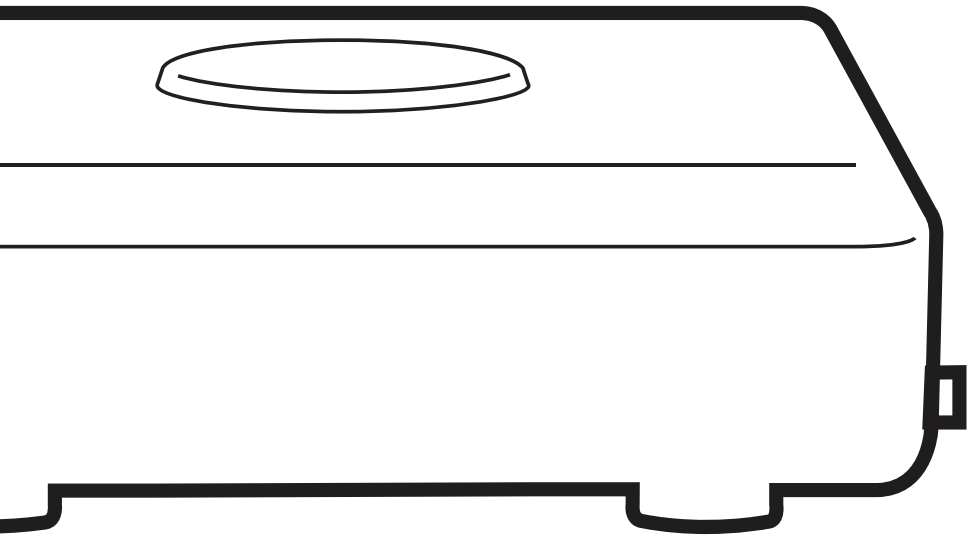
cradlepoint

Global Leader in 4G LTE Network Solutions

ARC Series Router

CBA850

User Manual



cradlepoint.com

TABLE OF CONTENTS

INTRODUCTION

WHAT'S IN THE BOX

- CBA850 with integrated MC400 Multi-Carrier Software-Defined Radio modem
- Universal 3G/4G/LTE antennas with dedicated active GPS antenna port
- 12VDC 1A power adapter (1.5 meter cord)
- Ethernet cable
- Quick Start Guide
- Mounting hardware
- Warranty and regulatory information

KEY FEATURES

WAN

- LP6: LTE Advanced LTE/HSPA+ (SIM-based Auto-Carrier Selection for all North American carriers and European operators)
- LPE: 4G LTE/HSPA+/EVDO (multi-carrier)
- LP3: 4G LTE/HSPA+ (Europe, EMEA, and Australia/New Zealand)
- Advanced Modem Failure Check
- IP Passthrough
- Standby
- Ethernet WAN for inline failover

LAN

- VLAN 802.1Q
- DHCP Server, Client, Relay
- DNS and DNS Proxy
- DynDNS
- UPnP
- DMZ
- MAC Address Filtering

MANAGEMENT

- Cradlepoint Enterprise Cloud Manager[1]
- Web UI, API, CLI, SSH
- Data Usage Alerts (router and per client)
- Advanced Troubleshooting (support)
- Device Alerts
- SNMP
- SMS control

ROUTING

- Routing Rules
- NAT-less Routing
- Virtual Server/Port Forwarding
- IPv6

SECURITY

- RADIUS and TACACS+ support*
- 802.1x authentication for Ethernet
- ALGs
- MAC Address Filtering
- Advanced Security Mode (local user management only)
- Per-Client Web Filtering
- IP Filtering
- Content Filtering (basic)
- Website Filtering

*-Native support for authentication. Authorization and accounting support through hotspot/captive portal services.

1 – **Enterprise Cloud Manager** requires a subscription

SPECIFICATIONS

WAN: Integrated LP6 Category 6 LTE Advanced LTE modem (with DC-HSPA+ failover) or LPE 4G LTE modem (with HSPA+/EVDO/3G and 2G failover) or LP3 4G LTE modem (with HSPA+ and 2G failover)

LAN:

- Two LAN 10/100/1000 Ethernet ports (default one NAT, one IP Passthrough)
- RJ45 Serial Port for console access or out-of-band management

TEMPERATURE:

- 0°C to 50°C (32°F to 122°F) operating
- -20°C to 70°C (-4°F to 158°F) storage

HUMIDITY (non-condensing):

- 10% to 85% operating
- 5% to 90% storage

POWER:

- 12VDC 1.5A adapter
- 802.3af (15W) or 802.3at (30W) PoE capable

SIZE: 4.8 x 4.8 x 1.7 in (122 x 122 x 42 mm)

HOUSING:

- White plastic, locking compatible
- Wall, desk, or DIN Rail mounting

CERTIFICATIONS:

- FCC, CE, IC
- Safety: UL/CUL/CB Scheme
- Materials: WEEE, RoHS, RoHS-2, California Prop 65

ACCESSORIES

- 700 MHz – 2700 MHz Wide Band Directional Antenna (Yagi/Log- Periodic) Part #: 170588-000
- 12" Mag-Mount Antenna with SMA Male Connector Part #: 170605-000
- 4" Mini Mag-Mount Antenna with SMA Male Connector Part #: 170606-000

- 2.4/5 GHz Dual-band Dual-concurrent WiFi Antenna Part #: 170628-000 (WiFi models only)
- Universal 3G/4G/LTE Modem Antenna Part #: 170649-000
- GPS Screw-Mount Antenna Part #: 170651-000
- GPS Mag-Mount Antenna Part #: 170652-000
- Universal 3G/4G multi-band cellular modem antenna (white) – 2dBi/3dBi (Part # 170659-000)
- Multi-Band Omni-Directional Antenna Part #: 170668-000
- Indoor/Outdoor Panel Patch Part #: 170669-000
- DIN Rail Mounting Bracket (Part # 170656-000)
- Wall/Ceiling Mounting Bracket (Part # 170666-000)
- Rollover Adapter for RJ45 Ethernet cable M/F (Part # 170662-000)
- RJ45 Rollover serial console cable 7ft (Part # 170663-000)
- RJ45 Rollover serial console cable 14ft (Part # 170663-001)

See the Cradlepoint **antenna accessories page** for more information about antennas. Also see the Antenna Ordering and Installation Guide, available as a PDF in the Resources section of antenna and router product pages.

BUSINESS-GRADE MODEM SPECIFICATIONS

ARC CBA850 LP6 models include an integrated LTE Advanced Category 6 4G LTE modem. The LP6 modems support SIM-Based Auto-Carrier selection so there is only one model for all of North America. Simply insert the SIM and wait for the router to automatically detect the SIM and establish a connection.

The LTE bands certified for each carrier are listed below.

ARC CBA850LP6-NA, CBA850LP6-EU, CBA850LP6-UK

- **Technology:** LTE Advanced, HSPA+
- **Downlink Rates:** LTE 300 Mbps, HSPA+ 42.2 Mbps
- **Uplink Rates:** LTE 50 Mbps, HSPA+ 5.76 Mbps
- **Frequency Bands:**
  - **LTE** Bands 1-5, 7, 8, 12, 13, 17, 20, 25, 26, 29, 30, 41
    - **Verizon:** 2, 4, 5, 13 (XLTE support w/carrier aggregation)
    - **AT&T:** 2, 4, 5, 12/17, 29, 30
    - **Sprint:** 25, 26, 41 (LTE Plus Support)
    - **T-Mobile:** 2, 4, 12 (T-Mobile Wideband LTE Support)
    - **Generic:** all
- **Carrier Aggregation:**
  - 1+ 8
  - 2+ 2/5/12 (17 w/MFBI)/13/29
  - 3+ 7/20
  - 4+ 4/5/12 (17 w/MFBI)/13/29
  - 5+ 2/4/30
  - 7+ 3/7/20
  - 8+ 1
  - 12 (17 w/MFBI) + 2/4/30
  - 13+ 2/4
  - 20+ 3/7
  - 30+ 5/12 (17 w/MFBI)
  - 41+ 41
- **Fallback:** WCDMA/DC-HSPA+ (42/5.76 Mbps): Bands 1, 2, 3, 4, 5, 8
- **Power:** LTE 23 dBm +/- 1, HSPA+ 23 dBm +/- 1
- **Antennas:** two SMA male (plug), finger tighten only (maximum torque spec is 7 kgfcm)
- **GPS:** active GPS support

- **SMS:** SMS support
- **Industry Standards & Certs:** CE, FCC, GCF-CC, IC, PTCRB, AT&T, Sprint (pending certification), Verizon
- **Modem Part Number:** MC400LP6

ARC CBA850LPE models include an integrated 4G LTE modem – specific model names include a specific modem (e.g., the ARC CBA850LPE-VZ includes a Verizon LTE modem).

Please note that LPE models are flexible and support bands for multiple cellular providers; however, only the frequency bands in **bold** below are supported by the listed provider.

ARC CBA850LPE-VZ – 4G LTE/EVDO for Verizon

- **Technology:** LTE, EVDO Rev A
- **Downlink Rates:** LTE 100 Mbps, EVDO 3.1 Mbps (theoretical)
- **Uplink Rates:** LTE 50 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)
  - GSM/GPRS/EDGE: (850/900/1800/1900 MHz)
  - **CDMA: EVDO Rev A/1xRTT (800/1900 MHz)**
- **Power:** LTE 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:** FCC, Verizon
- **Modem Part Number:** MC400LPE-VZ
- **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 (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)
- **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:** FCC, PTCRB, AT&T
- **Modem Part Number:** MC400LPE-AT
- **SIM:** two 2FF SIM slots

ARC CBA850LPE-SP – 4G LTE/HSPA+/EVDO for Sprint

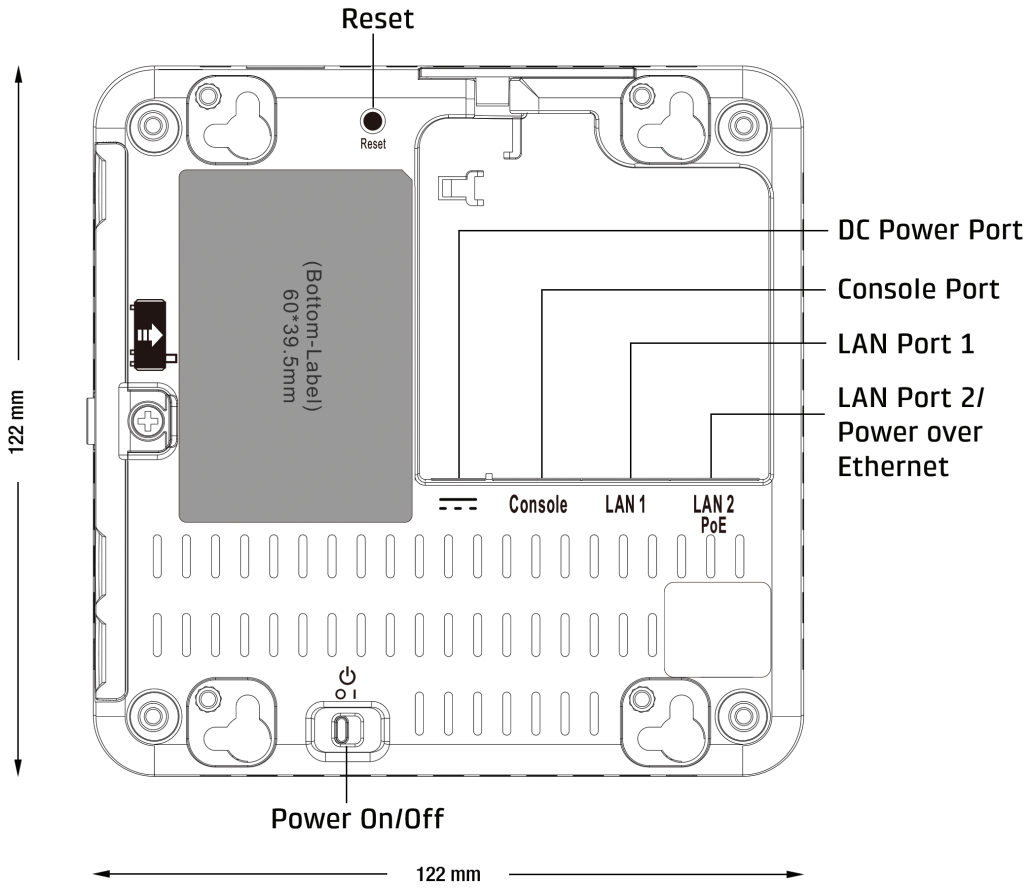
- **Technology:** LTE, HSPA+, EVDO Rev A
- **Downlink Rates:** LTE 100 Mbps, HSPA+ 21.1 Mbps, EVDO 3.1 Mbps (theoretical)
- **Uplink Rates:** LTE 50 Mbps, HSPA+ 5.76 Mbps, EVDO 1.8 Mbps (theoretical)
- **Frequency Bands:**
  - **LTE:** Band 2 (1900 MHz), Band 4 – AWS (1700/2100 MHz), Band 5 (850 MHz), 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)**
- **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:** FCC, Sprint
- **Modem Part Number:** MC400LPE-SP
- **SIM:** two 2FF SIM slots

