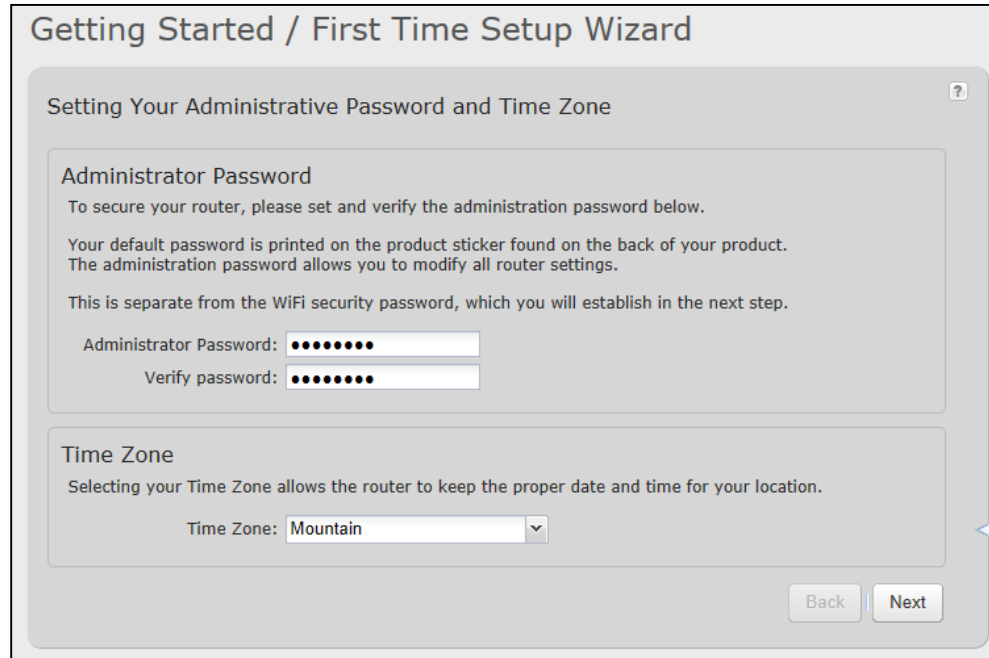
MODEM DETAILS

- **Manufacturer:** The name of the modem manufacturer (Cradlepoint, Novatel, etc.)
- **Model:** The name of the modem model
- **Signal:** The strength of the signal (dBm)
- **Mode:** (LTE, EVDO, HSPA, etc.)

4.2 Getting Started – First Time Setup

The **First Time Setup Wizard** will help you configure your APN and failure check settings and change your administrator password to something you choose.

1. Open a browser window and type “[cp/](#)” or “[192.168.0.1](#)” into the address bar. Press enter/return.
2. When prompted for your password, type the eight character **Default Password** found on the product label on the bottom of the CBA850 (this is also the last eight digits of the router’s MAC address).
3. When you log in for the first time, you will be automatically directed to the **First Time Setup Wizard**. (Otherwise, go to **Getting Started → First Time Setup**).
4. Cradlepoint recommends that you change the router’s **ADMINISTRATOR PASSWORD**, which is used to log in to the administration pages.
5. You can select your **TIME ZONE** from a dropdown list. (This may be necessary to properly show time in your router log, but typically your router will automatically determine your time zone through your browser.) Click **NEXT**.



6. Configuring Your Access Point Name (APN)

If you are using a SIM-based modem (LTE/GSM/HSPA) with your Cradlepoint router, you may need to configure the APN before it will properly connect to your carrier. Wireless carriers offer several APNs, so check with your carrier to confirm the appropriate one to use. Some examples include:

- AT&T: "broadband"
- T-Mobile: "epc.tmobile.com"
- Rogers LTE: "lteinternet.apn"
- Bell: "inet.bell.ca"
- TELUS: "isp.telus.com"

You can either leave this on the **Default** setting or select **Manual** and input a specific APN.

If your specific modem or SIM already has APNs programmed into it, you should leave this on the **Default** setting. After finishing this Wizard go to **Internet** → **Connection Manager**, select your modem, and edit the settings. The SIM PIN/APN tab has more available settings than are provided here.

Access Point Name (APN)

If you are using a SIM-based modem (LTE/GSM/HSPA) with your CradlePoint router you may need to configure the APN before it will properly connect to your carrier. Wireless carriers offer several APNs so check with your carrier to confirm the appropriate one to use.

Access Point Name (APN): ☒ Default
☐ Manual

DON'T USE THIS APN WIZARD if you have already configured an APN. Any specific modem settings will not be overwritten by this generic APN setup. Leave this setting as default and after finishing this Wizard go to the [Connection Manager](#) page, select your modem, and edit the settings. The SIM PIN/APN tab has more available settings than are provided here.

7. Modem Authentication

Some modems require a username and password to be entered to authenticate with a carrier. Do not fill in these fields unless you are sure your modem needs authentication.

Modem Authentication

Some modems require a username and password to be entered to authenticate with a carrier. Do not fill in these fields unless you are sure your modem needs authentication.

Authentication Protocol: 

Username:

Password:

- **Authentication**

Protocol – Set this only if your service provider requires a specific protocol and the **Auto** option chooses the wrong one.

Select from:

- o **Auto**
 - o **Pap**
 - o **Chap**
- **Username**
- **Password**

8. Configuring Failure Check

It is possible for a WAN interface to go down without the router recognizing the failure. (For example: the carrier for a cellular modem goes dormant.) Enable Failure Check to ensure that you can get out to the Internet via your primary WAN connection. This option is disabled by default because it may use data unnecessarily. Use this in combination with failover or Aggressive Reset (**Internet** → **Connection Manager** under Modem Settings in the interface/rule editor).

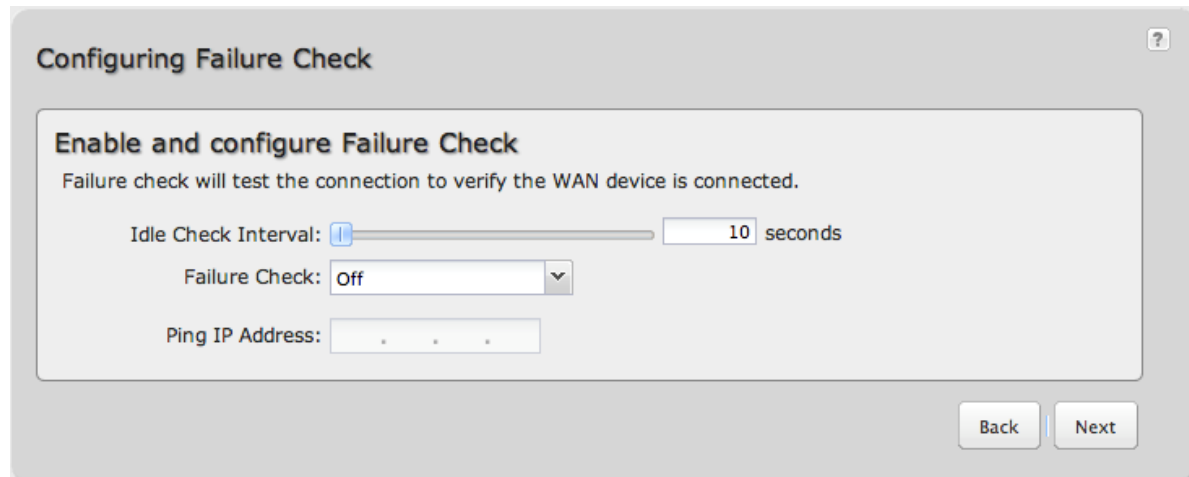
Idle Check Interval: Set the number of seconds the router will wait between checks to see if the WAN is still available. (Default: 30 seconds. Range: 10-3600 seconds.)

Monitor while connected: Select from the dropdown menu. (Default: Off)

- **Active Ping:** A ping request will be sent to the Ping Target. If no data is received, the ping request will be retried 4 times at 5-second intervals. If still no data is received, the device will be disconnected and failover will occur. When “Active Ping” is selected, the next line gives an estimate of data usage in this form: “Active Ping could use as much as **9.3 MB** of data per month.” This amount depends on the Idle Check Interval.
- **Off:** Once the link is established the router takes no action to verify that it is still up.

Ping IP Address: If you selected “Active Ping”, you will need to input an IP address that will respond to a ping request. This IP address must be an address that can be reached through your WAN connection. Some ISPs/Carriers block certain addresses, so choose an address that all of your WAN connections can use. For best results, select an established public IP address. *For example, you might ping Google Public DNS at 8.8.8.8 or Level 3 Communications at 4.2.2.2.*

Click **NEXT**.



9. Review the details and record your administrative password.
Click **APPLY** to save the settings and update them to your router.

Applying Your New Settings

Summary

Below is a detailed summary of your system settings. Please record these newly established router settings for future access.

When you are satisfied with the configuration, select the 'Apply' button below.

Administrator Password: *****

Time Zone: (UTC -7) Mountain

Access Point Name (APN): Default (router will choose APN automatically)

Idle Check Interval: 30

Monitor while connected: Off

Ping IP Address:

Apply

Back | Next

4.3 Quick Links



The Cradlepoint logo in the upper left-hand corner of all the administration pages is a link to the Dashboard (**Status** → **Dashboard**), which displays fundamental information about the router.

The black bar across the top provides quick access to important information and controls.



INTERNET CONNECTIONS

This links to **Status** → **Internet Connections** where you can view in-depth information about your Internet sources.

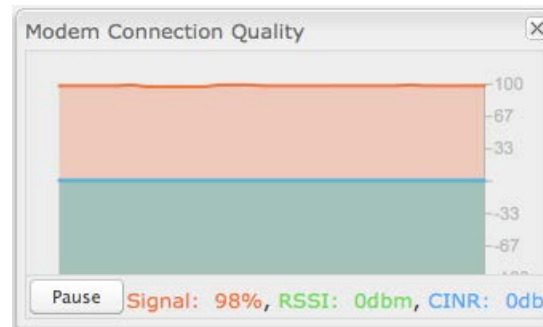


Click on the green dot to link to **Internet** → **Connection Manager** where you can manage your WAN interface(s).



Click on the image of four signal bars to open a “Modem Connection Quality” popup window that shows the strength of your Internet signal.

Logout Click to log out of the administration pages.



4.4 Configuration Pages

The following table shows the navigation layout of the administration pages. Click on the tabs along the top bar to reveal the following dropdown menus.

Getting Started	Status	Network Settings	Internet	System Settings
Enterprise Cloud Manager Registration First Time Setup IP Passthrough Setup	Client List Dashboard GPS Internet Connections Routing Statistics System Logs	Content Filtering DHCP Server DNS Firewall Local Networks MAC Filter/Logging Routing	Connection Manager Data Usage WAN Affinity/Load Balancing	Administration Device Alerts Enterprise Cloud Manager Serial Redirector SNMP Configuration System Control System Software

Getting Started – Setup wizards for Enterprise Cloud Manager, First Time Setup, and IP Passthrough. *NOTE: IP Passthrough Setup should not be needed as LAN Port 2 is pre-configured.*

Status – Displays various types of information about your router such as a list of clients that are attached to your networks (**Client List**), the details of each Internet source your router is using (**Internet Connections**), and a map of your router's location (**GPS**). Very few changes can be made from this tab because the primary purpose is to display information.

Network Settings – Provides configuration options for the network(s), or LAN, created by your router. For example, you can enable a VLAN (**Local Networks**) or set up rules to filter websites (**Content Filtering**).

Internet – Provides configuration options for the Internet sources, or WAN, used by the router. For example, you can set up a rule to track how much data you are using per month on a modem (**Data Usage**) or set the APN for a modem (**Connection Manager**).

System Settings – Provides broad administrative controls. For example, you can upgrade firmware (**System Software**), or enable remote management of the router (**Administration**).

4.4.1 Network Settings vs. Internet

When using the Web interface, it will be important to pay attention to the difference between the **Internet source** for your CBA850 and the **network** created by the CBA850. The “**Internet**” tab broadly refers to the router’s source of Internet, while the “**Network Settings**” tab broadly refers to the network created by the router.

Internet tab	Network Settings tab
Internet “input” Source for CBA850 WAN (Wide Area Network)	Internet “output” Network created by CBA850 LAN (Local Area Network)

Examples:

- If you want to change the content filtering settings for the network created by the CBA850, go to the **Network Settings** tab.
- If you want to track the data usage for your Internet source (such as your Cradlepoint business-grade modem), go to the **Internet** tab.



4.5 Enterprise Cloud Manager Registration

To register your device with Cradlepoint Enterprise Cloud Manager, navigate to **Getting Started** → **Enterprise Cloud Manager Registration**.

Input your **ECM Username** and **ECM Password** and click **Register**. You have now registered the device with Enterprise Cloud Manager.

If you do not have ECM credentials, see <http://www.Cradlepoint.com/ecm> for details or sign up at <http://www.Cradlepoint.com/ecm-signup>.

4.6 IP Passthrough Setup

The CBA850's IP passthrough function takes the IP address of the attached modem and passes it through to the LAN. By default, the CBA850 is configured for IP passthrough. Using IP passthrough disables some of the device's other router functionality.

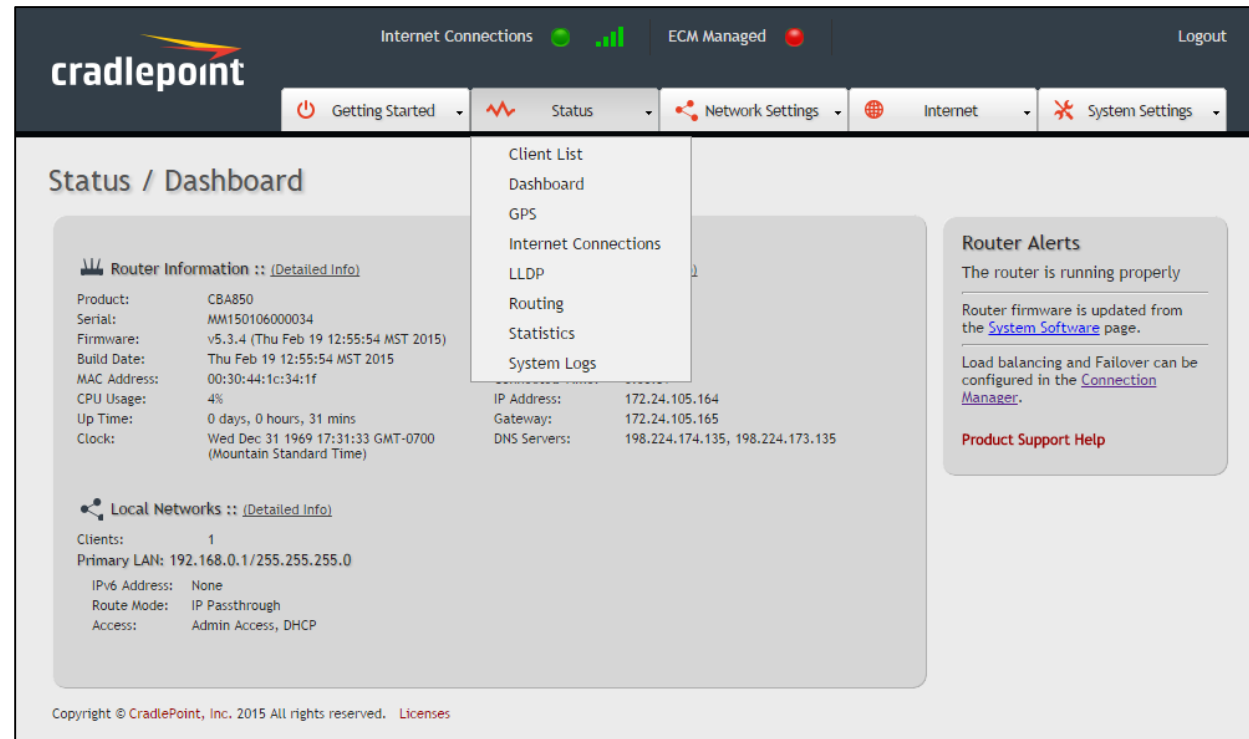
There are two methods for setting up IP passthrough:

1. In the administration pages, select **Getting Started** → **IP Passthrough Setup**. Simply read through the wizard and select **Enable IP Passthrough** on the second page.
2. For custom configuration, manually input IP passthrough settings in the administration pages (this is the preferred method for network professionals). Go to **Network Settings** → **Local Networks** for most of these changes. Depending on your settings, you may need to go to other pages as well (e.g. you may need to disable load balancing).

5 STATUS

The Status tab displays information about many different aspects of the router. It provides access to eight submenu options:

- Client List
- Dashboard
- GPS
- Internet Connections
- LLDP
- Routing
- Statistics
- System Logs



Status / Dashboard

Router Information :: (Detailed Info)

Product:	CBA850	IP Address:	172.24.105.164
Serial:	MM150106000034	Gateway:	172.24.105.165
Firmware:	v5.3.4 (Thu Feb 19 12:55:54 MST 2015)	DNS Servers:	198.224.174.135, 198.224.173.135
Build Date:	Thu Feb 19 12:55:54 MST 2015		
MAC Address:	00:30:44:1c:34:1f		
CPU Usage:	4%		
Up Time:	0 days, 0 hours, 31 mins		
Clock:	Wed Dec 31 1969 17:31:33 GMT-0700 (Mountain Standard Time)		

Local Networks :: (Detailed Info)

Clients:	1
Primary LAN:	192.168.0.1/255.255.255.0
IPv6 Address:	None
Route Mode:	IP Passthrough
Access:	Admin Access, DHCP

Router Alerts

The router is running properly

Router firmware is updated from the [System Software](#) page.

Load balancing and Failover can be configured in the [Connection Manager](#).

[Product Support Help](#)

Copyright © CradlePoint, Inc. 2015 All rights reserved. [Licenses](#)

5.1 Client List

The Client List displays the **Hostname**, **IP**, and **MAC** of the device connected to your router.

Status / Client List



Hostname	IP	MAC
jcramer-osx	192.168.0.121	c8:2a:14:38:22:be

Hostname: The name by which each computer or device in a network is known.

IP: The IP address, or “Internet Protocol address”, specifies a location for each device.

MAC: This is the “MAC address”, a factory-assigned identifier used to identify a specific attached computer or device.



5.2 Dashboard

The **Dashboard** shows fundamental information about your router, divided into the following basic categories:

- **Router Information**
- **Internet**
- **Local Networks**

For more in-depth information and/or configuration options, click on the **Detailed Info** link beside the category title. For each category, this links to:

Router Information: **System Settings** → **Administration**

Local Networks: **Network Settings** → **Local Networks**

Internet: **Internet** → **Connection Manager**

Router Information :: (Detailed Info)		Internet :: (Detailed Info)	
Product:	CBA850	State:	Connected
Serial:	MM150106000034	WAN Type:	Modem
Firmware:	v5.3.4 (Thu Feb 19 12:55:54 MST 2015)	Connection Type:	EVDO-A
Build Date:	Thu Feb 19 12:55:54 MST 2015	Signal Strength:	-59 dBm
MAC Address:	00:30:44:1c:34:1f	Connected Time:	0:06:59
CPU Usage:	4%	IP Address:	172.24.105.164
Up Time:	0 days, 0 hours, 31 mins	Gateway:	172.24.105.165
Clock:	Wed Dec 31 1969 17:31:33 GMT-0700 (Mountain Standard Time)	DNS Servers:	198.224.174.135, 198.224.173.135

Local Networks :: (Detailed Info)	
Clients:	1
Primary LAN:	192.168.0.1/255.255.255.0
IPv6 Address:	None
Route Mode:	IP Passthrough
Access:	Admin Access, DHCP



After the initial setup of the router, every time you log in you will automatically be directed to this **Dashboard**. Also, you can click on the Cradlepoint logo in the upper left-hand corner to return to the **Dashboard** from any page.

ROUTER INFORMATION

“Detailed Info” links to **System Settings → Administration**.

- **Product:** CBA850
- **Serial:** Device serial number
- **Firmware:** Gives the number of the current firmware version
- **Build Date:** Year-month-day-hours-minutes-seconds for the most recent firmware upgrade
- **MAC Address:** The router’s unique identifier
- **CPU Usage:** Expressed as a percentage
- **Up Time:** Total time for current session
- **Clock:** Current local date and time

To check for firmware upgrades, see **System Settings → System Software**.

INTERNET

“Detailed Info” links to **Internet → Connection Manager**.

- **State:** Connected/Disconnected
- **Signal Strength:** Expressed as a percentage
- **WAN Type:** Modem
- **Connection Type:** LTE, HSPA, etc.
- **Connected Time:** The time the current Internet source (WAN) has been connected
- **IP Address**
- **Gateway**
- **DNS Servers**

For configuration options, see **Internet → Connection Manager**.

The IP address and gateway describe your active WAN source.

For DNS server configuration options, see **Network Settings → DNS**.

LOCAL NETWORKS

“Detailed Info” links to **Network Settings** → **Local Networks**.

- **Clients:** The number of current clients.

For each network, the following information is displayed:

- **Network Name: IP Address/Netmask**
 - o **Route Mode:** NAT (Network Address Translation), Standard (NAT-less), IP Passthrough, or Disabled.
 - o **Access:** Admin Access, LAN Isolation, UPnP (Universal Plug and Play), and/or DHCP.

To configure a network, see **Network Settings** → **Local Networks**.

5.2.1 Router Alerts

On the right side of the **Dashboard** page is a brief set of “**Router Alerts**” that state basic information such as whether the router is running properly and/or if new firmware is available.

Router Alerts includes links to the **System Software** page (for new firmware) and the **Connection Manager**.

Router Alerts

The router is running properly

Router firmware is updated from the [System Software](#) page.

Load balancing and Failover can be configured in the [Connection Manager](#).

Product Support Help

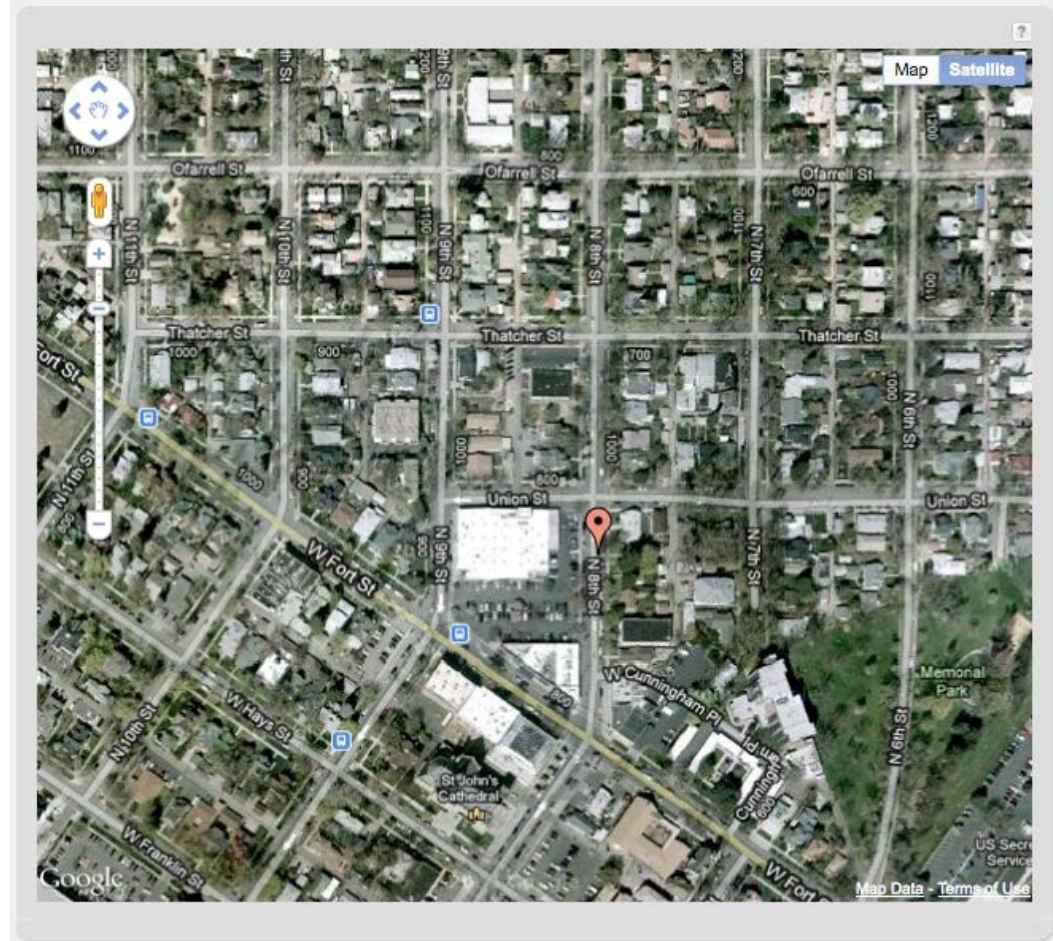
5.3 GPS

If GPS support is enabled and a modem capable of providing GPS coordinates is connected, this page shows a graphical view of your router's location.

See the GPS section in **System Settings** → **Administration** to enable GPS support.

GPS information is only displayed if 1) the modem supports GPS, 2) your carrier allows the GPS functionality, and 3) the modem has sufficient GPS signal strength. If no information is displayed, check that both the modem and your carrier support GPS. If GPS is supported, make sure the modem is in an area where it can receive a signal from the GPS satellites.

Status / GPS Status





5.4 Internet Connections

The Internet Connections submenu option provides a list of attached WAN devices used as the Internet source for the CBA850. Select one of these devices to see detailed information about that particular device.

Device List

	Device
☒	LTE: MC400LPE (SIM1)
☐	LTE: MC400LPE (SIM2)

Device Information: MC400LPE (SIM2)

Property	Value
Summary	
Modem	
Cellular Network	
General Information	
IPv4 Information	
Statistics	

See screenshots below for included detailed information.

Property	Value
Summary	
State	connected
Manufacturer	CradlePoint Inc.
Model	MC400LPE (SIM2)
Modem Firmware Version	SW19X15C_05.05.16.02 r21040 carmd-fwbuild1 2014/03/17 23:49:48
Service Display	EVDO-A
Home Carrier	Verizon
Roaming Status	Home
Signal Strength	100 %
RSSI	-68 dBm
SINR	9.0 dB
Ec/Io	-1.0 dBm
Mobile Directory Number	0000000000
MEID	A100001E7D02C5
IMEI	353547060481325
Network Address Identifier (NAI)	0020008381@vzims.com
Current APN	vzwinternet
IP Address	172.24.203.130
Netmask	255.255.255.252
Gateway	172.24.203.129
DNS Servers	198.224.174.135,198.224.173.135

Property	Value
Summary	
Modem	
Manufacturer	CradlePoint Inc.
Product	MC400LPE (SIM2)
Model	MC400LPE (SIM2)
Firmware Version	SW19X15C_05.05.16.02 r21040 carmd-fwbuild1 2014/03/17 23:49:48
Current Package Version	05.05.16.02_VZW,005.013_010
Mobile Directory Number	0000000000
ESN/IMEI	0x80CE8C37
MEID	A100001E7D02C5
IMEI	353547060481325
ICCID	89148000000069936194
IMSI	311480007275237
PRI ID	9903437
PRI Version	05.03
PIN Status	READY
Chipset	9X15C
Hardware Version	1.0

Property	Value
Summary	
Modem	
Cellular Network	
Home Carrier	Verizon
Roaming Status	Home
Carrier Status	UP
Connection State	Active
Service Display	EVDO-A
Signal Strength	100 %
RSSI	-52 dBm
SINR	9.0 dB
Ec/Io	-1.0 dBm
Profile 1:	vzwims
Profile 2:	vzwadmin
Profile 3:	vzwinternet
Profile 4:	vzwapp
Profile 5:	vzw800
Profile 6:	vzwadmin
Profile 9:	vzwims
Profile 10:	vzwadmin
Profile 11:	vzwinternet
Profile 12:	vzwapp
Profile 13:	
System ID	272 (0x110)
Network ID	1 (0x1)
Base Station ID	340 (0x154)
Base Station Latitude	0d 0m 0s
Base Station Longitude	0d 0m 0s
Operating Mode	Online
System Mode	HDR
IMS Registration State	No service
PS State	Attached
PRL Version	15003
RF Band	CDMA Band Class 0 (800 MHz)
RF Channel	630
EVDO Tx Power	-33.0 dBm
Network Address Identifier (NAI)	0020008381@vzims.com
Profile	0 Enabled
Home Address	0.0.0.0
Primary Home Agent	255.255.255.255
Secondary Home Agent	255.255.255.255
MN-AAA SPI	2
MN-HA SPI	300
MN-AAA SS	Set
MN-HA SS	Set
Reverse Tunneling	1
EVDO Color Code	78
EVDO Section ID	0080:0580:0000:0033:180a:f8f1:2900:5401
EVDO PIN Offset	495
EVDO AAA Auth Status	Success
Home PLMN ID	311480



Property	Value
⊞ Summary	
⊞ Modem	
⊞ Cellular Network	
⊞ General Information	
Unique Identifier	9cf6dd3e
Port	modem1
Type	lte
Model	MC400LPE (SIM2)

Property	Value
⊞ Summary	
⊞ Modem	
⊞ Cellular Network	
⊞ General Information	
⊞ IPv4 Information	
IP Address	172.24.87.83
Netmask	255.255.255.248
Gateway	172.24.87.81
DNS Servers	198.224.184.135,198.224.185.135



Property	Value
⊞ Summary	
⊞ Modem	
⊞ Cellular Network	
⊞ General Information	
⊞ IPv4 Information	
⊞ Statistics	
Connection Uptime	0:01:05

5.5 LLDP

The LLDP (Link Layer Discovery Protocol) submenu option provides a list of devices connected by Ethernet that have LLDP enabled.

LLDP Neighbors				
Interface	Sys Name	Sys Descr.	Port Descr.	Manufacturer
eth0.1	MBR1400-f76	CradlePoint_MBR140...	eth0.2	CradlePoint

Double-click on a device to view details for that device. The information displayed in this popup window varies significantly for different types of devices with different LLDP implementations.

Interface Details	
eth0.1, via: LLDP, RID: 2, Time: 0 day, 00:11:02	
Chassis:	
ChassisID:	mac 00:30:44:14:ff:76
SysName:	MBR1400-f76
SysDescr:	CradlePoint_MBR1400v2_5.3.0
MgmtIP:	203.0.113.70
Capability:	Bridge, on
Capability:	Router, on
Capability:	Wlan, on
Capability:	Station, off
Port:	
PortID:	mac 2a:30:44:14:ff:76
PortDescr:	eth0.2
LLDP-MED:	
Device Type:	Network Connectivity Device
Capability:	Capabilities
Capability:	Policy
Capability:	Location
Capability:	MDI/PSE
Capability:	MDI/PD
Capability:	Inventory
Inventory:	
Software Revision: 3.10.48-coconut	
Firmware Revision: 5.3.0	
Manufacturer: CradlePoint	

To enable LLDP for Ethernet on the WAN and/or LAN side, go to **System Settings** → **Administration** and select the LLDP tab.

5.6 Routing

System Routes displays routes associated with networks connected to the router.

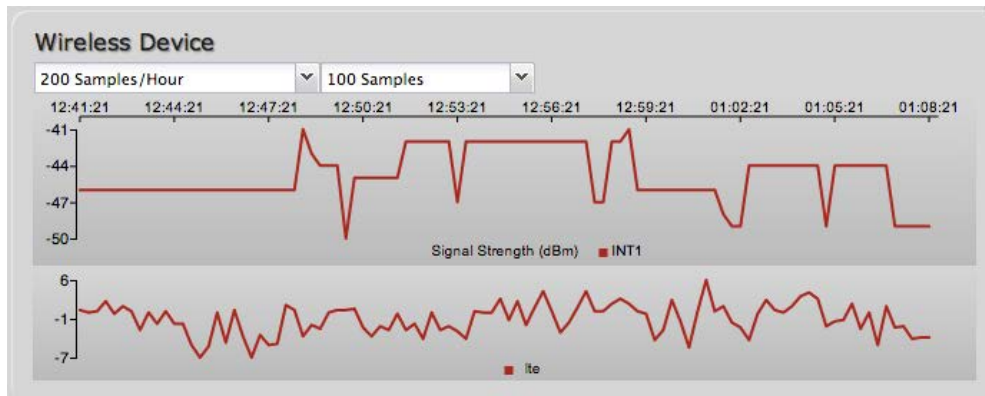
System Routes				
IP Address	Gateway	Netmask	Interface	Routing Protocol
172.22.0.0		255.255.0.0	wan-0	
192.168.11.0		255.255.255.0	primarylan	

Static Routes displays user-specified routes configured in **Network Settings → Routing**.

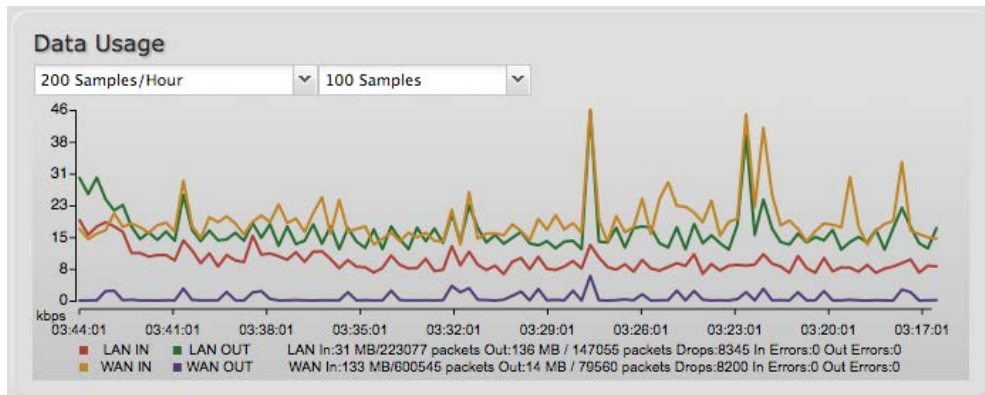
Static Routes			
IP Address	Gateway	Netmask	Interface
192.168.0.0	172.22.22.1	255.255.255.0	wan-0

5.7 Statistics

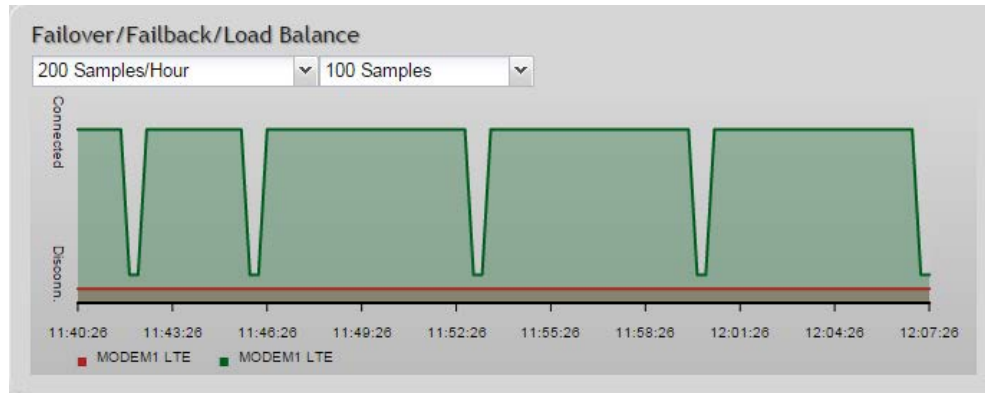
The Statistics submenu option displays basic traffic statistics.



Wireless Statistics: View the signal strength and other wireless modem information. The wireless device's signal strength will only be displayed as long as it supports "Live Diagnostics." Sample rate and size can be adjusted from the dropdown boxes.



Data Usage: A measure of amount of information that is currently being sent or received through the network. Sample rate and size can be adjusted from the dropdown boxes.



Failover/Failback/Load Balance: An easy way to view current connective states of the devices plugged into the router as compared to the past. Sample rate and size can be adjusted from the dropdown boxes.

5.8 System Logs

The router automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained. The log options allow you to filter the router logs so you can easily find relevant messages. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

Auto Update: The logs automatically refresh whenever the router creates a new message.

Update: Click to check for new router messages.

Clear Log: Clear the log file.

Save Log: This will open a dialog in your browser that will allow you to save the router's log to your computer.

Search: Enter keywords to find specific events.

Level: Select/Deselect from the following levels to filter messages by priority.

- Critical
- Error
- Warning
- Info

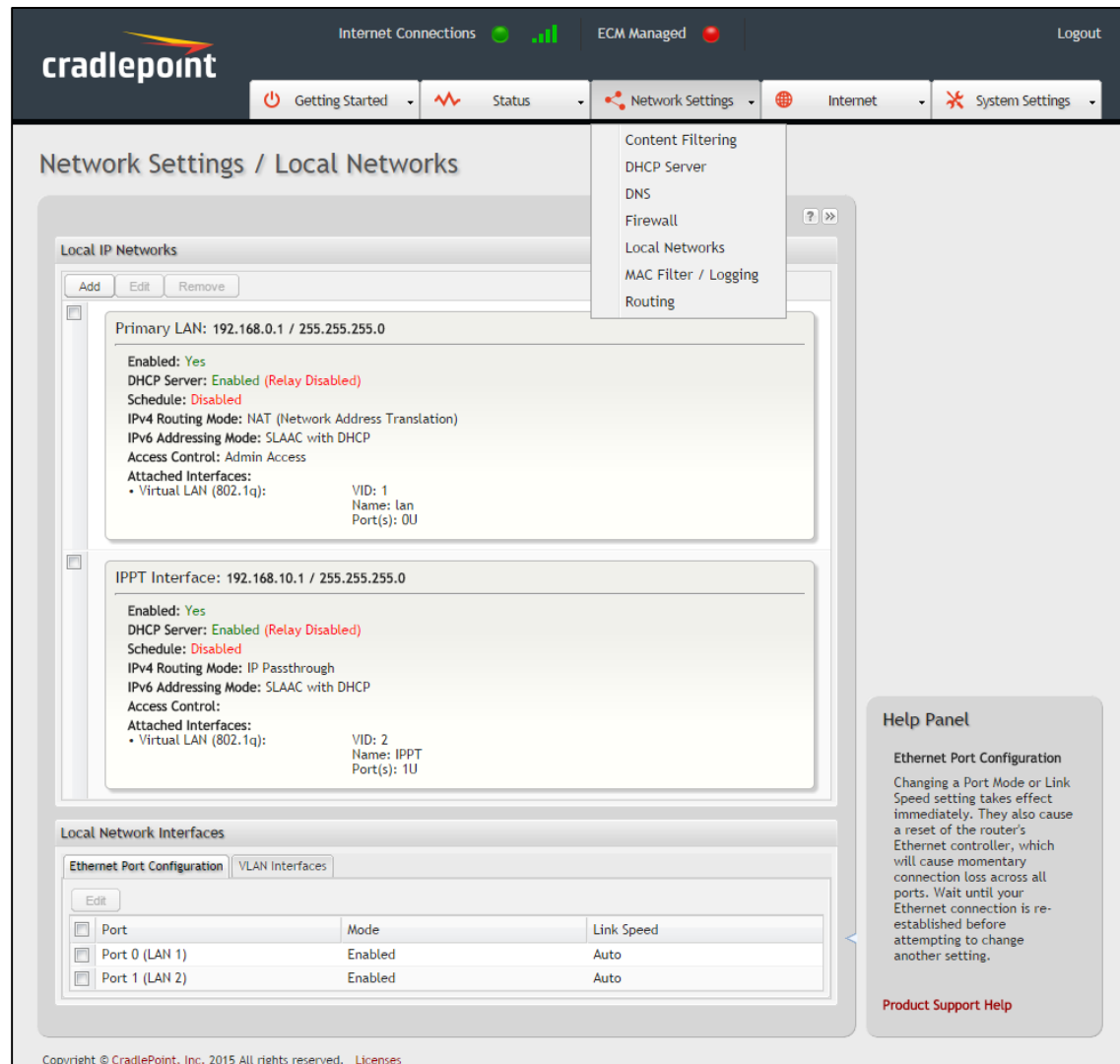
NOTE: The logs are erased whenever the router is rebooted or loses power.

☐ Auto Update Update Clear log Save Log search filter... Level ▼			
Time	Source	Level	Message
Thu Dec 13th 10:08:56	wlan	INFO	Client e4:ce:8f:13:f3:bc WPA2 key negotiation completed
Thu Dec 13th 09:59:17	WAN:2043	INFO	signal: 92% -> 100%
Thu Dec 13th 09:58:17	WAN:2043	INFO	signal: 100% -> 92%
Thu Dec 13th 09:57:17	WAN:2043	INFO	signal: 92% -> 100%
Thu Dec 13th 09:56:16	WAN:2043	INFO	signal: 100% -> 92%
Thu Dec 13th 09:55:16	WAN:2043	INFO	signal: unknown -> 100%
Thu Dec 13th 09:55:16	WAN:2043	INFO	Plug event: ok
Thu Dec 13th 09:55:10	kernel	INFO	usbcore: registered new interface driver cpusb5
Thu Dec 13th 09:55:09	kernel	INFO	sd 9:0:0:0: [sda] Attached SCSI removable disk
Thu Dec 13th 09:55:09	kernel	INFO	scsi 9:0:0:0: Direct-Access Nokia Datacard CD-ROM 0001 PQ: 0 ANSI: 0
Thu Dec 13th 09:55:08	kernel	INFO	scsi9 : usb-storage 1-2.1:1.6
Thu Dec 13th 09:55:08	kernel	INFO	usb 1-2.1: new high speed USB device number 13 using rt3xxx-ehci
Thu Dec 13th 09:55:08	kernel	INFO	usb 1-2.1: USB disconnect, device number 12

6 NETWORK SETTINGS

The Network Settings tab provides access to seven submenu options for administering the following functions/tasks. These functions are all related to controlling the LAN (Local Area Networks), the networks you set up with the CBA850.

- Content Filtering
- DHCP Server
- DNS
- Firewall
- Local Networks
- MAC Filter/Logging
- Routing



Internet Connections ● ● ● ECM Managed ● Logout

Getting Started ● Status ● Network Settings ● Internet ● System Settings ●

Network Settings / Local Networks

Local IP Networks

Add Edit Remove

Primary LAN: 192.168.0.1 / 255.255.255.0

Enabled: Yes
 DHCP Server: Enabled (Relay Disabled)
 Schedule: Disabled
 IPv4 Routing Mode: NAT (Network Address Translation)
 IPv6 Addressing Mode: SLAAC with DHCP
 Access Control: Admin Access
 Attached Interfaces:
 • Virtual LAN (802.1q): VID: 1
 Name: lan
 Port(s): 0U

IPPT Interface: 192.168.10.1 / 255.255.255.0

Enabled: Yes
 DHCP Server: Enabled (Relay Disabled)
 Schedule: Disabled
 IPv4 Routing Mode: IP Passthrough
 IPv6 Addressing Mode: SLAAC with DHCP
 Access Control:
 Attached Interfaces:
 • Virtual LAN (802.1q): VID: 2
 Name: IPPT
 Port(s): 1U

Local Network Interfaces

Ethernet Port Configuration VLAN Interfaces

Edit

Port	Mode	Link Speed
Port 0 (LAN 1)	Enabled	Auto
Port 1 (LAN 2)	Enabled	Auto

Help Panel

Ethernet Port Configuration

Changing a Port Mode or Link Speed setting takes effect immediately. They also cause a reset of the router's Ethernet controller, which will cause momentary connection loss across all ports. Wait until your Ethernet connection is re-established before attempting to change another setting.

[Product Support Help](#)

Copyright © CradlePoint, Inc. 2015 All rights reserved. Licenses

6.1 Content Filtering

You have two main options for filtering content in a network created by your router.

1. **Network WebFilter Rules:** Create a list of websites that will be either disallowed or allowed. Customize the filter settings for each network. (These rules will not block HTTPS websites.)
2. **OpenDNS Content Filtering:** Allows several options for filtering rules using OpenDNS, a third party service.



Filter Action	Domain / URL / IP Address	Rule Priority ▼	Enabled
---------------	---------------------------	-----------------	---------

6.1.1 Network WebFilter Rules

Network WebFilter Rules allow you to control access from your network to external domains or websites. Rules are assigned to a specific LAN network (or all networks). The highest priority rule will have precedence when there is a conflict. Addresses can be added by URL/Domain name or by IP address.

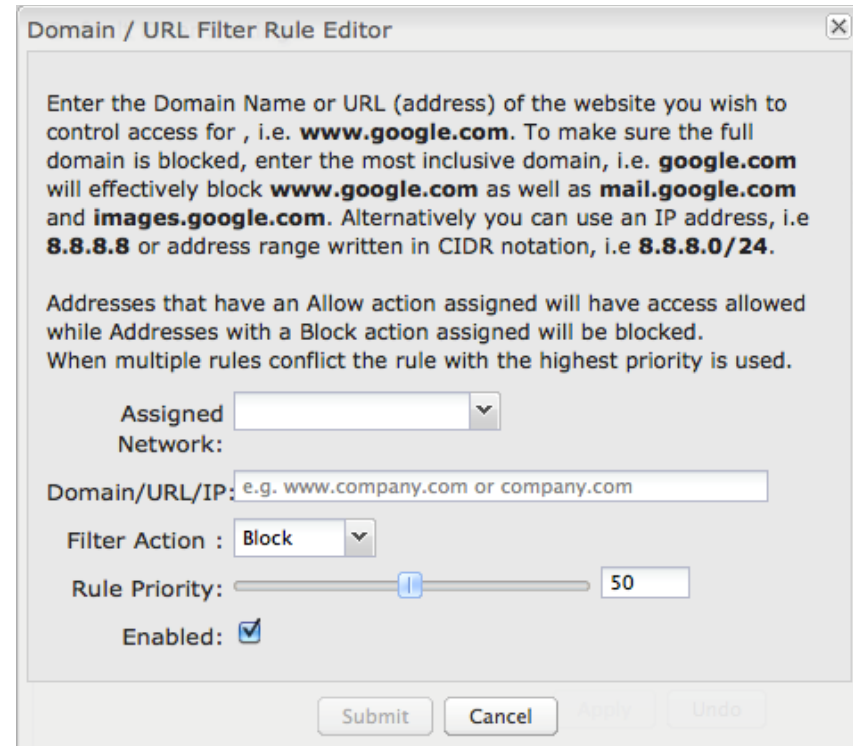
Exceptions to existing rules can be created by adding another rule with higher priority. For example, if access to espn.go.com is desired but go.com is blocked with a priority of 50, the addition of an “Allow” rule for espn.go.com with a priority of 51 or greater will allow access.

When creating rules keep in mind that some sites use multiple domains, so each domain may need a rule added to produce the desired behavior.

Click Add or Edit to open the **Filter Rule Editor**.

- **Assigned Network:** Select either “All Networks” or one of your LAN networks from the dropdown list.
- **Domain/URL/IP:** Enter the Domain Name or URL (address) of the website you wish to control access for, e.g. **www.google.com**. To make sure the full domain is blocked, enter the most inclusive domain (e.g. **google.com** will effectively block **www.google.com** as well as **maps.google.com** and **images.google.com**). Alternatively you can use an IP address, e.g. **8.8.8.8**, or address range written in CIDR notation, e.g. **8.8.8.0/24**.
- **Filter Action:** Select **Block** or **Allow**.
- **Rule Priority:** Higher number rules overrule lower number rules.
- **Enabled:** A rule can be enabled or disabled by selecting or deselecting the checkbox.

Click **Submit** to save your rule changes.



The image shows a screenshot of the 'Domain / URL Filter Rule Editor' dialog box. It contains the following fields and controls:

- Assigned Network:** A dropdown menu.
- Domain/URL/IP:** A text input field with a placeholder example: 'e.g. www.company.com or company.com'.
- Filter Action:** A dropdown menu currently set to 'Block'.
- Rule Priority:** A slider control with a numerical value of 50.
- Enabled:** A checkbox that is currently checked.
- Buttons:** 'Submit', 'Cancel', 'Apply', and 'Undo' at the bottom.

Instructions within the dialog box state: 'Enter the Domain Name or URL (address) of the website you wish to control access for, i.e. **www.google.com**. To make sure the full domain is blocked, enter the most inclusive domain, i.e. **google.com** will effectively block **www.google.com** as well as **mail.google.com** and **images.google.com**. Alternatively you can use an IP address, i.e. **8.8.8.8** or address range written in CIDR notation, i.e. **8.8.8.0/24**.' It also notes: 'Addresses that have an Allow action assigned will have access allowed while Addresses with a Block action assigned will be blocked. When multiple rules conflict the rule with the highest priority is used.'

6.1.2 Default Filter Settings

Default Network Filter Settings		
Edit		
Network Name	Default Action	Filter URLs by IP Address
Primary LAN	Allow Access	No
Guest LAN	Allow Access	No

Use **Default Network Filter Settings** together with **Network WebFilter Rules** to control website access. All of your networks are set to allow website access by default. Select a network and click **Edit** to change the default filter settings.

Default Action: Select from the following dropdown options:

- Allow Access (default)
- Block Access

When a network is set to **Allow Access**, it will allow access to sites not specifically *blocked* in the WebFilter Rules.

When a network is set to **Block Access**, it will block access to sites not specifically *allowed* in the WebFilter Rules.

Filter URLs by IP Address: (Default: No) Changing this option to "Yes" will cause the router to perform a DNS lookup on URL entries, and the IP addresses will be appended to the appropriate block/allow list. This can have the side effect of being very strict; sites that are hosted across many domains may need every domain added to the list for full functionality.

Change Default Network Filter Settings

When a network is set to Allow (Blacklist) it will allow access to any site not blocked in the Filter Rules. Selecting Block (Whitelist) will only allow access to websites with an assigned Allow action in the Filter rules, all other sites will be blocked.

Selecting to Filter URLs by IP Address will cause the router to perform a DNS lookup on URL entries and the IP addresses will be appended to the appropriate block/allow list. This can have side effect of being very strict and sites that are hosted across many domains may need every domain added the list for full functionality.

Default Action:

Filter URLs by IP Address:

6.1.3 Cloud Based Filtering/Security

Select a third-party **Cloud Provider** from the dropdown list.

- **Disabled**
- **Umbrella by OpenDNS**

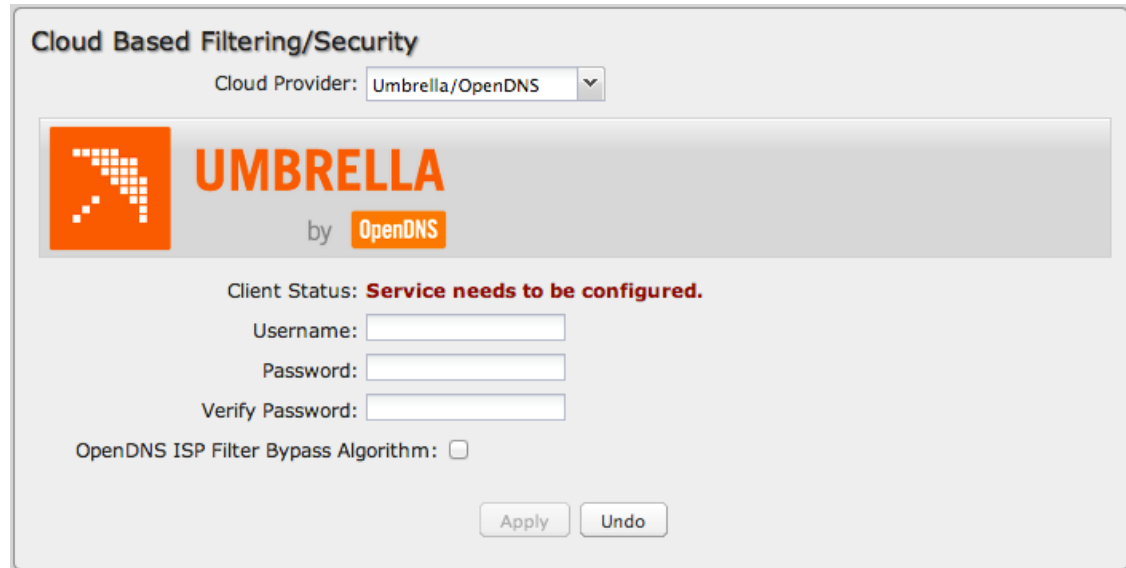
UMBRELLA BY OPENDNS

Umbrella by OpenDNS is a cloud-based web filtering and security solution that protects you online by filtering websites. Go to <http://www.opendns.com/business-security/> for information about Umbrella.

Enter your Umbrella account information in order to use these content filtering settings.

OpenDNS ISP Filter Bypass

Algorithm: It is possible that your Internet Service Provider (ISP) uses the port that OpenDNS is configured to access, port 53, which will prevent OpenDNS filtering. If OpenDNS does not appear to be working correctly, enabling this will attempt to bypass those ports when using an OpenDNS content filtering level.



The screenshot shows the 'Cloud Based Filtering/Security' configuration interface. At the top, the 'Cloud Provider' dropdown is set to 'Umbrella/OpenDNS'. Below this is the Umbrella logo, which consists of an orange square with a white pixelated arrow pointing up and to the right, followed by the word 'UMBRELLA' in large orange letters and 'by OpenDNS' in smaller text. The 'Client Status' is displayed in red as 'Service needs to be configured.'. Below the status are three input fields: 'Username:', 'Password:', and 'Verify Password:'. At the bottom left, there is a checkbox for 'OpenDNS ISP Filter Bypass Algorithm:'. At the bottom right, there are two buttons: 'Apply' and 'Undo'.

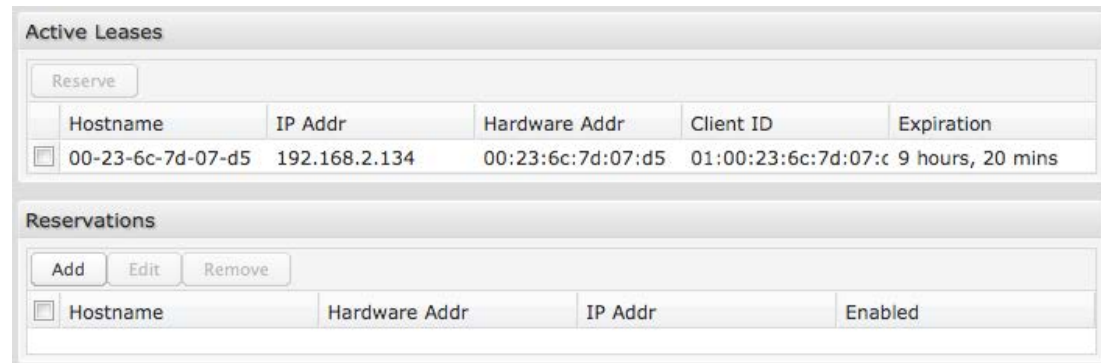
6.2 DHCP Server

DHCP stands for Dynamic Host Configuration Protocol. The built-in DHCP server automatically assigns IP addresses to the computers and other devices on each local area network (LAN). In this section you can view a list of assigned IP addresses and reserve IP addresses for particular devices.

Active Leases: A list of devices that have been provided DHCP leases. The DHCP server automatically assigns these leases. This list will not include any devices that have static IP addresses on the network. Select a device and click **Reserve** to add the device and its IP address to the list of **Reservations**.

Reservations: This is a list of devices with reserved IP addresses. This reservation is almost the same as when a device has a static IP address except that the device must still request an IP address from the router. The router will provide the device the same IP address every time. DHCP reservations are helpful for server computers on the local network that are hosting applications such as Web and FTP. Servers on your network should either use a static IP address or a reservation.

While you have the option to manually input the information to reserve an IP address (Hostname, Hardware Addr, IP Addr), it is much simpler to select a device under the **Active Leases** section and click “**Reserve**.” The selected device’s information will automatically be added under **Reservations**.



The screenshot shows the DHCP Server configuration interface. It has two main sections: 'Active Leases' and 'Reservations'.

Active Leases: This section has a 'Reserve' button at the top. Below it is a table with the following columns: Hostname, IP Addr, Hardware Addr, Client ID, and Expiration. There is one entry in the table with a checkbox on the left.

	Hostname	IP Addr	Hardware Addr	Client ID	Expiration
☐	00-23-6c-7d-07-d5	192.168.2.134	00:23:6c:7d:07:d5	01:00:23:6c:7d:07:c	9 hours, 20 mins

Reservations: This section has 'Add', 'Edit', and 'Remove' buttons at the top. Below them is a table with the following columns: Hostname, Hardware Addr, IP Addr, and Enabled. There is one empty row in the table with a checkbox on the left.

	Hostname	Hardware Addr	IP Addr	Enabled
☐				

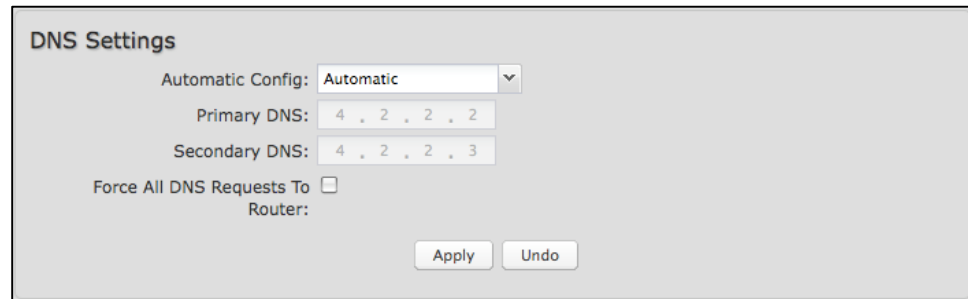
6.3 DNS

DNS, or Domain Name System, is a naming system that translates between domain names (www.Cradlepoint.com, for example) and Internet IP addresses (206.207.82.197). A DNS server acts as an Internet phone book, translating between names that make sense to people and the more complex numerical identifiers. The DNS page for the CBA850 has these distinct functions:

- **DNS Settings:** By default your router is set to automatically acquire DNS servers through your Internet provider (Automatic). **DNS Settings** allows you to specify DNS servers of your choosing instead (Static).
- **Dynamic DNS Configuration:** Allows you to host a server (Web, FTP, etc.) using a domain name that you have purchased (www.yourname.com) with your dynamically assigned IP address.
- **Known Hosts Configuration:** Allows you to map a name (printer, scanner, laptop, etc.) to an IP address of a device on the network.

6.3.1 DNS Settings

You have the option to choose specific DNS servers for your network instead of using the DNS servers assigned by your Internet provider. The default DNS servers are usually adequate. You may want to assign DNS servers if the default DNS servers are performing poorly or if you have a local DNS server on your network.



Automatic Config: Automatic or Static (default: Automatic). Switching to “Static” enables you to set specific DNS servers in the **Primary DNS** and **Secondary DNS** fields.

Primary DNS and **Secondary DNS:** If you choose to specify your DNS servers, enter the IP addresses of the servers you want as your primary and secondary DNS servers in these fields. The DNS server settings will be pre-populated with public DNS server IP addresses. You can override the IP address with any other DNS server IP address of your choice. For example, Google Public DNS servers have the IP addresses 8.8.8.8 and 8.8.4.4 while 4.2.2.2 and 4.2.2.3 are servers from Level 3 Communications.

Force All DNS Requests To Router: Enabling this will redirect all DNS requests from LAN clients to the router's DNS server. This will allow the router even more control over IP addresses even when clients have their own DNS servers statically set.

6.3.2 Dynamic DNS Configuration

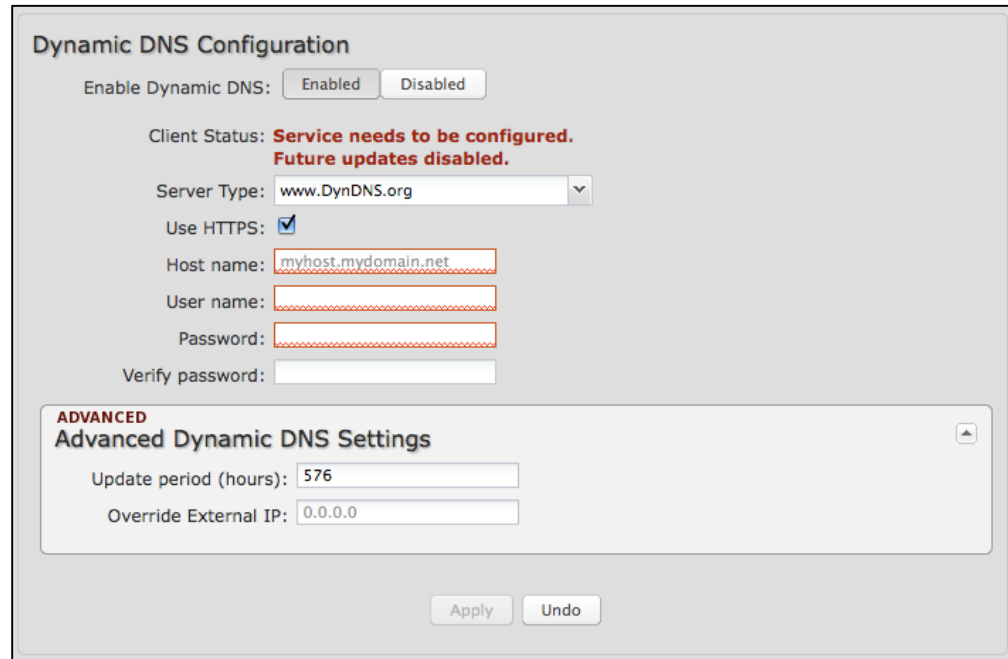
The Dynamic DNS feature allows you to host a server (Web, FTP, etc.) using a domain name that you have purchased (www.yourname.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. When you use a Dynamic DNS service provider, you can enter your host name to connect to your server, no matter what your IP address is.

Enable Dynamic DNS: Enable this option only if you have purchased your own domain name and registered with a Dynamic DNS service provider.

Server Type. Select a Dynamic DNS service provider from the pull-down list:

- www.DynDNS.org
- www.DNSomatic.com
- www.ChangeIP.com
- www.NO-IP.com
- Custom Server (DynDNS clone)

Custom Server Address. Only available if you select Custom Server from the Server Address dropdown list. Enter your custom dynamic DNS server address here. The server must support the Dynamic DNS protocol. See www.dyndns.org for details. Example: **myserver.mydomain.net**.



Use HTTPS: Use the more secure **HTTPS** protocol. This is recommended, but could be disabled if not compatible with the server.

Host name: Enter your host name, fully qualified. For example: **myhost.mydomain.net**.

User name: Enter the user name or key provided by the Dynamic DNS service provider. If the Dynamic DNS provider supplies only a key, enter that key for both the **User name** and **Password** fields.

Password: Enter the password or key provided by the Dynamic DNS service provider.

6.3.3 Advanced Dynamic DNS Settings

Update period (hours). (Default: 576) The time between periodic updates to the Dynamic DNS if your dynamic IP address has not changed. The timeout period is entered in hours so valid values are from 1 to 8760.

Override External IP. The external IP is usually configured automatically during connection. However, in situations where the unit is within a private network behind a firewall or router, the network's external IP address will have to be manually configured in this field.

You may find out what your external IP address is by going to <http://myip.dnsomatic.com/> in a web browser.

6.3.4 Known Hosts Configuration

The Known Hosts Configuration feature allows you to map a name (printer, scanner, laptop, etc.) to an IP address of a device on the network. This assigns a new hostname that can be used to conveniently identify a device within the network, such as an office printer.

Click **Add** to name a device in your network.

Fill in the following fields:

- **Hostname:** Choose a name that is meaningful to you. No spaces are allowed in this field.
- **IP address:** The address of the device within your network.

EXAMPLE: a personal laptop with IP address 192.168.0.164 could be assigned the name "MyLaptop".

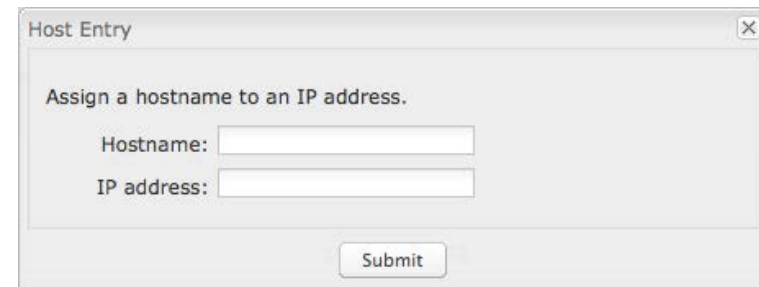
Since the assigned name is mapped to an IP address, the device's IP address should not change. To ensure that the device keeps the same IP address, go to **Network Settings** → **DHCP Server** and reserve the IP address for the device by selecting the device in the **Active Leases** list and clicking "Reserve".



Known Hosts Configuration

Buttons: Add, Edit, Remove

Hostname	IP address
MyLaptop	192.168.0.164



Host Entry

Assign a hostname to an IP address.

Hostname:

IP address:

Submit

6.4 Firewall

The router automatically provides a firewall. Unless you configure the router to the contrary, the router does not respond to unsolicited incoming requests on any port, thereby making your LAN invisible to cyber attackers.

However, some network applications cannot run with a tight firewall. Those applications need to selectively open ports in the firewall to function correctly. The options on this page control ways of opening the firewall to address the needs of specific types of applications.

6.4.1 Port Forwarding Rules

A port forwarding rule allows traffic from the Internet to reach a computer on the inside of your network. For example, a port forwarding rule might be used to run a Web server.

Exercise caution when adding new rules as they impact the security of your network.

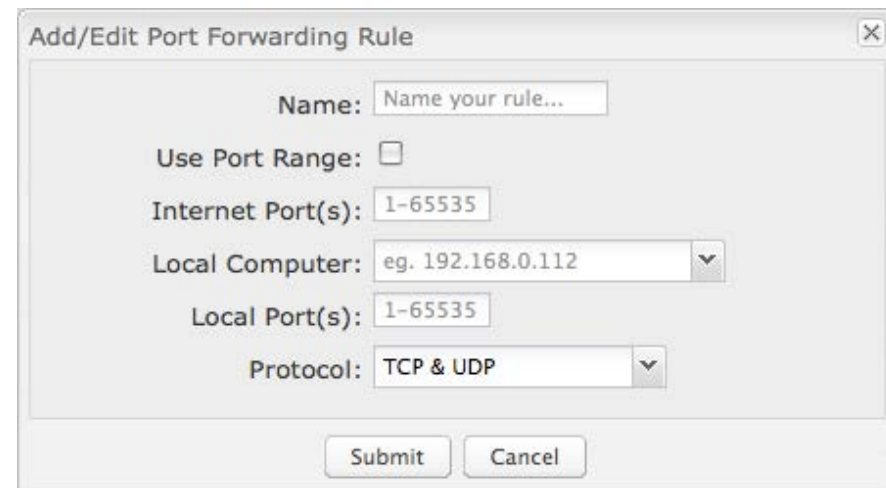
Click **Add** to create a new port forwarding rule, or select an existing rule and click **Edit**.

Add/Edit Port Forwarding Rule

- **Name:** Name your rule.
- **Use Port Range:** Changes the selection options to allow you to input a range of ports (if desired).
- **Internet Port(s):** The port number(s) as you want it defined on the Internet. Typically these will be the same as the local port numbers, but they do not have to be. These numbers will be mapped to the local port numbers.
- **Local Computer:** Select the IP address of an attached device from the dropdown menu, or manually input the IP address of a device.



Name	Internet Port(s)	Forwarding to	Protocol



Add/Edit Port Forwarding Rule

Name:

Use Port Range: ☐

Internet Port(s):

Local Computer:

Local Port(s):

Protocol:

- **Local Port(s):** The port number(s) that corresponds to the service (Web server, FTP, etc.) on a local computer or device. For example, you might input “80” in the **Local Port(s)** field to open a port for a Web server on a computer within your network. The **Internet Port(s)** field could then also be 80, or you could choose another port number that will be used across the Internet to access your Web server. If you choose a number other than 80 for the Internet Port, connections to that number will be mapped to 80—and therefore the Web server—within your network.
- **Protocol:** Select from the following options in the dropdown menu:
 - o TCP
 - o UDP
 - o TCP & UDP
- Click **Submit** to save your completed port forwarding rule.

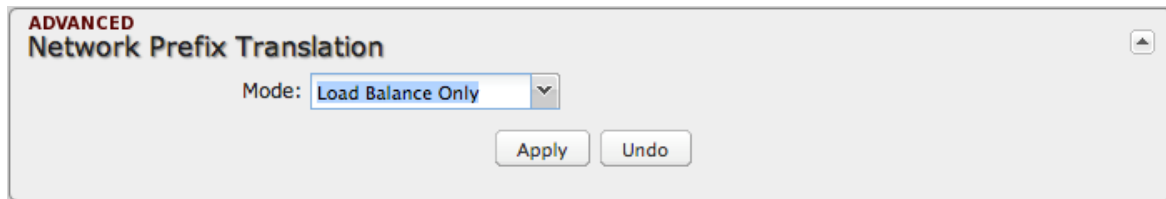
6.4.2 Network Prefix Translation (Advanced)

Network Prefix Translation is used in IPv6 networks to translate one IPv6 prefix to another. [IPv6 prefix translation](#) is an experimental specification ([RFC 6296](#)) trying to achieve address independence similar to NAT in IPv4. Unlike NAT, however, NPT is stateless and preserves the IPv6 principle that each device has a routable public address. However, it still breaks any protocol embedding IPv6 addresses (e.g. IPsec) and is generally not recommended for use by the IETF. NPT can help to keep internal network ranges consistent across various IPv6 providers, but it cannot be used effectively in all situations.

The primary purpose for Cradlepoint’s NPT implementation is for failover/failback and load balancing setups. LAN clients can potentially retain the original IPv6 lease information and may experience a more seamless transition when WAN connectivity changes than if not utilizing NPT.

Mode:

- **None** – No translation is performed
- **Load Balance Only** – (Default) Only translate networks when actively load balancing
- **First** – Use the first IPv6 prefix found



- **Static** – Always use a static IPv6 translation (input the prefix here)

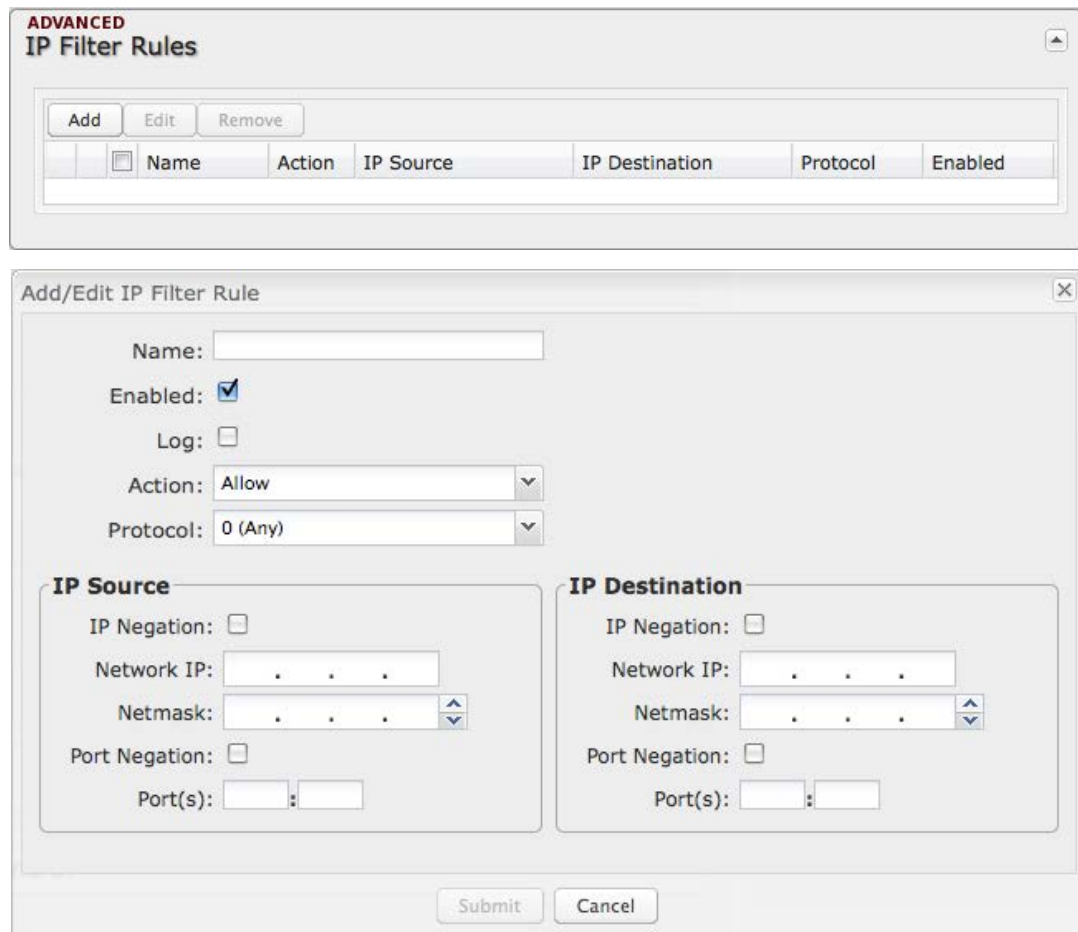
Transitioning from short prefix to a longer prefix (such as from /48 to /64) is not without problems, as some of the LANs may lose IPv6 connectivity.

6.4.3 IP Filter Rules (Advanced)

An "Incoming" IP filter rule restricts remote access to computers on your local network. "Outgoing" filter rules prevent computers on your local network from initiating communication to the address range specified in the rule.

This feature is especially useful when combined with port forwarding and/or DMZ to restrict remote access to a specified host or network range. For example, in order to host a server you might have opened ports with a port forwarding rule that could expose your LAN to cyberattacks. With an incoming IP filter rule, you can restrict the access to your LAN to only known devices.

- **Name:** Name your rule
- **Enabled:** Selected by default
- **Log:** When checked each packet matching this filter rule will be logged in the System Logs
- **Action:** "Allow" or "Deny"
- **Protocol:** Any, ICMP, TCP, UDP, GRE, ESP, or SCTP



ADVANCED IP Filter Rules

Add Edit Remove

	Name	Action	IP Source	IP Destination	Protocol	Enabled

Add/Edit IP Filter Rule

Name:

Enabled: ☒

Log: ☐

Action:

Protocol:

IP Source

IP Negation: ☐

Network IP: . . .

Netmask: . . .

Port Negation: ☐

Port(s): :

IP Destination

IP Negation: ☐

Network IP: . . .

Netmask: . . .

Port Negation: ☐

Port(s): :

Submit Cancel

IP Source/IP Destination

- **IP Negation:** Match on any IP address that is NOT in the specified IP network range.
- **Network IP:** Optional field to specify a matching network IP address for this rule to match against.
- **Netmask:** Use this to define a subnet size this rule will match against.
- **Port Negation:** Match on any port that is NOT in the specified port range.
- **Port(s):** Use for a single port or a range of ports. Fill in the left side for a single port.

Use **Network IP**, **Netmask**, and **Port(s)** to specify the ports and addresses for which the rule applies. You can specify a range of ports or a single port. Similarly, the netmask can be used to define either a range of addresses (i.e. 255.255.255.0) or a single address (255.255.255.255).

If you leave these values blank, then all IP addresses and ports will be included. **IP Source** and **IP Destination** options can be used to differentiate between the directions that packets go. You could permit packets to come from particular IP addresses but then not allow packets to return to those addresses.

Example of an IP Filter Rule: Suppose you have opened a port in your firewall in order to run a server. Someone, Johnny, is abusing that opening, so you would like to restrict his access. Create a rule that will deny Johnny's IP address.

Add IP Filter Rule

- **Name:** No more Johnny
- **Enabled:** Selected
- **Action:** Deny
- **Protocol:** Any

IP Source

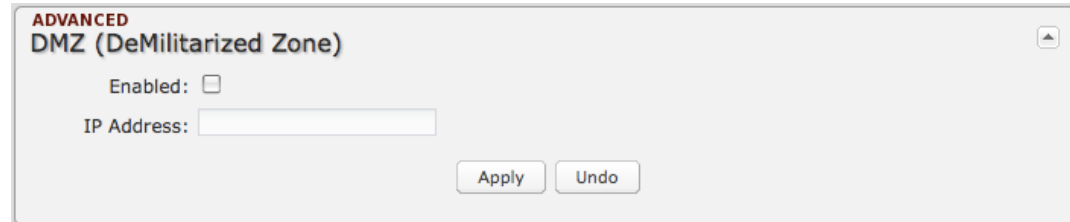
- **Network IP:** 172.22.24.160 (Johnny's IP address)
- **Netmask:** 255.255.255.255 (This netmask restricts the rule to one single address).
- **Port(s):** 80

6.4.4 DMZ: DeMilitarized Zone (Advanced)

A DMZ host is effectively not firewalled in the sense that any computer on the Internet may attempt to remotely access network services at the DMZ IP address. Typical uses involve running a public Web server or sharing files.