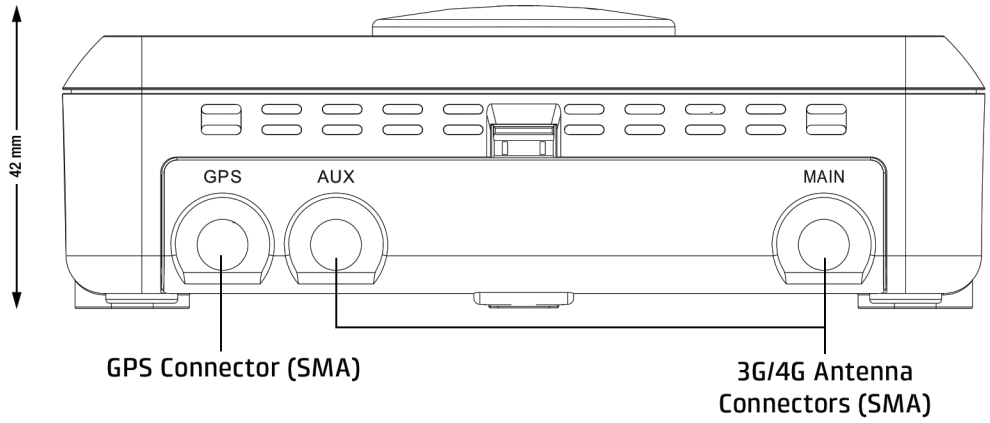
ARC CBA850LP3-EU – 4G LTE/HSPA+ for Europe
- **Technology:** LTE, HSPA+
- **Downlink Rates:** LTE 100 Mbps, HSPA+ 21.1 Mbps (theoretical)
- **Uplink Rates:** LTE 50 Mbps, HSPA+ 5.76 Mbps (theoretical)
- **Frequency Bands:**
  - **LTE: Band 1 (2100 MHz), Band 3 (1800 MHz), Band 7 (2600 MHz), Band 8 (900 MHz), Band 20 (800 MHz)**
  - **HSPA+/UMTS: (800/850/900/1900/2100 MHz)**
  - **GSM/GPRS/EDGE: Quad-Band (850/900/1800/1900 MHz)**
- **Power:** LTE Band 1/3/8/20 – 23 dBm +/– 1; LTE 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
- **GPS:** active GPS support
- **Industry Standards & Certs:** CE, GCF-CC
- **Modem Part Number:** MC400LP3-EU
- **SIM:** two 2FF SIM slots

ARC CBA850LPE-GN – 4G LTE/HSPA+/EVDO for Canada and T-Mobile and US Cellular in the U.S.
- **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), 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)**
- **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:** FCC, IC, PTCRB
- **Modem Part Number:** MC400LPE-GN
- **SIM:** two 2FF SIM slots
- **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

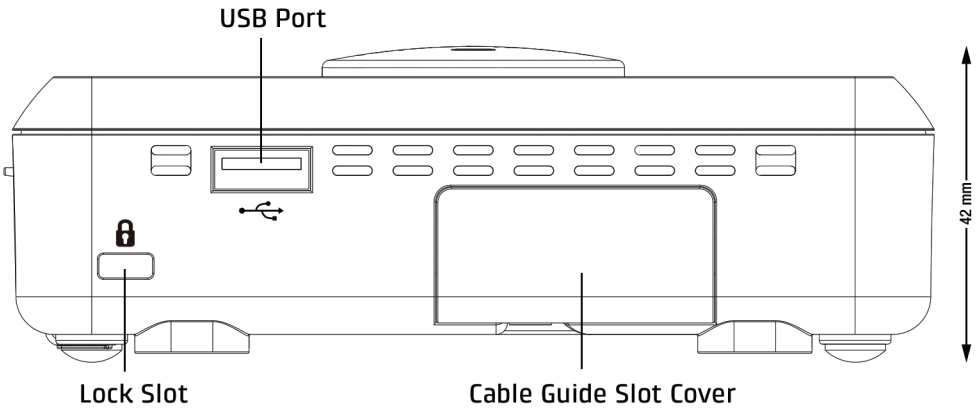
HARDWARE



BOTTOM VIEW

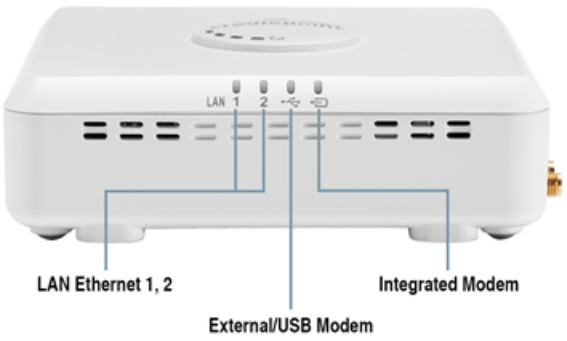


RIGHT VIEW



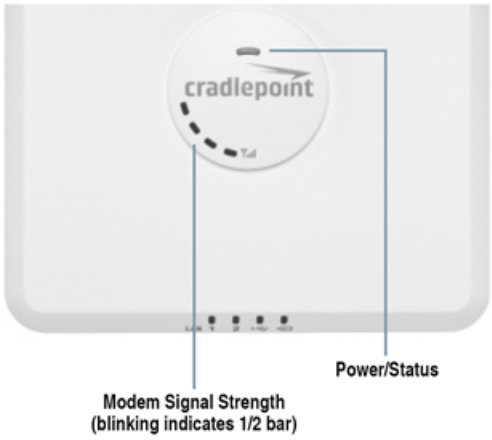
REAR VIEW

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

SUPPORT AND WARRANTY

CradleCare Support available with technical support, software upgrades, and advanced hardware exchange – 1-, 3-, and 5-year options.

One-year limited hardware warranty available in the US and Canada; two-year limited hardware warranty for integrated EU products when purchased from an authorized EU distributor – extend warranty to 2, 3, or 5 years.

QUICK START

BASIC SETUP

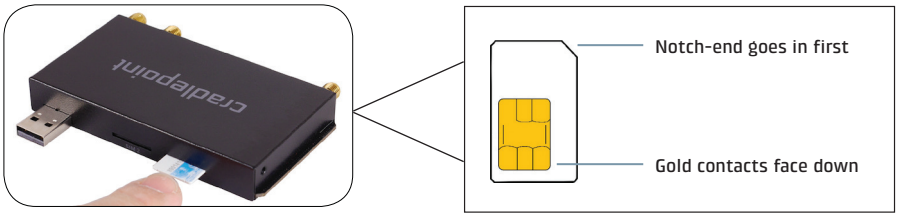
1. Insert an activated SIM

The Cradlepoint ARC CBA850 requires a SIM with an activated wireless broadband data plan. Contact your carrier for details about selecting a data plan and about the process for provisioning your SIM.

Once you have an activated SIM, insert it into the integrated modem:

1. Remove the modem cover and pull out the integrated modem.
2. Insert the SIM card into the slot marked SIM 1 (use the other slot, SIM 2, for a secondary/backup SIM).

Be sure to insert the card with the notch-end first and the gold contacts facing down – it will click into place.



2. Insert the removable modem

Slide the integrated modem back into its slot. Put the cover back into place and insert the included security screw if desired (requires small Phillips screwdriver). **NOTE:** To remove modem, attach included modem antennas (finger-tighten only) and pull modem straight out.

3. Attach included modem antennas.

Antennas are finger-tighten only. Attach to connectors marked MAIN and AUX.

4. Connect to a power source.

Attach the included adapter to the device and to a power source OR connect a POE-enabled RJ45 cable to LAN 2. Then turn the power switch on (I).

5. Connect to a computer or other network equipment.

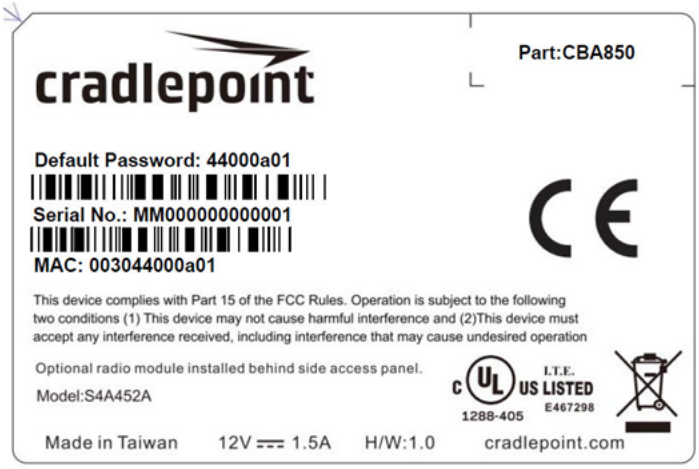
Connect via Ethernet to LAN 1 for local management. Connect LAN 2 (Default IP Passthrough 0/24) to networking equipment to Passthrough 3G/4G Internet to Ethernet.

ACCESSING THE ADMINISTRATION PAGES

Once you are connected, open the Cradlepoint CBA850's GUI-based administration pages to make configuration changes to your router.

1. Open a browser window and type "**cp/**" or "**192.168.0.1**" in the address bar. Press **ENTER/RETURN**.
2. When prompted for your password, type the eight character **DEFAULT PASSWORD** found on the product label.

NOTE: The product label below is an example only: your **DEFAULT PASSWORD** *and* **SSID** *will be unique.*



It's possible – and more efficient – to do all your configuration changes through Cradlepoint **Enterprise Cloud Manager** (ECM) without logging into the local administration pages. Set up a group of routers and set the configuration for all of them at once. See **below** for more information about ECM.

FIRST TIME SETUP WIZARD

When you log in for the first time, you will be automatically directed to the **FIRST TIME SETUP WIZARD**, which will walk you through the steps to customize your Cradlepoint CBA850. You have the ability to configure any of the following:

- Administrator Password
- Time Zone
- Security Mode
- Access Point Name (APN) for SIM-based modems
- Modem Authentication
- Failure Check

NOTE: To return to the First Time Setup Wizard after your initial login, select **SYSTEM** *from the navigation bar, expand* **Setup Wizard**, *and select* **First Time Setup**.

USING 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 (ECM) integrates cloud management with your Cradlepoint devices to improve productivity, increase reliability, reduce costs, and enhance the intelligence of your network and business operations.

Click **here** to sign up for a free 30-day ECM trial.

Depending on your ordering process, your devices may have already been bulk-loaded into ECM. If so, simply log in at **cradlepointecm.com** using your ECM credentials and begin managing your devices seamlessly from the cloud.

If your device has not yet been loaded into your ECM account, you need to register. Log into the device administration pages and select **Enterprise Cloud Manager** from the **SYSTEM** menu. Enter your ECM username and password, and click on "Register".

Once you have registered your device, go to **cradlepointecm.com** and log in using your ECM credentials.

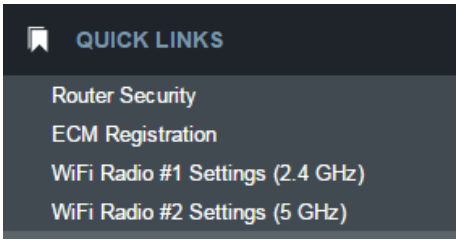
For more information about how to use Cradlepoint Enterprise Cloud Manager, see the following:

- **Getting Started**
- **ECM on the Knowledge Base**

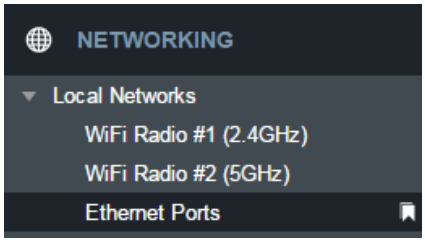
ADMINISTRATION PAGES

QUICK LINKS

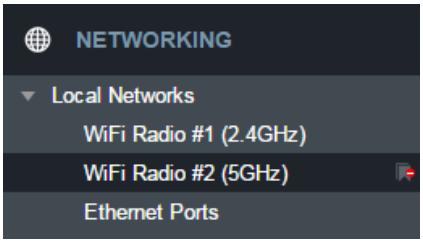
Quick Links allows you to bookmark your most commonly-used settings. Simply click on the bookmark icon ( ) to add an item to your Quick Links menu. To remove an item from your Quick Links menu, select the item and click on the remove bookmark icon ( ).



Quick Links Menu

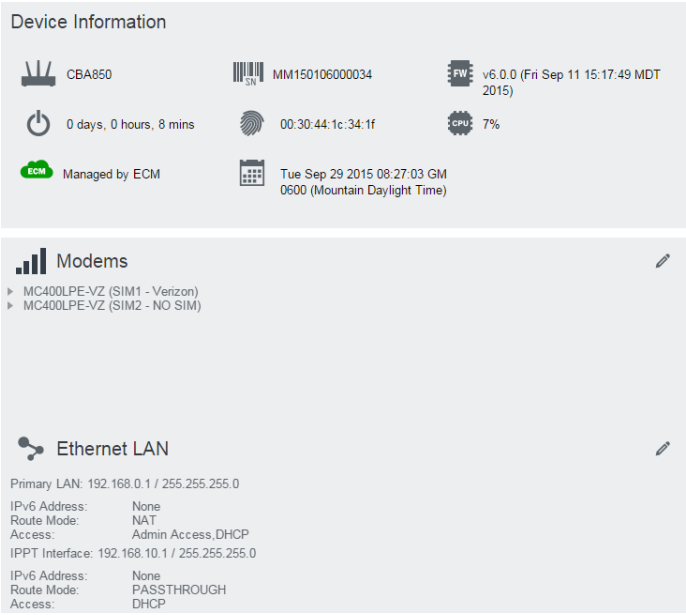


Add Quick Link



Delete Quick Link

DASHBOARD



The **Dashboard** is a centralized location for basic information about the status of your router. The areas include:

- Device Information
- Ethernet WAN*
- Modems*
- WWAN*
- Ethernet LAN*

*-To quickly edit settings for any of these areas, click on the pencil icon ( ) in the top-right of the desired dialog box.

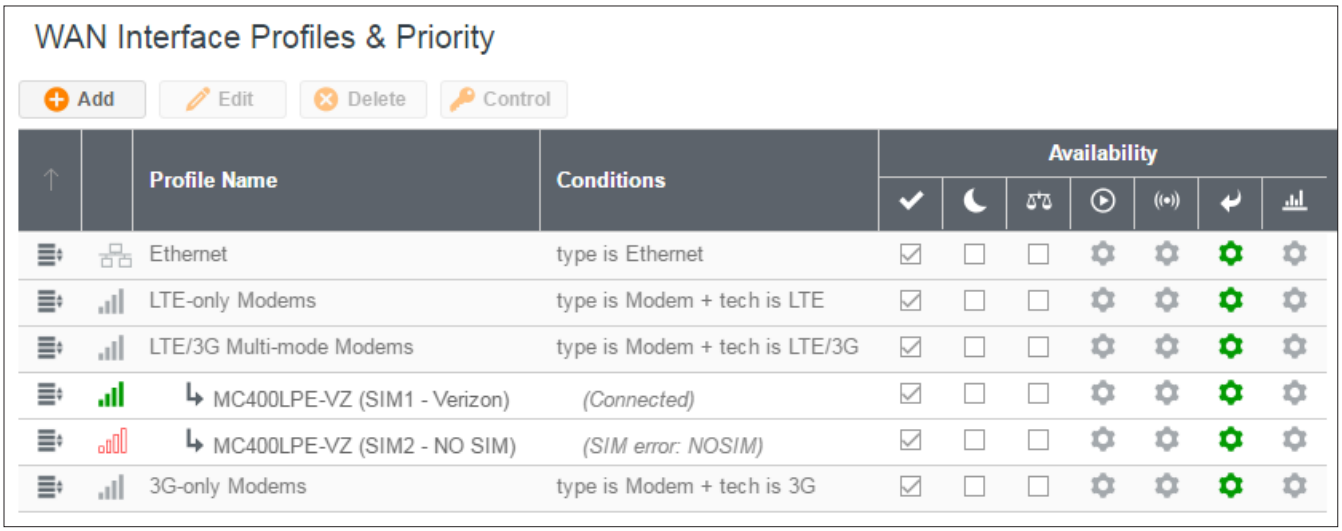
You may return to the Dashboard at any time by clicking on **DASHBOARD** from the left menu or by clicking on the Cradlepoint logo at the top-left of the screen.