Input the **IP Address** of a single device in your network to create a DeMilitarized Zone for that device. To ensure that the IP address of the selected device remains consistent, go to the “Reservations” section under **Network Settings** → **DHCP Server** and reserve the IP address for the device.

As with port forwarding, use caution when enabling the DMZ feature as it can threaten the security of your network. Only use DMZ as a last resort.



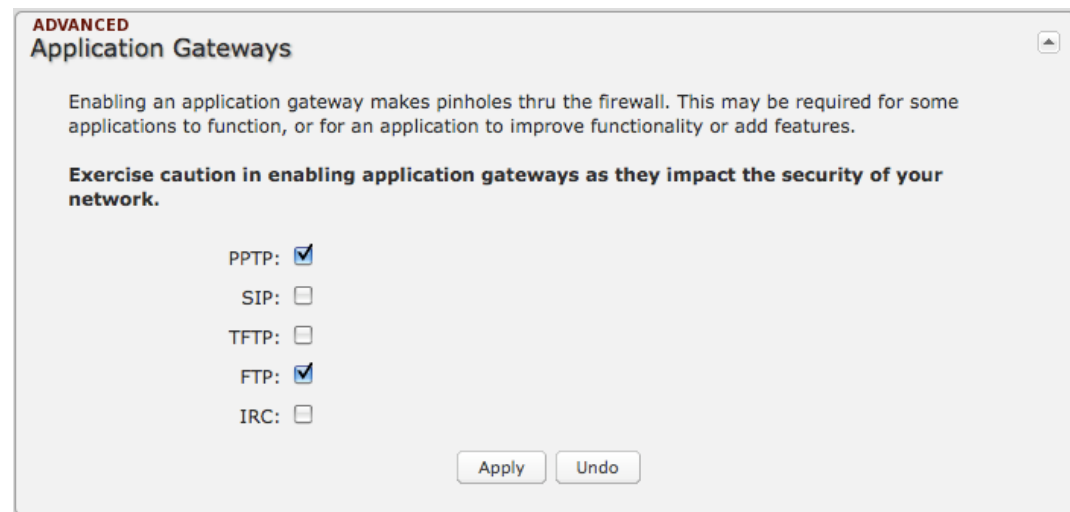
6.4.5 Application Gateways (Advanced)

Enabling an application gateway makes pinholes thru the firewall. This may be required for some applications to function, or for an application to improve functionality or add features.

Exercise caution in enabling application gateways as they impact the security of your network.

Enable any of the following types of application gateways:

- **PPTP:** For virtual private network access using Point to Point Tunneling Protocol. This is enabled by default.
- **SIP:** For Voice over IP using Session Initiation Protocol.
- **TFTP:** Enables file transfer using Trivial File Transfer Protocol.

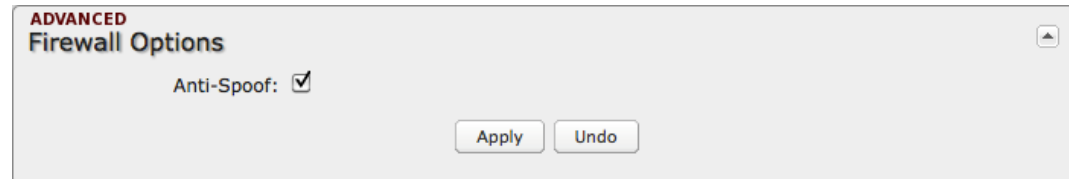


- **FTP:** To allow normal mode when using File Transfer Protocol. This is not needed for passive mode. This is enabled by default.
- **IRC:** For Direct Client to Client (DCC) transfer when using Internet Relay Chat. You may wish to forward TCP port 113 for incoming identd (RFC 1413) requests.

6.4.6 Firewall Options (Advanced)

Anti-Spoof: Anti-Spoof checks help protect against malicious users faking the source address in packets they transmit in order to either hide themselves or to impersonate someone else. Once the user has spoofed

their address they can launch a network attack without revealing the true source of the attack or attempt to gain access to network services that are restricted to certain addresses.



6.4.7 Remote Administration Access Control (Advanced)

Enable Remote Administration Access

Control: Selecting this option allows you to make remote administration tools available to only the specified IP addresses. Access from all other IP addresses will be blocked. This option only filters IP addresses: you must enable Remote Management separately (**System Settings → Administration**).

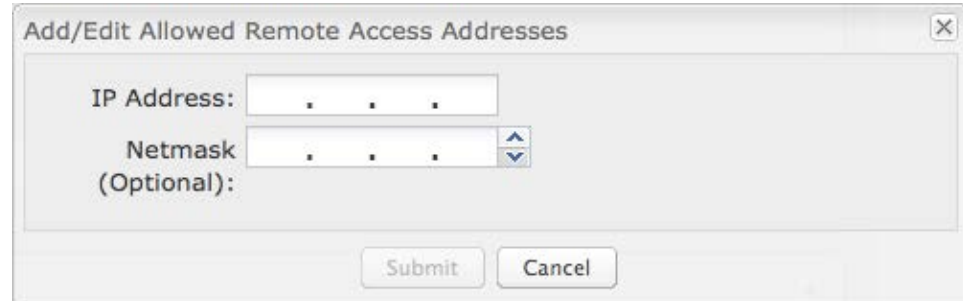
The services affected by this include remote HTTP, HTTPS, SNMP, and SSH configuration tools. This does not restrict access to LAN-based administration, i.e. devices within your network still have administration access. The individual remote administration services can be enabled under **System Settings → Administration --> Remote Management**.



REMOTE ADMINISTRATION ACCESS CONTROL EDITOR

IP Address: The IP address that will be allowed to access administrative services through the WAN.

Netmask (Optional): The netmask allows you to specify what IP address sets will be allowed access. If this field is left empty a netmask of 255.255.255.255 will be used, which means that only the single specified IP address would have remote administration access.

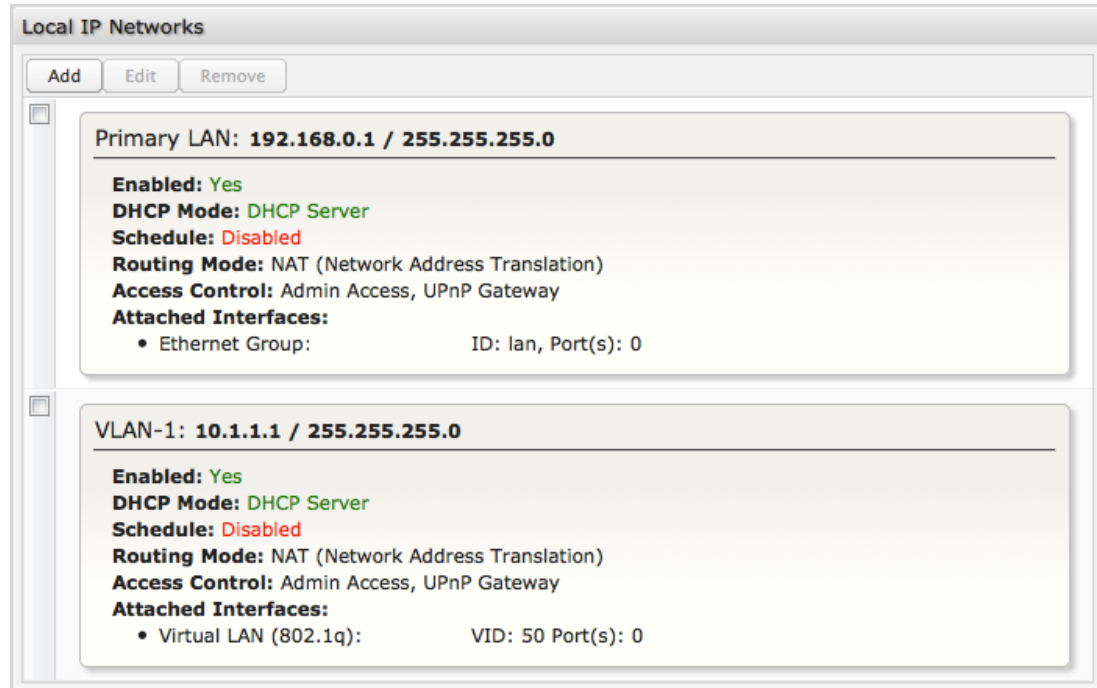


The dialog box titled "Add/Edit Allowed Remote Access Addresses" contains two input fields. The first field is labeled "IP Address:" and contains three dots. The second field is labeled "Netmask (Optional):" and contains three dots. To the right of the second field is a small up/down arrow icon. At the bottom of the dialog are two buttons: "Submit" and "Cancel".

6.5 Local Networks

This section is used to configure the settings for networks created by your router. The user can set up multiple networks on the CBA850, each with its own unique configuration and its own selection of interfaces. Each local network can be attached to either (or both) of the following types of interfaces:

- Ethernet
- VLAN



The screenshot shows the 'Local IP Networks' configuration page. At the top, there are 'Add', 'Edit', and 'Remove' buttons. Below these, there are two network entries, each with a checkbox on the left. The first entry is 'Primary LAN: 192.168.0.1 / 255.255.255.0'. Its settings are: Enabled: Yes, DHCP Mode: DHCP Server, Schedule: Disabled, Routing Mode: NAT (Network Address Translation), Access Control: Admin Access, UPnP Gateway, and Attached Interfaces: Ethernet Group (ID: lan, Port(s): 0). The second entry is 'VLAN-1: 10.1.1.1 / 255.255.255.0'. Its settings are: Enabled: Yes, DHCP Mode: DHCP Server, Schedule: Disabled, Routing Mode: NAT (Network Address Translation), Access Control: Admin Access, UPnP Gateway, and Attached Interfaces: Virtual LAN (802.1q) (VID: 50 Port(s): 0).

Network Name	IP Address	Subnet Mask	Enabled	DHCP Mode	Schedule	Routing Mode	Access Control	Attached Interfaces
Primary LAN	192.168.0.1	255.255.255.0	Yes	DHCP Server	Disabled	NAT (Network Address Translation)	Admin Access, UPnP Gateway	Ethernet Group (ID: lan, Port(s): 0)
VLAN-1	10.1.1.1	255.255.255.0	Yes	DHCP Server	Disabled	NAT (Network Address Translation)	Admin Access, UPnP Gateway	Virtual LAN (802.1q) (VID: 50 Port(s): 0)

6.5.1 Local IP Networks

Local IP Networks displays the following information for each network:

- **Network Name and IP address/Netmask** (along the top bar)
- **Enabled** (Yes/No)
- **DHCP Mode** (e.g. DHCP Server mode)
- **Schedule** (Enabled/Disabled – See the Schedule tab in the Local Network Editor)
- **IPv4 Routing Mode** (NAT, Standard, IP Passthrough, Disabled)
- **IPv6 Addressing Mode** (SLAAC Only, SLAAC with DHCP, Disable SLAAC and DHCP)
- **Access Control** (Admin Access, UPnP Gateway, LAN Isolation)
- **Attached Interfaces** (Ethernet port, VLAN)

Primary LAN: **192.168.0.1 / 255.255.255.0**

Enabled: Yes

DHCP Mode: DHCP Server

Schedule: Enabled

IPv4 Routing Mode: NAT (Network Address Translation)

IPv6 Addressing Mode: SLAAC with DHCP

Access Control: Admin Access, UPnP Gateway

Attached Interfaces:

- Ethernet Group: ID: lan, Port(s): 0

Click **Add** to configure a new network, or select an existing network and click **Edit** to view configuration options.

6.5.2 Local Network Editor

Click **Add** or select a network and click **Edit** to open the **Local Network Editor** to make configure a LAN. The **Local Network Editor** contains the following tabs:

- General Settings
- IPv4 Settings
- IPv6 Settings
- Interfaces
- Access Control
- IPv4 DHCP
- IPv6 Addressing
- Schedule

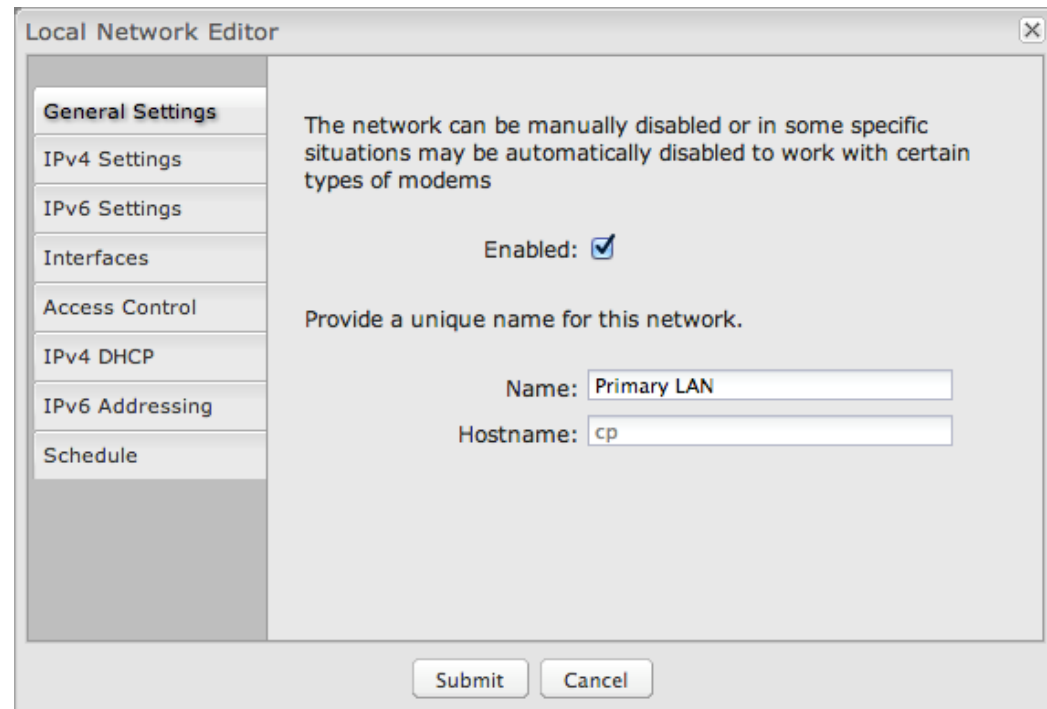
GENERAL SETTINGS

Enabled: Push to manually disable a network. Also, some settings could cause a network to be automatically disabled: click here to re-enable the network.

Name: This primarily helps to identify this network during other administration tasks.

Hostname: [Default: cp (for Cradlepoint)] The hostname is the DNS name associated with the router's local area network IP address.

NOTE: You can access the router's administration pages by typing the hostname into your browser, so if you change "cp" to another hostname, you can access the administration pages through the new hostname.



The screenshot shows the 'Local Network Editor' window. On the left is a vertical tab bar with the following options: General Settings (selected), IPv4 Settings, IPv6 Settings, Interfaces, Access Control, IPv4 DHCP, IPv6 Addressing, and Schedule. The main area on the right contains the following text: 'The network can be manually disabled or in some specific situations may be automatically disabled to work with certain types of modems'. Below this is a checkbox labeled 'Enabled:' which is checked. Further down is the instruction 'Provide a unique name for this network.' followed by two input fields: 'Name:' with the value 'Primary LAN' and 'Hostname:' with the value 'cp'. At the bottom right are 'Submit' and 'Cancel' buttons.

IPV4 SETTINGS

IP Address: This is the address used by the router for local area network communication. Changes to this parameter may require a restart to computers on this network.

Each network must have a distinct IP address. Most users will want an address from one of the following private IP ranges:

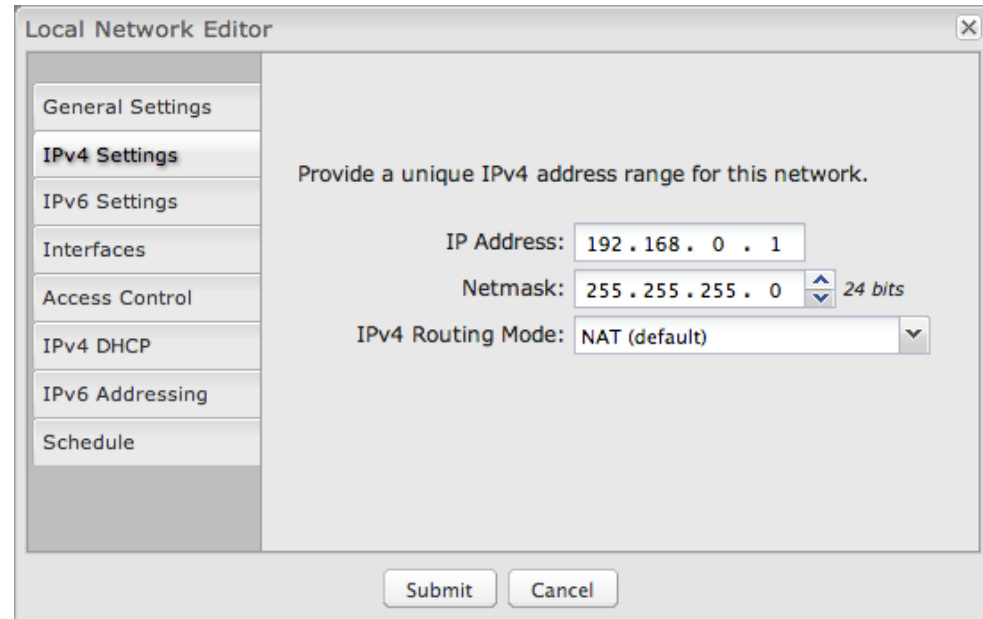
- 10.0.0.1 - 10.255.255.1
- 172.16.0.1 - 172.31.255.1
- 192.168.0.1 - 192.168.255.1

NOTE: The final number does not have to be 1, but it is a simple, logical convention for routers that leaves higher numbers free for other devices.

Netmask: (Default: 255.255.255.0) Controls how many IP addresses can be used in this network. The default value allows for 254 IP addresses.

IPv4 Routing Mode: (Default: NAT) Each network can use a unique routing mode to connect to the Internet and other local networks. NAT is desirable for most configurations. Select from the following options in the dropdown list:

- **NAT:** Network Address Translation hides private IP addresses behind the router's IP address. This is the simplest and most common choice for users, because NAT does the translation work for you.
- **Standard:** NAT-less routing. If you select **Standard**, you must separately configure your IP addresses so that they will be publically accessible. Typically you will not select this option unless you have a specific reason to bypass NAT.
- **IP Passthrough:** IP Passthrough passes the IP address given by a cellular modem (WAN) through the router to Ethernet (LAN). The easiest way to enable IP Passthrough mode is with the **IP Passthrough Setup Wizard** (see [Getting Started → IP Passthrough Setup](#)).
- **Disabled:** Disable this network.

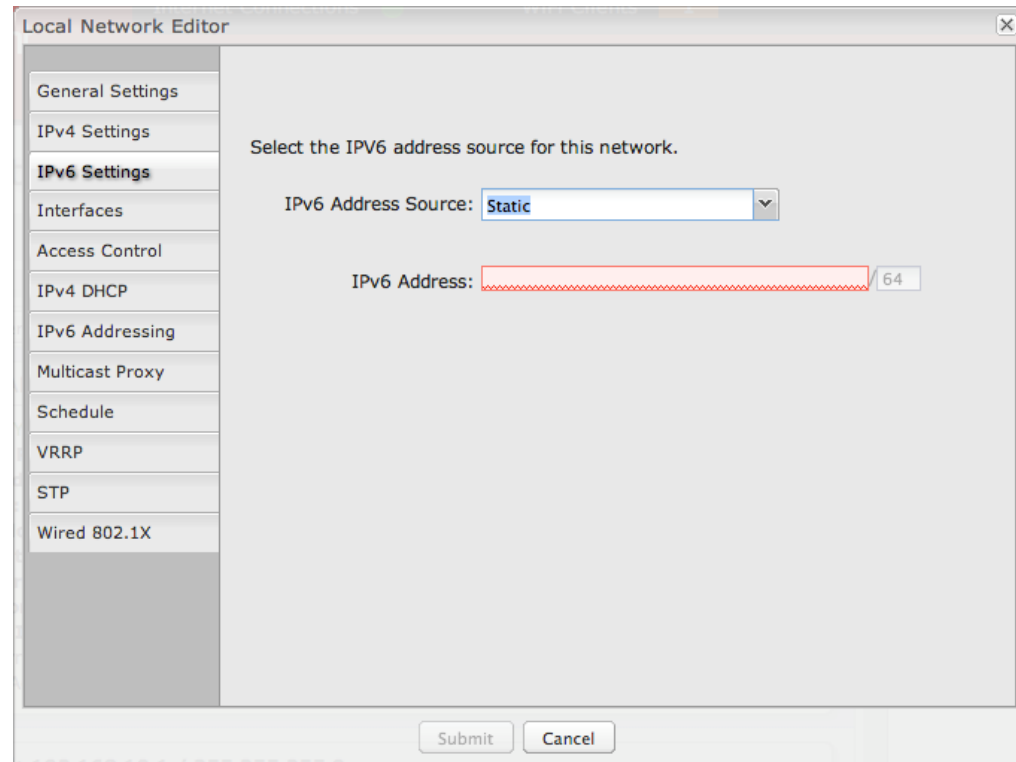


The image shows a screenshot of the 'Local Network Editor' window. On the left is a sidebar with a list of settings: General Settings, IPv4 Settings (which is highlighted), IPv6 Settings, Interfaces, Access Control, IPv4 DHCP, IPv6 Addressing, and Schedule. The main area of the window contains the text 'Provide a unique IPv4 address range for this network.' Below this text are three fields: 'IP Address:' with the value '192 . 168 . 0 . 1', 'Netmask:' with the value '255 . 255 . 255 . 0' and a '24 bits' indicator, and 'IPv4 Routing Mode:' with a dropdown menu set to 'NAT (default)'. At the bottom right of the window are 'Submit' and 'Cancel' buttons.

IPv6 SETTINGS

IPv6 must be enabled through the WAN initially: go to **Internet** → **Connection Manager** to enable IPv6.

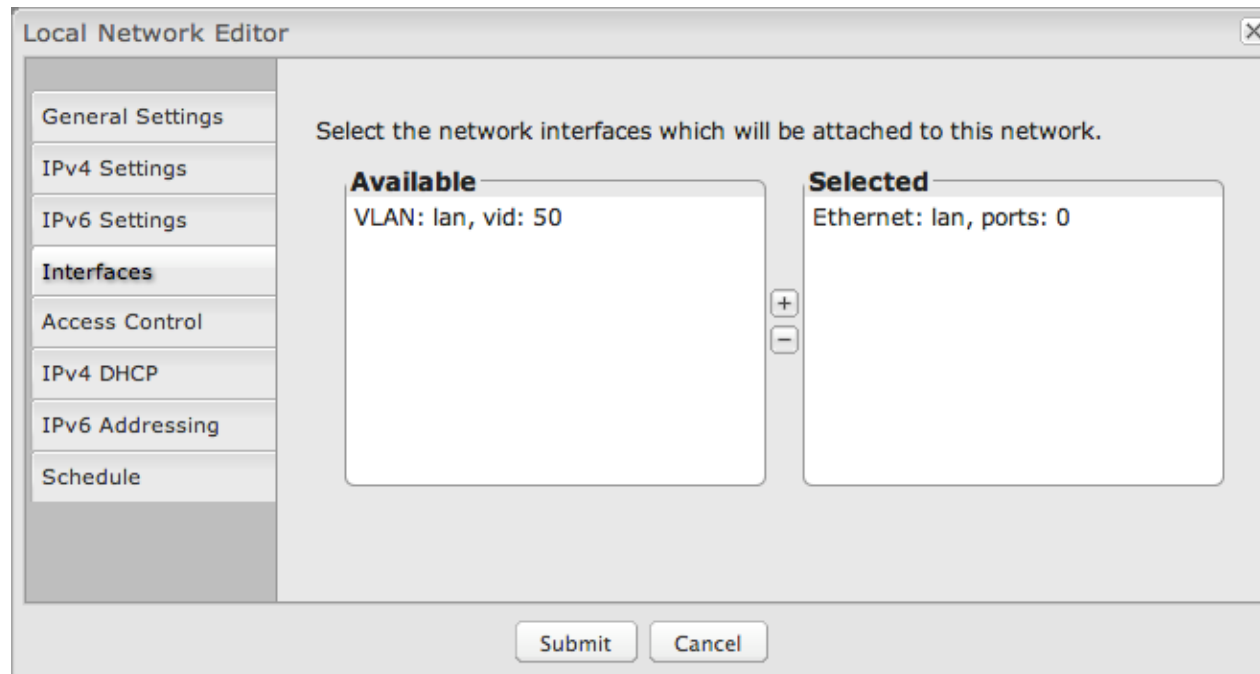
IPv6 Address Source: By default, this is set to **Delegated**, which means the IPv6 address range for the LAN is passed through from the WAN side. Change this to **Static** to input your own IPv6 address range here, or select **None** to explicitly disable IPv6 LAN connectivity.



The screenshot shows the 'Local Network Editor' window. On the left is a sidebar with a list of settings: General Settings, IPv4 Settings, **IPv6 Settings** (highlighted), Interfaces, Access Control, IPv4 DHCP, IPv6 Addressing, Multicast Proxy, Schedule, VRRP, STP, and Wired 802.1X. The main area of the window is titled 'Select the IPv6 address source for this network.' It contains two fields: 'IPv6 Address Source:' with a dropdown menu set to 'Static', and 'IPv6 Address:' with a text input field containing a redacted address and a small box with the number '64'. At the bottom right are 'Submit' and 'Cancel' buttons.

INTERFACES

Select network interfaces to attach to this network. Choose from the Ethernet ports and VLAN interfaces. Double-click on an interface shown on the left in the **Available** section to move them to the **Selected** section on the right (or highlight an interface and click the “+” button). To deselect an interface, double-click on an interface in the **Selected** section (or highlight the interface and click the “-” button).

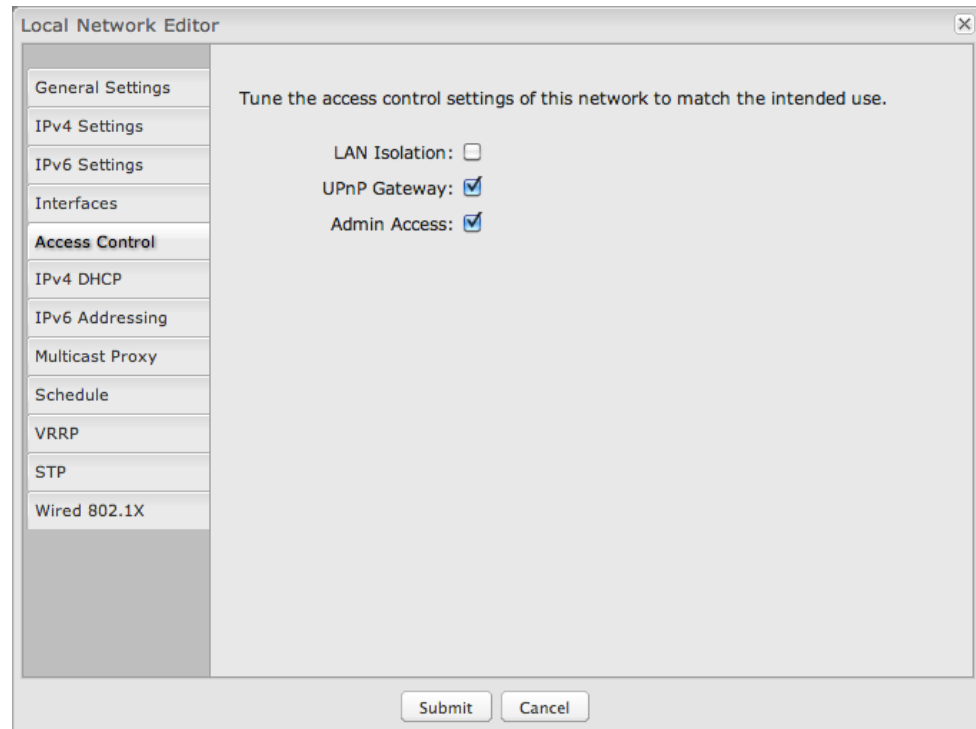


If you want more interface options, you must configure additional interfaces separately. See the **LOCAL NETWORK INTERFACES** section below (on this same administration page: **NETWORK SETTINGS** → **LOCAL NETWORKS**).

ACCESS CONTROL

Tune the access control settings of this network to match the intended use. Simply select or deselect any of the following:

- **LAN Isolation:** When checked, this network will NOT be allowed to communicate with other local networks.
- **UPnP Gateway:** Select the UPnP (Universal Plug and Play) option if you want to enable the UPnP Gateway service for computers on this network.
- **Admin Access:** When enabled, users may access these administration pages on this network.



The image shows a screenshot of the 'Local Network Editor' window. On the left is a sidebar with a list of settings: General Settings, IPv4 Settings, IPv6 Settings, Interfaces, Access Control (which is highlighted), IPv4 DHCP, IPv6 Addressing, Multicast Proxy, Schedule, VRRP, STP, and Wired 802.1X. The main area of the window contains the text 'Tune the access control settings of this network to match the intended use.' followed by three settings: 'LAN Isolation:' with an unchecked checkbox, 'UPnP Gateway:' with a checked checkbox, and 'Admin Access:' with a checked checkbox. At the bottom right of the window are 'Submit' and 'Cancel' buttons.

IPv4 DHCP

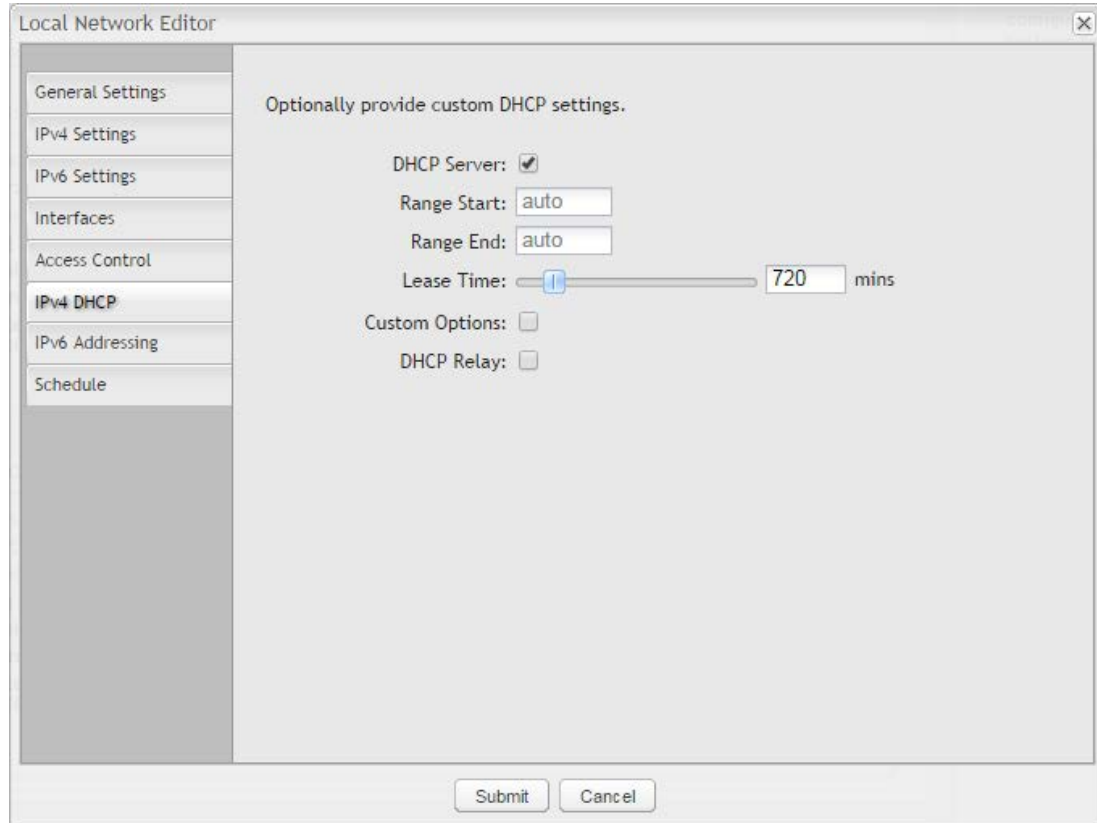
Changing settings for the IPv4 DHCP server is optional. The default selections are almost always sufficient.

DHCP Server: (Default: Enabled) When the DHCP server is enabled, users of your network will be able to automatically connect to the Internet without any special configuration. **It is recommended that you leave this enabled.** Disabling the DHCP server is only recommended if you have another DHCP server on your network and it is configured properly.

Range Start and Range End: These designate the range of values in the reserved pool of IP addresses for the DHCP server. Values within this range will be given to any DHCP enabled computers on your network. The default values are almost always sufficient (default: 72 to 200, as in 192.168.0.72 to 192.168.0.200).

Example: The router uses an IP address of 192.168.0.1 for its primary network by default. A computer designated as a Web server has a static IP address of 192.168.0.3. Another computer is designated as an FTP server with a static IP address of 192.168.0.4. The starting IP address for the DHCP server needs to be 192.168.0.5 or higher.

Lease Time: (Default: 720 minutes [12 hours]) Specifies how long DHCP-enabled computers will wait before requesting a new DHCP lease. Smaller values are better suited to busy environments.



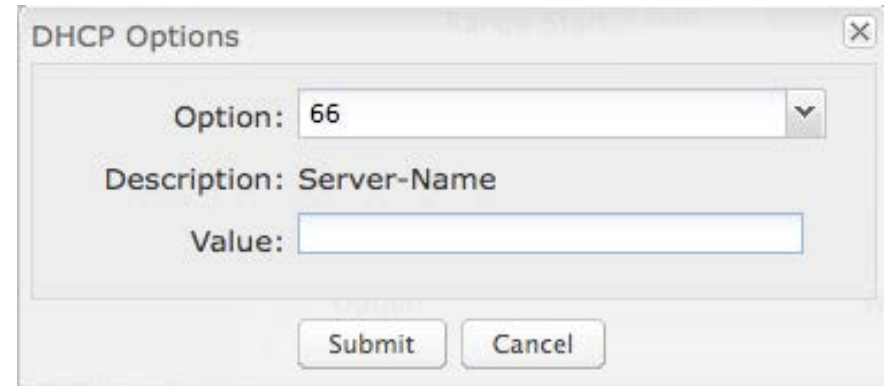
The screenshot shows the 'Local Network Editor' window with the 'IPv4 DHCP' tab selected in the left sidebar. The main area contains the following settings:

- Optionally provide custom DHCP settings.
- DHCP Server: ☒
- Range Start:
- Range End:
- Lease Time: 720 mins
- Custom Options: ☐
- DHCP Relay: ☐

At the bottom of the window are 'Submit' and 'Cancel' buttons.

Custom Options: Input a custom DHCP option by first clicking the **Custom Options** field to enable it and then clicking “Add” at the top of the table that appears. There are close to 200 possible DHCP options available. One of the more common uses is to assign a VoIP phone server using option 66 (Server name).

- **Option:** Select an option from the dropdown list or manually enter the number of an option. A [complete list of options](#) is available from IANA.
- **Value:** Generally this field should be a string, IP address, or numeric value. Some fields can accept both IP addresses and hostnames – in these cases you may need to wrap this value in quotes. For example, option 66 (Server name) requires quotes around IP addresses.



DHCP Relay: Communicates with a DHCP server and acts as a proxy for DHCP broadcast messages that must be routed to remote segments. This is accomplished by converting broadcast DHCP messages to unicast messages to communicate between clients and servers.

DHCP Server Address: An **optional** DHCP server address if more than one DHCP server is located on the network. This field is only available when **DHCP Relay** is enabled.

IPV6 ADDRESSING

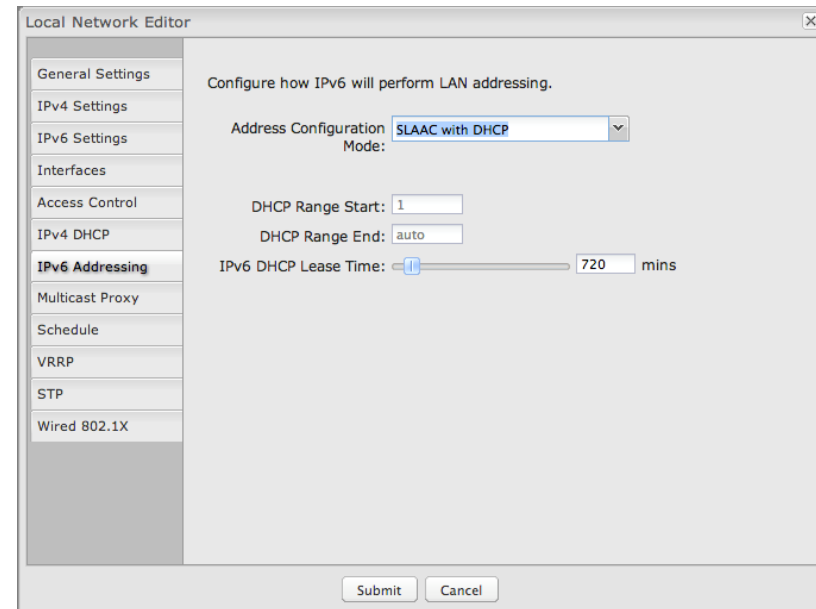
Address Configuration Mode

SLAAC Only – [SLAAC](#) stands for stateless address autoconfiguration. The router regularly generates a router advertisement that includes network prefix and routing information, allowing clients to autogenerate an address and start communicating on the network. Clients utilize neighbor discovery protocols to ensure multiple clients on the subnet have not chosen an identical address.

SLAAC with DHCP – (Default) IPv6 DHCP provides an additional client configuration method and is regularly combined with SLAAC to provide DNS servers (a shortcoming in the original SLAAC specification) and additional options not supported by SLAAC. By defaulting to SLAAC with DHCPv6, all IPv6-capable clients on the network should be configurable with IPv6 connectivity.

- **DHCP Range Start:** The beginning of the range that will be used for IPV6 DHCP addresses. The IPv6 range will always start at 1.
- **DHCP Range End:** The ending IP address in the DHCP Server range is the end of the reserved pool of IP addresses that will be given to any DHCP-enabled computers on your network.
- **IPv6 DHCP Lease Time:** This specifies how long DHCP-enabled computers will wait before requesting a new DHCP lease.

Disable SLAAC and DHCP – Disable both IPv6 address configuration modes.



The screenshot shows the 'Local Network Editor' window with the 'IPv6 Addressing' tab selected. The configuration area is titled 'Configure how IPv6 will perform LAN addressing.' and includes the following settings:

- Address Configuration Mode:** A dropdown menu set to 'SLAAC with DHCP'.
- DHCP Range Start:** A text input field containing the value '1'.
- DHCP Range End:** A text input field containing the value 'auto'.
- IPv6 DHCP Lease Time:** A slider control set to 720 minutes.

At the bottom of the window are 'Submit' and 'Cancel' buttons.

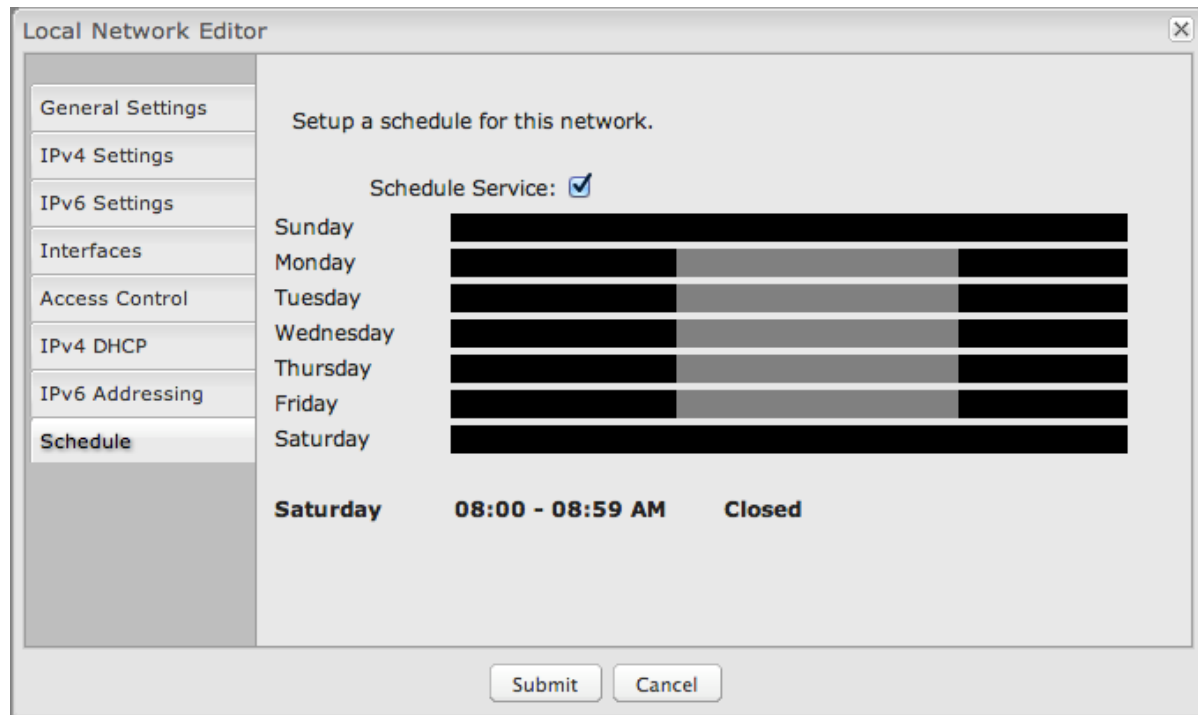
SCHEDULE

Set up a schedule for this network interface. This allows an interface to be enabled or disabled during specific hours of a day. For example, use this to limit the network to business hours.

Schedule Service: (Default: Disabled.) Select to enable. This will open a configurable chart for setting the schedule.

Each hour of the week is represented by a black or gray square. Black represents disabled, while gray represents enabled. Hover over a square to reveal the hour it represents. Click on the squares to toggle between black and gray.

In the example shown, the network is enabled from 8-5 on Monday through Friday, but disabled at all other times.



Local Network Editor

General Settings

IPv4 Settings

IPv6 Settings

Interfaces

Access Control

IPv4 DHCP

IPv6 Addressing

Schedule

Setup a schedule for this network.

Schedule Service: ☒

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Saturday 08:00 - 08:59 AM Closed

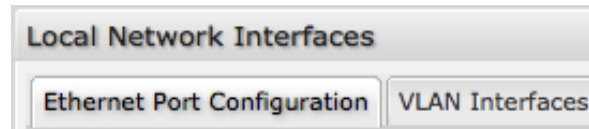
Submit Cancel

6.5.3 Local Network Interfaces

Each LAN type—Ethernet and VLAN—has a separate section with configuration options. Unless the default configuration is sufficient, **YOU MUST CONFIGURE EACH INTERFACE SEPARATELY** in order to create the desired interface options for a network. You can then select these interfaces to add to a network in the **Local Network Editor** (see above).

Select from the following tabs:

- **Ethernet Port Configuration**
- **VLAN Interfaces**

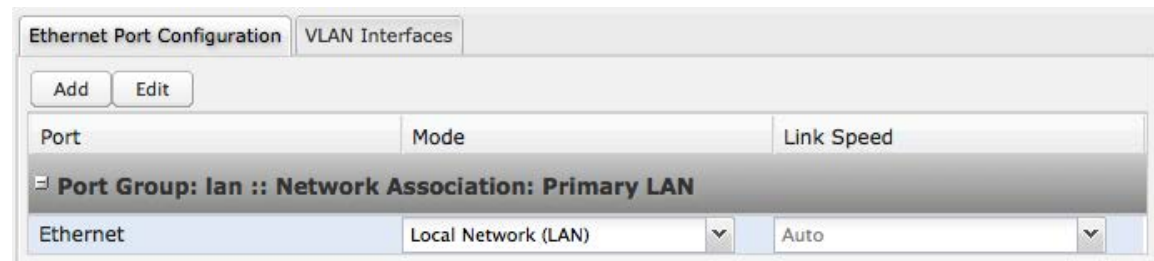


Ethernet Port Configuration

Ethernet Port Configuration provides controls for your router's Ethernet ports. While default settings will be sufficient in most circumstances, you have the ability to control the **Link Speed**. Additional controls for WAN ports are available in **Internet** → **Ethernet Settings**.

Link Speed: Default setting is Auto. The Auto setting is preferred in most cases.

- Auto
- 10Mbps - Half Duplex
- 10Mbps - Full Duplex
- 100Mbps - Half Duplex
- 100Mbps - Full Duplex
- 1000Mbps - Full Duplex

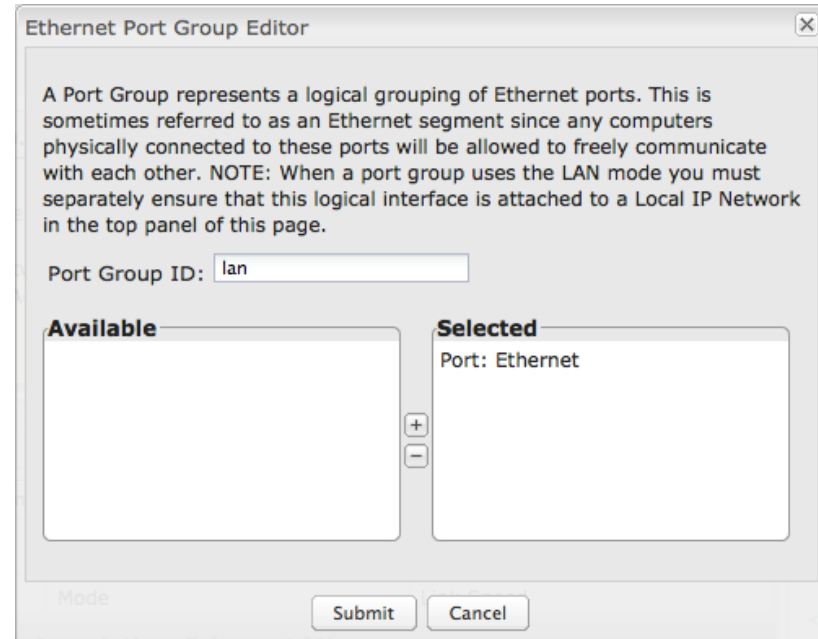


ETHERNET PORT GROUP EDITOR

A Port Group represents a logical grouping of Ethernet ports. Any computers physically connected to ports in a group will be allowed to freely communicate with each other.

*NOTE: You must separately ensure that this logical interface is attached to a **Local IP Network** in the top panel of this page.*

Port Group ID: The Group ID field provides a reference to this port group to be used in other parts of the router configuration. For example, this ID is referenced in the **Local IP Networks** configuration to attach this group of Ethernet ports to a network configuration. Use a simple short text phrase to describe a group, such as "main", "guestport", etc.



The screenshot shows the 'Ethernet Port Group Editor' dialog box. It contains a text area with explanatory text and a note. Below this is a text field for 'Port Group ID' containing the value 'lan'. There are two list boxes: 'Available' (empty) and 'Selected' (containing 'Port: Ethernet'). Between these boxes are '+' and '-' buttons. At the bottom, there is a 'Mode' label and 'Submit' and 'Cancel' buttons.

Ethernet Port Group Editor

A Port Group represents a logical grouping of Ethernet ports. This is sometimes referred to as an Ethernet segment since any computers physically connected to these ports will be allowed to freely communicate with each other. **NOTE:** When a port group uses the LAN mode you must separately ensure that this logical interface is attached to a Local IP Network in the top panel of this page.

Port Group ID:

Available

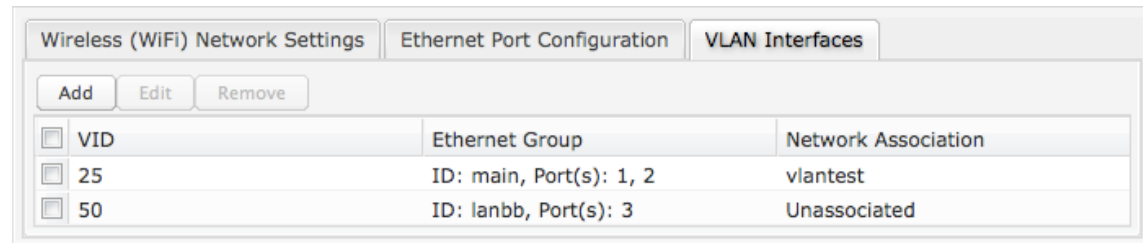
Selected
Port: Ethernet

Mode

Submit Cancel

VLAN INTERFACES

A virtual local area network, or VLAN, functions as any other physical LAN, but it enables computers and other devices to be grouped together even if they are not physically attached to the same network switch.



	VID	Ethernet Group	Network Association
☐	25	ID: main, Port(s): 1, 2	viantest
☐	50	ID: lanbb, Port(s): 3	Unassociated

To enable a VLAN, select a VID (virtual LAN ID) and an Ethernet port group through which users can access the VLAN. Then go back up to the **Local Network Editor** to attach your new VLAN to a network. To use a VLAN, the VID must be shared with another router or similar device so that multiple physical networks have access to the one virtual network.

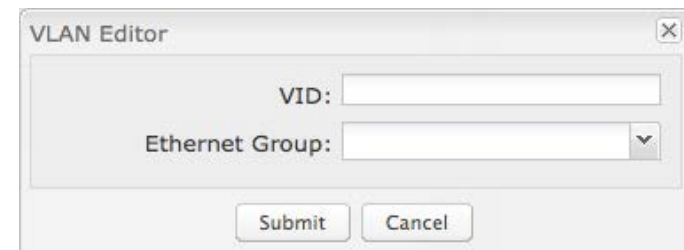
Click **Add** to create a new VLAN interface.

VLAN EDITOR

VID: An integer value that is the Virtual LAN ID.

Ethernet Group: Select the LAN port with which you want to associate the VLAN ID from a dropdown list.

Click **Submit** to save your configured VLAN.



6.6 MAC Filter/Logging

A MAC (Media Access Control) address is a unique identifier for a computer or other device. This page allows you to manage clients by MAC address. You can filter clients by MAC addresses and/or keep a log of devices connected to your router.

6.6.1 Filter Configuration

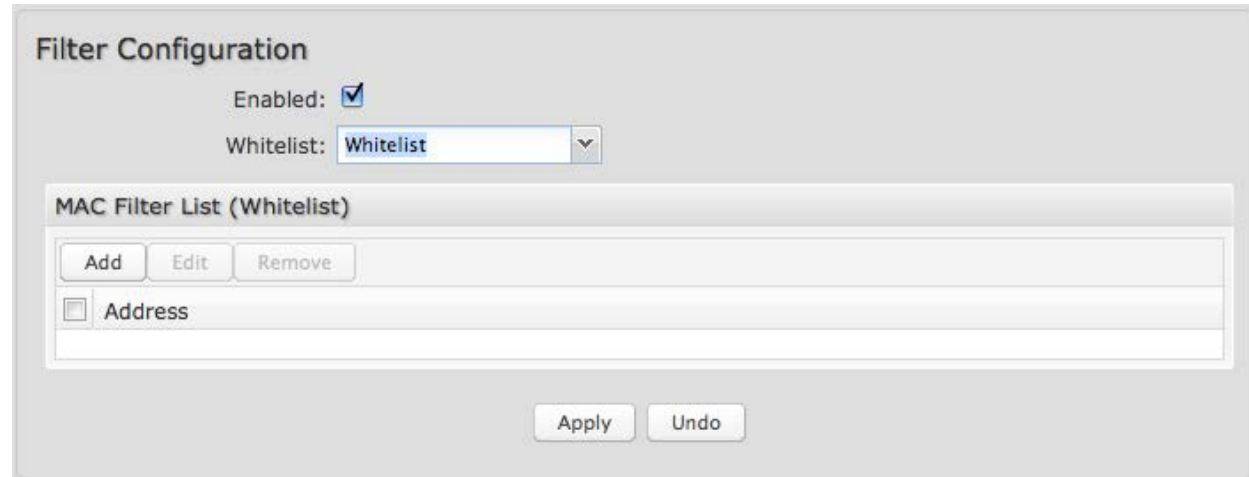
The MAC Filter allows you to create a list of devices that have either exclusive access (whitelist) or no access (blacklist) to your LAN.

Enabled: Click to allow MAC Filter options.

Whitelist: Select either "Whitelist" or "Blacklist" from a dropdown menu. In "Whitelist" mode, the router will restrict access to all computers except those contained in the "MAC Filter List" panel. In "Blacklist" mode, listed devices are completely blocked.

MAC Filter List (Whitelist or Blacklist): Add devices to either your whitelist or blacklist simply by inputting each device's MAC address.

NOTE: Use caution when using the MAC Filter to avoid accidentally blocking yourself from accessing the router.



The screenshot shows the "Filter Configuration" web interface. At the top, there is a section titled "Filter Configuration". Below this title, there is a checkbox labeled "Enabled:" which is checked. To the right of the checkbox is a dropdown menu labeled "Whitelist:" with "Whitelist" selected. Below this is a section titled "MAC Filter List (Whitelist)". Inside this section, there are three buttons: "Add", "Edit", and "Remove". Below these buttons is a table with a single column header "Address" and a checkbox to its left. The table is currently empty. At the bottom of the interface, there are two buttons: "Apply" and "Undo".

6.6.2 MAC Logging Configuration

Enable MAC Logging: Enabling MAC Logging will cause the router to log MAC addresses that are connected to the router. MAC addresses that you do not want to have logged (addresses that you expect to be connected) should be added to the “Ignored MAC Addresses” list.

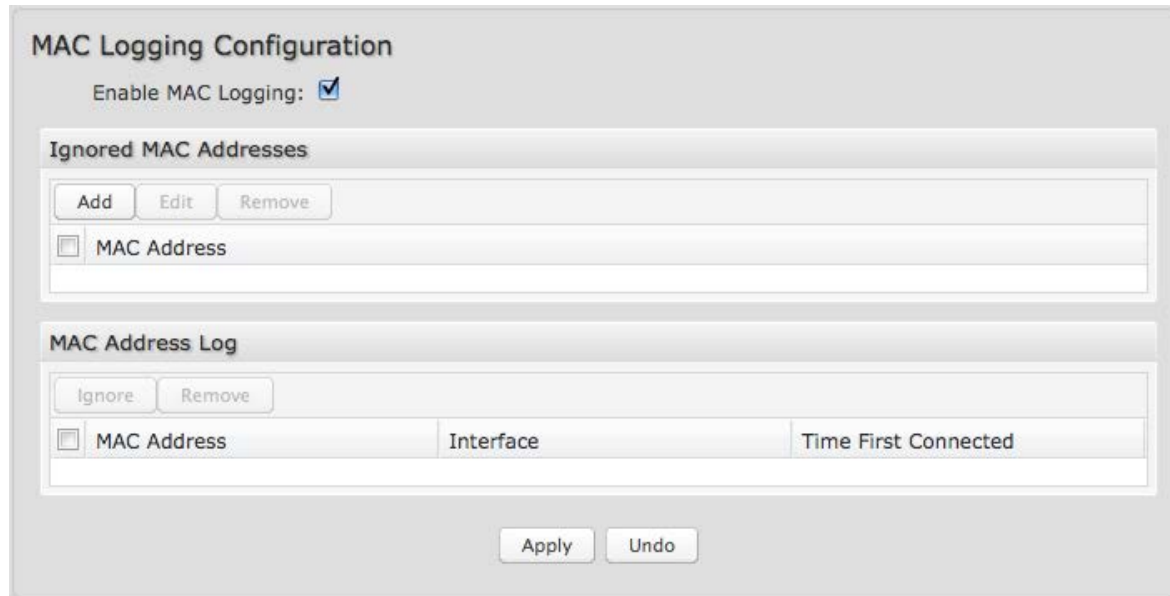
You can configure the router to send an alert if a connected device has a MAC address that the router doesn’t recognize. Go to **System Settings** → **Device Alerts** to set up these email alerts.

Ignored MAC Addresses: This is the list of MAC addresses that will not produce an alert or a log entry when they are connected to the router. These should be MAC addresses that you expect to be connected to the router.

To add MAC addresses to this list, simply select devices shown in the MAC Address Log and click “Ignore.” You can also add addresses manually.

MAC Address Log: This shows the last 64 MAC addresses that have connected to the router, as well as which interface was used to connect. The time/date that is logged is the time of the first connection. The page may need to be refreshed to show the most recent log entries.

Double-clicking on entries from this list will add them to the **Ignored MAC Addresses** list.



The screenshot shows the 'MAC Logging Configuration' web page. At the top, there is a section 'Enable MAC Logging:' with a checked checkbox. Below this is a section titled 'Ignored MAC Addresses' which contains three buttons: 'Add', 'Edit', and 'Remove'. Underneath these buttons is a table with one row containing a checkbox and the text 'MAC Address'. Below the 'Ignored MAC Addresses' section is another section titled 'MAC Address Log'. This section contains two buttons: 'Ignore' and 'Remove'. Below these buttons is a table with three columns: 'MAC Address', 'Interface', and 'Time First Connected'. At the bottom of the page, there are two buttons: 'Apply' and 'Undo'.

6.7 Routing

Add a new static route to the IP routing table or edit/remove an existing route.

Static routes are used in networks with more than one layer, such as when there is a network within a network so that packet destinations are hidden behind an additional router. Adding a static route is a way of telling the router about an additional step that packets will need to take to reach their destination.

Click **Add** to create a new static route.

IP/Network Address: The IP address of the target network or host.

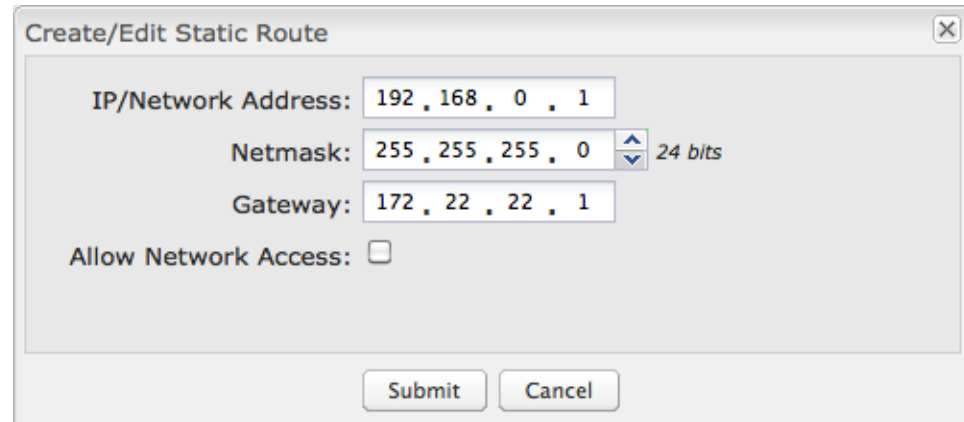
Add Edit Remove		
☐ IP/Network Address	Netmask	Gateway
☒ 192.168.0.1	255.255.255.0	172.22.22.1

Netmask: The Netmask, along with the IP address, defines the network the computer belongs to and which other IP addresses the computer can see in the same LAN. An IP address of 192.168.0.1 along with a Netmask of 255.255.255.0 defines a network with 256 available IP addresses from 192.168.0.0 to 192.168.0.255.

NOTE: 255.255.255.255 is used to signify only the host that was entered in the IP/Network Address field.

Gateway: Specifies the next hop to be taken if this route is used. A gateway of 0.0.0.0 implies there is no next hop, and the IP address matched is directly connected to the router on the interface specified: **LAN** or **WAN**.

Allow Network Access: (Default: Deselected.) Some static routes will need an IP Filter Rule via the Firewall to allow packets through the route without being blocked. Selecting this option automatically creates this IP Filter Rule. If the **IP/Network Address** falls outside the LAN IP range, you probably need to select this option.



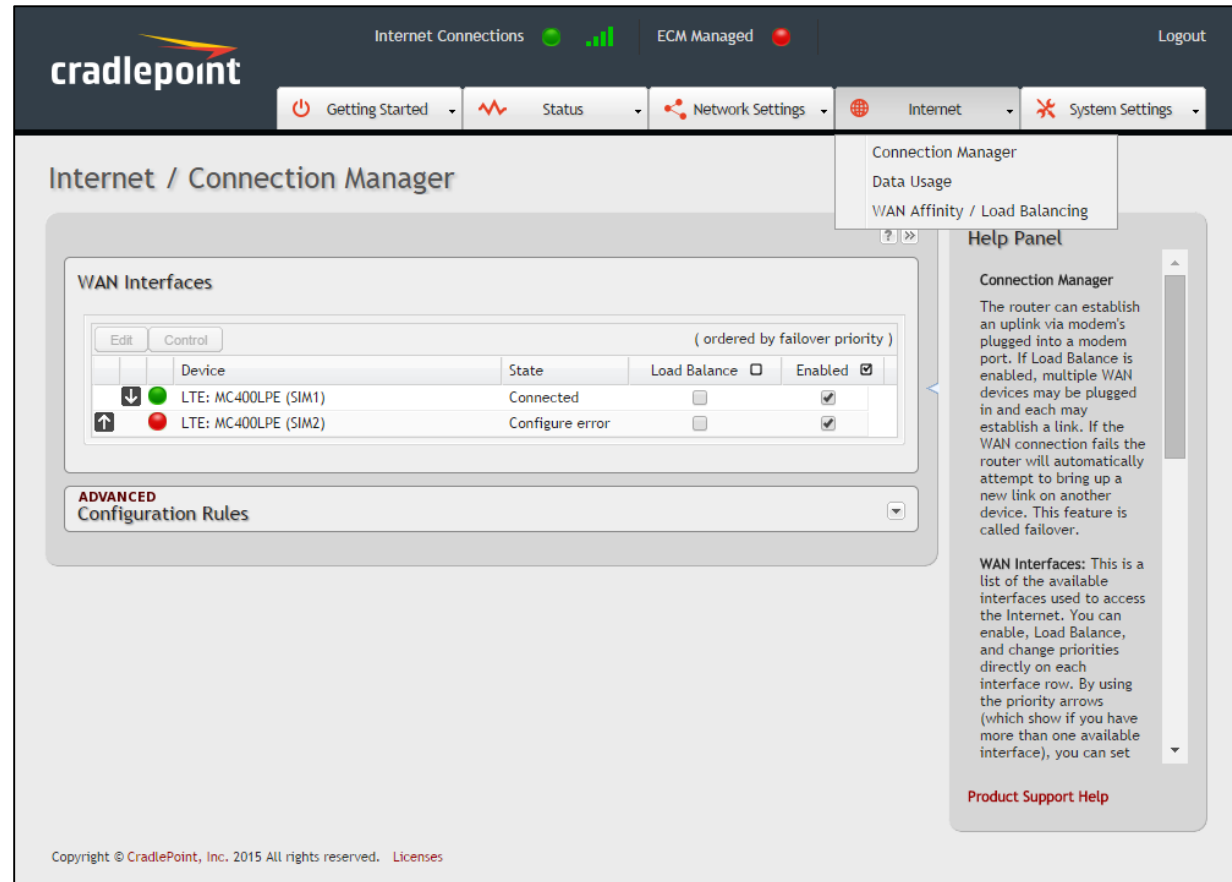
The dialog box titled "Create/Edit Static Route" contains the following fields and controls:

- IP/Network Address:** A text field with the value "192 , 168 , 0 , 1".
- Netmask:** A text field with the value "255 , 255 , 255 , 0" and a dropdown menu set to "24 bits".
- Gateway:** A text field with the value "172 , 22 , 22 , 1".
- Allow Network Access:** A checkbox that is currently unchecked.
- Buttons:** "Submit" and "Cancel" buttons at the bottom right.

7 INTERNET

The Internet tab provides access to three submenu items for managing a variety of Internet connection options.

- Connection Manager
- Data Usage
- WAN Affinity/Load Balancing



Internet / Connection Manager

WAN Interfaces

	Device	State	Load Balance	Enabled
↓	LTE: MC400LPE (SIM1)	Connected	☐	☒
↑	LTE: MC400LPE (SIM2)	Configure error	☐	☒

ADVANCED Configuration Rules

Help Panel

Connection Manager
The router can establish an uplink via modem's plugged into a modem port. If Load Balance is enabled, multiple WAN devices may be plugged in and each may establish a link. If the WAN connection fails the router will automatically attempt to bring up a new link on another device. This feature is called failover.

WAN Interfaces: This is a list of the available interfaces used to access the Internet. You can enable, Load Balance, and change priorities directly on each interface row. By using the priority arrows (which show if you have more than one available interface), you can set

Product Support Help

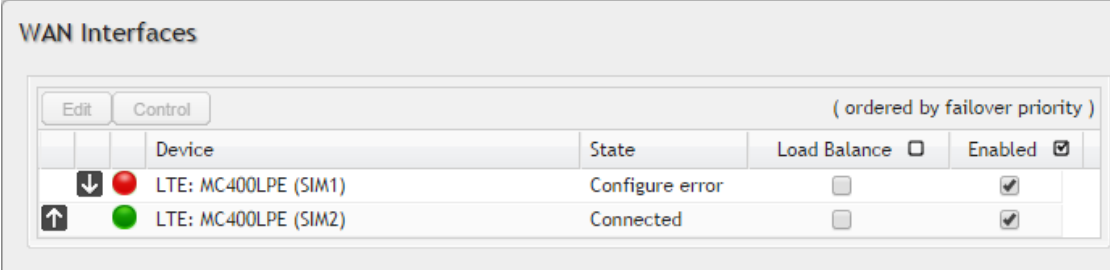
Copyright © CradlePoint, Inc. 2015 All rights reserved. Licenses

7.1 Connection Manager

The router can establish an uplink via any modems plugged into a modem port. If there is more than one modem attached and the primary connection fails, the router will automatically attempt to bring up a new link on another device. This feature is called failover. If Load Balance is enabled, multiple WAN devices establish a link at the same time.

7.1.1 WAN Interfaces

This is a list of the available interfaces used to access the Internet. You can enable, stop, or start devices from this section. By using the priority arrows (the arrows in the boxes to the left—these show if you have more than one available interface), you can set the interface the router uses by default and the order that it allows failover.



WAN Interfaces				
		Edit	Control	(ordered by failover priority)
	Device	State	Load Balance ☐	Enabled ☒
↓	LTE: MC400LPE (SIM1)	Configure error	☐	☒
↑	LTE: MC400LPE (SIM2)	Connected	☐	☒

Load Balance: If this is enabled, the router will use multiple WAN interfaces to increase the data transfer throughput by using any connected WAN interface consecutively. Selecting Load Balance will automatically start the WAN interface and add it to the pool of WAN interfaces to use for data transfer. Turning off Load Balance for an active WAN interface may require the user to restart a current browsing session.

Enabled: Selected by default. Deselect to disable an interface.

Click on the small box at the top of the list to select/deselect all devices for either **Load Balance** or **Enabled**.

Click on a device in the list to reveal additional information about that device and to enable configuration options.

7.1.2 Device Configuration

Clicking on a device reveals the following information:

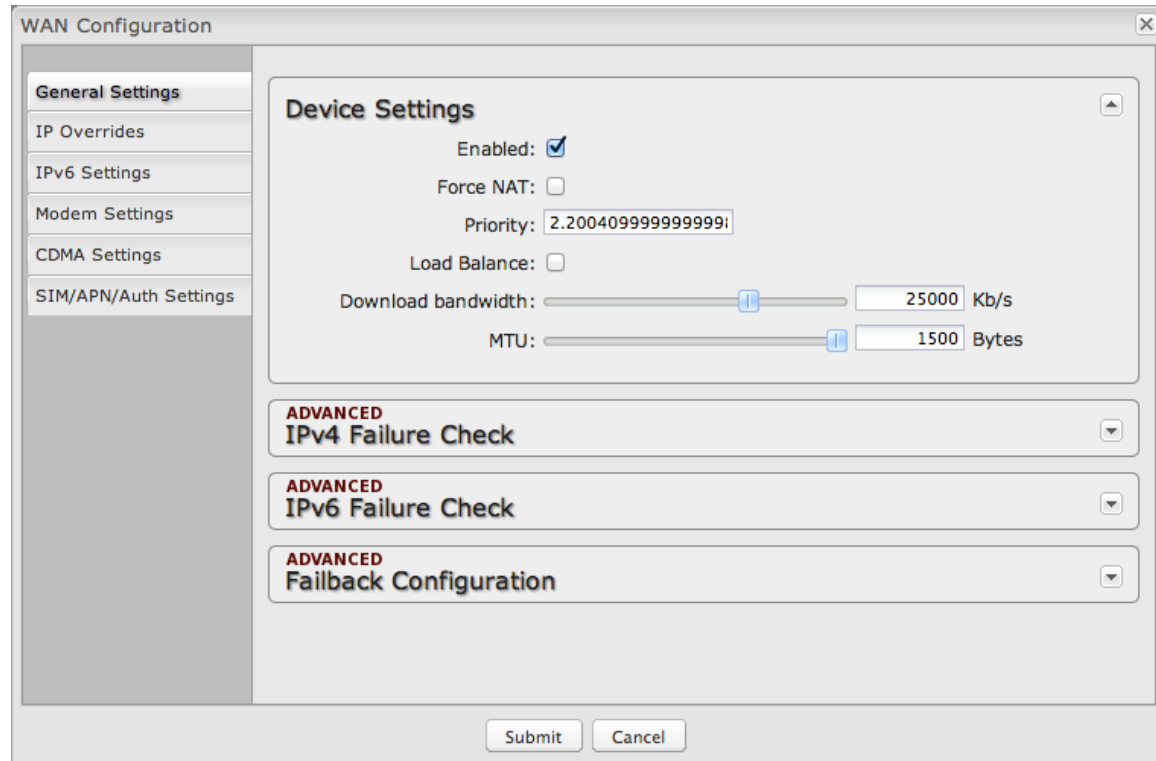
- State (Connected, Available, etc.)
- Port
- UID (Unique identifier. This could be a name or number/letter combination.)
- IP Address
- Gateway
- Netmask
- Stats: bytes in, bytes out
- Uptime

Edit Control		(ordered by failover priority)		
	Device	State	Load Balance ☐	Enabled ☒
↓	LTE: MC400LPE (SIM1)	Configure error	☐	☒
↑	LTE: MC400LPE (SIM2)	Connected	☐	☒
State: Connected Port: modem1 UID: 9cf6dd3e IP Address: 172.25.98.68 Gateway: 172.25.98.69 Netmask: 255.255.255.252 Stats: 0 bytes IN / 0 bytes OUT Uptime: 00:01:03 secs				

Click “Edit” to view configuration options for the selected device. Click “Control” to view options to activate or update the device.

7.1.3 General Settings

- **Enabled:** Select/deselect to enable/disable.
- **Force NAT:** Normally the LAN Route Mode controls the use of NAT (network address translation). When this option is selected the router will always perform NAT when traffic is sent out from this device.
- **Priority:** This number controls failover and failback order. The lower the number, the higher the priority and the more use the device will get. This number will change when you move devices around with the priority arrows in the WAN Interfaces list.
- **Load Balance:** Select to allow this device to be available for the Load Balance pool.
- **Download bandwidth:** Defines the default download bandwidth for use in Load Balance algorithms. (Range: 128 Kb/s to 76800 Kb/s.)
- **MTU:** Maximum transmission unit. This is the size of the largest protocol data unit that the device can pass. (Range: 46 to 1500 Bytes.)



The screenshot shows the 'WAN Configuration' dialog box with the 'General Settings' tab selected. The 'Device Settings' section includes the following options:

- Enabled:** ☒
- Force NAT:** ☐
- Priority:** 2.2004099999999999
- Load Balance:** ☐
- Download bandwidth:** 25000 Kb/s
- MTU:** 1500 Bytes

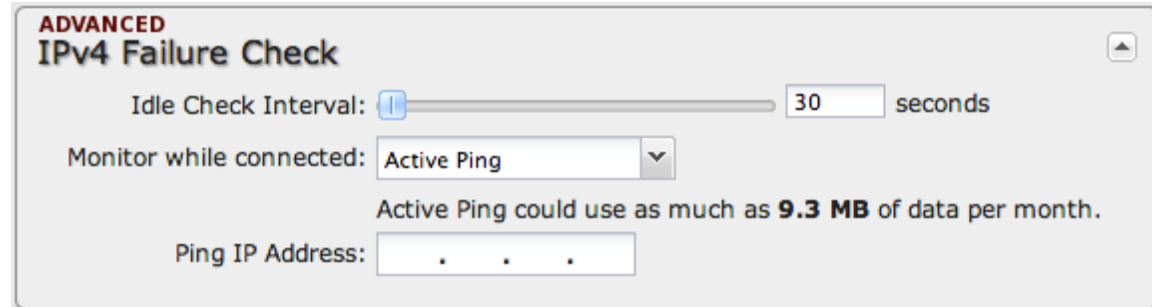
Below the 'Device Settings' section, there are three expandable sections, each with an 'ADVANCED' label and a dropdown arrow:

- IPv4 Failure Check
- IPv6 Failure Check
- Failback Configuration

At the bottom of the dialog box are 'Submit' and 'Cancel' buttons.

IPv4 FAILURE CHECK (ADVANCED)

If this is enabled, the router will check that the highest priority active WAN interface can get to the Internet even if the WAN connection is not actively being used. If the interface goes down, the router will switch to the next highest priority interface available. If this is not selected, the router will still failover to the next highest priority interface but only after the user has attempted to get out to the Internet and failed.



Idle Check Interval: The amount of time between each check. (Default: 30 seconds. Range: 10-3600 seconds.)

Monitor while connected: (Default: Off) Select from the following dropdown options:

- **Passive DNS (modem only):** The router will take no action until data is detected that is destined for the WAN. When this data is detected, the data will be sent and the router will check for received data for 2 seconds. If no data is received the router behaves as described below under **Active DNS**.
- **Active DNS (modem only):** A DNS request will be sent to the DNS servers. If no data is received, the DNS request will be retried four times at 5-second intervals. (The first two requests will be directed at the Primary DNS server and the second two requests will be directed at the Secondary DNS server.) If still no data is received, the device will be disconnected and failover will occur.
- **Active Ping:** A ping request will be sent to the Ping Target. If no data is received, the ping request will be retried four times at 5-second intervals. If still no data is received, the device will be disconnected and failover will occur. When “Active Ping” is selected, the next line gives an estimate of data usage in this form: “Active Ping could use as much as **9.3 MB** of data per month.” This amount depends on the Idle Check Interval.
- **Off:** Once the link is established the router takes no action to verify that it is still up.

Ping IP Address: If you selected “Active Ping”, you will need to input an IP address. This must be an address that can be reached through your WAN connection (modem/Ethernet). Some ISPs/Carriers block certain addresses, so choose an address

that all of your WAN connections can use. For best results, select an established public IP address. *For example, you might ping Google Public DNS at 8.8.8.8 or Level 3 Communications at 4.2.2.2.*

IPv6 FAILURE CHECK (ADVANCED)

These settings match **IPv4 Failure Check**; the only difference in the UI is that the ping address uses IPv6.

FAILBACK CONFIGURATION (ADVANCED)

This is used to configure failback, which is the ability to go back to a higher priority WAN interface if it regains connection to its network.

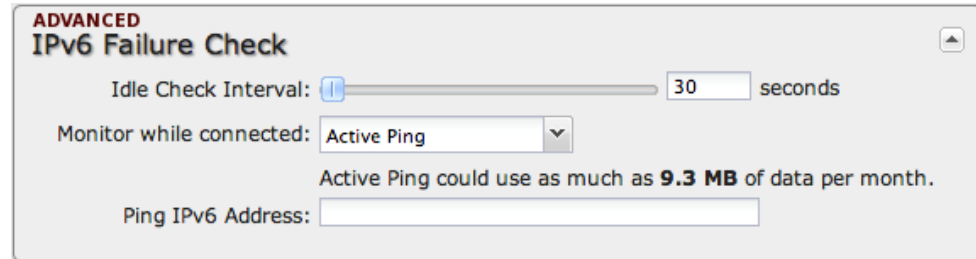
Usage: Fail back based on the amount of data passed over time.