CONNECTION MANAGER

The Connection Manager is used to manage the various WAN interfaces you have available on your router. WAN interface types (Ethernet, modems) are prioritized in connection preference and failover order (with the top of the list being highest priority).

WAN INTERFACE PROFILES & PRIORITY

This is a list of the available interfaces used to access the Internet. You can enable, stop, or start devices from this section. Drag the priority icon (≡) up or down to set the interface the router uses by default and the order that it allows failover.



Availability Key

- Enable
- Standby
- Load Balance
- On Demand
- WAN Verify
- Failback
- Data Usage

STANDBY

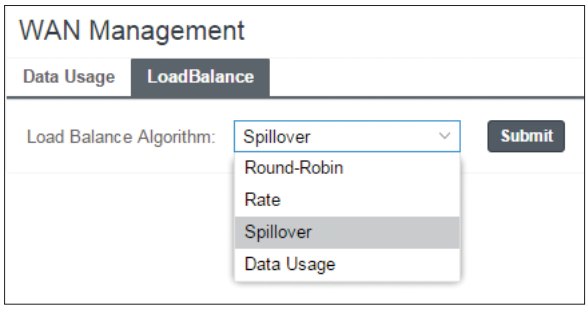
Standby is used to decrease failover time from one WAN interface to another. When Standby is enabled for a WAN profile or interface, the relevant interfaces are kept in a connected-but-idle (minimal, non-routed traffic) state. When the current WAN connection is disrupted, the traffic will failover to the next priority WAN. If that interface is on Standby, the connection is already established and failover will take much less time.

Note that the current connected interface(s) is/are indicated by a green connection state. For interfaces on Standby, the interface is indicated by a yellow connection state. If the interface is indicated in red, the interface is not currently connected or in Standby.

Standby is used to enable faster failover times only. If you want to manage traffic to a specific WAN interface, you will need to use WAN Affinity. If WAN Affinity is enabled for a particular profile or interface, do not enable Standby for that profile or interface as the failover results may vary and be unexpected.

LOAD BALANCE

To enable Load Balancing, select the check box for each desired device. 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 any current browsing session.



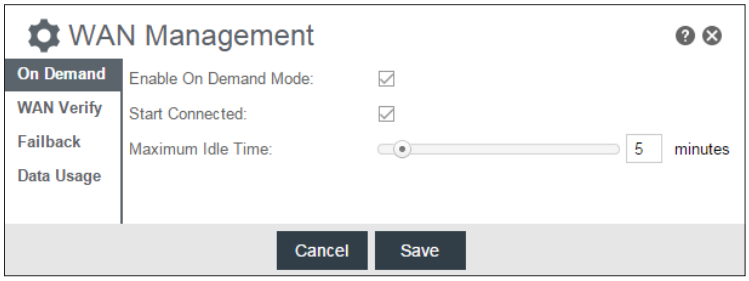
From **WAN Management**, select the **Load Balance Algorithm** from the following dropdown options:

- **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 functioning 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.

ON DEMAND

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



WAN VERIFY

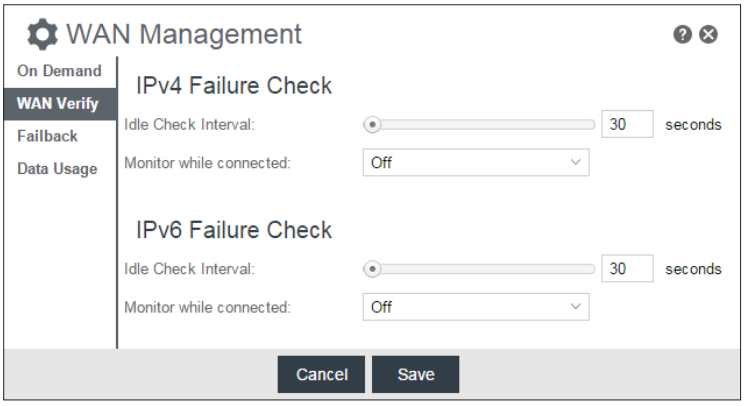
If this is enabled, the router will check that the highest priority active WAN interface can get to the Internet even if the WAN connection is not actively being used. If the interface goes down, the router will switch to the next highest priority interface available. If this is not selected, the router 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 two seconds. If no data is received the router behaves as described below under **Active DNS**.

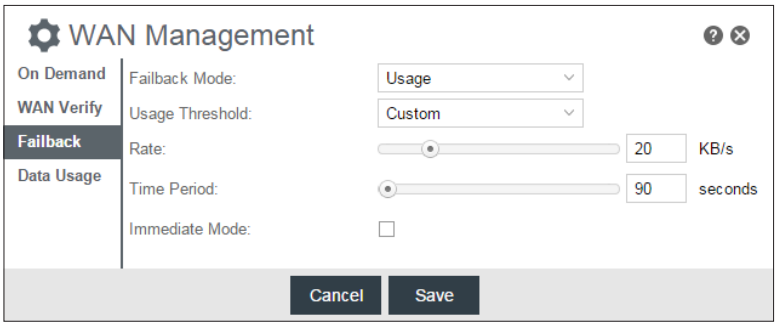


- **Active DNS** (modem only): A DNS request will be sent to the DNS servers. If no data is received, the DNS request will be retried four times at five-second intervals. (The first two requests will be directed at the Primary DNS server and the second two requests will be directed at the Secondary DNS 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 five-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.

FAILBACK

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.

Select the **Failback Mode** from the following options:



- Usage
- Time
- Disabled

Usage Threshold: Fail back based on the amount of data passed over time. This is a good setting for when you have a dual-mode EVDO/WiMAX modem and you are going in and out of WiMAX coverage. If the router has failed over to EVDO it will wait until you have low data usage before bringing down the EVDO connection to check if a WiMAX connection can be made.

- 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 is a good setting if you have a primary wired WAN connection and only use a modem for failover when your wired connection goes down. 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.

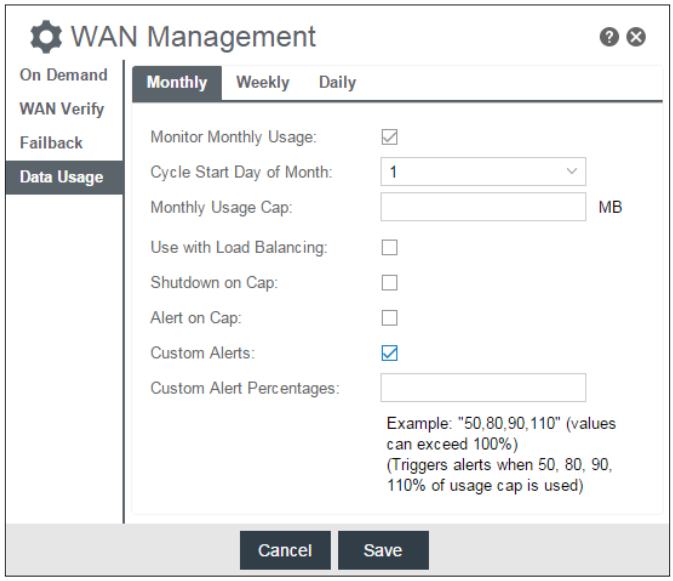
DATA USAGE

Data Usage displays upload and download traffic for each LAN client. Check **Monitor Monthly** (or Weekly or Daily) **Usage** to begin tracking this information. This data is not retained between router reboots.

For **Monthly** and **Weekly** you are able to specify the day to start each cycle (e.g. the 1st or Tuesday, respectively).

Usage Cap: Enter a Cap amount in Megabytes. 1024 Megabyte is equal to 1 Gigabyte.

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 WAN Affinity/Load Balancing page must be selected or this checkbox has no effect.



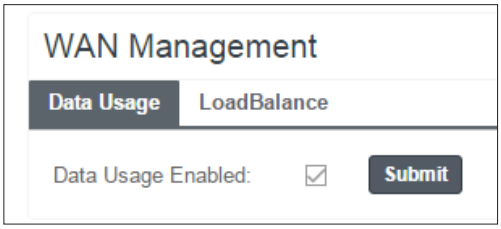
Shutdown on Cap: When checked, the WAN device will shutdown when the assigned usage is reached. A cycle reset or a rule deletion will re-enable the device.

Alert on Cap: An email alert will be generated and sent when the assigned data cap is reached. **NOTE:** The SMTP mail server must be configured in **System > Device Alerts**.

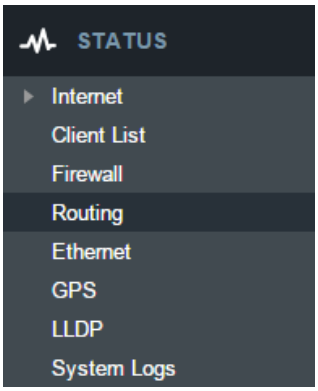
Custom Alerts: Check to enable custom alerts at specified percentage of usage cap.

Custom Alert Percentages: *Example*: "50,80,90,110" (values can exceed 100%) (Triggers alerts when 50, 80, 90, 110% of usage cap is used)

NOTE: To enable data usage, check **Data Usage Enabled** from WAN Management.



STATUS

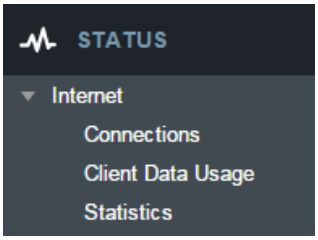


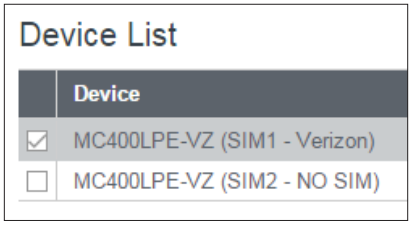
INTERNET

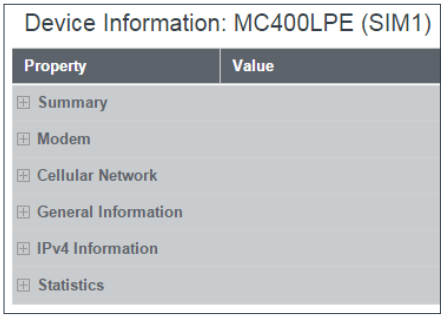
CONNECTIONS

Select your device to reveal detailed information about the following device properties:

- Summary
- Modem
- Cellular Network
- General Information
- IPv4 Information
- Statistics







Property	Value
Summary	
State	connected
Manufacturer	Cradlepoint Inc.
Model	MC400LPE (SIM1)
Modem Firmware Version	SWI9X15C_05.05.16.02 r21040 carm
Service Display	LTE
Home Carrier	Verizon
Roaming Status	Home
Signal Strength	100 %
RSSI	-53 dBm
SINR	19.4 dB
RSRP	-80 dB
RSRQ	-12 dB
Mobile Directory Number	[redacted]
MEID	[redacted]
IMEI	[redacted]
Network Address Identifier (NAI)	[redacted]
Current APN	VZWINTERNET
IP Address	100.67.93.1
Netmask	255.255.255.252
Gateway	100.67.93.2
DNS Servers	198.224.164.135,198.224.160.135

Property	Value
Summary	
Modem	
Manufacturer	Cradlepoint Inc.
Product	MC400LPE (SIM1)
Model	MC400LPE (SIM1)
Supported Technologies	lte/3g
Firmware Version	SWI9X15C_05.05.16.02 r21040
Package Version	05.05.16.02_VZW,005.013_010
Mobile Directory Number	[redacted]
ESN/IMEI	[redacted]
MEID	[redacted]
IMEI	[redacted]
ICCID	[redacted]
Mobile Subscriber Identification	[redacted]
IMSI	311480206582221
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	LTE
Signal Strength	100 %
RSSI	-53 dBm
SINR	19.4 dB
RSRP	-80 dB
RSRQ	-12 dB
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:	
Cell ID	2965526 (0x2d4016)
Operating Mode	Online
System Mode	LTE
IMS Registration State	In Progress
PS State	Attached
PRL Version	15414
RF Band	Band 4
Bandwidth	10 MHz
RX Channel	2000
TX Channel	20000
LTE Tx Power	-3.0 dBm
RX Frequency Band	2110-2155 MHz
TX Frequency Band	1710-1755 MHz
EMM State	Registered
EMM Sub State	Normal Service
EMM Connection State	RRC Connected
Network Address Identifier (NAI)	[redacted]
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 AAA Auth Status	Not Requested
Home PLMN ID	311480
Tracking Area Code	2817

Property	Value
⊞ Summary	
⊞ Modem	
⊞ Cellular Network	
⊟ General Information	
Unique Identifier	9cd858ae
Port	modem1
Type	mdm
Model	MC400LPE (SIM1)

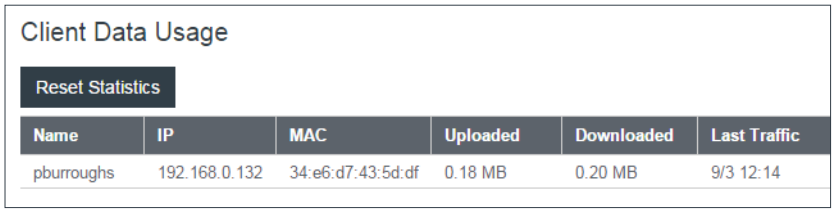
Property	Value
⊞ Summary	
⊞ Modem	
⊞ Cellular Network	
⊞ General Information	
⊟ IPv4 Information	
IP Address	100.67.93.1
Netmask	255.255.255.252
Gateway	100.67.93.2
DNS Servers	198.224.164.135,198.224.160.135