- **High** (Rate: 80 KB/s. Time Period: 30 seconds.)
- **Normal** (Rate: 20 KB/s. Time Period: 90 seconds.)
- **Low** (Rate: 10 KB/s. Time Period: 240 seconds.)
- **Custom** (Rate range: 1-100 KB/s. Time Period range: 10-300 seconds.)

Time: Fail back only after a set period of time. (Default: 90 seconds. Range: 10-300 seconds.) This ensures that the higher priority interface has remained online for a set period of time before it becomes active (in case the connection is dropping in and out, for example).

Disabled: Deactivate failback mode.

Immediate Mode: Fail back immediately whenever a higher priority interface is plugged in or when there is a priority change. Immediate failback returns you to the use of your preferred Internet source more quickly which may have advantages such as reducing the cost of a failover data plan, but it may cause more interruptions in your network than **Usage** or **Time** modes.



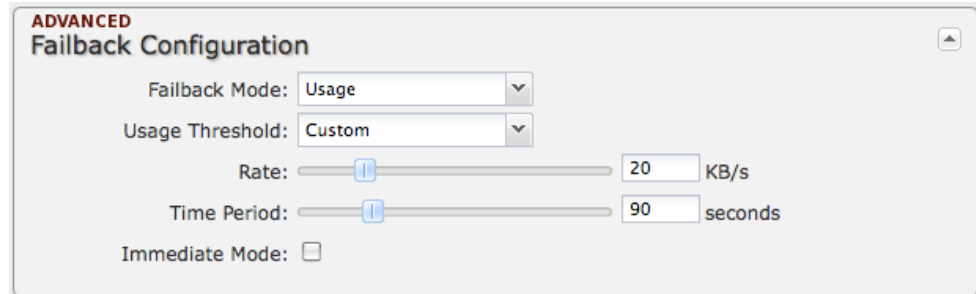
ADVANCED
IPv6 Failure Check

Idle Check Interval: 30 seconds

Monitor while connected: Active Ping

Active Ping could use as much as **9.3 MB** of data per month.

Ping IPv6 Address:



ADVANCED
Failback Configuration

Failback Mode: Usage

Usage Threshold: Custom

Rate: 20 KB/s

Time Period: 90 seconds

Immediate Mode: ☐

7.1.4 IP Overrides

IP overrides allow you to override IP settings after a device's IP settings have been configured. Only the fields that are filled out will be overridden. Override any of the following fields:

- IP Address
- Subnet Mask
- Gateway IP
- Primary DNS Server
- Secondary DNS Server



The screenshot shows a web interface titled "IP Overrides" with a close button in the top right corner. Below the title, there are five input fields, each with a label and a text box containing three dots (representing IP octets):

- IP Address: [. . .]
- Subnet Mask: [. . .] with a small blue up/down arrow icon to the right.
- Gateway IP: [. . .]
- Primary DNS Server: [. . .]
- Secondary DNS Server: [. . .]

7.1.5 IPv6 Settings

The IPv6 (<http://en.wikipedia.org/wiki/IPv6>) configuration allows you to enable and configure IPv6 for a WAN device. These settings should be configured in combination with the IPv6 LAN settings (go to **Network Settings** → **Local Networks**, select the LAN under **Local IP Networks**, and click **Edit**) to achieve the desired result.

This is a dual-stacked implementation of IPv6, so IPv6 and IPv4 are used alongside each other. If you enable IPv6, the router will not allow connections via IPv4. When IPv6 is enabled, some router features are no longer supported. These are:

- RADIUS/TACACS+ accounting for wireless clients and admin/CLI login
- IP Passthrough (not needed with IPv6)
- NAT (not needed with IPv6)
- Bounce pages
- UPnP
- Syslog
- SNMP over the WAN (LAN works)

There are two main types of IPv6 WAN connectivity: native (**Auto** and **Static**) and tunneling over IPv4 (**6to4**, **6in4**, and **6rd**).

- **Native** – (**Auto** and **Static**) The upstream ISP routes IPv6 packets directly.
- **IPv6 tunneling** – (**6to4**, **6in4**, and **6rd**) Each IPv6 packet is encapsulated by the router in an IPv4 packet and routed over an IPv4 route to a tunnel endpoint that decapsulates it and routes the IPv6 packet natively. The reply is encapsulated by the tunnel endpoint in an IPv4 packet and routed back over an IPv4 route. Some tunnel modes do not require upstream ISPs to route or even be aware of IPv6 traffic at all. Some modes are utilized by upstream ISPs to simplify the configuration and rollout of IPv6.

Enable IPv6 and select the desired IPv6 connection method for this WAN interface.

- **Disabled** (default) – IPv6 disabled on this interface.
- **Auto** – IPv6 will use automatic connection settings (if available).
- **Static** – Input a specific IPv6 address for your WAN connection. This is provided by the ISP if it is supported.
- **6to4 Tunnel** (<http://en.wikipedia.org/wiki/6to4>) – Encapsulates the IPv6 data and transfers it to an automatic tunnel provider (if your ISP supports it).
- **6in4 Tunnel** (<http://en.wikipedia.org/wiki/6in4>) – Encapsulates the IPv6 data and sends it to the configured tunnel provider.
- **6rd Tunnel** (IPv6 rapid deployment: http://en.wikipedia.org/wiki/IPv6_rapid_deployment) – Encapsulates the IPv6 data and sends it to a relay server provided by your ISP.

When you configure IPv6, you have the option to designate **DNS Servers** and **Delegated Networks**. Because of the dual-stack setup, these settings are optional: when configured for IPv6, the router will fall back to IPv4 settings when necessary.

DNS Servers

Each WAN device is required to connect IPv4 before connecting IPv6. Because of this, DNS servers are optional, as most IPv4 DNS servers will respond with AAAA records (128-bit IPv6 DNS records, most commonly used to map hostnames to the IPv6 address of the host) if requested. If no IPv6 DNS servers are configured, the system will fall back to the DNS servers provided by the IPv4 configuration.

Delegated Networks

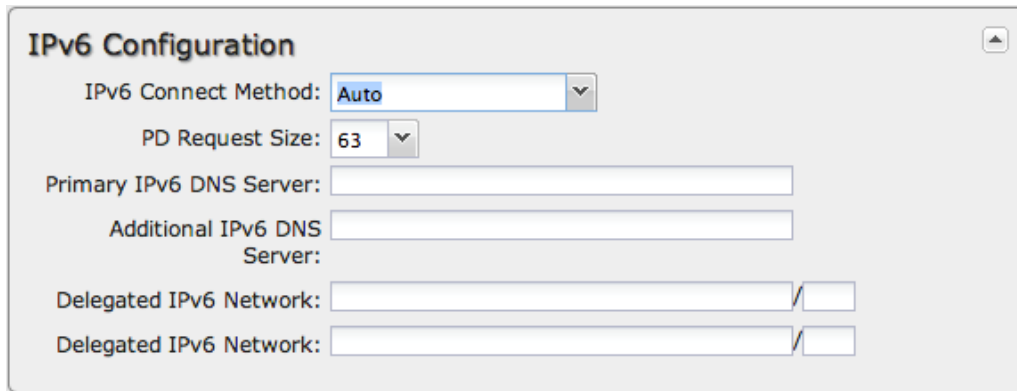
A delegated network is an IPv6 network that is inherently provided by or closely tied to a WAN IP configuration. The IPv6 model is for each device to have end-to-end IP connectivity without relying on any translation mechanism. In order to achieve this, each client device on the LAN network needs to have a publicly routable IPv6 address.

AUTO

IPv6 auto-configuration mode uses DHCPv6 and/or SLAAC to configure the IPv6 networks. When you select **Auto**, all of the following settings are optional (depending on your provider's requirements):

- **PD Request Size** – Prefix Delegation request size. This is the size of IPv6 network that will be requested from the ISP to delegate to LAN networks. (Default: 63)
- **Primary IPv6 DNS Server** – (optional) Depending on your provider, this may be required. This only takes effect if the default global DNS setting on the **Network Settings** → **DNS** page is "Automatic".
- **Additional IPv6 DNS Server** – Secondary DNS server.
- **Delegated IPv6 Network** – (optional) Network available for delegation to LANs. Depending on your provider, this may be required. Prefixes specified here only take effect if those supplied by the connection are insufficient to configure your LANs.
- **Delegated IPv6 Network** – Additional network available for delegation to LANs.

Example Configuration:



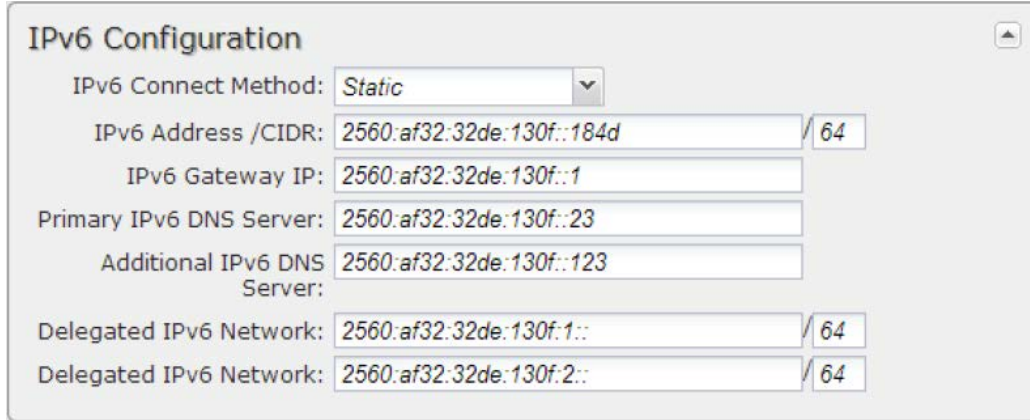
The screenshot shows the 'IPv6 Configuration' window. The 'IPv6 Connect Method' is set to 'Auto'. The 'PD Request Size' is set to 63. The 'Primary IPv6 DNS Server' and 'Additional IPv6 DNS Server' fields are empty. The 'Delegated IPv6 Network' field is empty, and the 'Delegated IPv6 Network' field is also empty.

STATIC

As with IPv4, static configuration is available for situations where the WAN IPv6 topology is fixed.

- **IPv6 Address/CIDR** – Input the IPv6 static IP address and mask length provided by your ISP (see http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing for an explanation of CIDR).
- **IPv6 Gateway IP** – Input the IPv6 remote gateway IP address provided by your ISP.
- **Primary IPv6 DNS Server** – (optional) Depending on your provider/setup, this may be required. This only takes effect if the default global DNS setting on the **Network Settings** → **DNS** page is "Automatic".
- **Additional IPv6 DNS Server** – Secondary DNS server.
- **Delegated IPv6 Network** – (optional) Network available for delegation to LANs. Depending on your provider, this may be required. Prefixes specified here only take effect if those supplied by the connection are insufficient to configure your LANs.
- **Delegated IPv6 Network** – Additional network available for delegation to LANs.

Example Configuration:



The screenshot displays the 'IPv6 Configuration' window. The 'IPv6 Connect Method' is set to 'Static'. The 'IPv6 Address /CIDR' field contains '2560:af32:32de:130f::184d' with a '/ 64' suffix. The 'IPv6 Gateway IP' field contains '2560:af32:32de:130f::1'. The 'Primary IPv6 DNS Server' field contains '2560:af32:32de:130f::23'. The 'Additional IPv6 DNS Server' field contains '2560:af32:32de:130f::123'. There are two 'Delegated IPv6 Network' fields; the first contains '2560:af32:32de:130f:1::' with a '/ 64' suffix, and the second contains '2560:af32:32de:130f:2::' with a '/ 64' suffix.

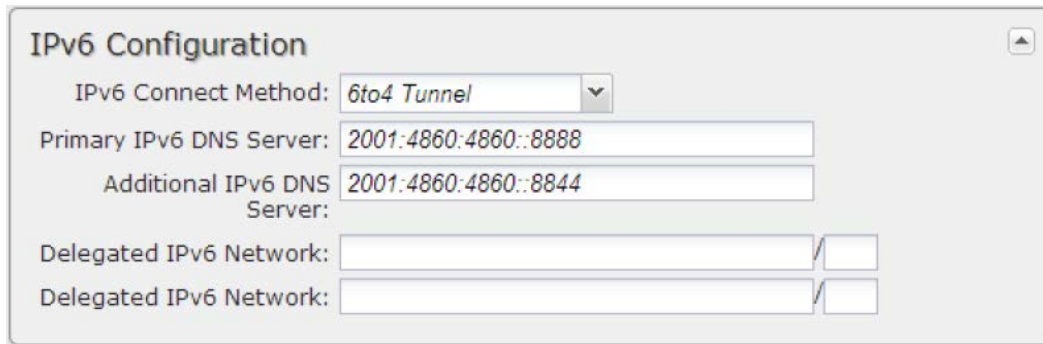
IPv6 Configuration	
IPv6 Connect Method:	Static
IPv6 Address /CIDR:	2560:af32:32de:130f::184d / 64
IPv6 Gateway IP:	2560:af32:32de:130f::1
Primary IPv6 DNS Server:	2560:af32:32de:130f::23
Additional IPv6 DNS Server:	2560:af32:32de:130f::123
Delegated IPv6 Network:	2560:af32:32de:130f:1:: / 64
Delegated IPv6 Network:	2560:af32:32de:130f:2:: / 64

6TO4 TUNNEL

Out of the box, 6to4 is the simplest mode to enable full end-to-end IPv6 connectivity in an organization if the upstream ISP properly routes packets to and from the 6to4 unicast relay servers.

- **Primary IPv6 DNS Server** – (optional) Depending on your provider, this may be required. This only takes effect if the default global DNS setting on the **Network Settings** → **DNS** page is "Automatic".
- **Additional IPv6 DNS Server** – Secondary DNS server.
- **Delegated IPv6 Network** – (optional) Network available for delegation to LANs. Depending on your provider, this may be required. Prefixes specified here only take effect if those supplied by the connection are insufficient to configure your LANs.
- **Delegated IPv6 Network** – Additional network available for delegation to LANs.

Example Configuration:



The screenshot shows a configuration window titled "IPv6 Configuration". It contains the following fields and settings:

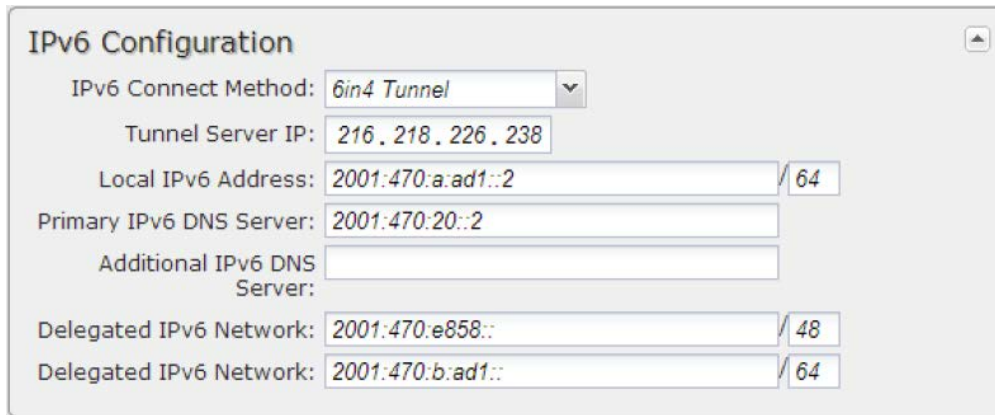
- IPv6 Connect Method:** A dropdown menu set to "6to4 Tunnel".
- Primary IPv6 DNS Server:** A text field containing "2001:4860:4860::8888".
- Additional IPv6 DNS Server:** A text field containing "2001:4860:4860::8844".
- Delegated IPv6 Network:** Two identical rows, each consisting of a text field and a checked checkbox.

6IN4 TUNNEL

The 6in4 tunnel mode utilizes explicit IPv4 tunnel endpoints and encapsulates IPv6 packets using 41 as the specified protocol type in the IP header. A 6in4 tunnel broker provides a static IPv4 server endpoint, decapsulates packets and provides routing for both egress and ingress IPv6 packets. Most tunnel brokers provide a facility to request delegated networks for use through the tunnel.

- **Tunnel Server IP** – Input the tunnel server IP address provided by your tunnel service.
- **Local IPv6 Address** – Input the local IPv6 address provided by your tunnel service.
- **Primary IPv6 DNS Server** – (optional) Depending on your provider, this may be required. This only takes effect if the default global DNS setting on the **Network Settings** → **DNS** page is "Automatic".
- **Additional IPv6 DNS Server** – Secondary DNS server.
- **Delegated IPv6 Network** – (optional) Network available for delegation to LANs. Depending on your provider, this may be required. Prefixes specified here only take effect if those supplied by the connection are insufficient to configure your LANs.
- **Delegated IPv6 Network** – Additional network available for delegation to LANs.

Example Configuration:



The screenshot displays the 'IPv6 Configuration' window with the following settings:

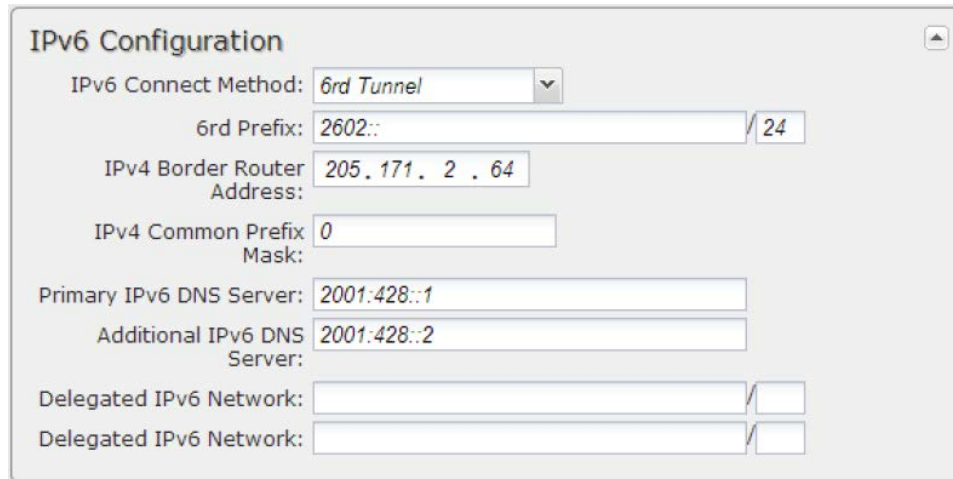
- IPv6 Connect Method:** 6in4 Tunnel (selected from a dropdown)
- Tunnel Server IP:** 216.218.226.238
- Local IPv6 Address:** 2001:470:a:ad1::2 (with a /64 prefix)
- Primary IPv6 DNS Server:** 2001:470:20::2
- Additional IPv6 DNS Server:** (empty field)
- Delegated IPv6 Network:** 2001:470:e858:: (with a /48 prefix)
- Delegated IPv6 Network:** 2001:470:b:ad1:: (with a /64 prefix)

6RD TUNNEL

IPv6 Rapid Deployment (6rd) is a method of IPv6 site configuration derived from 6to4. It is different from 6to4 in that the ISP provides explicit 6rd infrastructure that handles the IPv4 $\leftrightarrow$ IPv6 translation within the ISP network. 6rd is considered more reliable than 6to4 as the ISP explicitly maintains infrastructure to support tunneled IPv6 traffic over their IPv4 network.

- **6rd Prefix** – The 6rd prefix and prefix length should be supplied by your ISP.
- **IPv4 Border Router Address** – This address should be supplied by your ISP.
- **IPv4 Common Prefix Mask** – Input the number of common prefix bits that you can mask off of the WAN's IPv4 address.
- **Primary IPv6 DNS Server** – (optional) Depending on your provider, this may be required. This only takes effect if the default global DNS setting on the **Network Settings** → **DNS** page is "Automatic".
- **Additional IPv6 DNS Server** – Secondary DNS server.
- **Delegated IPv6 Network** – (optional) Network available for delegation to LANs. Depending on your provider, this may be required. Prefixes specified here only take effect if those supplied by the connection are insufficient to configure your LANs.
- **Delegated IPv6 Network** – Additional network available for delegation to LANs.

Example Configuration:



The screenshot displays the 'IPv6 Configuration' window. The 'IPv6 Connect Method' is set to '6rd Tunnel'. The '6rd Prefix' is '2602::' with a prefix length of '24'. The 'IPv4 Border Router Address' is '205.171.2.64'. The 'IPv4 Common Prefix Mask' is '0'. The 'Primary IPv6 DNS Server' is '2001:428::1' and the 'Additional IPv6 DNS Server' is '2001:428::2'. There are two empty fields for 'Delegated IPv6 Network'.

Field	Value
IPv6 Connect Method	6rd Tunnel
6rd Prefix	2602:: / 24
IPv4 Border Router Address	205.171.2.64
IPv4 Common Prefix Mask	0
Primary IPv6 DNS Server	2001:428::1
Additional IPv6 DNS Server	2001:428::2
Delegated IPv6 Network	
Delegated IPv6 Network	

7.1.6 Modem Settings

Not all modems will have all of the options shown below; the available options are specific to the modem type.

On Demand: Typically modem connections are not always on. When this mode is selected a connection to the Internet is made as needed. When this mode is not selected a connection to the Internet is always maintained.

IP WAN Subnet Filter: This feature will filter out any packets going to the modem that do not match the network (address and netmask).

Aggressive Reset: When Aggressive Reset is enabled the system will attempt to maintain a good modem connection. If the Internet has been unreachable for a period of time, a reset of the modem will occur in attempt to re-establish the connection.

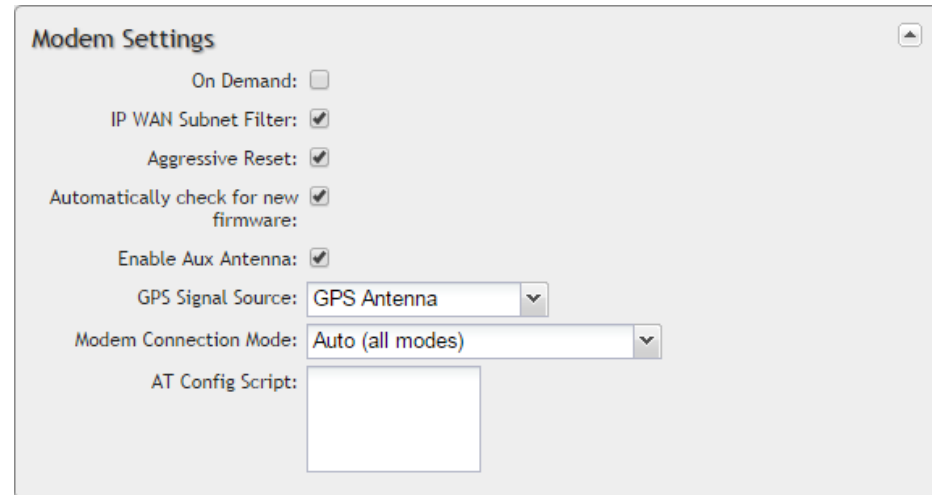
Automatically check for new firmware: Select this box to automatically check for new firmware.

Enable Aux Antenna: Enable or disable the modem's auxiliary diversity antenna. This should normally be left enabled.

GPS Signal Source: Specify GPS Antenna or Aux Antenna.

Modem Connection Mode: Specify how the modem should connect to the network. Not all options are available for all modems; this will default to Auto if an incompatible mode is selected.

- **Auto (all modes):** Let the modem decide which network to use
- **Auto 3G (3G or less):** Let the modem decide which 2G or 3G network to use. Do not attempt to connect to LTE
- **Force LTE:** Connect to LTE only and do not attempt to connect to 3G
- **Force 3G (EVDO, UMTS, HSPA):** Connect to 3G network only
- **Force 2G (1xRTT, EDGE, GPRS):** Connect to 2G network only



AT Config Script: Enter the custom AT configuration scripts(s) to be applied to the modem at configuration time, one time shortly after plug of the modem. Each script must be entered on a separate line. The interpretation of the script and associated response will be logged so you should check the system log to make sure there were no error.

NOTE: Should not be used unless instructed to do so by your modem's cellular provider or by a support technician.

7.1.7 CDMA Settings

These settings are usually specific to your wireless carrier's private networks. You should not set these unless directed to by a carrier representative. If a field below is left blank, that particular setting will not be changed in the modem. You should only fill in fields that are required by your carrier.

- **Persist Settings:** If this is not checked, these settings will only be in place until the router is rebooted or the modem is unplugged.
- **Active Profile:** Select a number from 0-5 from the dropdown list.

The following fields can be left blank. If left blank they will remain unchanged in the modem.

- **NAI (Username@realm):** Network Access Identifier. NAI is a standard system of identifying users who attempt to connect to a network.
- **AAA Shared Secret (Password):** "Authentication, Authorization, and Accounting" password.
- **Verify AAA Shared Secret.**
- **HA Shared Secret:** "Home Agent" shared secret.

CDMA Settings

NOTE: These settings are usually specific for your Wireless Carrier's private networks. You should not set these unless directed to by a Carrier Representative. If a field below is left blank, that particular setting will not be changed in the modem. You should only fill in fields that are required by your Carrier.

Persist Settings: ☐

Active Profile:

NAI (Username@realm):

AAA Shared Secret (Password):

Verify AAA Shared Secret (Password):

HA Shared Secret (Password):

Primary HA:

Secondary HA:

AAA SPI:

HA SPI:

- **Primary HA.**
- **Secondary HA.**
- **AAA SPI:** AAA Security Parameter Index.
- **HA SPI:** HA Security Parameter Index.

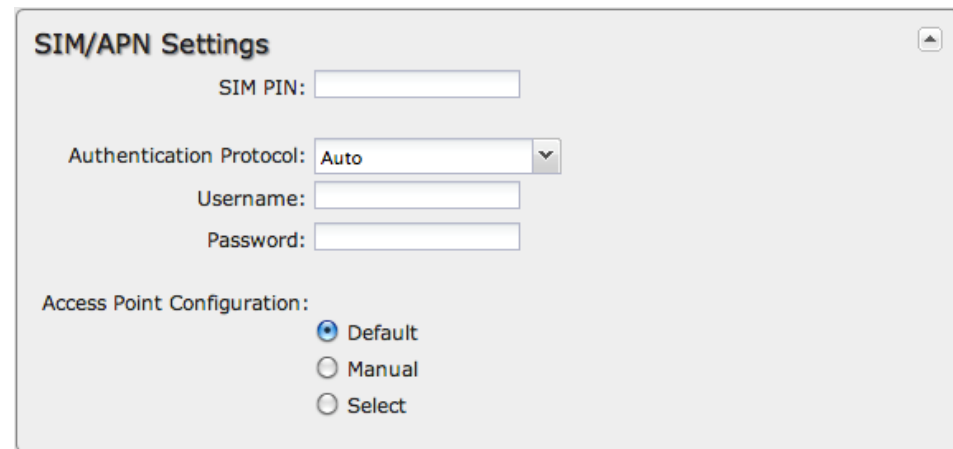
7.1.8 SIM/APN/Auth Settings

SIM PIN: PIN number for a GSM modem with a locked SIM.

Authentication Protocol: Set this only if your service provider requires a specific protocol and the **Auto** option chooses the wrong one. Choose from **Auto**, **PAP**, and **CHAP** and then input your username and password.

Access Point Configuration: Some wireless carriers provide multiple Access Point configurations that a modem can connect to. Some APN examples are "isp.cingular" and "vpn.com".

- **Default:** Let the router choose an APN automatically.
- **Manual:** Enter an APN by hand.
- **Select:** This opens a table with 16 slots for APNs, each of which can be set as IP, IPV4V6, or IPV6. The default APN is marked with an asterisk (*). You can change the APN names, select a different APN, etc. For Verizon modems, only the third slot is editable. Changes made here are written to the modem, so a factory reset of the router will not impact these settings.



SIM/APN Settings

SIM PIN:

Authentication Protocol:

Username:

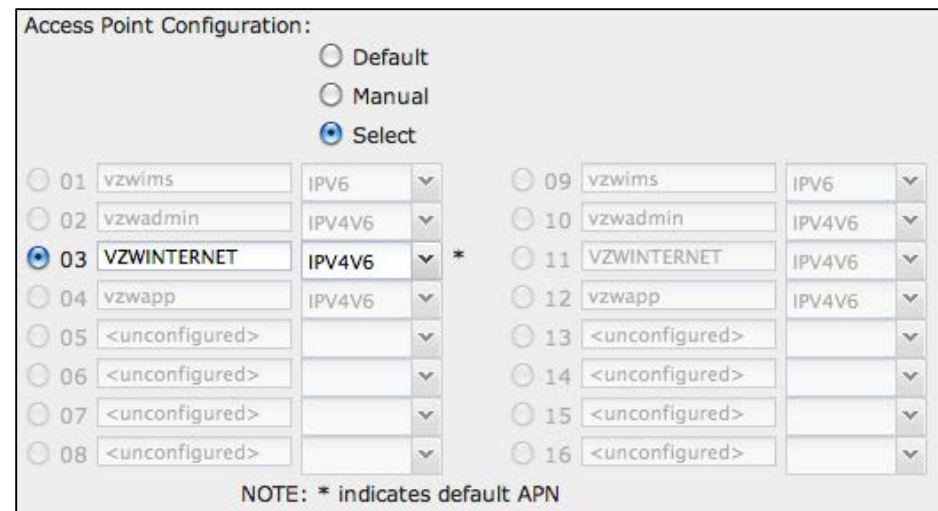
Password:

Access Point Configuration:

☒ Default

☐ Manual

☐ Select



Access Point Configuration:

☐ Default

☐ Manual

☒ Select

☐ 01	vzwims	IPV6	☐ 09	vzwims	IPV6
☐ 02	vzwadmin	IPV4V6	☐ 10	vzwadmin	IPV4V6
☒ 03	VZWINTERNET	IPV4V6 *	☐ 11	VZWINTERNET	IPV4V6
☐ 04	vzwapp	IPV4V6	☐ 12	vzwapp	IPV4V6
☐ 05	<unconfigured>		☐ 13	<unconfigured>	
☐ 06	<unconfigured>		☐ 14	<unconfigured>	
☐ 07	<unconfigured>		☐ 15	<unconfigured>	
☐ 08	<unconfigured>		☐ 16	<unconfigured>	

NOTE: * indicates default APN

7.1.9 Update/Activate a Modem

Some 3G/4G modems can be updated and activated while plugged into the router. Updates and activation methods vary by modem model and service provider. Possible methods are: PRL Update, Activation, and FUMO. All supported methods will be displayed when you select your modem and click “Control”. If no methods are displayed for your device then you will need to update and activate your device externally.

To update or activate a modem, select the device and click “Control”.

The modem *does not* support Update/Activate methods: A message will state that there is no support for PRL Update, Activation, or FUMO.

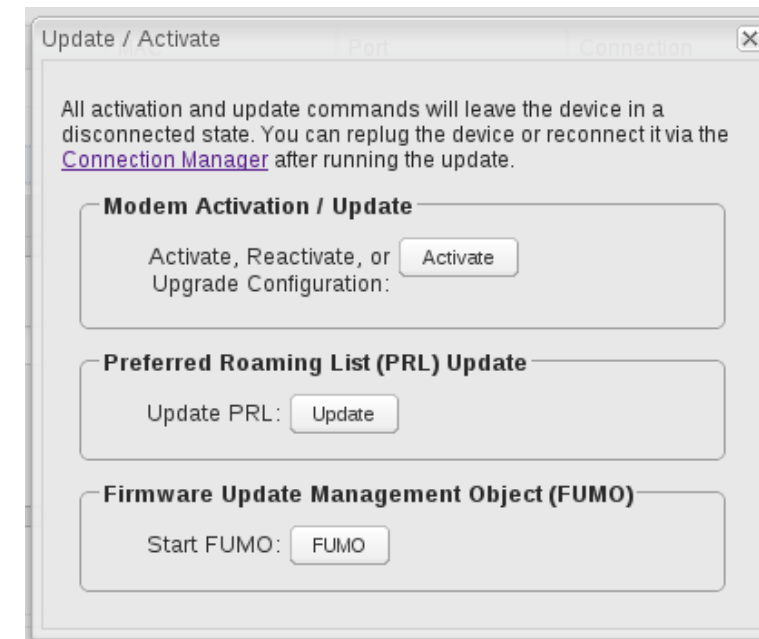
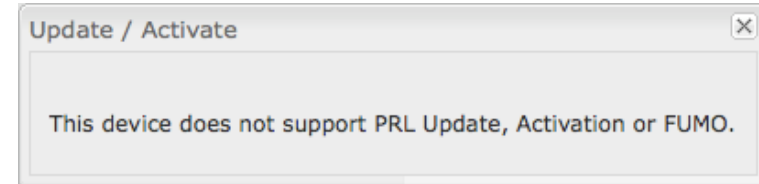
The modem supports Update/Activate methods: A message will display showing options for each supported method:

- **Modem Activation / Update:** Activate, Reactivate, or Upgrade Configuration.
- **Preferred Roaming List (PRL) Update**
- **Firmware Update Management Object (FUMO)**

Click the appropriate icon to start the process.

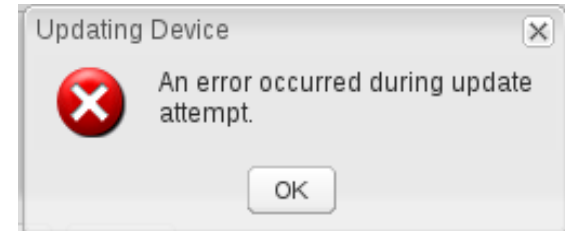
If the modem is connected when you start an operation the router will automatically disconnect it. The router may start another modem as a failover measure. When the operation is done the modem will go back to an idle state, at which point the router may restart it depending on failover and fallback settings.

*NOTE: Only one operation is supported at a time. If you try to start the same operation on the same modem twice the UI will not report failure and the request will finish normally when the original request is done. However if you try to start a **different** operation or use a **different** modem, this second request will fail without interfering with the pending operation.*



Process Timeout: If the process fails an error message will display.

Activation has a 3-minute timeout, PRL update has a 4-minute timeout, and FUMO has a 10-minute timeout.

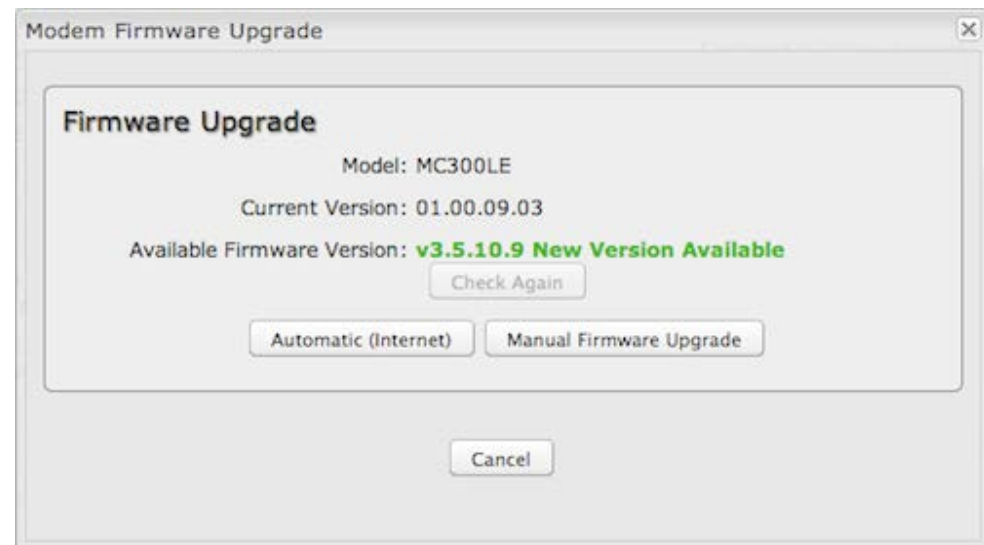


UPDATE MODEM FIRMWARE

Click on the **Firmware** button to open the Modem Firmware Upgrade window. This will show whether there is new modem firmware available.

If you select **Automatic (Internet)** the firmware will be updated automatically. Use **Manual Firmware Upgrade** to instead manually upload firmware from a local computer or device.

NOTE: Only Cradlepoint integrated modems have this firmware upgrade option.



RESET THE MODEM

Click on the **Reset** button to power cycle the modem. This will have the same effect as unplugging the modem.

7.1.10 Configuration Rules (Advanced)

This section allows you to create general rules that apply to the Internet connections of a particular type. These can be general or very specific. For example, you could create a rule that applies to all WiMAX modems, or a rule that only applies to an Internet source with a particular MAC address.

The Configuration Rules list shows all rules that you have created, as well as all of the default rules. These are listed in the order they will be applied. The most general rules are listed at the top, and the most specific rules are at the bottom. The router goes down the list and applies all rules that fit for attached Internet sources. Configuration settings farther down the list will override previous settings.

Select any of these rules and click “Edit” to change the settings for a rule. To create a new rule, click “Add.”