Property	Value
⊞ Summary	
⊞ Modem	
⊞ Cellular Network	
⊞ General Information	
⊞ IPv4 Information	
⊟ Statistics	
Outgoing Bytes	288098
Incoming Bytes	144940
Connection Uptime	0:08:00

CLIENT DATA USAGE

Displays the following client information:

- Name
- IP Address
- MAC Address
- Data Uploaded
- Data Downloaded
- Last Traffic

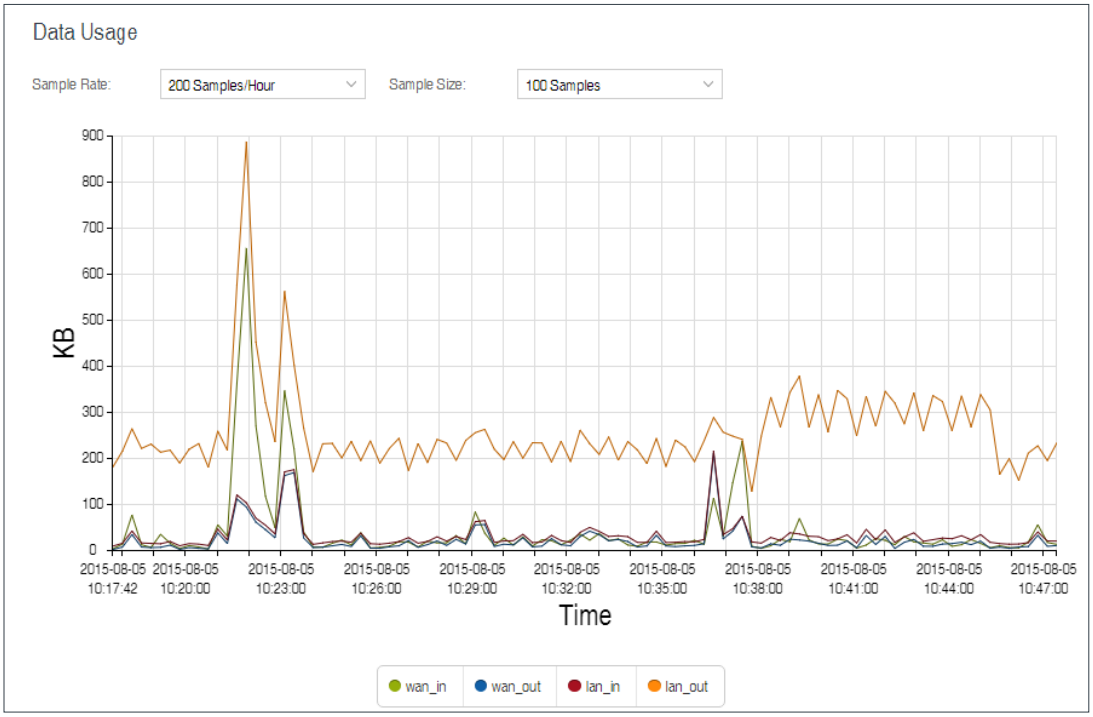


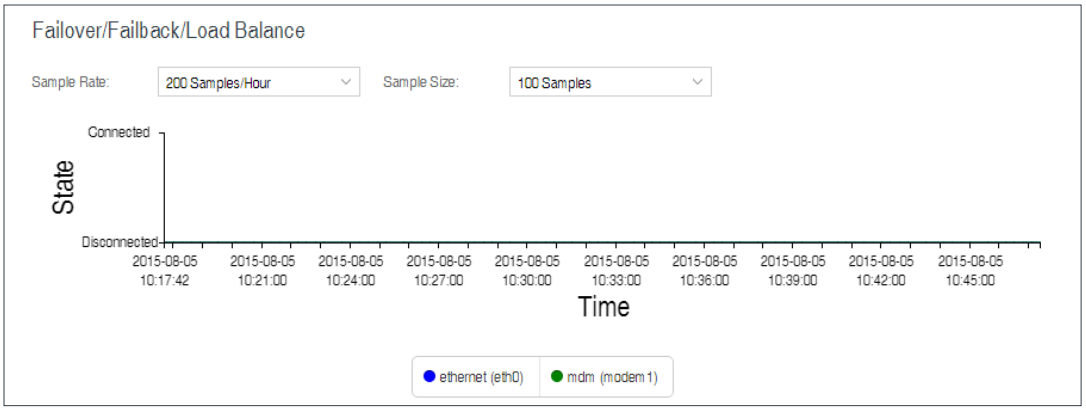
To reset information, click **Reset Statistics**.

STATISTICS

Statistics can be gathered at variable Sample Rate and Sample Size for the following areas:

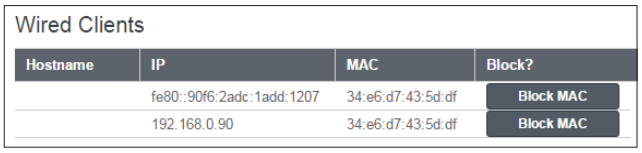
- Data Usage
- Failover/Failback/Load Balance





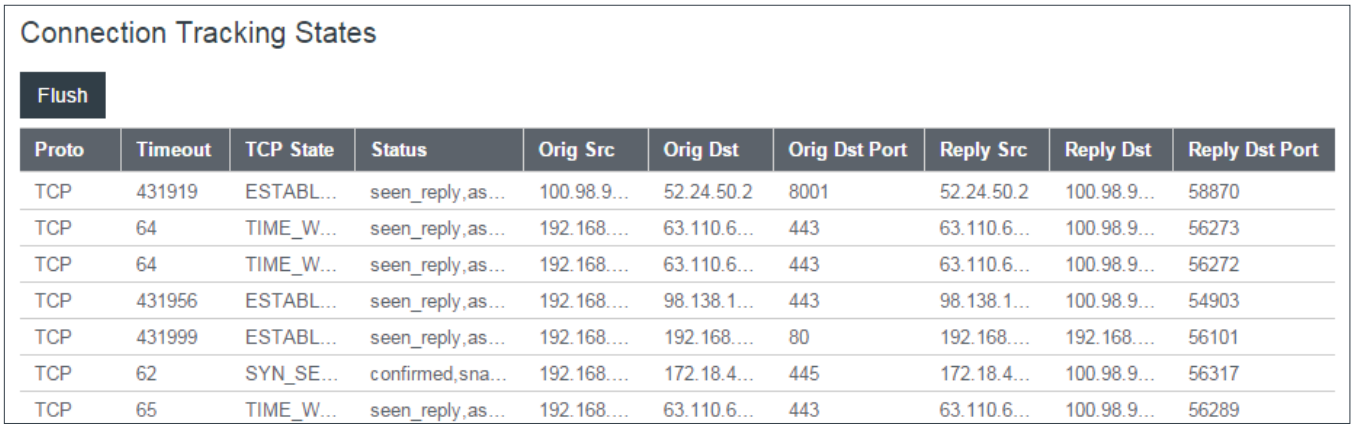
CLIENT LIST

Displays information about your Wired Clients and allows you to block MAC addresses of Wired Clients.



FIREWALL

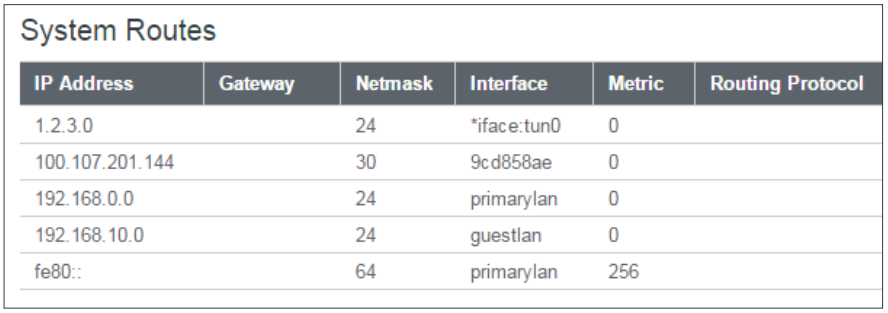
Displays information about your Firewall Connection Tracking States. To configure your firewall, select **SECURITY** from the left navigation.



Proto	Timeout	TCP State	Status	Orig Src	Orig Dst	Orig Dst Port	Reply Src	Reply Dst	Reply Dst Port
TCP	431919	ESTABL...	seen_reply,as...	100.98.9...	52.24.50.2	8001	52.24.50.2	100.98.9...	58870
TCP	64	TIME_W...	seen_reply,as...	192.168....	63.110.6...	443	63.110.6...	100.98.9...	56273
TCP	64	TIME_W...	seen_reply,as...	192.168....	63.110.6...	443	63.110.6...	100.98.9...	56272
TCP	431956	ESTABL...	seen_reply,as...	192.168....	98.138.1...	443	98.138.1...	100.98.9...	54903
TCP	431999	ESTABL...	seen_reply,as...	192.168....	192.168....	80	192.168....	192.168....	56101
TCP	62	SYN_SE...	confirmed,sna...	192.168....	172.18.4...	445	172.18.4...	100.98.9...	56317
TCP	65	TIME_W...	seen_reply,as...	192.168....	63.110.6...	443	63.110.6...	100.98.9...	56289

ROUTING

Displays information about your System, GRE, and NEMO Routes. To configure these routes, go to **NETWORKING > Tunnels**.



ETHERNET

Displays information about your Ethernet ports. To configure Ethernet ports, go to **NETWORKING > Local Networks > Ethernet Ports**.

Ethernet

Port	Link Status	Link Speed	PoE Power	PoE Class	PoE Detection	PoE Voltage	PoE Current
0	down	none	n/a	n/a	n/a	n/a	n/a
1	up	1000FD	n/a	n/a	n/a	n/a	n/a

GPS

Displays GPS location and status. To enable and configure GPS, go to **SYSTEM > Administration > GPS**.

LLDP

Displays LLDP information. To enable LLDP, go to **SYSTEM > Administration > LLDP**.

LLDP

Interface	Sys Name	Sys Descr.	Port Descr.	Manufacturer	Neighbor Info
No items to display					

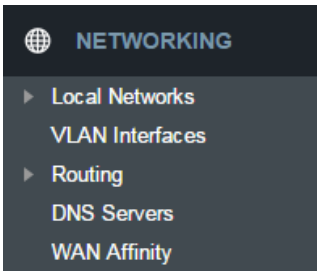
SYSTEM LOGS

Displays System Log information. To configure System Logging, go to **SYSTEM > Administration > System Logging**.

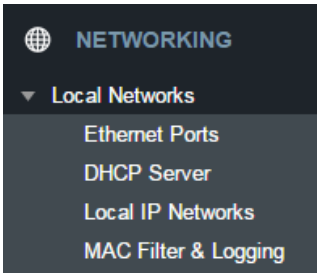
System Logs

Time	Source	Level	Message
Type to filter	Type to filter	Type to filter	Type to filter
Tue Sep 29th 09:52:05 2015	httpserver	INFO	Accepted web login from local address 192.168.0.90, user...
Tue Sep 29th 09:20:35 2015	WAN:9cd858ae.DHCP	INFO	ipinfo={'netmask': '255.255.255.248', 'ip_address': '100.105...
Tue Sep 29th 09:20:35 2015	udhcpc[413]	INFO	Lease of 100.105.91.251 obtained, lease time 7200
Tue Sep 29th 09:20:35 2015	udhcpc[413]	INFO	Sending renew...
Tue Sep 29th 08:28:51 2015	ecm	INFO	Updated status.ecm.info.Group
Tue Sep 29th 08:28:51 2015	ecm	INFO	Updated status.ecm.info.Account
Tue Sep 29th 08:28:50 2015	ecm	INFO	Config patch accepted on reconnect

NETWORKING



LOCAL NETWORKS



ETHERNET PORTS

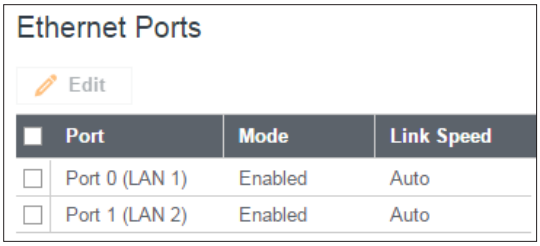
The CBA850 has two Ethernet ports for local network connections. LAN2 can also be used for PoE (optional). While default settings will be sufficient in most circumstances, you have the ability to control: **Mode** (Enabled or Disabled) and **Link Speed**. Additional controls for WAN ports are available in **CONNECTION MANAGER**.

NOTE: USB port may not be used for external modem if router is being run using PoE.

Mode: Enabled or Disabled.

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



To change port settings, select desired port and click **Edit**.

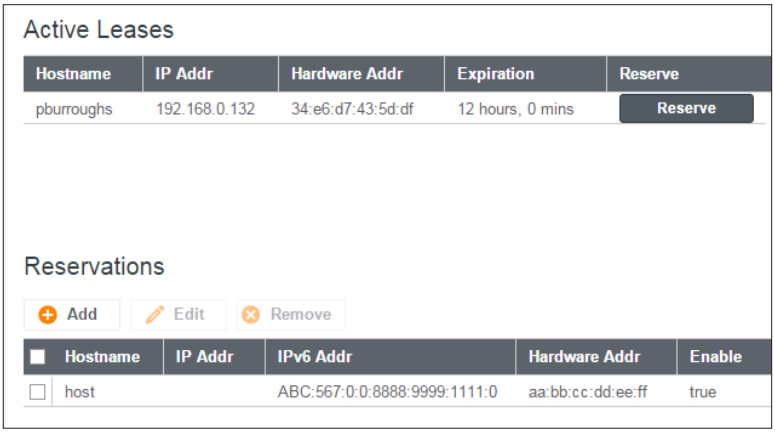
DHCP SERVER

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.

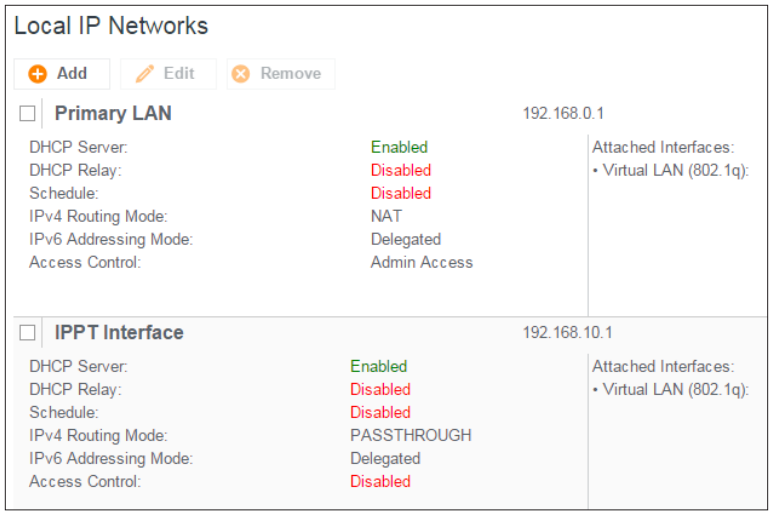


While you have the option to manually input the information to reserve an IP address (Hostname, Hardware Addr, IP Addr), it is much simpler to select a device under the **Active Leases** section and click "**Reserve**." The selected device's information will automatically be added under **Reservations**.

LOCAL IP NETWORKS

Local IP Networks displays the following information for each network:

- **Network Name**, **IP address/Netmask**, and **Enabled/Disabled** (along the top bar)
- **DHCP Server** (Enabled/Disabled)
- **DHCP Relay** (Enabled/Disabled)
- **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 ports, VLAN)



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

General Settings

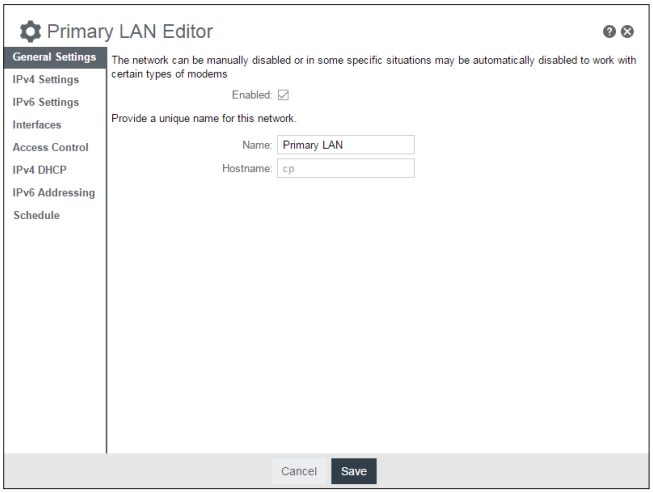
Enabled: The network can be manually disabled or in some specific situations may be automatically disabled to work with certain types of modems.
Name: The "name" property primarily helps to identify this network during other administration tasks.
Hostname: The hostname is the DNS name associated with the router's local area network IP address.

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.
Netmask: The netmask controls how many IP addresses can be used in this network. The default value is usually acceptable for most situations.

IPv4 Routing Mode: Each network can use a unique routing mode to connect to the Internet. The default of NAT is desirable in most configurations.

- **NAT:** Network Address Translation hides private IP addresses behind the router's IP address.
- **Standard:** Without NAT exposes the subnet addresses which requires them to be externally routable.
- **IP Passthrough:** IP Passthrough passes the IP address given by the modem WAN through the router. Hotspot, VPN, and GRE must be disabled.



IPv6 Settings

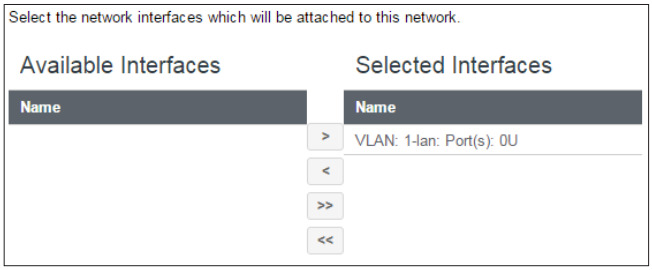
IPv6 Address Source: The Address source has three settings. The default of **Delegated** is desirable in most configurations.

- **Delegated:** The address is provided by a router connected to this router's WAN.
- **Static:** The address is provided by the router admin.
- **None:** No use of an IPv6 WAN address, IPv6 is disabled on the WAN.

IPv6 Address: An IPv6 Address is a unique numerical label for a computer or device using the Internet Protocol (IP). IPv6 addresses are typically in the format composed of 8 sets of 4 hexadecimal numbers. Leading zeros can be ignored and the longest set of continuous zeros can be replaced with **::**. For example, the IPv6 address of 0001:0000:0234:5678:0000:0000:9abc:0def can be expressed as 1:0:234:5678**::**9abc:def.

Interfaces

Select the network interfaces which will be attached to this network by either dragging desired interface or clicking left or right arrows to move them between **Available Interfaces** and **Selected Interfaces**.



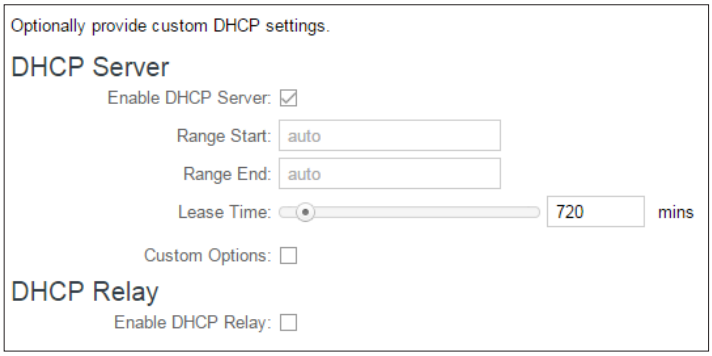
Access Control

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 admin pages from this network.

IPv4 DHCP

DHCP Server

- **Enable DHCP Server:** 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. Advanced DHCP server configuration is available at **NETWORKING > Local Networks > DHCP Server**.
- **Range Start:** The starting IP address in the DHCP Server range is the beginning of the reserved pool of IP addresses which will be given to any DHCP enabled computers on your network. The default value is almost always sufficient.
- **Range End:** The ending IP address in the DHCP Server range is the end of the reserved pool of IP addresses which will be given to any DHCP enabled computers on your network. The default value is almost always sufficient.



- **Lease Time:** The lease time specifies how long DHCP enabled computers will wait before requesting a new DHCP lease. Smaller values are better suited to busy environments.
- **Custom Options:** Send optional extra options to DHCP clients of this network. This can be used to, for example, set the boot TFTP server of a network for disk-less clients.

DHCP Relay

- **Enable DHCP Relay:** 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.

IPv6 Addressing
Address Configuration Mode: SLAAC stands for Stateless address autoconfiguration. A network can be configured to use SLAAC only, or it can be configured to also use DHCPv6 to provide ip addresses to clients.
DHCP Range Start: The DHCP Range Start is 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 which will be given to any DHCP enabled computers on your network.
IPv6 DHCP Lease Time: Specifies how long DHCP enabled computers will wait before requesting a new DHCP lease.

Schedule
Enable Schedule Service: Enable the interface scheduler. A schedule allows an interface to be enabled or disabled during specific hours of a day.

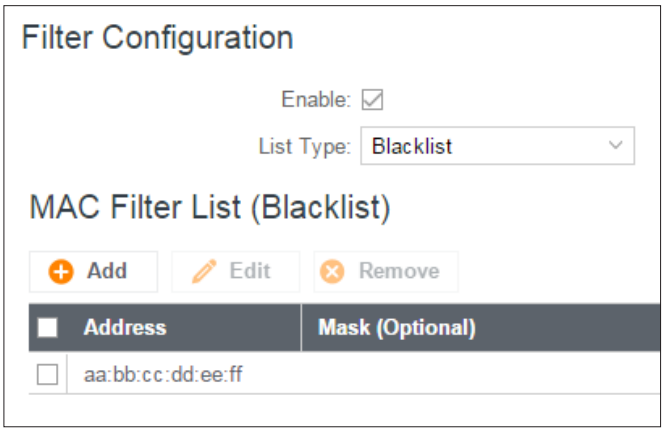
MAC FILTER & LOGGING

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.

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 local network.

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

MAC Filter List (Whitelist or Blacklist)

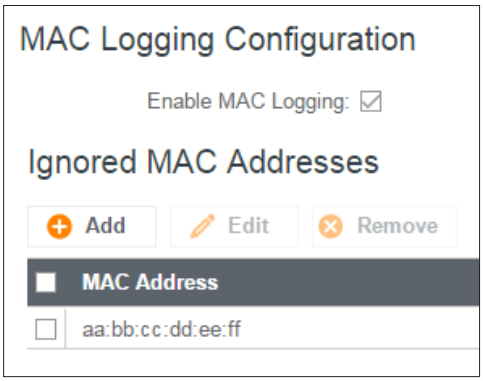


Add devices to either your whitelist or blacklist simply by inputting each device's MAC address.

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

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 > 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.

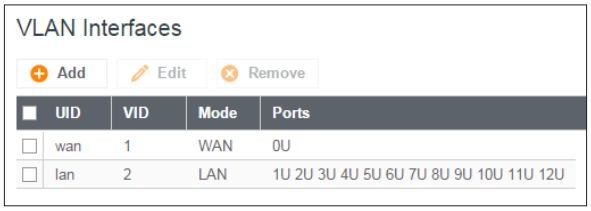
Double-clicking on entries from this list will add them to the **Ignored MAC Addresses** list.

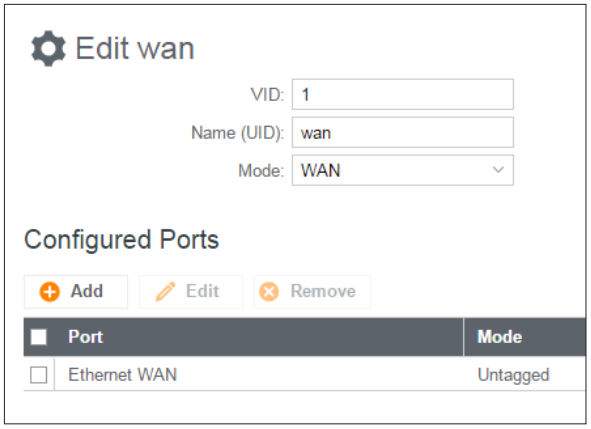
VLAN INTERFACES

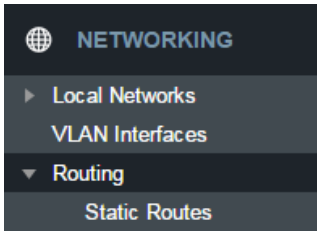
A virtual local area network, or VLAN, functions as any other physical LAN, but it enables computers and other devices to be grouped together even if they are not physically attached to the same network switch.

To enable a VLAN, select a VID (virtual LAN ID) and a group of Ethernet ports 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. To edit an interface, select the check box next to the desired interface.







ROUTING

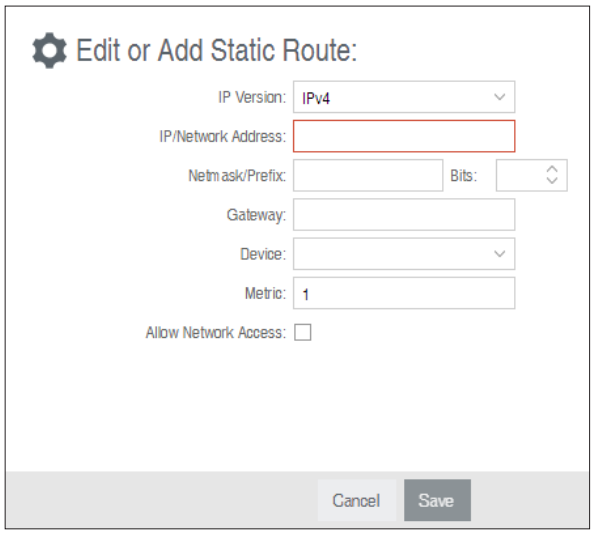
STATIC ROUTES

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 Version: Select IPv4 or IPv6. Depending on your selection, you have different options for defining the address range.



IP/Network Address or **IPv6 Address**: The IP address of the target network or host. The IPv6 address field includes **CIDR notation** to declare a range of addresses.

Netmask/Prefix: The Netmask, along with the IPv4 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.

Gateway or **IPv6 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**.

Device: Select the network interface from the dropdown menu (e.g. ethernet-wan). You can use this instead of defining the IP address, especially in cases when the IP address is changing.

Metric: Set the numerical priority of the route. Lower numbers have higher priority.

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.

DNS SERVERS

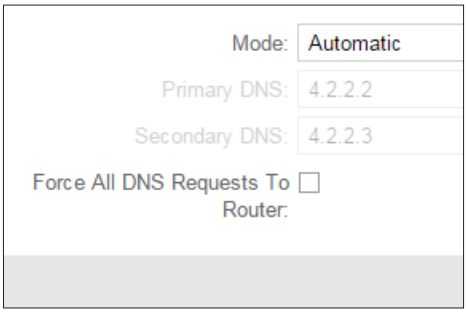
DNS, or Domain Name System, is a naming system that translates between domain names (www.cradlepoint.com, for example) and Internet IP addresses (206.207.82.197). A DNS server acts as an Internet phone book, translating between names that make sense to people and the more complex numerical identifiers. The DNS page for the device 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).
- **Split DNS**: Enable or disable the redirecting of specified domains to alternate DNS servers.
- **Dynamic DNS Configuration**: Allows you to host a server (Web, FTP, etc.) using a domain name that you have purchased (www.example.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.

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.

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

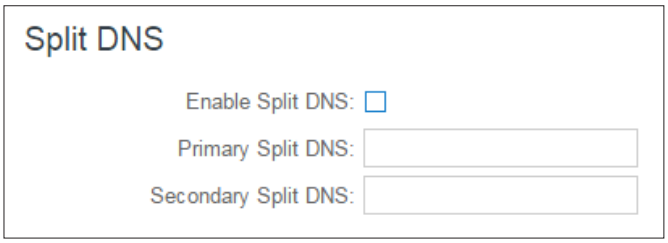


Primary DNS and **Secondary DNS**: If you choose to specify your DNS servers, then enter the IP addresses of the servers you want as your primary and secondary DNS servers in these fields. The DNS server settings will be pre-populated with public DNS server IP addresses. You can override the IP address 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.