ADVANCED
Configuration Rules

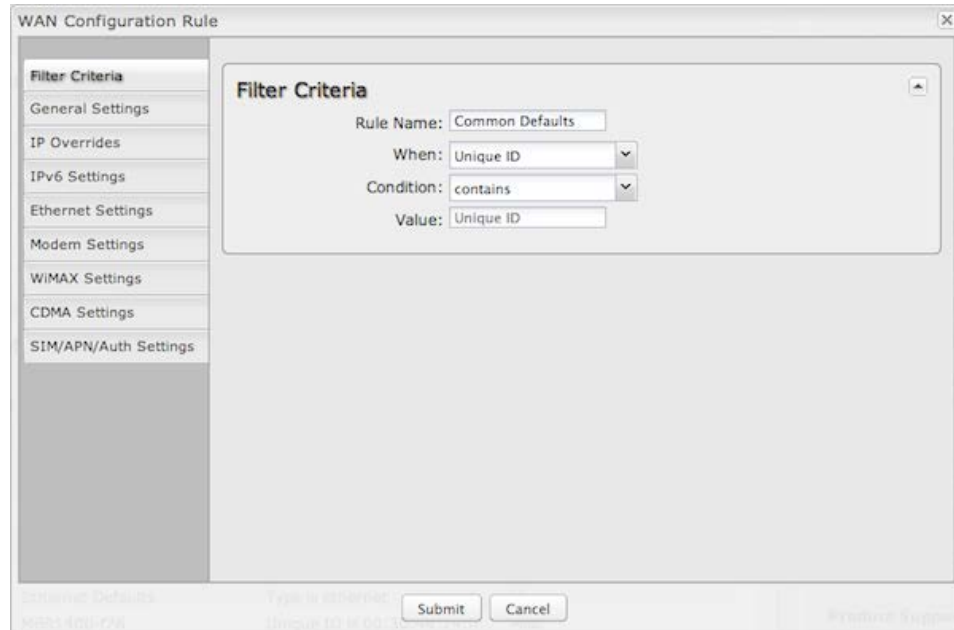
Add Edit Remove (ordered by rule application priority)

☐		Rule Name	Conditions	Apply Settings
☐	↓	Common Defaults	Unique ID contains	Misc
☐	↑ ↓	3G Modem Defaults	Type is modem	Misc
☐	↑ ↓	WiMax Defaults	Type is wimax	Misc
☐	↑	LTE Defaults	Type is lte	Misc

WAN CONFIGURATION RULE EDITOR

After clicking “Add” or “Edit,” you will see a popup with the following tabs:

- Filter Criteria
- General Settings
- IP Overrides
- IPv6 Settings
- Ethernet Settings
- Modem Settings
- WiMAX Settings
- CDMA Settings
- SIM/APN/Auth Settings



WAN Configuration Rule

Filter Criteria

Rule Name: Common Defaults

When: Unique ID

Condition: contains

Value: Unique ID

Submit Cancel Product Support

FILTER CRITERIA

Begin by setting the **Filter Criteria** if you are creating a new rule. Create a name for your rule and the condition for which the rule applies:

Rule Name: Create a name meaningful to you. This name is optional.

Select each of the following to create a condition for your rule. **When:**

- **Port** (USB Port): Select by the port that you are plugging the modem into.
- **Manufacturer:** Select by the manufacturer, such as Sierra Wireless.
- **Model:** Set your rule according to the specific model of modem.
- **Type** (LTE, Modem, HSPA): Select by type of Internet source.
- **Serial Number:** Select 3G or LTE modem by Serial Number.



- **MAC Address:** Select WiMAX modem by MAC Address.
- **Unique ID:** Select by ID. This is generated by the router and displayed when the device is connected to the router.

Condition: Select “is,” “is not,” “starts with,” “contains,” or “ends with” to create your condition’s statement.

Value: If the correct values are available, select from the dropdown list. You may need to manually input the value.

The condition will be of the following form:

“ (When) is/is not (value) ”

For example:

“Type is not LTE”

“Port is USB Port 1”

Once you have established the condition for your configuration rule, choose from the other tabs to set the desired configuration. All of the tab options – **General Settings**, **IP Overrides**, **IPv6 Settings**, **Ethernet Settings**, **Modem Settings**, **WiMAX Settings**, **CDMA Settings**, and **SIM/APN/Auth Settings** – have the same configuration options shown above in the WAN Configuration section (the options for Configuration Rules are the same as they are for individual devices).

7.2 Data Usage

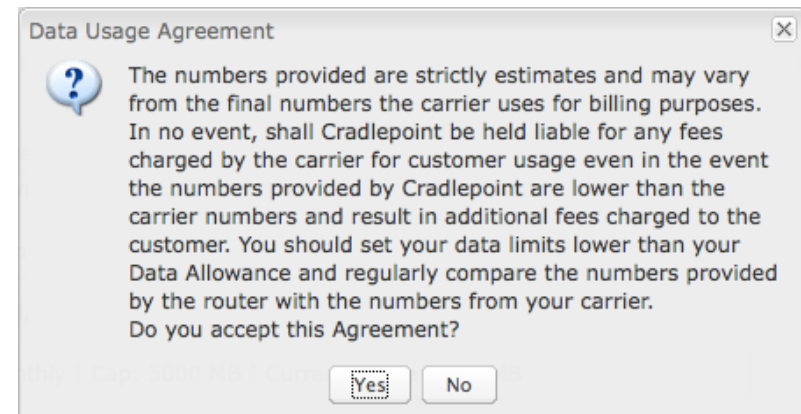
Data Usage Management & Alerts allows you to create and manage rules that help control the data usage of a modem. If you have a limited data plan or a price increase on your plan after a certain amount of usage, a **Data Usage Rule** can help you track these amounts. You can set a rule to shut down use of a modem and/or send a message when you reach a data usage amount you set.

Enable Data Usage: ☐

Enable Data Usage: Enabled/Disabled. (Default: Disabled.)

When you select **Enabled**, you will see the **Data Usage Agreement** shown to the right. The purpose of this agreement is to ensure that you understand that the data numbers for the CBA850 may not perfectly match those of your carrier: Cradlepoint cannot be held responsible. You must accept the agreement by clicking **Yes** in order to begin creating data usage rules.

WARNING: You should set your data limits lower than your Data Allowance and regularly compare the numbers provided by the router with the numbers from your carrier.

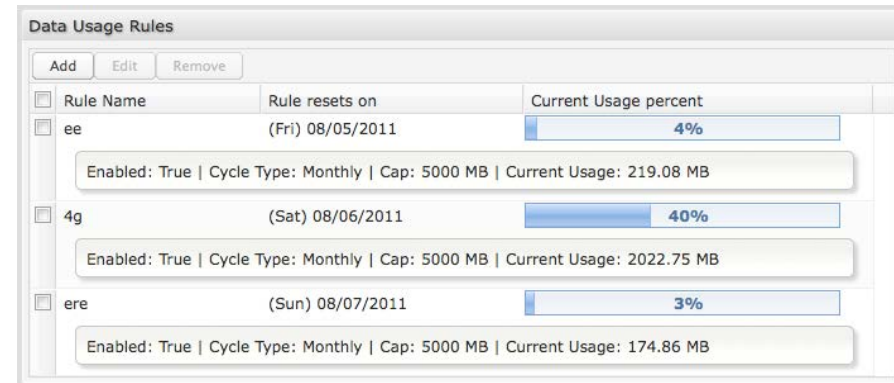


7.2.1 Data Usage Rules

The Date Usage Rule display shows basic information for each rule you have created (including rules created with a template). The following information is displayed:

- **Rule Name**
- **Enabled:** True/False
- **Date for Rule Reset**
- **Cycle Type:** Daily, Weekly, or Monthly
- **Cap:** Amount in MB.
- **Current Usage:** Shown as an amount in MB, as a percentage of the cap, and in a bar graph.

Click **Add** to configure a new Data Usage Rule.



DATA USAGE RULE – PAGE 1

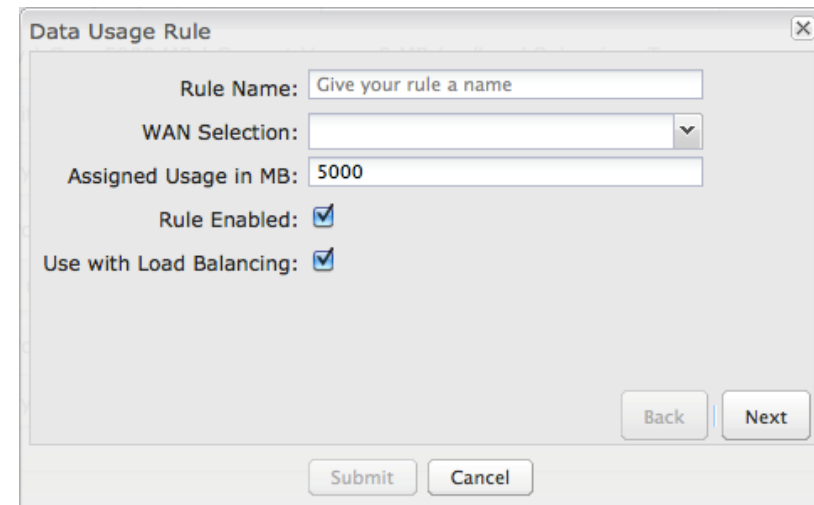
Rule Name: Give your rule a name for later recognition.

WAN Selection: Select from the dropdown list of currently attached WAN devices.

Assigned Usage in MB: Enter a cap amount in megabytes. 1024 megabytes equals 1 gigabyte.

Rule Enabled: (Default: Enabled.) Click to disable.

Use with Load Balancing: When checked, the Load Balancing feature is *allowed* to use the thresholds and metrics of this rule when making balance decisions. This causes Load Balancing to spread the data usage between interfaces according to the assigned usage rather than bandwidth. This is a best effort to keep



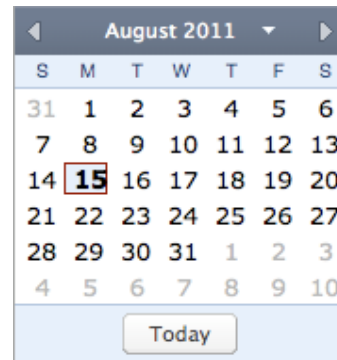
all interfaces with these rules at a similar percentage utilization of data (e.g. 10%, 50%, 90%) as the cycle progresses, rather than quickly using 100% of a fast 1GB capped interface while using only a fraction of a slow 10GB capped interface, thus leaving the rest of the cycle with only the slow interface. The **Data Usage algorithm** on the Load Balancing page must be selected or this checkbox has no effect.

DATA USAGE RULE – PAGE 2

Cycle Type: How often the rule will reset. The data usage amount will be reset at the end of each cycle. Select the length of a cycle from a dropdown menu with the following choices:

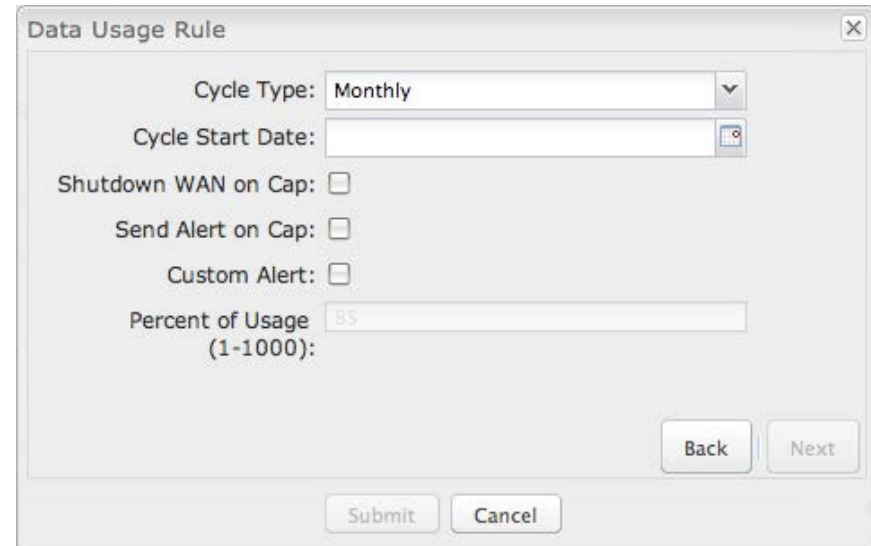
- Daily
- Weekly
- Monthly

Cycle Start Date: Select the date you wish the rule to begin. This date will be used to track when the rule will reset.



August 2011						
S	M	T	W	T	F	S
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

Today



Data Usage Rule

Cycle Type: Monthly

Cycle Start Date:

Shutdown WAN on Cap: ☐

Send Alert on Cap: ☐

Custom Alert: ☐

Percent of Usage (1-1000):

Back Next

Submit Cancel

Shutdown WAN on Cap: If selected, the WAN device will shut down when the assigned usage is reached. A cycle reset or a rule deletion will re-enable the device.

Send Alert on Cap: An email alert will be generated and sent when the assigned usage is reached.

WARNING: The SMTP mail server must be configured in **System Settings** → **Device Alerts**.

Custom Alert: When checked you enable a second email to be configured for a percentage of the assigned usage.

Percent of Usage (1-1000): If selected, a custom alert will be sent when your data usage reaches this percentage of your usage cap. For example, you could set this at 90 percent so that you know when your usage is nearing 100 percent of the cap.

7.2.2 Template Configuration

Templates allow you to control multiple WAN devices with the same rule. Each WAN device that matches a template will automatically have its own rule created.

For example, you can set a template rule for all mobile data modems that causes your router to send an alert after 1000 MB of usage in a month. When you attach a new 4G USB modem, your template will immediately create a new **Data Usage Rule** for the attached modem that sends the alert as specified.

Click **Add** to configure a new Template rule.

Create a **Template Name** that you can recognize.

The template will apply to one of the following **WAN types**:

- All WAN
- All Modems

Select one of these types.

The rest of the rule settings options match those in the **Data Usage Rules**. See the section above for additional information about how to configure your template usage rules.

Add Edit Remove			
☐	Template Name	WAN type	Assigned Usage in MB
☐	USB data plans	modem	5000
			Cycle Type
			monthly

Template Rule Creation

Template Name:

Give your template a name

WAN type:

☐ All WAN
 ☐ All Ethernet
 ☐ All Modems

Assigned Usage in MB:

5000

Cycle Type:

Monthly

Cycle Start Date:

1

Shutdown WAN on Cap:

☐

Send Alert on Cap:

☐

Extra Email Alert:

☐

Percent of Usage (1-1000):

85

Submit

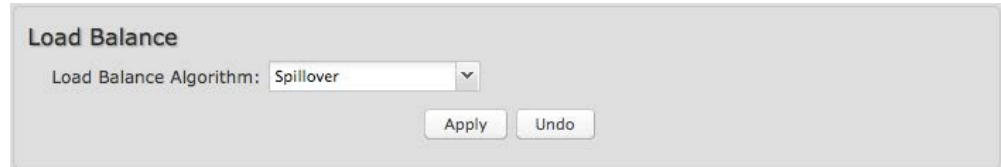
Cancel

7.3 WAN Affinity and Load Balancing

WAN affinity and load balancing both require multiple WAN devices, which is not typical usage

LOAD BALANCE

Select the Load Balance Algorithm from the following dropdown options:



- **Round-Robin:** Evenly distribute each session to the available WAN connections.
- **Rate:** Distribute load based on the current upload and download rates. A WAN device's upload and download bandwidth values can be set in **Internet** → **Connection Manager**.
- **Spillover:** This was the default algorithm in older (version 3) firmware. Load is always given to devices with the most available bandwidth. The estimated bandwidth rate is based on a combination of the upload and download configuration values and the observed capabilities of the device.
- **Data Usage:** This mode works in concert with the Data Usage feature (**Internet** → **Data Usage**). The router will make a best effort to keep data usage between interfaces at a similar percentage of the assigned data cap in the Data Usage rule for each interface, rather than distributing sessions based solely on bandwidth. For proper function you need to create data usage rules for each WAN device you will be load balancing. Make certain to select the "Use with Load Balancing" checkbox in the Data Usage rule editor.

WAN AFFINITY

WAN Affinity rules allow you to manage traffic in your network so that particular bandwidth uses are associated with particular WAN sources. This allows you to prioritize bandwidth.

EXAMPLE: You could specify that your guest LAN is only associated with your Ethernet connection with no failover. Then if your Ethernet connection goes down and the embedded modem connects for failover for your primary LAN, your guest LAN will not take bandwidth from your primary LAN, saving you money.

Click "Add" to open the WAN Affinity Policy Editor and create a new WAN Affinity rule.

Name: Give a name for your rule that is meaningful to you.

DSCP (DiffServ): Differentiated Services Code Point is the successor to TOS (Type of Service). Use this field to select traffic based on the DSCP header in each IP packet. This field is sometimes set by latency sensitive equipment such as VoIP phones. If you know specific DSCP values, you can input one here.

DSCP Negate: When checked this rule will match on any packet that does NOT match the DSCP field.

Protocol: Select from the dropdown list to specify the protocol for a particular data use. Otherwise, leave “Any” selected.

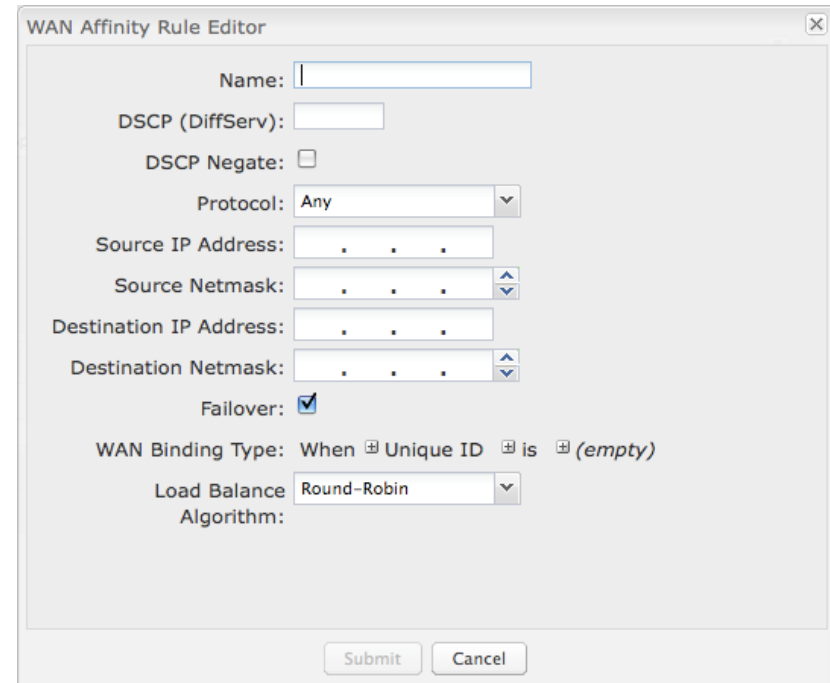
- Any
- ICMP
- TCP
- UDP
- GRE
- ESP
- SCTP

Source IP Address, Source Netmask, Destination IP Address, and Destination Netmask: Specify an IP address or range of IP addresses by combining an IP address with a netmask for either “source” or “destination” (or both). Source vs. destination is defined by traffic flow. Leave these blank to include all IP addresses (such as if your rule is defined by a particular port instead).

EXAMPLE: If you want to associate this rule with your guest LAN, you could input the IP address and netmask for the guest LAN here (leaving the last slot “0” to allow for any user attached to the guest network):

- **Source IP Address:** 192.168.10.0
- **Source Netmask:** 255.255.255.0

Failover: (Default: Selected.) When this is selected and traffic from the chosen WAN device for this rule is interrupted, the router will fail over to another available WAN device. Deselect this option to restrict this traffic to only the selected WAN interface.



The image shows a screenshot of the 'WAN Affinity Rule Editor' dialog box. It contains the following fields and options:

- Name:** A text input field.
- DSCP (DiffServ):** A text input field.
- DSCP Negate:** A checkbox, currently unchecked.
- Protocol:** A dropdown menu with 'Any' selected.
- Source IP Address:** A text input field with three dots as placeholders.
- Source Netmask:** A text input field with three dots as placeholders and up/down arrow buttons.
- Destination IP Address:** A text input field with three dots as placeholders.
- Destination Netmask:** A text input field with three dots as placeholders and up/down arrow buttons.
- Failover:** A checkbox, currently checked.
- WAN Binding Type:** A dropdown menu with 'When Unique ID is (empty)' selected.
- Load Balance Algorithm:** A dropdown menu with 'Round-Robin' selected.
- Buttons:** 'Submit' and 'Cancel' buttons at the bottom right.

WAN Binding Type: You have several options for specifying the type of WAN interface(s) you want associated with your rule. Designate the interface(s) by **Port**, **Manufacturer**, **Model**, **Type**, **Serial Number**, **MAC Address**, or **Unique ID**. This selection will create a dropdown list of options to complete a sentence with the following form: “When ____ is ____,” such as, “When Type is LTE.” You also have the option to replace “is” with “isn’t,” “starts with,” “ends with,” or “contains.”

- **Port:** Select from the dropdown list of possible WAN ports on the router.
 - o USB 1
 - o USB 2
 - o ExpressPort
- **Manufacturer:** Select from a dropdown list of attached devices.
- **Model:** Select from a dropdown list of attached devices.
- **Type:** Select from the dropdown list of possible WAN types.
 - o Modem
 - o LTE
- **Serial Number:** Select from a dropdown list of attached devices.
- **MAC Address:** Select from a dropdown list of attached devices.
- **Unique ID:** Select from a dropdown list of attached devices.

Load Balance Algorithm: Select the Load Balance Algorithm for this WAN Affinity rule from the following dropdown options:

- **Round-Robin:** Evenly distribute each session to the available WAN connections.
- **Rate:** Distribute load based on the current upload and download rates. A WAN device's upload and download bandwidth values can be set in **Internet** → **Connection Manager**.
- **Spillover:** This was the default algorithm in older (version 3) firmware. Load is always given to devices with the most available bandwidth. The estimated bandwidth rate is based on a combination of the upload and download configuration values and the observed capabilities of the device.
- **Data Usage:** This mode works in concert with the Data Usage feature (**Internet** → **Data Usage**). The router will make a best effort to keep data usage between interfaces at a similar percentage of the assigned data cap in the Data Usage rule for each interface, rather than distributing sessions based solely on bandwidth. For proper function you need to create data usage rules

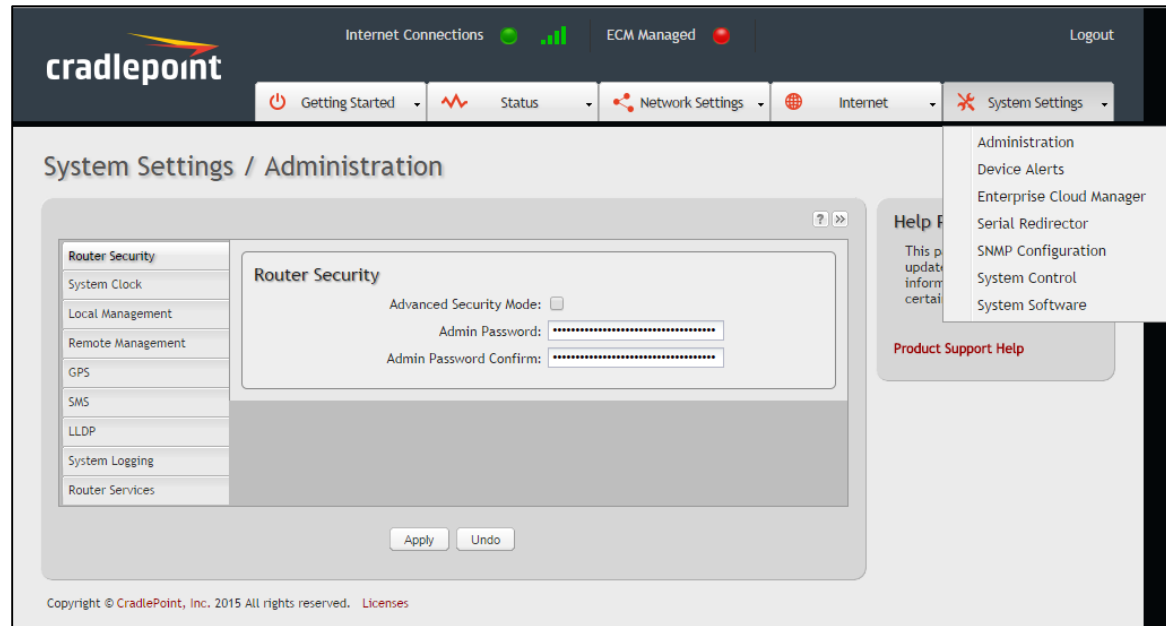


for each WAN device you will be load balancing. Make certain to select the "Use with Load Balancing" checkbox in the Data Usage rule editor.

8 SYSTEM SETTINGS

The System Settings tab has seven submenu items that provide access to tools for broad administrative control of the CBA850:

- Administration
- Device Alerts
- Enterprise Cloud Manager
- Serial Redirector
- SNMP Configuration
- System Control
- System Software



8.1 Administration

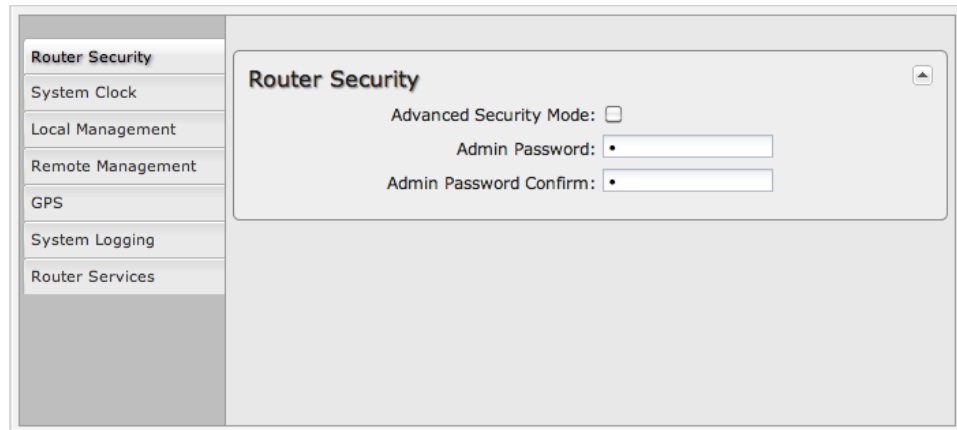
Select the Administration submenu item in order to control any of the following functions:

- Router Security
- System Clock
- Local Management
- Remote Management
- GPS
- SMS
- System Logging
- Router Services

8.1.1 Router Security

Advanced Security Mode: When the router is configured to use the advanced security mode, several aspects of the router's configuration and networking functionality will be extended to support high security environments. This includes support for multiple user accounts, increased password security, and additional network spoofing filters. If you plan to use your router in a PCI DSS compliant environment this option is mandatory.

Admin Password: Enter a password for the administrator who will have full access to the router's management interface. You can use the default password on the back of your product, or you can create a custom Administrator Password.



The screenshot shows the 'Router Security' configuration page. On the left is a sidebar menu with the following items: Router Security (highlighted), System Clock, Local Management, Remote Management, GPS, System Logging, and Router Services. The main content area is titled 'Router Security' and contains the following settings:

- Advanced Security Mode:** A checkbox that is currently unchecked.
- Admin Password:** A text input field with a small eye icon to toggle visibility.
- Admin Password Confirm:** A text input field with a small eye icon to toggle visibility.

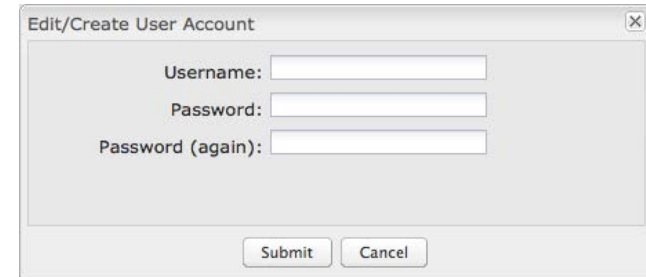
ADVANCED SECURITY MODE

When you enable **Advanced Security Mode**, you have three different options for the **Authentication Mode**:

- Local Users
- TACACS+
- RADIUS

LOCAL USERS

Create users with administrative privileges by inputting usernames and passwords in the **Advanced User Management** table.



A dialog box titled "Edit/Create User Account" with a close button (X) in the top right corner. It contains three input fields: "Username:", "Password:", and "Password (again):". At the bottom, there are two buttons: "Submit" and "Cancel".

TACACS+

TACACS+ stands for "Terminal Access Controller Access-Control System plus". The router will use a TACACS+ server (or two, optionally) to authorize administration.

Server Timeout: If the servers are not reached within the set time (possibly because the WAN is down), the router will automatically fall back to using **Local Users** mode to prevent users from being locked out.

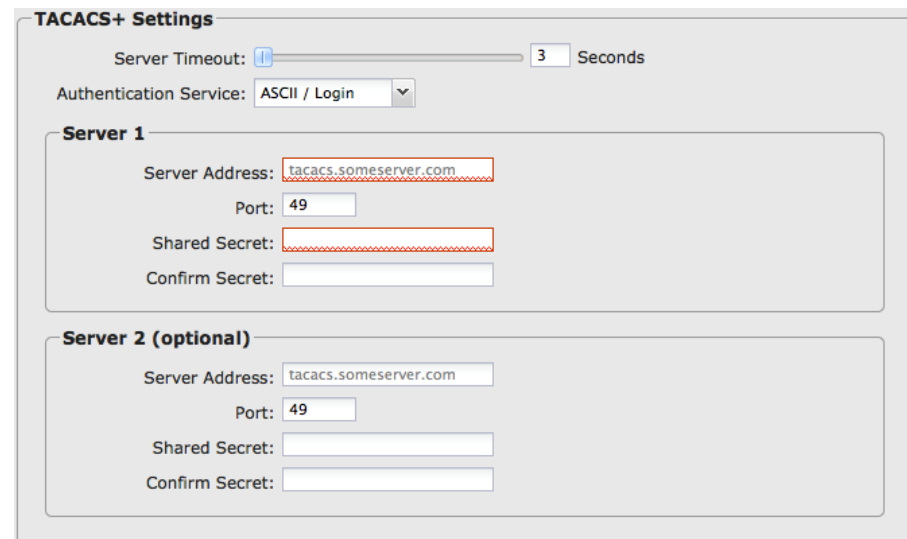
Authentication Service: Choose from:

- ASCII / Login
- PAP
- CHAP

Server Address: This can be either an IP address in the form of "1.2.3.4", or a DNS name in form of "host.domain.com". Only lower case letters are allowed for a DNS name.

Port: Port 49 is default for TACACS+.

Shared Secret



A configuration window titled "TACACS+ Settings". It includes a "Server Timeout" slider set to 3 seconds. Below it is a dropdown menu for "Authentication Service" set to "ASCII / Login". There are two sections for server configuration: "Server 1" and "Server 2 (optional)". Each section contains fields for "Server Address", "Port" (set to 49), "Shared Secret", and "Confirm Secret". In the "Server 1" section, the "Server Address" and "Shared Secret" fields are highlighted with red dashed boxes.

RADIUS

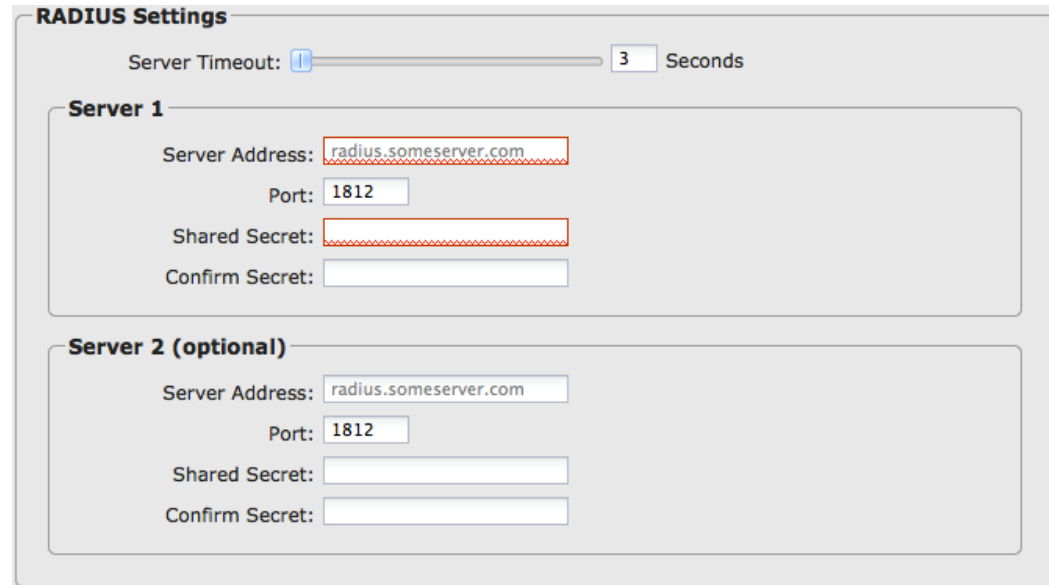
RADIUS stands for “Remote Authentication Dial In User Service”. The router will use a RADIUS server (or two, optionally) to authorize administration.

Server Timeout: If the servers are not reached within the set time (possibly because the WAN is down), the router will automatically fall back to using **Local Users** mode to prevent users from being locked out.

Server Address: This can be either an IP address in the form of "1.2.3.4", or a DNS name in form of "host.domain.com". Only lower case letters are allowed for a DNS name.

Port: Port 1812 is common for RADIUS servers.

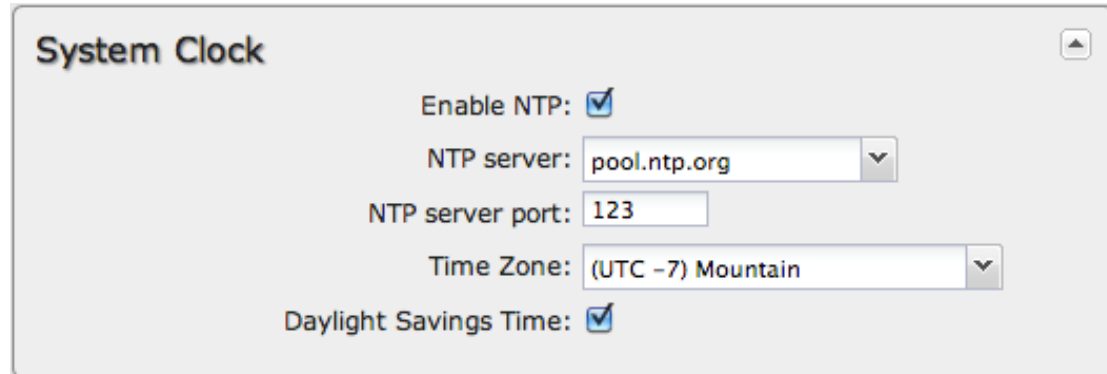
Shared Secret



The image shows a screenshot of the "RADIUS Settings" configuration page. At the top, there is a "Server Timeout" slider set to 3 seconds. Below this, there are two sections for configuring RADIUS servers. The first section, "Server 1", contains fields for "Server Address" (with the value "radius.someserver.com"), "Port" (with the value "1812"), "Shared Secret" (with a red dashed border), and "Confirm Secret" (empty). The second section, "Server 2 (optional)", contains similar fields: "Server Address" (with the value "radius.someserver.com"), "Port" (with the value "1812"), "Shared Secret" (empty), and "Confirm Secret" (empty).

8.1.2 System Clock

Enabling NTP will tell the router to get its system time from a remote server on the Internet. If you do not enable NTP then the router time will be based on when the router firmware was built, which is guaranteed to be wrong. Whenever the Internet connection is re-established and once a week thereafter the router will ask the server for the current time so it can correct itself.



The image shows a web-based configuration interface for the 'System Clock'. It includes a title bar 'System Clock' with a close button. The settings are as follows:

- Enable NTP:** A checked checkbox.
- NTP server:** A dropdown menu with 'pool.ntp.org' selected.
- NTP server port:** A text input field containing '123'.
- Time Zone:** A dropdown menu with '(UTC -7) Mountain' selected.
- Daylight Savings Time:** A checked checkbox.

You then have the option of selecting an NTP server and adjusting the NTP server port. Select the NTP server from the dropdown list. Any of the given NTP servers will be sufficient unless, for example, you need to synchronize your router's time with other devices in a network.

Time Zone: Select from a dropdown list. Setting your Time Zone is required to properly show time in your router log.

Daylight Savings Time: Select this checkbox if your location observes daylight saving time.

8.1.3 Local Management

Enable Internet Bounce Pages: Bounce pages show up in your web browser when the router is not connected to the Internet. They inform you that you are not connected and try to explain why. If you disable bounce pages then you will just get the usual browser timeout. In the normal case when the router is connected to the Internet you don't see them at all.

Reboot Count: Select this to track number of router reboots.

Enable Login Banner: Select this to add the CLI banner to the router's login page.

Local Domain: The local domain is used as the suffix for DNS entries of local hosts. This is tied to the hostnames of DHCP clients as DHCP_HOSTNAME.LOCAL_DOMAIN.

System Identifier: This is a customizable identity that will be used in router reporting and alerting. The default value is the MAC address of the router.

Set System Identifier: Select this to automatically set the system ID to the name of the first client that gets a DHCP lease. This feature cannot be used with email alerts, but alerts can be sent to ECM.

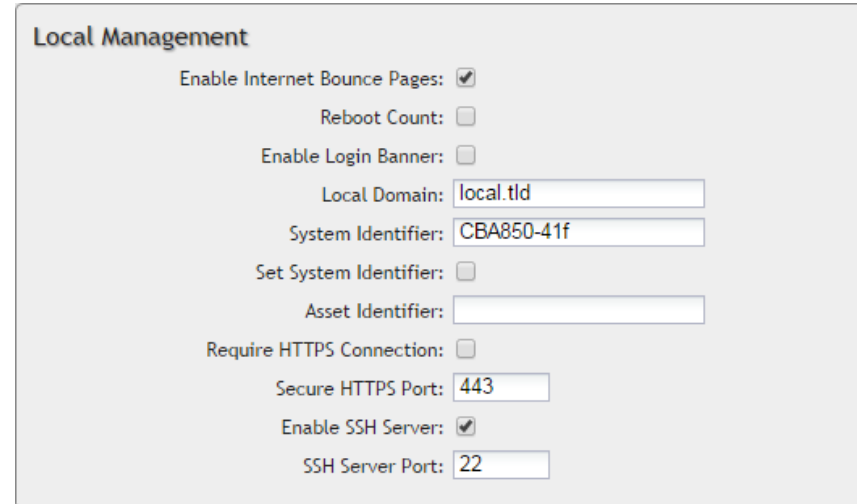
Asset Identifier: This is a customizable string that will be used in router reporting and alerting.

Require HTTPS Connection: Check this box if you want to encrypt all router administration communication.

Secure HTTPS Port: Enter the port number you want to use. The default is 443.

Enable SSH Server: When the router's SSH server is enabled you may access the router's command line interface (CLI) using the standards-based SSH protocol. Use the username "admin" and the standard system password to log in.