Split DNS

Split DNS allows you create two zones for the same domain, one to be used by the internal network, the other used by the external network. Split DNS directs internal hosts to an internal domain name server for name resolution and external hosts are directed to an external domain name server for name resolution.

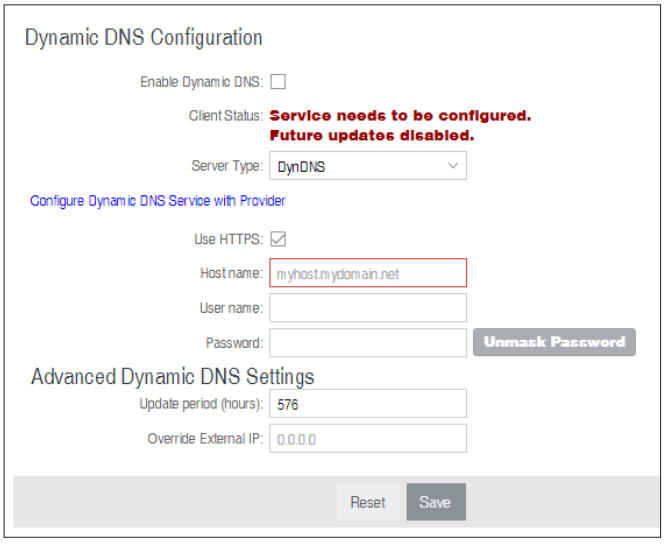


Primary Split DNS and **Secondary Split DNS**: If you choose to specify your DNS servers, then enter the IP addresses of the servers you want as your primary and secondary DNS servers in these fields. The Secondary DNS is optional.

Domain: Click **Add** to add desired domain for Split DNS.

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 dropdown list:
  - **DynDNS**
  - **DNS-O-Matic**
  - **ChangeIP**
  - **NO-IP**

- Custom Server (DynDNS clone)
- **Custom Server Address**. Only available if you select Custom Server from the Server Address dropdown list. Enter your custom DynDNS clone server address here. For example: www.mydyndns.org.
- **Use HTTPS**: Use the more secure HTTPS protocol. This is recommended, but can 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.

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.

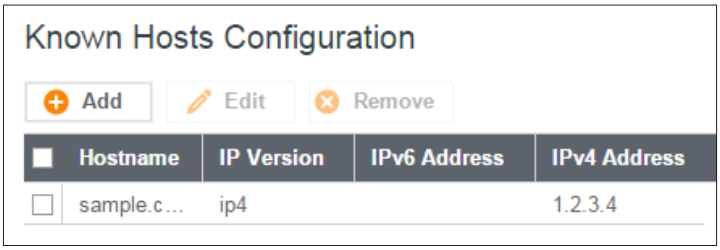
Known Hosts Configuration

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."

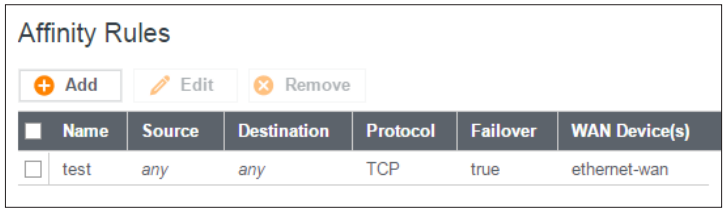
Since the assigned name is mapped to an IP address, the device's IP address should not change. To ensure that the device keeps the same IP address, go to **NETWORKING > Local Networks > DHCP Server** and reserve the IP address for the device by selecting the device in the **Active Leases** list and clicking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

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

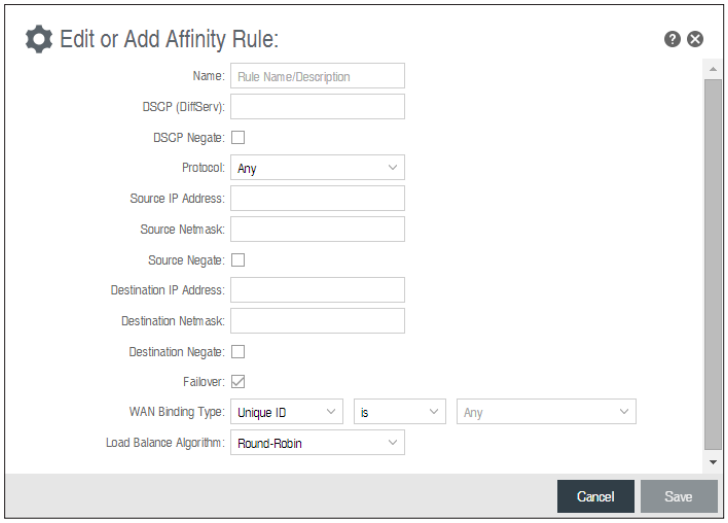
your primary LAN, your guest LAN will not take bandwidth from your primary LAN, saving you money.



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.

When	Condition	Value
Port	Is	USB Port 1
Type	Is not	WiMax

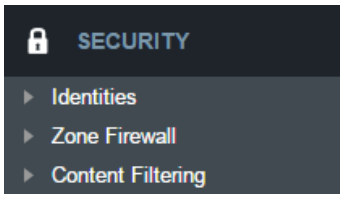
- **When**:
  - **Port** – Select by the physical port on the router that you are plugging the modem into (e.g., "USB Port 2").

  - **Manufacturer** – Select by the modem manufacturer (e.g., "Cradlepoint Inc.").
  - **Model** – Set your rule according to the specific model of modem.
  - **Type** – Select by type of Internet source (Ethernet, LTE, Modem).
  - **Serial Number** – Select a 3G or LTE modem by the serial number.
  - **MAC Address** – Select from a dropdown list of attached devices.
  - **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.

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

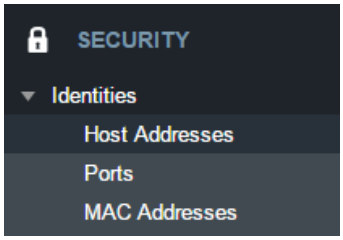
- **Round-Robin**: Evenly distribute each session to the available WAN connections.
- **Rate**: Distribute load based on the current upload and download rates. A WAN device's upload and download bandwidth values can be set in **CONNECTION MANAGER**.
- **Spillover**: This was the default algorithm in 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. 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 functioning 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.

SECURITY



IDENTITIES

Identities are reusable groups of items that are added to filter policy rules. A match on any single item in the group will cause the rule to match. Identities are referenced in rules by their name. Choosing descriptive names like “NW Sales Team” or “Engineering” will aid in understanding existing rules and in choosing identities for new rules.



HOST ADDRESSES

A Host identity can contain IPv4, IPv6, and Fully Qualified Domain Name addresses. A single identity can contain a combination of IPv4 and IPv6 addresses. IPv4/6 addresses cannot be combined with FQDN addresses in the same identity.

IP addresses are entered using CIDR notation, e.g. 1.2.3.4/32 and 0123:4567::CDEF/128. FQDN addresses are entered with at least one dot separating a top-level domain from a root zone, e.g. cradlepoint.com.

To add a Host Address Identity, click **Add**.

PORTS

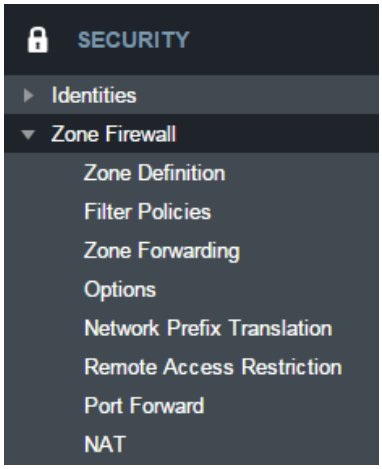
A port identity member can be entered as a single Start port number or as a port range by entering both a Start and End port number.

To add a Port Identity, click **Add**.

MAC ADDRESSES

MAC addresses are entered in the form aa:bb:cc:dd:ee:ff.

To add a MAC Address Identity, click **Add**.



ZONE FIREWALL

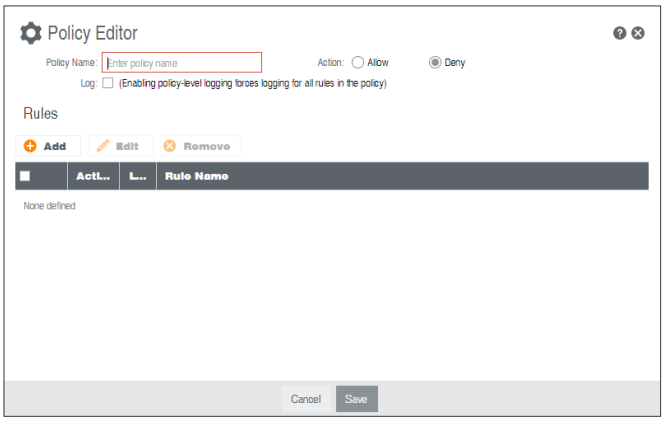
ZONE DEFINITION

A Zone is a group of network interfaces. By default all interfaces within a zone are allowed to initialize network communication with each other, however any network traffic initialized outside of a zone to the interfaces within the zone will be denied.

To add a zone, click **Add**.

FILTER POLICIES

A Filter Policy is a one-way filter applied to initialized network traffic flowing from one zone to another. A Filter Policy needs to be assigned to a Forwarding for it to take effect. Filter Policies can either be Added, Edited, or Removed.

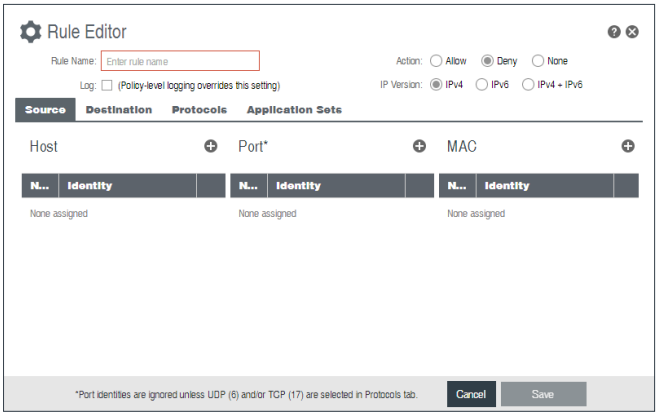


- **Default Allow All** is a preconfigured policy to allow all traffic initialized from one zone to flow to another zone. The state of the connection is tracked to allow responses to traverse the zones back to the source. LAN to WAN forwardings use this policy by default. The policy can be removed or altered to filter the traffic flow.
- **Default Deny All** is a preconfigured policy to deny all traffic initialized from one zone to be blocked to another zone. WAN to LAN forwardings use this policy by default. The policy can be removed or altered to filter the traffic flow.

Click **Add** to create a new filter policy, or select an existing policy and click Edit to open the filter policy editor.

- **Name**: Create a name meaningful to you.
- **Action**: Choose either **Allow** or **Deny**. This is the action taken by the firewall if none of the filter policy rules match the traffic being filtered.
- **Log**: When checked, every rule in the policy will log matching packets as if the rule's Log option had been selected.

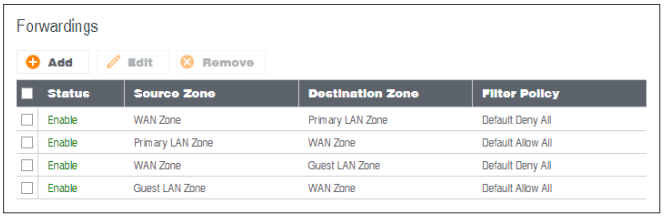
Click **Add** to create a new rule for this filter policy, or select an existing rule and click Edit to open the Rule Editor.



- **Name**: Create a rule name meaningful to you.
- **Action**: Choose either Allow or Deny. This is the action taken by the firewall if the rule criteria match the traffic being filtered.
- **Log**: When checked, each packet matching this filter rule will be logged in the System Log.
- **IP Version**: Select the IP version to match.
- Enter match criteria under **Source**, **Destination**, **Protocols** and **Application Sets**.
  - **Source**: Select defined identities or enter individual criteria for the appropriate **Host**, **Port** and **MAC** address columns to match the source of the traffic.
    - **Host**: Enter an IP address or select a host identity.
    - **Port**: Enter a port, port range, or select a port identity.
    - **MAC**: Enter a MAC address or select a MAC address identity.
  - **Destination**: Select defined identities or enter individual criteria for the appropriate Host, Port and MAC address columns to match the destination of the traffic. See **Source** for the column definitions.
  - **Protocols**: Select protocols (such as TCP, UDP, GRE, etc) from the defined list or enter a numeric code for other protocols to match traffic of that protocol.
  - **Application Sets**: Select the defined application set or sets to match traffic related to those sets.

ZONE FORWARDING

Forwardings define how Filter Policies affect traffic flowing between zones in one direction. Simply configure the Source Zone, Destination Zone, and Filter Policy to define a Forwarding. Forwardings can be Added, Edited, Removed, or Toggled. Toggling a Forwarding will either enable or disable the Forwarding.



Source and Destination zones are chosen from the list of Zone Definitions. In addition, two special zones can be selected for forwarding endpoints:

- The **All** zone will match any traffic handled by the router and is used as an endpoint for IP Filter Rules migrated from previous firmware versions. User editable zones are preferred when adding new forwardings.
- The **Router** zone will match any traffic initialized from or directed to router services and can be used to filter router service traffic. An example of traffic initialized by a router service would be the ECM Management service. An example of traffic destined to a router service would be the SNMP service.

OPTIONS

Firewall Options

- **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.
- **Log Web Access**: Enable this option to create a syslog record of web (IP port 80) access. Each entry will contain the the IP address of the server and the client. Note that this may create a lot of log entries, especially on a busy network. Sending the system log to a syslog server is recommended.

Application Gateways

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.

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

- **PPTP**: For virtual private network access using Point to Point Tunneling Protocol.
- **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. Not needed for passive mode.
- **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.

DMZ (Demilitarized Zone)

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, supporting older games, or sharing files.

NOTE: As with port forwarding, caution should be used when enabling the DMZ feature as it can threaten the security of your network.

NETWORK PREFIX TRANSLATION

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. But 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.