SSH Server Port: Default: 22.



The screenshot shows the 'Local Management' configuration page. It contains the following settings:

- Enable Internet Bounce Pages: ☒
- Reboot Count: ☐
- Enable Login Banner: ☐
- Local Domain:
- System Identifier:
- Set System Identifier: ☐
- Asset Identifier:
- Require HTTPS Connection: ☐
- Secure HTTPS Port:
- Enable SSH Server: ☒
- SSH Server Port:

8.1.4 Remote Management

Allows a user to enable incoming WAN pings or to change settings for the router from the Internet using the router's Internet address.

Allow WAN pings: When enabled the functionality allows an external WAN client to ping the router.

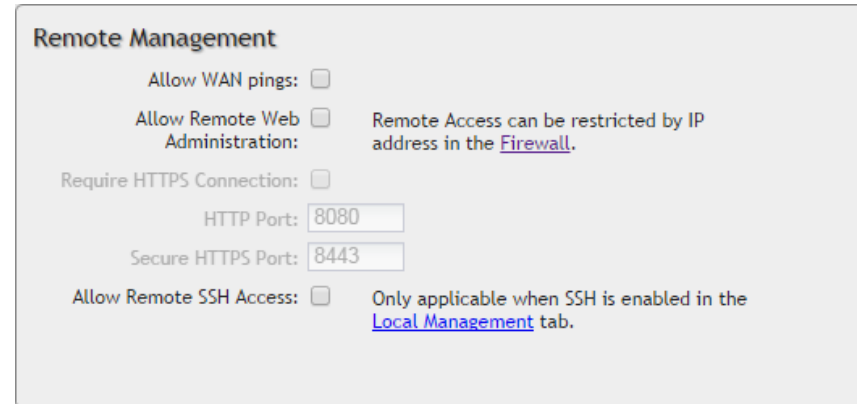
Allow Remote Web Administration: When remote administration is enabled it allows access to these administration web pages from the Internet. With it disabled, you must be a client on the local network to access the administration website. For security, remote access is usually done via a non-standard http port. Additionally, encrypted connections can be required for an added level of security.

- **Require HTTPS Connection:** Requiring a secure (**https**) connection is recommended
- **HTTP Port:** Default: 8080. This option is disabled if you select "Require Secure Connection"
- **Secure HTTPS Port:** Default: 8443

NOTE: You can restrict remote access to specified IP addresses in [Network Settings](#) → [Firewall](#) under Remote Administration Access Control.

Allow Remote SSH Access: This will enable SSH access to the router from the Internet. It is only available when the SSH access is enabled in the **Local Management** tab.

Some Carriers block the remote SSH Access ports. If a ping to the router's WAN port does not work, it is unlikely that remote SSH Access will work.



The screenshot shows the 'Remote Management' configuration page. It contains several settings with checkboxes and input fields. 'Allow WAN pings' is unchecked. 'Allow Remote Web Administration' is unchecked, with a note that remote access can be restricted by IP address in the 'Firewall' tab. 'Require HTTPS Connection' is unchecked. The 'HTTP Port' is set to 8080, and the 'Secure HTTPS Port' is set to 8443. 'Allow Remote SSH Access' is unchecked, with a note that it is only applicable when SSH is enabled in the 'Local Management' tab.

Remote Management	
Allow WAN pings:	☐
Allow Remote Web Administration:	☐ Remote Access can be restricted by IP address in the Firewall .
Require HTTPS Connection:	☐
HTTP Port:	8080
Secure HTTPS Port:	8443
Allow Remote SSH Access:	☐ Only applicable when SSH is enabled in the Local Management tab.

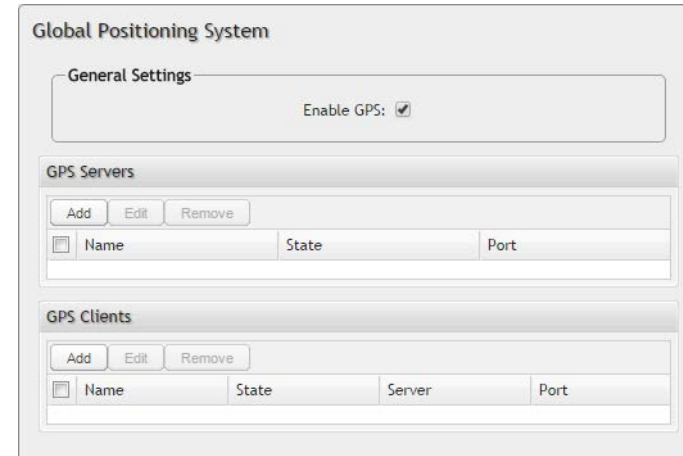
8.1.5 GPS

If you have an attached device with GPS support, you can enable a graphical view of your router's location which will appear in **Status → GPS**.

Users can also configure GPS NMEA GGA format sentence reporting, available through a router-based server and/or a remote server.

NOTE: Some carriers disable GPS support in otherwise supported modems. If you encounter issues with obtaining a fix, contact your carrier and ensure that GPS is supported.

- **Enable GPS:** Enables support for querying GPS information from supported modems. To add a GPS Server or Client, click "Add."
- **Enable this Server:** Select to enable specified server.
- **Server Name:** Specify server name.
- **Enable GPS server on LAN:** Enables a TCP server on the LAN side of the firewall, which will periodically send GPS NMEA sentences to connected clients.
- **Enable GPS server on WAN:** Enables a TCP server on the WAN side of the firewall, which will periodically send GPS NMEA sentences to connected clients.
- **Port:** Specify desired port.



Global Positioning System

General Settings

Enable GPS: ☒

GPS Servers

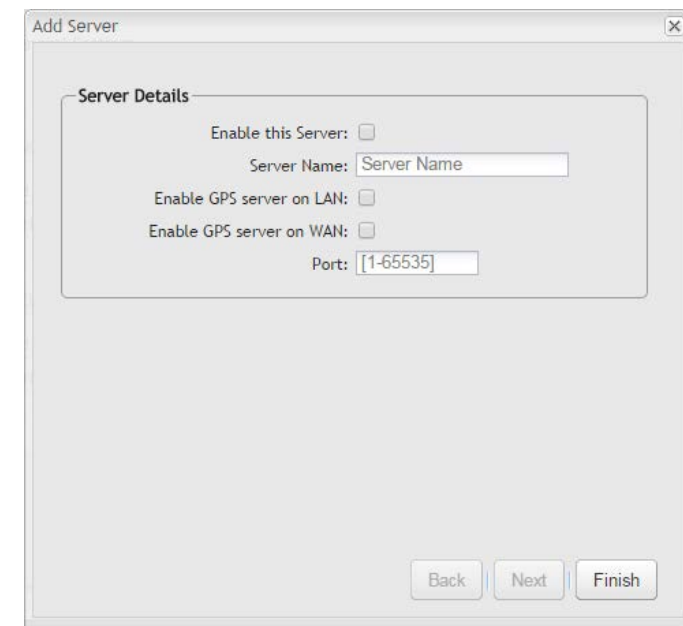
Add Edit Remove

☐	Name	State	Port
☐			

GPS Clients

Add Edit Remove

☐	Name	State	Server	Port
☐				



Add Server

Server Details

Enable this Server: ☐

Server Name:

Enable GPS server on LAN: ☐

Enable GPS server on WAN: ☐

Port:

Back Next Finish

\$GPGGA – Essential fix data including 3D location and accuracy information

Example: \$GPGGA,1753405,4916.450,N,12311.127,W,2,06,1.5,117.3,M,-26.574,M,6.0,0138*47

1753405	Time of fix – 17:34:05 UTC
4916.450,N	Latitude 49 deg. 16.450 min North
12311.127,W	Longitude 123 deg. 11.127 min West
2	Fix quality: • 0 = fix not available • 1 = GPS fix • 2 = Differential GPS fix • 3 = PPS fix • 4 = Real Time Kinematic • 5 = Float RTK • 6 = estimated (dead reckoning) • 7 = Manual input mode • 8 = Simulation mode
06	Number of satellites being tracked
1.5	Horizontal dilution of precision (HDOP) – relative accuracy of horizontal position
117.312,M	Altitude in meters above mean sea level
-26.574,M	Geoidal separation: height of mean sea level above WGS-84 earth ellipsoid (negative value means mean sea level is below ellipsoid)
6.0	Time in seconds since last update from differential reference stations
0138	Differential reference station ID number
*47	Checksum – used by program to check for transmission errors

8.1.6 SMS

SMS (Short Message Service, or text messaging) requires a cellular modem with an active data plan. SMS is not designed to be a full remote management feature: SMS allows you to connect to the router for a few simple queries or commands with a text messaging service (e.g., from your phone). A modem that does not have an active data connection may still be reachable by SMS because Internet traffic and SMS traffic operate on separate channels, so SMS can be used to bring an offline router back online.

SMS is enabled on the router by default. However, it only works if SMS is supported and enabled on the modem. Most modems have SMS enabled by default, but the carrier may charge a fee for each text message sent or received. Contact your carrier to review these fees and/or to enable an SMS plan.

Important notes about SMS:

- Messages are limited to 160 characters.
- SMS is not a guaranteed delivery protocol. The carriers do not guarantee that the SMS message will be delivered to the modem or that the modem's response will be delivered to the sender. This means an administrator might have to send messages multiple times before the desired action is performed.
- SMS is a slow protocol. It can take seconds or up to a few minutes for messages to be delivered.
- SMS messages are not encrypted; they are sent in full readable text over the network.

Enable SMS support

SMS support is enabled by default on the router. Deselect this to disable.

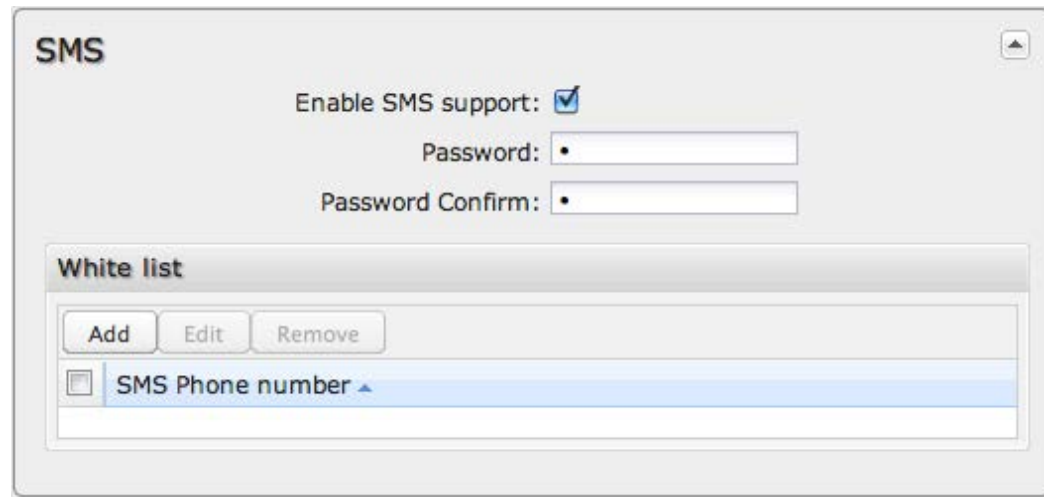
Password

By default, the password is the last eight characters of the router's MAC address (i.e., the Default Password on the product label). You can change this password to anything between 1 and 16 characters. It should be long enough to be useful for security but short enough to easily type into your phone (or other texting client).

White List

This list is blank by default, which means that the router will accept SMS messages from any phone number. Leaving this blank is unsecure, so Cradlepoint recommends that you add phone numbers to this list. Once any numbers are listed, only those numbers have the ability to connect to the router via SMS.

NOTE: You cannot add email addresses to the White list. When a phone number is added to the White List, email SMS messages will be rejected.



The screenshot shows the 'SMS' configuration window. At the top, 'Enable SMS support:' is checked. Below it are 'Password:' and 'Password Confirm:' fields, each with a bullet point icon. A 'White list' section contains 'Add', 'Edit', and 'Remove' buttons. Below these buttons is a table with one row: a checkbox, the text 'SMS Phone number', and a small upward arrow icon. The table has a light blue header and a white body.

HOW TO SEND AN SMS MESSAGE

You can send SMS messages to the router via phone or email. The key elements are:

1. the modem's MDN
2. the SMS password (defined above)
3. the command

You must know the MDN (Mobile Directory Number) of the modem to send SMS messages to the router. This is a phone number that can be found under **Status → Internet Connections** in the router administration pages (or under **Devices → Network Interfaces** in Enterprise Cloud Manager).

How to Text from a Phone

1. Open the text messaging tool on your phone and start a new message.
2. In the **To** field, enter the modem's MDN.
3. In the **Subject** field, enter the SMS password and command.
4. Click **Send**.

How to Text from an Email

NOTE: There are limitations with sending texts via email. The SMS engine is currently only compatible with GSM-based carrier operators.

1. Start a new email message.
2. In the **To** field, enter the modem's MDN *plus* the modem's carrier domain name (e.g., 2085555555@txt.att.net).
3. Enter the password and command in *either* the **Subject** field or **Body** of the email message. If you use the subject field, leave the body blank, and if you use the body, leave the subject blank.

NOTE: The subject field may be limited to a certain number of characters, so if you get an error when sending the command on the subject line, switch to using the body instead.)

SMS Commands

Below is a list of supported SMS messages and the syntax format.

Due to security concerns, the set of commands are intentionally limited to those that can configure a modem's connection, but cannot lock the administrator out due to malicious modem changes. Therefore, if an unsolicited request adjusts the modem's configuration via SMS, an administrator can still access the modem via SMS.

Command syntax: <password>,<command>,[arg1,][arg2,]

All commands start with the password – either the default of the last 8 digits of the router's MAC address or the administrator-configured password. Commands can have an optional number of arguments.

NOTE: The trailing comma on the command is important to allow the SMS engine to distinguish the final argument from other information the SMS client might append to the message without your knowledge.

SUPPORTED COMMANDS:

reboot: Reboot the router (not the modem)

- Syntax: <password>,reboot,
- Example: 1234,reboot,

restore: Restore the router to factory defaults

- Syntax: <password>,restore,
- Example: 1234,restore,

rstatus: Get router status

- Syntax: <password>,rstatus,
- Example: 1234,rstatus,

This command returns info about the router along with the port names for ports with attached modems. These port names may be helpful for using the commands that follow.

Example of response:

```
uptime: 0:35:13
FW: v4.4.0
eth0: 10/100/1000 Ethernet Switch: connected
usb3: MC200P: connected
```

mstatus: Get modem status*

- Syntax: <password>,mstatus,[port,]
- Example: 1234,mstatus, //return status of highest priority modem
- Example: 1234,mstatus,usb1, //return status of modem plugged into port usb1

This command returns info about the indicated modem's status. The resulting data reflects the modem model number, service type, and connection status and values.

Example of response:

```
Model: MC200P
Service: HSPA+
SIM Status: READY
RSSI: -62 dbm
ECIO: -4
APN: wwan.ccs
IP Addr: 166.136.142.172
```

mreboot: Reboot the modem*

- Syntax: <password>,mreboot,[port,]
- Example: 1234,mreboot, //This will reboot the highest priority modem.
- Example: 1234,mreboot,usb1, //This will reboot the modem on port usb1

apn: Set the APN on the modem (for SIM-based modems)*

- Syntax: <password>,apn,<new APN>,[port,]
- Example: 1234,apn,[myapn@apn.com](#), //set APN of highest priority modem

- Example: 1234,apn,[myapn@apn.com](#),usb1, //set APN for modem in port usb1

userpass: Set the modem's authentication username and password*

- Syntax: <password>,userpass,<username>,<userpassword>,[port,]
- Example: 1234,userpass,joe,mypassword, //set information of highest priority modem
- Example: 1234,userpass,joe,mypassword,usb3, //set information on modem in port usb3

simpin: Set the SIM's PIN*

- Syntax: <password>,simpin,<pin>,[port,]
- Example: 1234,simpin,5678, //set simpin in highest priority modem
- Example: 1234,simpin,5678,usb2 //set simpin in modem on port usb2

log: Return a portion of the router log

- Syntax: <password>,log,[start,]
- Example: 1234,log, //return the first 10 items of the log (items 0 through 9)
- Example: 1234,log,10, //return items 10 through 19 of the log
- Example: 1234,log,20, //return items 20 through 29 of the log

Sending log information via SMS messages likely results in several resulting texts. Please be aware of the costs of text messages on the modem's account, and use this command only if necessary.

* The "port" parameter is optional. It specifies which port to perform the action on. If not given, the action will happen on the highest priority modem.

Sample Debug Session

The following is an example of a debug session to discover a modem's APN is misconfigured and needs to be set.

Figure out the state of the modems on the router:

1234,rstatus,

Receive the modem's status and settings:

1234,mstatus,

Set the modem's APN to the correct setting:

1234,apn,broadband,

Verify the APN was set properly:

1234,mstatus,

Continue to verify the status periodically to ensure that the modem connects:

1234,rstatus,

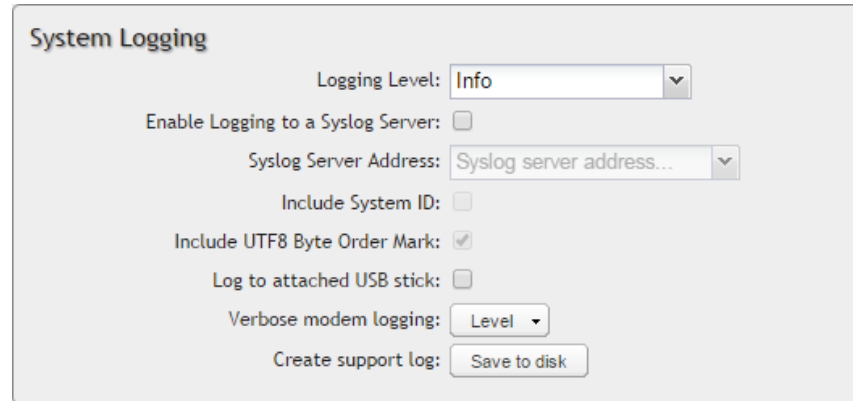
8.1.7 LLDP

Select to enable Link Layer Discovery Protocol.

8.1.8 System Logging

Logging Level: Setting the log level controls which messages are stored or filtered out. A log level of **Debug** will record the most information while a log level of **Critical** will only record the most urgent messages. Each level includes all messages from all of the levels below it on the list (e.g. “Warning” includes all “Error” and “Critical” messages as well).

- **Debug**
- **Info**
- **Warning**
- **Error**
- **Critical**



The image shows a screenshot of the 'System Logging' configuration page. It includes the following settings:

- Logging Level:** A dropdown menu currently set to 'Info'.
- Enable Logging to a Syslog Server:** An unchecked checkbox.
- Syslog Server Address:** A dropdown menu showing 'Syslog server address...'.
- Include System ID:** An unchecked checkbox.
- Include UTF8 Byte Order Mark:** A checked checkbox.
- Log to attached USB stick:** An unchecked checkbox.
- Verbose modem logging:** A dropdown menu set to 'Level'.
- Create support log:** A button labeled 'Save to disk'.

Enable Logging to a Syslog Server: Enabling this option will send log messages to a specified Syslog server. After enabling, type the Hostname or IP address of the Syslog server (or select from the dropdown menu).

Syslog Server Address: Select the Hostname or IP address from the dropdown menu, or type this in manually.

Include System ID: This option will include the router’s “System ID” at the beginning of every log message. This is often useful when a single remote Syslog server is handling logs for several routers.

Include UTF8 Byte Order Mark: The log message is sent using UTF-8 encoding. By default the router will attach the Unicode Byte Order Mark (BOM) to the Syslog message in compliance with the Syslog protocol, RFC5424. Some Syslog servers may not fully support RFC5424 and will treat the BOM as ASCII text, which will appear as garbled characters in the log. If this occurs, disable this option.

Log to attached USB stick: Only enable this option if instructed by a Cradlepoint support agent. This will write a very verbose log file to the root level of an attached USB stick. Please disable the feature before removing the USB stick, or you may lose some logging data.

Verbose modem logging: Only enable this option if instructed by a Cradlepoint support agent.

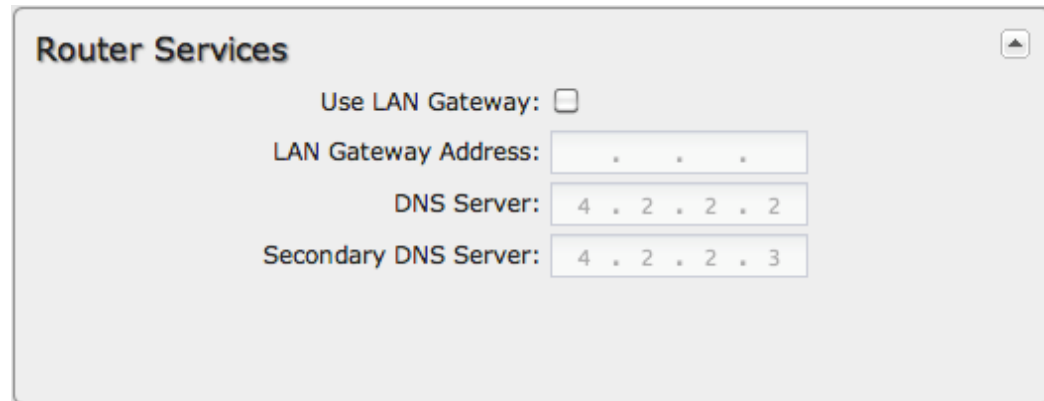
Create support log: This functionality allows for a quick collection of system logging. Create this log file when instructed by a Cradlepoint support agent.

8.1.9 Router Services

By default, router services (Enterprise Cloud Manager, NTP, etc.) connect to the router via the WAN. In some setups it makes sense to use the LAN instead. For example, if your router is used strictly for 3G/4G failover behind another router, you may not want to use 3G/4G data unnecessarily. Select **Use LAN Gateway** to set your router services to connect via the LAN.

LAN Gateway Address: Input the IP address of the LAN side connection. If this is a 3G/4G failover router operating behind another router, the **LAN Gateway Address** is the IP address of that other router.

DNS Server and **Secondary DNS Server:** The primary and secondary DNS server numbers match the static DNS values (set at **Network Settings** → **DNS**). You can leave the default values or set them manually here. (Changing these values also changes the static DNS values.)



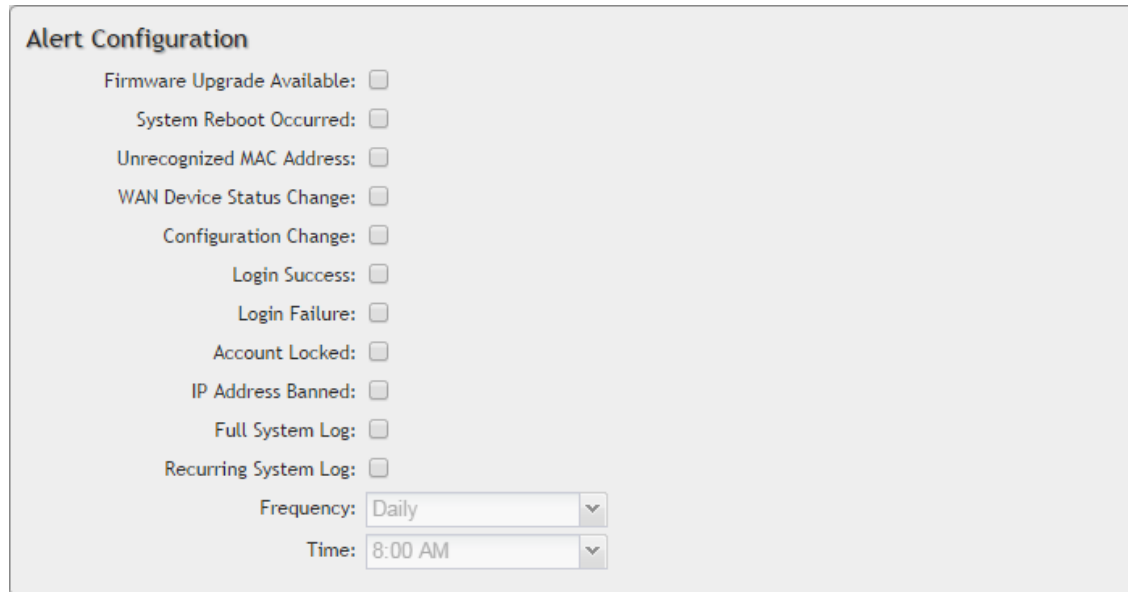
The image shows a screenshot of the 'Router Services' configuration window. It has a title bar with the text 'Router Services' and a close button. Inside the window, there are four settings:

- Use LAN Gateway:** A checkbox that is currently unchecked.
- LAN Gateway Address:** A text input field with three dots, indicating a placeholder for an IP address.
- DNS Server:** A text input field containing the value '4 . 2 . 2 . 2'.
- Secondary DNS Server:** A text input field containing the value '4 . 2 . 2 . 3'.

8.2 Device Alerts

The Device Alerts submenu choice allows you to receive email notifications of specific system events. **YOU MUST ENABLE AN SMTP EMAIL SERVER TO RECEIVE ALERTS.** Alerts can be included for the following:

- **Firmware Upgrade Available:** A firmware update is available for this device.
- **System Reboot Occurred:** This router has rebooted. This depends on NTP being enabled and available to report the correct time.
- **Unrecognized MAC Address:** Used with the MAC monitoring lists. An alert is sent when a new unrecognized MAC address is connected to the router.
- **WAN Device Status Change:** An attached WAN device has changed status. The possible statuses are plugged, unplugged, connected, and disconnected.
- **Configuration Change:** A change to the router configuration.
- **Login Success:** A successful login attempt has been detected.
- **Login Failure:** A failed login attempt has been detected.
- **Account Locked:** The account has been locked due to too many failed login attempts.
- **IP Address Banned:** The IP address has been blocked due to too many failed login attempts.
- **Full System Log:** The system log has filled. This alert contains the contents of the system log.
- **Recurring System Log:** The system log is sent periodically. This alert contains all of the system events since the last recurring alert. It can be scheduled for daily, weekly and monthly reports. You also choose the time you want the Alert sent.



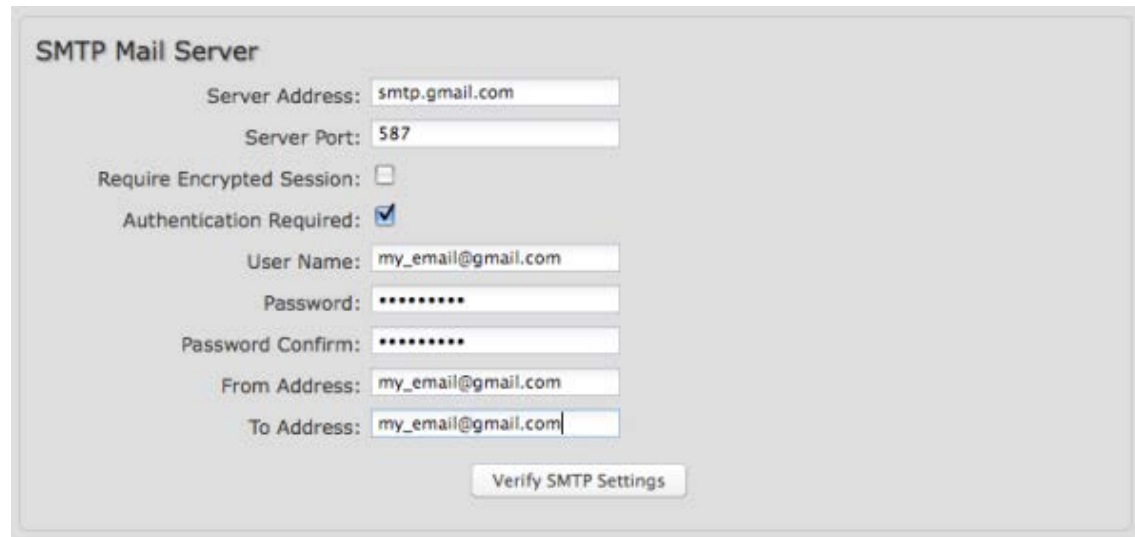
The screenshot shows the 'Alert Configuration' interface. It contains a list of alert types, each with an unchecked checkbox: Firmware Upgrade Available, System Reboot Occurred, Unrecognized MAC Address, WAN Device Status Change, Configuration Change, Login Success, Login Failure, Account Locked, IP Address Banned, Full System Log, and Recurring System Log. Below these checkboxes, there are two dropdown menus: 'Frequency' set to 'Daily' and 'Time' set to '8:00 AM'.

8.2.1 SMTP Mail Server

Since the CBA850 does not have its own email server, to receive alerts you must enable an SMTP server. This is possible through most email services (Gmail, Yahoo, etc.)

Each SMTP server will have different specifications for setup, so you have to look those up separately. The following is an example using Gmail:

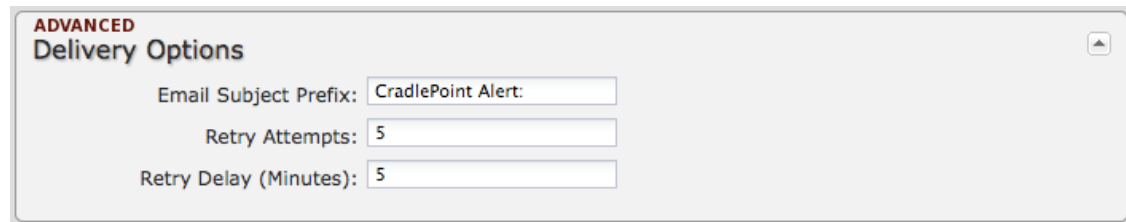
- **Server Address:** smtp.gmail.com
- **Server Port:** 587 (for TLS, or Transport Layer Security port; the CBA850 does not support SSL).
- **Authentication Required:** For Gmail, mark this checkbox.
- **User Name:** Your full email address
- **Password:** Your Gmail password
- **From Address:** Your email address
- **To Address:** Your email address



Once you have filled in the information for the SMTP server, click on the “Verify SMTP Settings” button. You should receive a test email at your account.

Advanced: Delivery Options

Email Subject Prefix: This optional string is prefixed to the alert subject. It can be customized to help you identify alerts from specific routers.





Retry Attempts: The number of attempts made to send an alert to the mail server. After the attempts are exhausted, the alert is discarded.

Retry Delay: The delay between retry attempts.

8.3 Enterprise Cloud Manager

Cradlepoint ECM is a cloud-based management service for configuring, monitoring, and organizing your Cradlepoint routers.

Key features include:

- Group based configuration management
- Health monitoring of router connectivity and data usage
- Remote management and control of routers
- Historical record keeping of device logs and status

Visit <http://Cradlepoint.com/ecm> to learn more about Cradlepoint ECM.

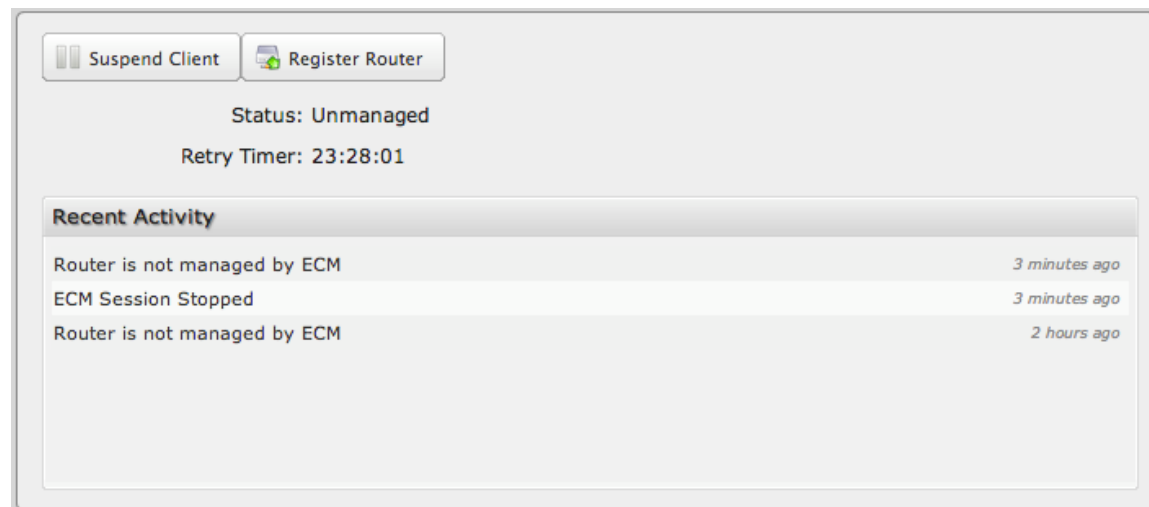
If you do not have ECM credentials, sign up at: <http://www.Cradlepoint.com/ecm-signup>.

REGISTERING YOUR ROUTER

Once you have signed up for ECM, click on the **Register Router** button to begin managing the router through ECM. Input your **ECM Username** and **ECM Password** and click **Register**. You have now registered the device with Enterprise Cloud Manager.

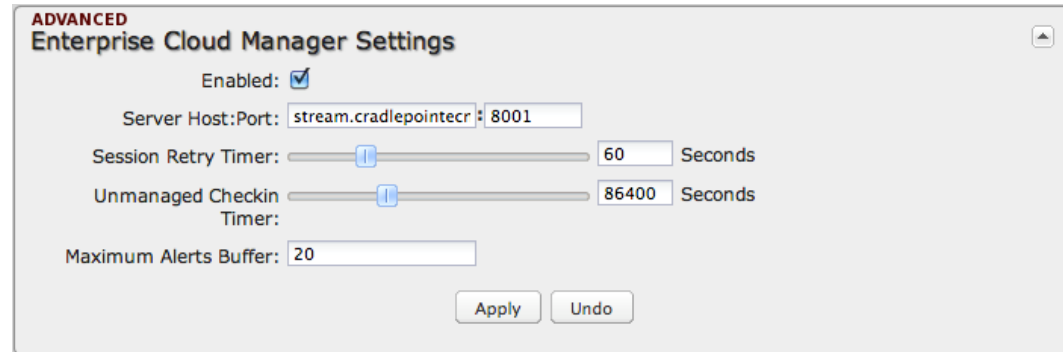
SUSPENDING THE ECM CLIENT

Click on the **Suspend Client** button to stop communication between the device and ECM. Suspending the client will make it stop any current activity and go dormant. It will not attempt to contact the server while suspended. This is a temporary setting that will not survive a router reboot; to disable the client altogether use the Advanced Enterprise Cloud Manager Settings panel (below).



8.3.1 Enterprise Cloud Manager Settings (Advanced)

- **Enabled:** Enable the ECM client to contact the server. While this box is unchecked, the ECM client will never attempt to contact the server. (Default: Enabled)
- **Server Host:Port:** The DNS hostname and port number for your ECM server. (Default: stream.Cradlepoint.com)
- **Session Retry Timer:** How long to wait, in seconds, before starting a new ECM session following a connection drop or connectivity failure. Note that this value is a starting point for an internal backoff timer that prevents superfluous retries during connectivity loss.
- **Unmanaged Checkin Timer:** How often, in seconds, the router checks with ECM to see if the router is remotely activated. Note that this value is a starting point for an internal backoff timer that reduces network usage over time.
- **Maximum Alerts Buffer:** The maximum number of alerts to buffer when offline.



ADVANCED Enterprise Cloud Manager Settings

Enabled: ☒

Server Host:Port: stream.cradlepointecr : 8001

Session Retry Timer: 60 Seconds

Unmanaged Checkin Timer: 86400 Seconds

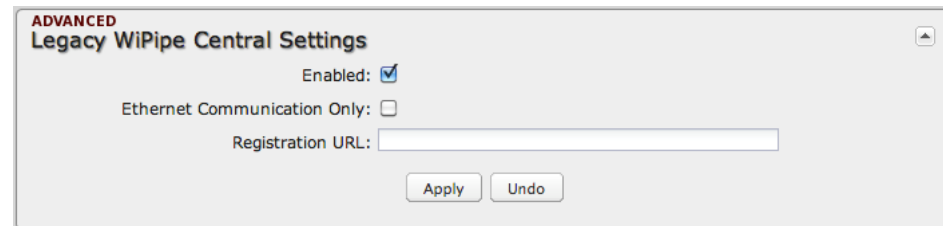
Maximum Alerts Buffer: 20

Apply Undo

8.3.2 Legacy WiPipe Central Settings (Advanced)

WiPipe Central is Cradlepoint's legacy remote management system.

- **Enabled:** Enables the WiPipe Central client to contact the server.
- **Ethernet Communication Only:** Select this to ensure that the WiPipe Central client will not start unless the WAN is Ethernet.
- **Registration URL:** Register your router using the code provided by Cradlepoint when you purchase WiPipe Central.



ADVANCED Legacy WiPipe Central Settings

Enabled: ☒

Ethernet Communication Only: ☐

Registration URL:

Apply Undo

8.4 Serial Redirector

A single USB Serial device can be used to establish a serial link to a host port on the router. The USB Serial device can also be accessed by running "serial" from an SSH session.

8.4.1 Telnet to Serial Configuration

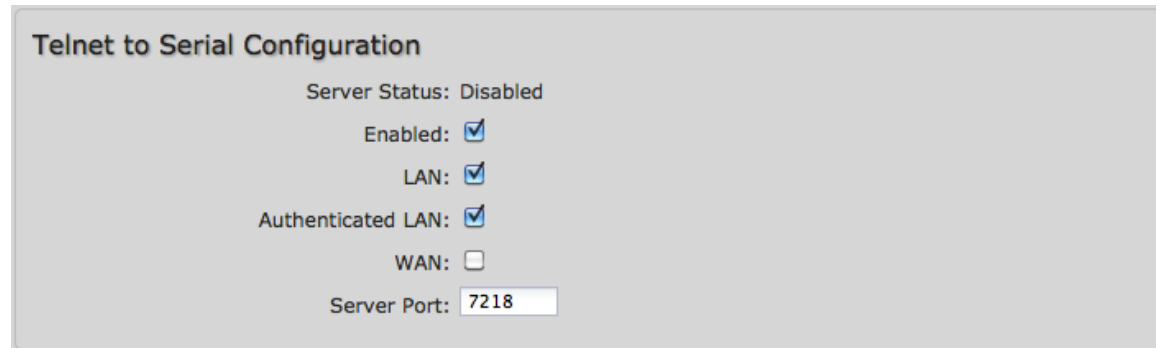
Enabled: Enabling Telnet to Serial will start a Telnet server that passes its connection to the serial adapter. Enabling this service is not necessary when accessing serial through SSH.