REMOTE ACCESS RESTRICTION

Add any IPv4 addresses that need access to remote administration to this list. Clicking **Add** will allow the addition of IP address and netmask pairs to the administration filter. **Edit** will allow you to change settings for the selected address. **Remove** will remove a selected entry.

PORT FORWARD

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.

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

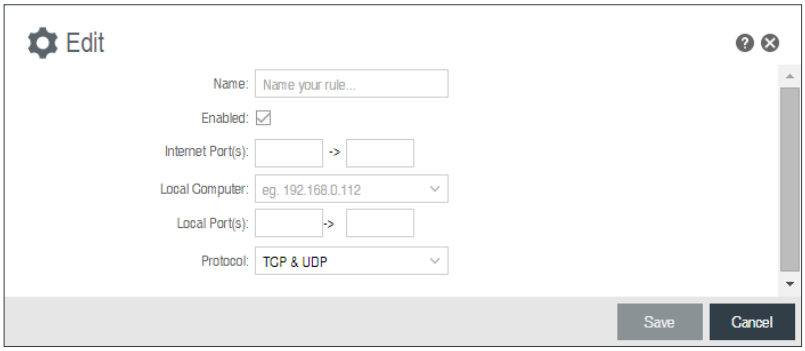
Click **Add** to create a new port forwarding rule, or select an existing rule and click **Edit**.

Add/Edit Port Forwarding Rule

- **Name**: Name your rule.
- Enabled: Toggle whether your rule is enabled. Selected by default.
- **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.
- **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:
  - **TCP**
  - **UDP**
  - **TCP & UDP**



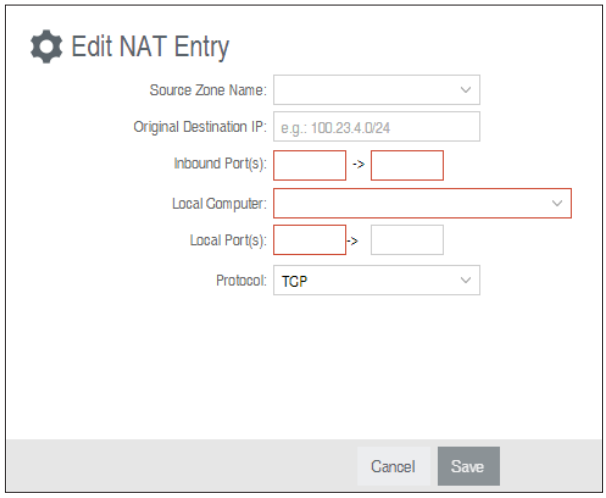
Click **Save** to save your completed port forwarding rule.

NAT

NAT is similar to Port Forwarding and provides that functionality by mapping ports available on interfaces associated with the Zone to ports available on local clients. NAT also has the ability to map many types interfaces selectable via a Zone. For example, GRE interfaces can be used to port forward traffic from the GRE endpoints to local client thereby limiting exposure to the local LAN while still gaining the benefits of GRE.

Click **Add** to create a Destination NAT.

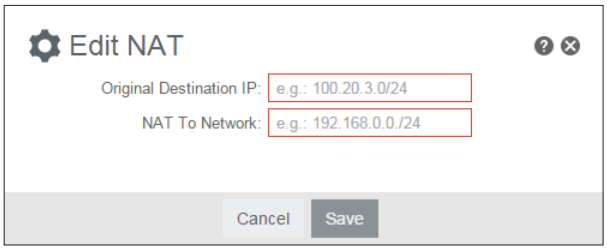
- **Source Zone Name:** The Zone created in Zone Firewall. Select the Zone to NAT.
- **Original Destination IP:** Specify which inbound traffic to this router will have the destination IP translated to an internal network.
- **Inbound Port(s):** Specify the IP port(s) on the inbound traffic to forward to a local computer.
- **Local Computer:** Specify the local computer to receive forwarded traffic.
- **Local Port(s):** Specify the IP port (first if a range) on the local computer to receive forwarded traffic.
- **Protocol:** Select the IP protocol traffic to forward.

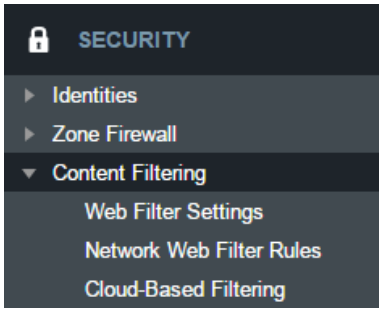


NAT

Dynamic NAT allows translating the destination IP of incoming network traffic to a local network. All ports and protocols will be forwarded. Netmasks should generally match. If the local network range is larger than the incoming destination range then network traffic will begin using port overloading. One-to-One NAT can be accomplished by specifying a host address or a /32 cidr address.

Click **Add** to create a NAT.





CONTENT FILTERING

WEBFILTER SETTINGS

General Settings

Enbable Webfilter: Selecting "Enable Webfilter" will enable the webfiltering service. This is used to enable or disable all router-based webfiltering and forwarding.

Filter HTTPS: Selecting "Filter HTTPS" enables redirection of all port 443 traffic into the proxy. The proxy will then extract the host name from the SNI (Server Name Indication). If SNI is unavailable then the original destination IP address is used for filtering. No decoding of the SSL/TLS session is done.

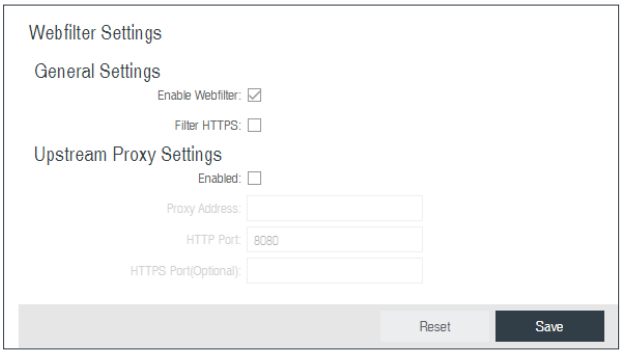
Upstream Proxy Settings

Enabled: Select whether the use of an Upstream Proxy server is enabled.

Proxy Address: The Proxy Address is the address the desired HTTP proxy is hosted at. Addresses can be input as host names or as ip addresses. If the proxy is unavailable HTTP traffic will fail to cross the network and a notification page will be shown.

HTTP Port: The port the HTTP Proxy is listening on.

HTTPS Port (Optional): The port for the proxy to forward HTTPS traffic to. HTTPS is not transparently intercepted and must have the LAN clients configured to use the Cradlepoint router as a proxy for HTTPS to work properly.



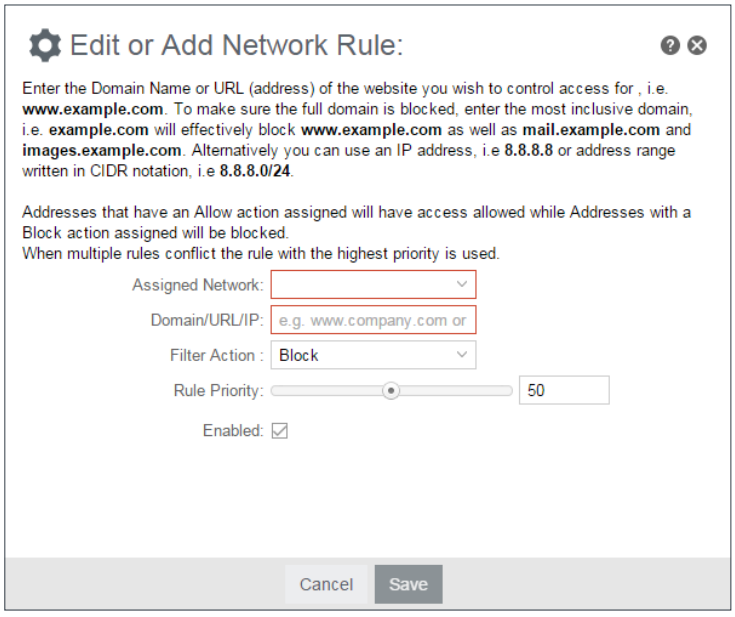
NETWORK WEB FILTER RULES

Domain / URL filter rules allow you to control access from your network to any external domain or website. Rules are assigned to a specific LAN network and the highest priority rule will have precedence when there is a conflict. Addresses can be added by URL/Domain name or by IP address. IP address ranges can be filtered by using CIDR notation, e.g. 4.2.2.2/24.

Exceptions to existing rules can be created by adding another rule with higher priority. For example if access to maps.example.com is desired, but example.com is blocked with a priority of 50. The addition of an allow rule for maps.example.com with a priority of 49 or less 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.

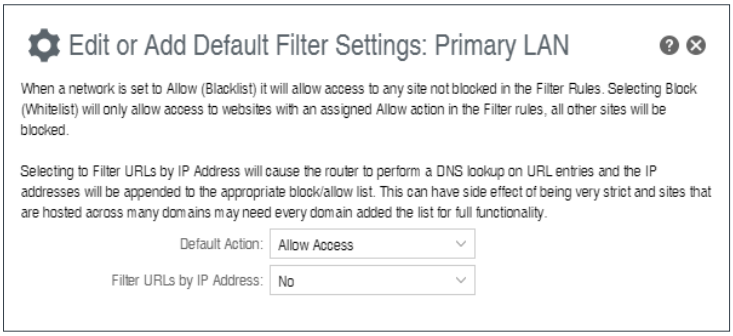
To add a Network Web Filter Rule, click **Add**.



Default Network Filter Settings

When a network is set to Allow (Blacklist) it will allow access to those sites not blocked in the Filter Rules. Selecting Block (Whitelist) will only allow access to websites with an 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.

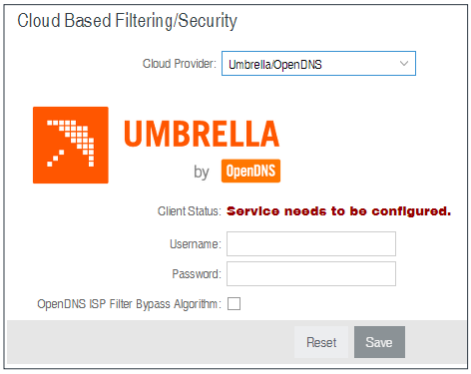


The settings can be changed by selecting a network and clicking the **Edit** button.

CLOUD-BASED FILTERING

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

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

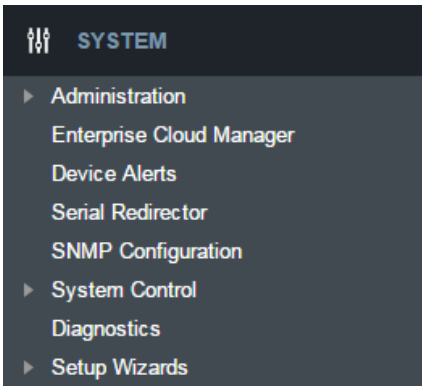


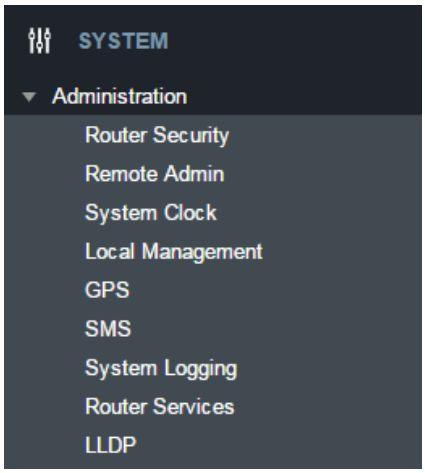
Umbrella by OpenDNS
Umbrella by OpenDNS is a cloud-based web filtering and security solution that protects you online by filtering websites. Go to **http://www.opendns.com/business-security** for information about Umbrella.

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.

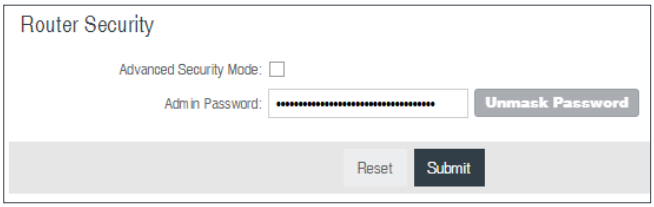
SYSTEM





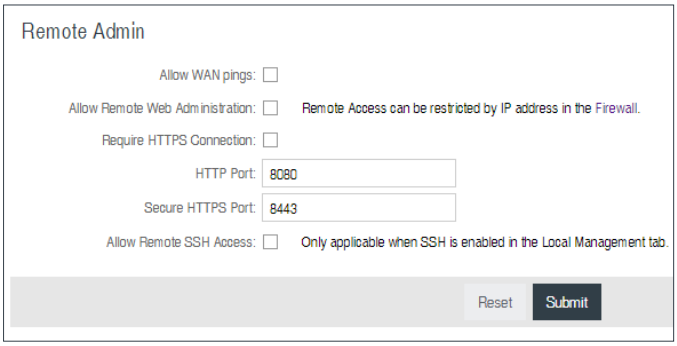
ADMINISTRATION

ROUTER SECURITY



When the router is configured to use the advanced security mode, several aspects of the routers 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.

REMOTE ADMIN



Remote Management allows a user to enable incoming WAN pings or 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.

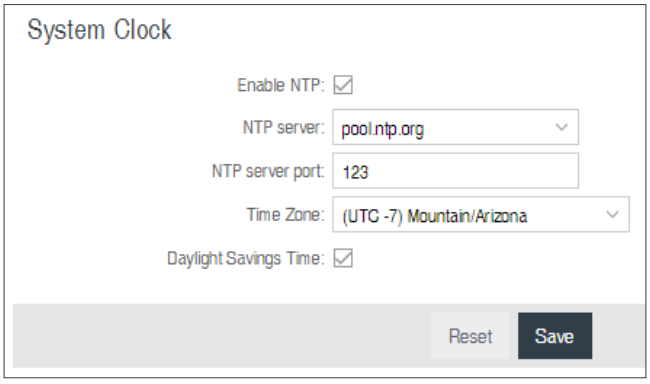
NOTE: You can restrict remote access to only specified IP addresses in **SECURITY > Zone Firewall > Remote Access Restriction**.

Allow Remote SSH Access – This will enable SSH access to the router from the Internet. It is only available when 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.