LAN: Enable serial redirector for LAN connections.

Authenticated LAN: Enable serial redirector for Authenticated LAN connections. You must be logged into the router to use the redirector.

WAN: Enable serial redirector for WAN connections.

Server Port: Enter a port number for the redirector to use. (Default: 7218)



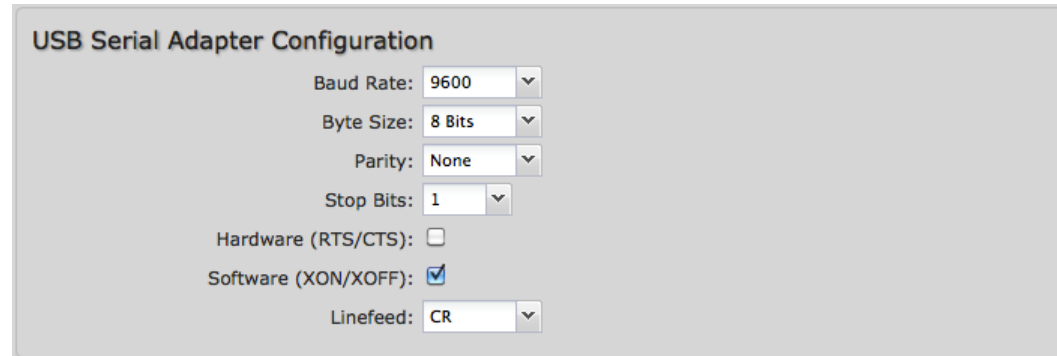
The screenshot shows the 'Telnet to Serial Configuration' page. It has a title 'Telnet to Serial Configuration' at the top. Below the title, the 'Server Status' is 'Disabled'. There are four checkboxes: 'Enabled' (checked), 'LAN' (checked), 'Authenticated LAN' (checked), and 'WAN' (unchecked). At the bottom, there is a 'Server Port' field with the value '7218' entered.

Configuration Option	Status
Server Status	Disabled
Enabled	☒
LAN	☒
Authenticated LAN	☒
WAN	☐
Server Port	7218

8.4.2 USB Serial Adapter Configuration

Baud Rate: Select from the dropdown list.

- 50
- 75
- 110
- 134
- 150
- 200
- 300
- 600
- 1200
- 1800
- 2400
- 4800
- 9600
- 19200



USB Serial Adapter Configuration

Baud Rate: 9600

Byte Size: 8 Bits

Parity: None

Stop Bits: 1

Hardware (RTS/CTS): ☐

Software (XON/XOFF): ☒

Linefeed: CR

Byte Size: The number of bits in a byte. Select from: 5, 6, 7, and 8.

Parity: Change this value to enable parity bit checking. Select from the following dropdown options:

- None: No parity checking (Default)
- Even: parity bit will always be even
- Odd: parity bit will always be odd
- Mark: parity bit will always be odd and always 1
- Space: parity bit will always be even and always 0

Stop Bits: Number of bits to initiate the stop period. Select from these dropdown values: 1, 1.5, and 2.

Hardware (RTS/CTS): Use RTS (Request To Send)/CTS (Clear To Send) to enable flow control.

Software (XON/XOFF): Use XON/XOFF to enable flow control.



Linefeed: Select how you want linefeeds translated (CR = carriage return and LF = line feed).

- Ignore
- CR/LF
- CR
- LF

8.5 SNMP Configuration

SNMP, or Simple Network Management Protocol, is an Internet standard protocol for remote management. You might use this instead of Cradlepoint Enterprise Cloud Manager if you want to remotely manage a set of routers that include both Cradlepoint and non-Cradlepoint products.

Enable SNMP: Selecting “Enable SNMP” will reveal the router’s SNMP configuration options.

Enable SNMP on LAN: Enabling SNMP on LAN will make SNMP services available on the LAN networks provided by this router. SNMP will not be available on guest or virtual networks that do not have administrative access.

LAN port #: Use the LAN port # field to configure the LAN port number you wish to access SNMP services on. (Default: 161)

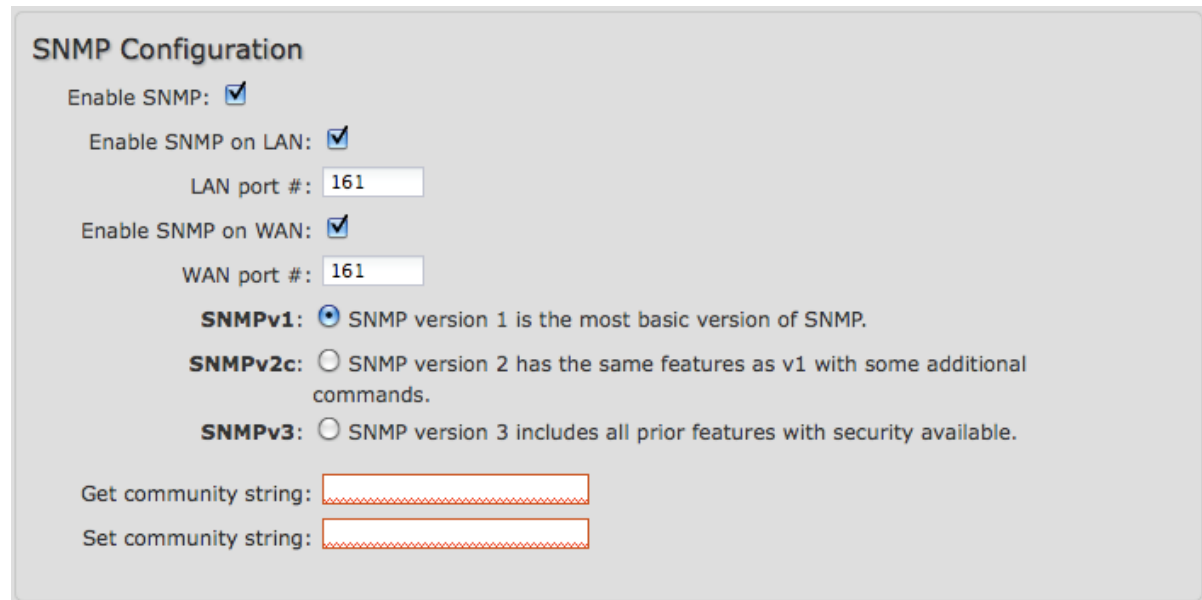
Enable SNMP on WAN: Enabling SNMP on WAN will make SNMP services available to the WAN interfaces of the router.

WAN port #: Use the WAN port # field to configure which publicly accessible port you wish to make SNMP services available on. (Default: 161)

SNMPv1: SNMP version 1 is the most basic version of SNMP. SNMPv1 will configure the router to transmit with settings compatible with SNMP version 1 protocols.

SNMPv2c: SNMP version 2c has the same features as v1 with some additional commands. SNMPv2c will configure the router to use settings and data formatting compatible with SNMP version 2c.

SNMPv3: SNMP version 3 includes all prior features with security available. SNMPv3 is the most secure setting for SNMP. If you wish to configure traps then you must use SNMP version 3.



The screenshot shows the 'SNMP Configuration' web interface. It includes checkboxes for 'Enable SNMP', 'Enable SNMP on LAN', and 'Enable SNMP on WAN', all of which are checked. Below these are input fields for 'LAN port #' and 'WAN port #', both set to '161'. There are three radio button options for SNMP versions: 'SNMPv1' (selected), 'SNMPv2c', and 'SNMPv3'. Each option has a descriptive text line. At the bottom, there are two empty text input fields labeled 'Get community string:' and 'Set community string:'.

Get community string: The “Get community string” is used to read SNMP information from the router. This string is like a password that is transmitted in regular text with no protection.

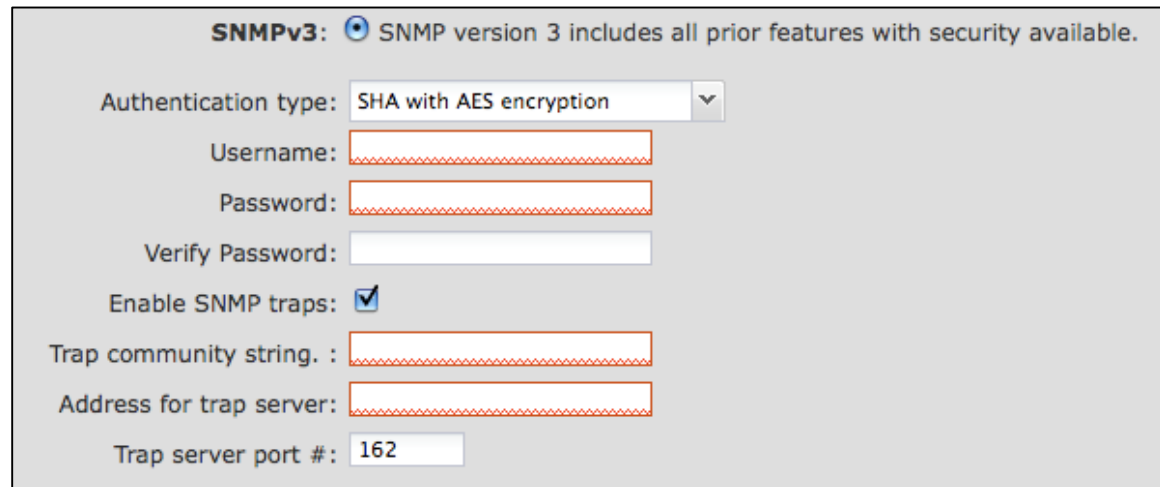
Set community string: The “Set community string” is used when writing SNMP settings to the router. This string is like a password. It is a good idea to make it different than the “Get community string.”

8.5.1 SNMPv3

If you select SNMPv3, you have several additional configuration options for added security.

Authentication type: Select the authentication and encryption type that will be used when connecting to the router from the following dropdown list. These settings must match the configuration used on any SNMP clients.

- MD5 with no encryption
- SHA with no encryption
- MD5 with DES encryption
- SHA with DES encryption
- MD5 with AES encryption
- SHA with AES encryption



SNMPv3:  SNMP version 3 includes all prior features with security available.

Authentication type: SHA with AES encryption ▼

Username:

Password:

Verify Password:

Enable SNMP traps: ☒

Trap community string:

Address for trap server:

Trap server port #:

Username: Enter the Username configured on your SNMP host in the username field.

Password: Enter the Password for your SNMP host in the password and verify password fields. This password must be at least eight characters long.

Enable SNMP traps: Enabling traps will allow you to configure a destination server, community, and port for trap notifications. Trap notifications are returned to the server with SNMPv1.



Trap community string: The trap notifications will be returned to the trap server using this SNMPv1 trap community name.

Address for trap server: Enter the address of the host system that you want trap alerts sent to.

Trap server port #: Enter the port number that the remote host will be listening for trap alerts on. (Default: 162)

8.5.2 System Information

System information via SNMP is Read-Writable by default. However, if a value is set here, that field will become Read-Only.

System Contact: Input the email address of the system administrator.

System Name: Input the router's hostname.

System Location: Input the physical location of the router. This is simply a string for your own information.

8.6 System Control

8.6.1 Device Control

Restore to Factory Defaults: This changes all settings back to their default values.

Reboot The Device: This causes the router to restart.

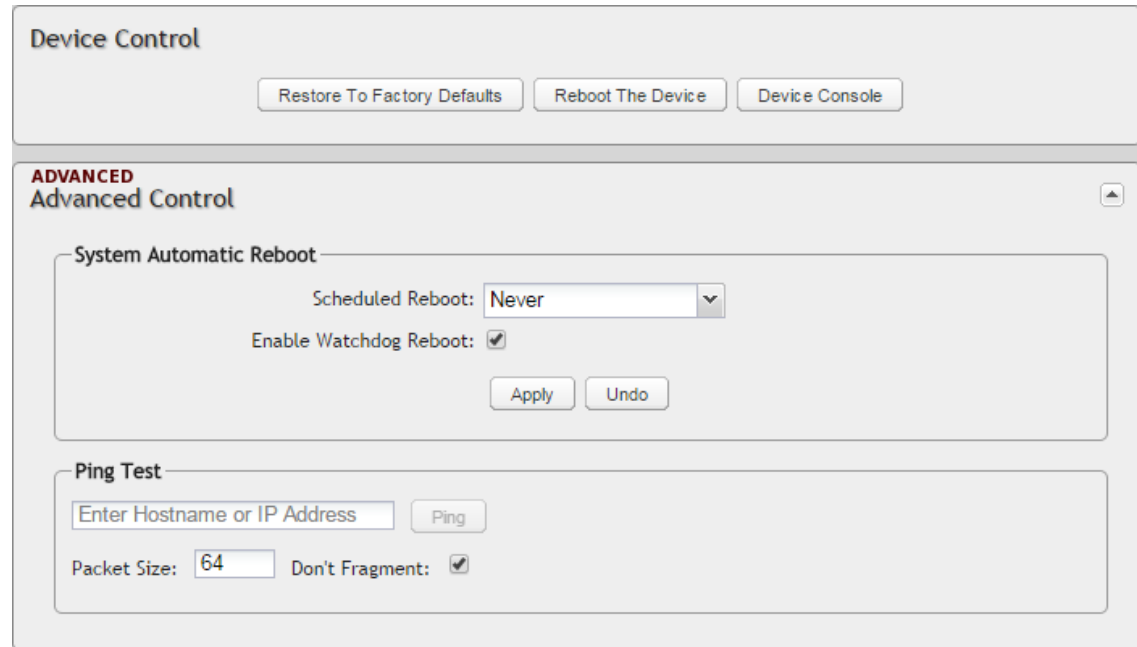
Device Console: Launches the device console.

8.6.2 Advanced Control

Scheduled Reboot: This causes the router to restart at a user-determined time.

Enable Watchdog Reboot: This causes the router to automatically restart when it determines an unrecoverable error condition has occurred.

Ping Test: A simple test to check Internet connectivity. Type the Hostname or IP address of the computer you want to ping and press 'Enter' or click the 'Ping' button.

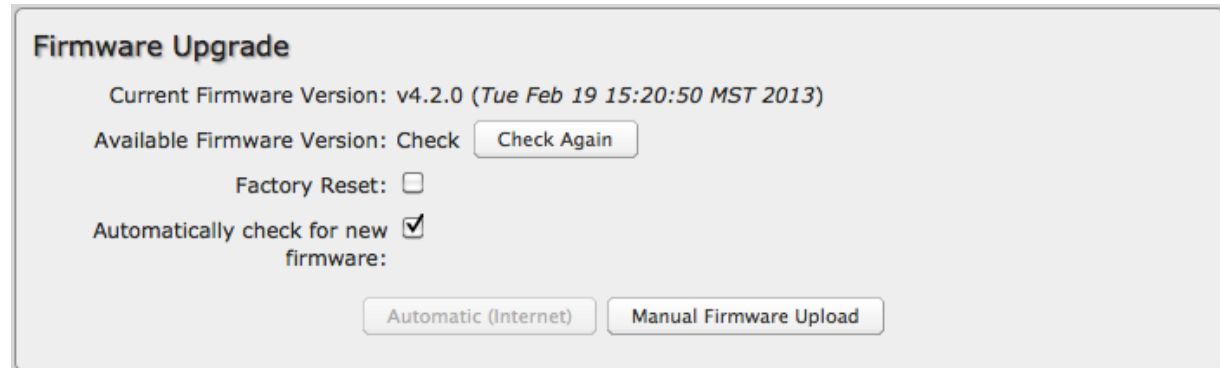


The screenshot shows the 'Device Control' section with three buttons: 'Restore To Factory Defaults', 'Reboot The Device', and 'Device Console'. Below this is the 'ADVANCED Advanced Control' section, which is expandable. It contains two sub-sections: 'System Automatic Reboot' and 'Ping Test'. In the 'System Automatic Reboot' section, 'Scheduled Reboot' is set to 'Never' and 'Enable Watchdog Reboot' is checked. In the 'Ping Test' section, there is a text input field for 'Enter Hostname or IP Address', a 'Ping' button, 'Packet Size' set to 64, and 'Don't Fragment' checked.

8.7 System Software

8.7.1 Firmware Upgrade

This allows the administrator to load new firmware onto the router to add new features or fix defects. If you are happy with the operation of the router, you may not want to upgrade just because a new version is available. Check the firmware release notes (www.Cradlepoint.com/firmware) for information to decide if you should upgrade.



The screenshot shows a 'Firmware Upgrade' panel. It displays the 'Current Firmware Version' as v4.2.0, updated on Tue Feb 19 15:20:50 MST 2013. Below this, there is a section for 'Available Firmware Version' with a 'Check' button and a 'Check Again' button. A 'Factory Reset' checkbox is present and unchecked. An 'Automatically check for new firmware' checkbox is checked. At the bottom, there are two buttons: 'Automatic (Internet)' and 'Manual Firmware Upload'.

Current Firmware Version: Shows the number of the current firmware and the date it was updated.

Available Firmware Version: If there is a new firmware version available, this will list the version number. Click “Check Again” to have the router check the newest firmware.

Factory Reset: Set default settings to match the new firmware. This is safest, as settings may have changed. You should back up your current settings and restore them after the new firmware is loaded.

Automatically check for new firmware: Check for an available firmware update once a day.

Automatic (Internet): Have the router download the file and perform the upgrade with no user interaction.

Manual Firmware Upload: Upload the router firmware from an attached computer. (Go to www.Cradlepoint.com/firmware to download the firmware.)

8.7.2 System Config Save/Restore

Backup Current Settings: Click on “Save to disk” to save your current settings to a file on a computer.

Restore Settings: Click on “Upload from file” to restore your previous settings from a file on a computer.

System Config Save/Restore
Backup Current Settings:
Restore Settings:

8.7.3 Firmware Upgrade and System Config Restore

Load new firmware and restore your previous settings from a file on a computer without rebooting between steps.

Firmware Upgrade and System Config Restore
Select Files:

9 GLOSSARY

802.11

A family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).

Access Control List

ACL. This is a database of network devices that are allowed to access resources on the network.

Access Point

AP. Device that allows wireless clients to connect to it and access the network.

ActiveX

A Microsoft specification for the interaction of software components.

Ad-hoc network

Peer-to-Peer network between wireless clients.

Address Resolution Protocol

ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

ADSL

Asymmetric Digital Subscriber Line.

Advanced Encryption Standard

AES. Government encryption standard.

Alphanumeric

Characters A-Z and 0-9.

Antenna

Used to transmit and receive RF signals.

AppleTalk

A set of Local Area Network protocols developed by Apple for their computer systems.

AppleTalk Address Resolution Protocol

AARP: Used to map the MAC addresses of Apple computers to their AppleTalk network addresses, so that conversions can be made in both directions.

Application layer

7th Layer of the OSI model. Provides services to applications to ensure that they can communicate properly with other applications on a network.

ASCII

American Standard Code for Information Interchange. This system of characters is most commonly used for text files.

Attenuation

The loss in strength of digital and analog signals. The loss is greater when the signal is being transmitted over long distances.

Authentication

To provide credentials, like a Password, in order to verify that the person or device is really who they are claiming to be.



Automatic Private IP Addressing

APIPA. An IP address that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network.

Backward Compatible

The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability.

Bandwidth

The maximum amount of bytes or bits per second that can be transmitted to and from a network device.

Basic Input/Output System

BIOS. A program that the processor of a computer uses to startup the system once it is turned on.

Baud

Data transmission speed.

Bit rate

The amount of bits that pass in given amount of time.

Bit/sec

Bits per second.

BOOTP

Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention.

Bottleneck

A time during processes when something causes the process to slow down or stop altogether.

Broadband

A wide band of frequencies available for transmitting data.

Broadcast

Transmitting data in all directions at once.

Browser

A program that allows you to access resources on the web and provides them to you graphically.

Cable modem

A device that allows you to connect a computer to a coaxial cable and receive Internet access from your Cable provider.

CardBus

A newer version of the PC Card or PCMCIA interface. Supports a 32-bit data path, DMA, and consumes less voltage.

CAT 5

Category 5. Used for 10/100 Mbps or 1 Gbps Ethernet connections.

Client

A program or user that requests data from a server.

Collision

When two devices on the same Ethernet network try and transmit data at the exact same time.

Cookie

Information that is stored on the hard drive of your computer that holds your preferences for the site that issued the cookie.

**Data**

Information that has been translated into binary so that it can be processed or moved to another device.

Data Encryption Standard

Uses a randomly selected 56-bit key that must be known by both the sender and the receiver when information is exchanged.

Data-Link layer

The second layer of the OSI model. Controls the movement of data on the physical link of a network.

Database

Organizes information so that it can be managed, updated, and easily accessed by users or applications.

DB-25

A 25-pin male connector for attaching External modems or RS-232 serial devices.

DB-9

A 9-pin connector for RS-232 connections.

dBd

Decibels related to dipole antenna.

dB_i

Decibels relative to isotropic radiator.

dB_m

Decibels relative to one milliwatt.

Decrypt

To unscramble an encrypted message back into plain text.

Default

A predetermined value or setting that is used by a program when no user input has been entered for this value or setting.

Demilitarized zone

DMZ. A single computer or group of computers that can be accessed by both users on the Internet as well as users on the Local Network, but that is not protected by the same security as the Local Network.

DHCP

Dynamic Host Configuration Protocol. Used to automatically assign IP addresses from a predefined pool of addresses to computers or devices that request them.

Digital certificate

An electronic method of providing credentials to a server in order to have access to it or a network.

Direct Sequence Spread Spectrum

DSSS. Modulation technique used by 802.11b wireless devices.

DNS

Domain Name System. Translates Domain Names to IP addresses.

Domain name

A name that is associated with an IP address.

Download

To send a request from one computer to another and have the file transmitted back to the requesting computer.

**DSL**

Digital Subscriber Line. High bandwidth Internet connection over telephone lines.

Duplex

Sending and Receiving data transmissions at the same time.

Dynamic DNS service

Dynamic DNS is provided by companies to allow users with Dynamic IP addresses to obtain a Domain Name that will always be linked to their changing IP address. The IP address is updated by either client software running on a computer or by a router that supports Dynamic DNS, whenever the IP address changes.

Dynamic IP address

IP address that is assigned by a DHCP server and that may change. Cable Internet providers usually use this method to assign IP addresses to their customers.

EAP

Extensible Authentication Protocol.

Email

Electronic Mail is a computer-stored message that is transmitted over the Internet.

Encryption

Converting data into ciphertext so that it cannot be easily read.

Ethernet

The most widely used technology for Local Area Networks.

Fiber optic

A method of sending data through light impulses over glass or plastic wire or fiber.

File server

A computer on a network that stores data so that the other computers on the network can access it.

File sharing

Allowing data from computers on a network to be accessed by other computers on the network with different levels of access rights.

Firewall

A device that protects resources of the Local Area Network from unauthorized users outside of the local network.

Firmware

Programming that is inserted into a hardware device that tells it how to function.

Fragmentation

Breaking up data into smaller pieces to make it easier to store.

FTP

File Transfer Protocol. Easiest way to transfer files between computers on the Internet.

Full-duplex

Sending and Receiving data at the same time.

Gain

The amount an amplifier boosts the wireless signal.

**Gateway**

A device that connects your network to another, like the Internet.

Gbps

Gigabits per second.

Gigabit Ethernet

Transmission technology that provides a data rate of 1 billion bits per second.

GUI

Graphical user interface.

H.323

A standard that provides consistency of voice and video transmissions and compatibility for video conferencing devices.

Half-duplex

Data cannot be transmitted and received at the same time.

Hashing

Transforming a string of characters into a shorter string with a predefined length.

Hexadecimal

Characters 0-9 and A-F.

Hop

The action of data packets being transmitted from one router to another.

Host

Computer on a network.

HTTP

Hypertext Transfer Protocol. Used to transfer files from HTTP servers (web servers) to HTTP clients (web browsers).

HTTPS

HTTP over SSL is used to encrypt and decrypt HTTP transmissions.

Hub

A networking device that connects multiple devices together.

ICMP

Internet Control Message Protocol.

IEEE

Institute of Electrical and Electronics Engineers.

IGMP

Internet Group Management Protocol. Used to make sure that computers can report their multicast group membership to adjacent routers.

IIS

Internet Information Server. A WEB server and FTP server provided by Microsoft.

IKE

Internet Key Exchange. Used to ensure security for VPN connections.

Infrastructure

In terms of a wireless network, this is when wireless clients use an access point to gain access to the network.

**Internet**

A system of worldwide networks that use TCP/IP to allow for resources to be accessed from computers around the world.

Internet Explorer

A World Wide Web browser created and provided by Microsoft.

Intranet

A private network.

Intrusion Detection

A type of security that scans a network to detect attacks coming from inside and outside of the network.

IP

Internet Protocol. The method of transferring data from one computer to another on the Internet.

IP address

A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the Internet or on an intranet.

IPsec

Internet Protocol Security. Provides security at the packet processing layer of network communication.

IPX

Internetwork Packet Exchange. A networking protocol developed by Novell to enable their Netware clients and servers to communicate.

ISP

Internet Service Provider. Provides access to the Internet to individuals or companies.

Java

A programming language used to create programs and applets for web pages.

Kbps

Kilobits per second.

Kbyte

Kilobyte.

L2TP

Layer 2 Tunneling Protocol.

LAN

Local Area Network. A group of computers in a building that usually access files from a server.

Latency

The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay.

LED

Light Emitting Diode.

Legacy

Older devices or technology.

LLDP

Link Layer Discovery Protocol. A vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices



for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet.

LPR/LPD

Line Printer Requestor/Line Printer Daemon. A TCP/IP protocol for transmitting streams of printer data.

MAC Address

A unique hardware ID assigned to every Ethernet adapter by the manufacturer.

Mbps

Megabits per second.

MDI

Medium Dependent Interface. An Ethernet port for a connection to a straight-through cable.

MDIX

Medium Dependent Interface Crossover. An Ethernet port for a connection to a crossover cable.

MIB

Management Information Base. A set of objects that can be managed by using SNMP.

Modem

A device that modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also demodulates the analog signals coming from the phone lines to digital signals for your computer.

MPPE

Microsoft Point-to-Point Encryption. Used to secure data transmissions over PPTP connections.

MTU

Maximum Transmission Unit. The largest packet that can be transmitted on a packet-based network like the Internet.

Multicast

Sending data from one device to many devices on a network.

NAT

Network Address Translation. Allows many private IP addresses to connect to the Internet, or another network, through one IP address.

NetBEUI

NetBIOS Extended User Interface. A Local Area Network communication protocol. This is an updated version of NetBIOS.

NetBIOS

Network Basic Input/Output System.

Netmask

Determines what portion of an IP address designates the Network and which part designates the Host.

Network Layer

The third layer of the OSI model which handles the routing of traffic on a network.

**NIC**

Network Interface Card. A card installed in a computer or built onto the motherboard that allows the computer to connect to a network.

NTP

Network Time Protocol. Used to synchronize the time of all the computers in a network.

OFDM

Orthogonal Frequency-Division Multiplexing. Modulation technique for both 802.11a and 802.11g.

OSI

Open Systems Interconnection. Reference model for how data should travel between two devices on a network.

OSPF

Open Shortest Path First. A routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other routers in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions.

Password

A sequence of characters that is used to authenticate requests to resources on a network.

Personal Area Network

The interconnection of networking devices within a range of 10 meters.

Physical layer

The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier.

Ping

A utility program that verifies that a given Internet address exists and can receive messages. The utility sends a control packet to the given address and waits for a response.

PoE

Power over Ethernet. The means of transmitting electricity over the unused pairs in a category 5 Ethernet cable.

POP3

Post Office Protocol 3 is used for receiving email.

Port

A logical channel endpoint in a network. A computer might have only one physical channel (its Ethernet channel) but can have multiple ports (logical channels) each identified by a number.

PPP

Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line.

PPPoE

Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet.

PPTP

Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks.

**Preamble**

Used to synchronize communication timing between devices on a network.

QoS

Quality of Service.

RADIUS

Remote Authentication Dial-In User Service. Allows remote users to dial into a central server and be authenticated in order to access resources on a network.

Reboot

To restart a computer and reload its operating software or firmware from nonvolatile storage.

Rendezvous

Apple's version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings.

Repeater

Retransmits the signal of an access point in order to extend its coverage.

RIP

Routing Information Protocol. Used to synchronize the routing table of all the routers on a network.

RJ-11

The most commonly used connection method for telephones.

RJ-45

The most commonly used connection method for Ethernet.

RS-232C

The interface for serial communication between computers and other related devices.

RSA

Algorithm used for encryption and authentication.

Server

A computer on a network that provides services and resources to other computers on the network.

Session key

An encryption and decryption key that is generated for every communication session between two computers.

Session layer

The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends.

SIP

Session Initiation Protocol. A standard protocol for initiating a user session that involves multimedia content, such as voice or chat.

SMTP

Simple Mail Transfer Protocol. Used for sending and receiving email.

SNMP

Simple Network Management Protocol. Governs the management and monitoring of network devices.

SOHO

Small Office/Home Office.

**SPI**

Stateful Packet Inspection. A feature of a firewall that monitors outgoing and incoming traffic to ensure that only valid responses to outgoing requests are allowed to pass through the firewall.

SSH

Secure Shell. A command line interface that allows for secure connections to remote computers.

SSID

Service Set Identifier is a name for a wireless network.

Subnet mask

Determines what portion of an IP address designates the Network and which part designates the Host.

Syslog

System Logger. A distributed logging interface for collecting in one place the logs from different sources. Originally written for UNIX, it is now available for other operating systems, including Windows.

TCP

Transmission Control Protocol.

TCP Raw

A TCP/IP protocol for transmitting streams of printer data.

TCP/IP

Transmission Control Protocol/Internet Protocol.

TFTP

Trivial File Transfer Protocol. A utility used for transferring files that is simpler to use than FTP but with less features.

Throughput

The amount of data that can be transferred in a given time period.

Traceroute

A utility that displays the routes between your computer and a specific destination.

UDP

User Datagram Protocol.

Unicast

Communication between a single sender and receiver.

Update

To install a more recent version of a software or firmware product.

Upgrade

To install a more recent version of a software or firmware product.

Upload

To send a request from one computer to another and have a file transmitted from the requesting computer to the other.

UPnP

Universal Plug and Play. A standard that allows network devices to discover each other and configure themselves to be a part of the network.

URL

Uniform Resource Locator. A unique address for files accessible on the Internet.

USB

Universal Serial Bus.

**UTP**

Unshielded Twisted Pair.

Virtual Private Network

VPN. A secure tunnel over the Internet to connect remote offices or users to their company's network.

VLAN

Virtual LAN.

VoIP

Voice over IP. Sending voice information over the Internet as opposed to the PSTN.

Wake on LAN

Allows you to power up a computer through its Network Interface Card.

WAN

Wide Area Network. The larger network that your LAN is connected to, which may be the Internet itself, or a regional or corporate network

WCN

Windows Connect Now. A Microsoft method for configuring and bootstrapping wireless networking hardware (access points) and wireless clients, including PCs and other devices.

WDS

Wireless Distribution System. A system that enables the interconnection of access points wirelessly.

Web browser

A utility that allows you to view content and interact with information on the World Wide Web.

WEP

Wired Equivalent Privacy. Security for wireless networks that is designed to be comparable to that of a wired network.

WiFi

Wireless Fidelity. Used to describe any of the 802.11 wireless networking specifications.

WiFi Protected Access

An updated version of security for wireless networks that provides authentication as well as encryption.

Wireless (WiFi) LAN

Connecting to a Local Area Network over one of the 802.11 wireless standards.

WISP

Wireless Internet Service Provider. A company that provides broadband Internet service over a wireless connection.

WLAN

Wireless Local Area Network.

WPA

WiFi Protected Access. A WiFi security enhancement that provides improved data encryption relative to WEP.

xDSL

A generic term for the family of digital subscriber line (DSL) technologies, such as ADSL, HDSL, RADSL, and SDSL.

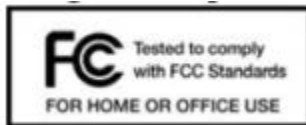
Yagi antenna

A directional antenna used to concentrate wireless signals on a specific location.

10 APPENDIX

10.1 Regulatory and Safety Information

Read all operating instructions and the safety information below and before using the CBA850 device to avoid injury.



FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which

can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC CAUTION: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Exposure Statement: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator & your body. To comply with FCC regulations limiting both maximum RF output power and human exposure to RF radiation, for the CBA850-LE the maximum antenna gain must not exceed 8 dBi in the cellular band, 3 dBi in the PCS band and 10 dBi in the LTE band. For the CBA850-LP the maximum antenna gain including cable loss must not exceed 7.5 dBi in the cellular band, 3 dBi in the PCS band, 5.5 dBi in LTE Band 4, and 9 dBi in LTE Band 17. For the CBA850-W the maximum antenna gain must not exceed 9.2 dBi in the 2.5 GHz band (2496-2690 MHz).

SAFETY AND HAZARDS

Under no circumstances should the CBA850 device be used in any areas (a) where blasting is in progress, (b) where explosive atmospheres may be present, or (c) that are near (i) medical or life support equipment, or (ii) any equipment which may be susceptible to any form of radio interference. In such areas, the CBA850 device **MUST BE POWERED OFF AT ALL TIMES** (since the device otherwise could transmit signals that might interfere with such equipment). In addition, under no circumstances should the CBA850 device be used in any aircraft, regardless of whether the aircraft is on the ground or in flight. In any aircraft, the CBA850 device **MUST BE POWERED OFF AT ALL TIMES** (since the device otherwise could transmit signals that might interfere with various onboard systems on such aircraft). Furthermore, under no circumstances should the CBA850 device be used by the driver or operator of any vehicle. Such use of the device will detract from the driver's or operator's control of that vehicle. In some jurisdictions, use of the CBA850 device while driving or operating a vehicle constitutes a civil and/or criminal offense.

Due to the nature of wireless communications, transmission and reception of data by the CBA850 device can never be guaranteed, and it is possible that data communicated or transmitted wirelessly may be delayed, corrupted (i.e., contain errors), or totally lost. The CBA850 device is not intended for, and Cradlepoint recommends the device not be used in, any critical applications where failure to transmit or receive data could result in property damage or loss or personal injury of any kind (including death) to the user or to any other party. Cradlepoint expressly disclaims liability for damages of any kind resulting from: (a) delays, errors, or losses of any data transmitted or received using the device; or (b) any failure of the device to transmit or receive such data.



Warning: This product is only to be installed by qualified personnel!

**Industry Canada Statement**

This device complies with RSS-210, RSS-102, and RSS-Gen of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Déclaration d'Industrie Canada

Ce dispositif est conforme à la norme CNR-210, CNR-102, et CNR-Gen d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

10.2 Warranty, Liability, Privacy, etc.

Cradlepoint, Inc. warrants this product against defects in materials and workmanship to the original purchaser (or the first purchaser in the case of resale by an authorized distributor) for a period of one (1) year from the date of shipment. This warranty is limited to a repair or replacement of the product, at Cradlepoint's discretion as purchaser's sole and exclusive remedy. Cradlepoint does not warrant that the operation of the device will meet your requirements or be error free. Within thirty (30) days of receipt should the product fail for any reason other than damage due to customer negligence, purchaser may return the product to the point of purchase for a full refund of the purchase price. If the purchaser wishes to upgrade or convert to another Cradlepoint, Inc. product within the thirty (30) day period, purchaser may return the product and apply the full purchase price toward the purchase of the other product. Any other return will be subject to Cradlepoint, Inc.'s existing return policy.

LIMITATION OF CRADLEPOINT LIABILITY

The information contained in this Quick Start Guide is subject to change without notice and does not represent any commitment on the part of Cradlepoint or its affiliates. CRADLEPOINT AND ITS AFFILIATES HEREBY SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL: (A) DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES, INCLUDING WITHOUT LIMITATION FOR LOSS OF PROFITS OR REVENUE OR OF ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE THE DEVICE, EVEN IF CRADLEPOINT AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND EVEN IF SUCH DAMAGES ARE FORESEEABLE; AND (B) CLAIMS BY ANY THIRD PARTY. Notwithstanding the foregoing, in no event shall the aggregate liability of Cradlepoint and/or its affiliates arising under or in connection with this device or integrated modems, regardless of the number of events, occurrences, or claims giving rise to liability, exceed the price paid by the original purchaser of the device or integrated modems.

OPEN SOURCE SOFTWARE

This product contains software distributed under one or more of the following open source licenses: GNU General Public License Version 2, BSD License, Net-SNMP License, and PSF License Agreement for Python 3.3. For more information on this software, including licensing terms and your rights to access source code, please visit: www.Cradlepoint.com/opensource.

PRIVACY

Cradlepoint collects general data pertaining to the use of Cradlepoint products via the Internet including, by way of example, IP address, device ID, operating system, browser type and version number, etc. To review Cradlepoint's privacy policy, please visit: <http://www.Cradlepoint.com/privacy>.

OTHER BINDING DOCUMENTS; TRADEMARKS; COPYRIGHT

By activating or using your Cradlepoint device, you agree to be bound by Cradlepoint's Terms of Use, User License and other Legal Policies, all as posted at www.Cradlepoint.com/legal. Please read these documents carefully.



10.3 Specifications

MODEL NAME

CBA850 Cellular Broadband Adapter

WAN

Via embedded 3G/4G modem

LAN

Two Ethernet ports (10/100/1000)

BUTTONS/SWITCHES

Power, reset

LED INDICATORS

Power, Ethernet LAN1, Ethernet LAN2, WAN data activity, USB modem status, External USB status indicator, signal strength

DIMENSIONS

4.8 x 4.8 x 1.7 in (122 x 122 x 42 mm)

CERTIFICATIONS

FCC, CE, IC, PTCRB, GCF-CC, carrier (some certifications are specific to particular ARC models)

OPERATING TEMPERATURE

0°C to 50°C

For more in-depth specifications and router details, see the product data sheet.



<http://www.Cradlepoint.com/>

Copyright © 2015 by Cradlepoint, Inc. All rights reserved.