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.

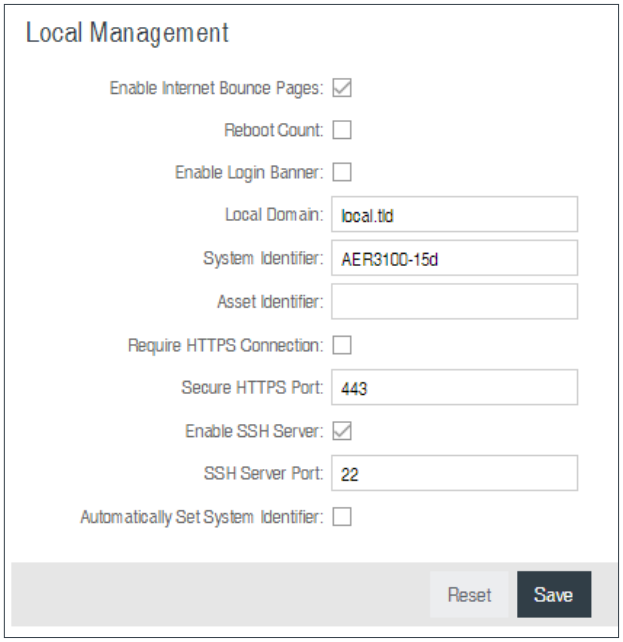
You then have the option of selecting an NTP server and adjusting the NTP server port. Select the NTP server from the dropdown list. Any of the given NTP servers will be sufficient unless, for example, you need to synchronize your router's time with other devices in a network.



- **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.

LOCAL MANAGEMENT

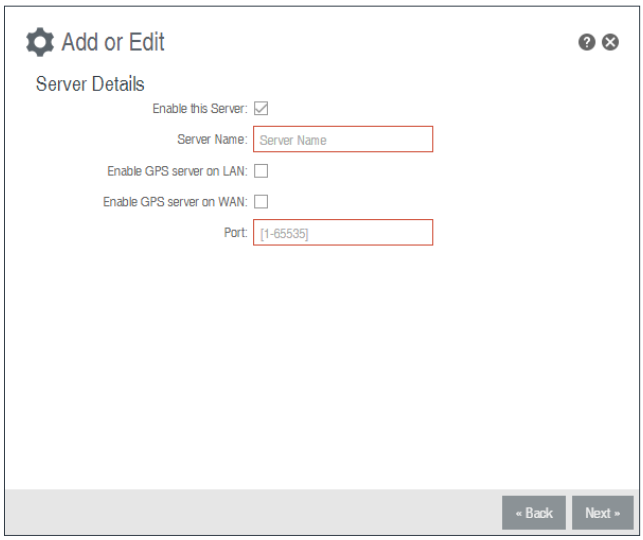
- **Enable Internet Bounce Pages** – Bounce pages show up in your web browser when the router is not connected to the Internet. They inform you that you are not connected and try to explain why. If you disable bounce pages then you will just get the usual browser timeout. In the normal case when the router is connected to the Internet you don't see them at all.
- **Reboot Count** – Track number of router reboots.
- **Enable Login Banner** – 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 product name and the last three characters of the MAC address of the router.
- **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.
- **Automatically Set System Identifier** – This will 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.

GPS

If you have an attached device with GPS support, you can enable a graphical view of your router's location, which appears in **STATUS > GPS**. SIM-based models with GPS support require that the SIM be inserted. 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.

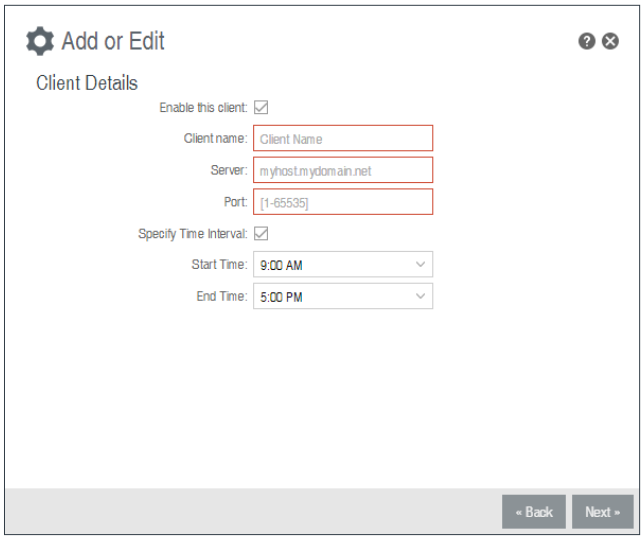


Enable GPS – Enable support for querying GPS information from capable modems.

Send to Client(s)

- **Enable this Server** - Enables a local server to which clients can connect and recieve GPS sentences.
- **Server Name** - Your server's name should include only Aa-Zz, numerals, and '_'.
- **Enable GPS server on LAN** - Enables a server on the LAN side of the firewall which will periodically send GPS sentences to TCP connected clients.
- **Enable GPS server on WAN** - Enables a server on the WAN side of the firewall which will periodically send GPS sentences to TCP connected clients.
- **Port** - Choose a port between 1 and 65535.

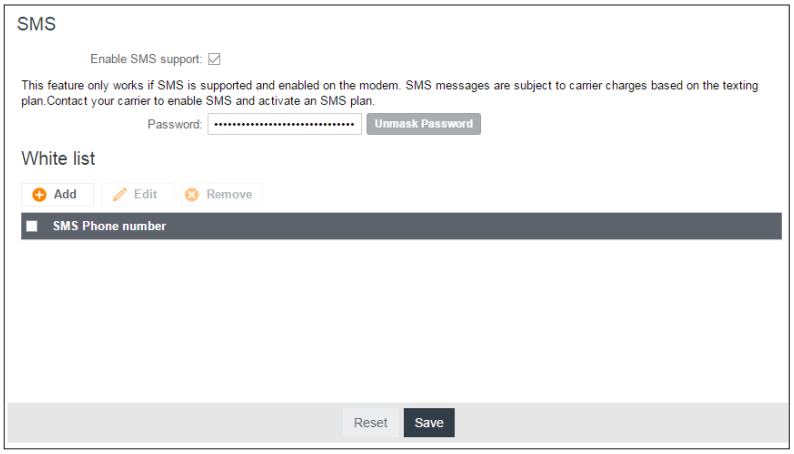
Send to Server(s)



- **Enable this client** - Enables periodic reporting of GPS sentences to a remote server. The router will buffer GPS sentences if errors are encountered or if the Internet connection goes down, and send the buffered sentences when the connection is restored.
- **Client name** - Your client's name should include only Aa-Zz, numerals, and '_'.
- **Server** - Remote server hostname or IP.
- **Port** - Remote server port.
- **Specify Time Interval** - Restricts the GPS sentence reporting to a remote server to a specific time interval.
- **Start Time** - Reporting start time.
- **End Time** - Reporting end time.

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.

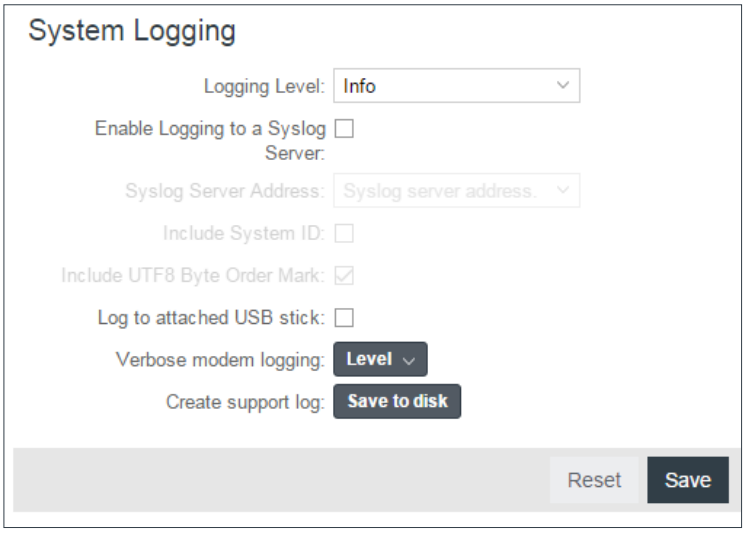
SYSTEM LOGGING

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**

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.

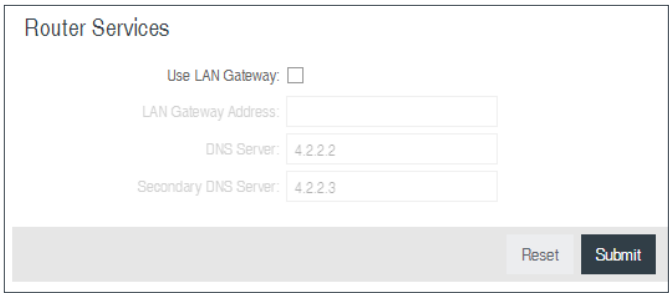
Log to attached USB stick: Only enable this option if instructed by a Cradlepoint support agent. This will write a very verbose log file to the root level of an attached USB stick. Please disable the feature before removing the USB stick, or you may lose some logging data.

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.

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.

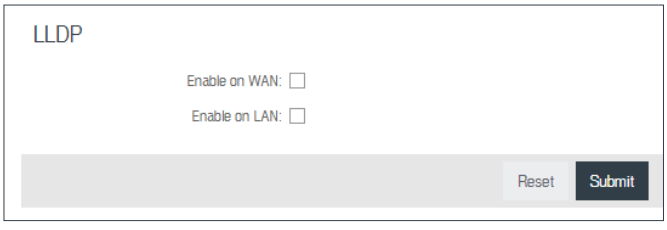


DNS Server and **Secondary DNS Server**: The primary and secondary DNS server numbers match the static DNS values (set at **NETWORKING > DNS Servers**). You can leave the default values or set them manually here. (Changing these values also changes the static DNS values.)

LLDP

The **Link Layer Discovery Protocol** (LLDP) is a standard method for network devices to share information about themselves among their neighbors. The router stores the information it receives from its neighbors, which can be viewed on the **STATUS > LLDP** page.

Enable LLDP for Ethernet on the WAN and/or LAN.



ENTERPRISE CLOUD MANAGER

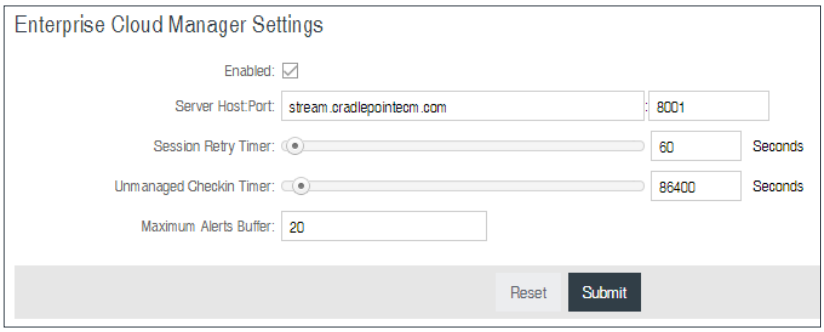
Cradlepoint **Enterprise Cloud Manager** (ECM) is a cloud-based management service for configuring, monitoring, and organizing your Cradlepoint routers. Key features include the following:

- 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

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).

Enterprise Cloud Manager Settings (Advanced)



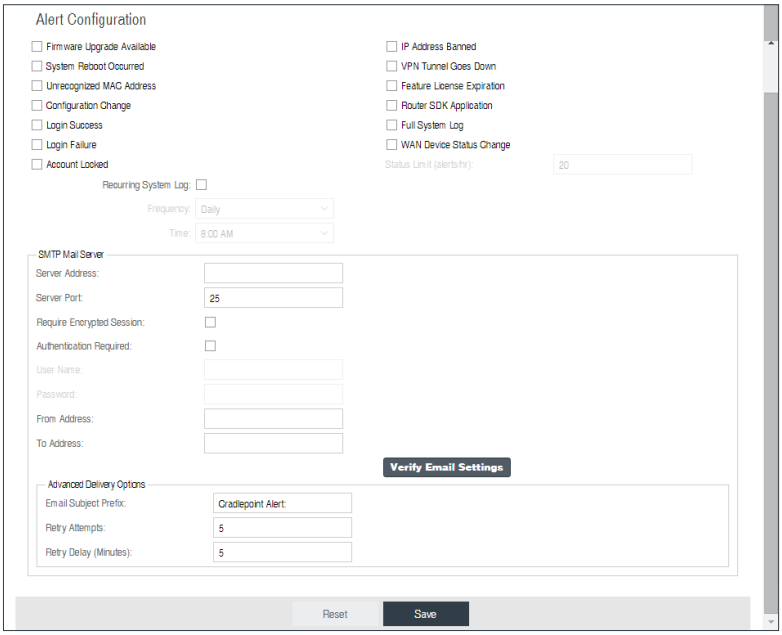
- **Enabled**: Enable the ECM client to contact the server. While this box is unchecked, the ECM client will never attempt to contact the server. (Default: Enabled)
- **Server Host:Port**: The DNS hostname and port number for your ECM server. (Default: stream.cradlepoint.com)
- **Session Retry Timer**: 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.

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**: Account has been locked due to excessive failed login attempts.
- **IP Address Banned**: An IP address has been banned.
- **VPN Tunnel Goes Down**: Sends an alert when a VPN tunnel goes down.
- **Feature License Expiration**: Sends an alert when a feature license is about to expire.
- **Router SDK Application**: A router SDK Application may send an alert.
- **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 (**Frequency**). You also choose the **Time** you want the alert sent.

SMTP Mail Server

Since your router 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 router 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.

Delivery Options (Advanced)

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

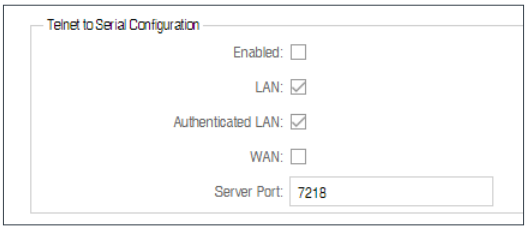
Retry Attempts: The number of attempts made to send an alert to the mail server. After the attempts are exhausted, the alert is discarded.

Retry Delay: The delay between retry attempts.

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.

Telnet to Serial Configuration

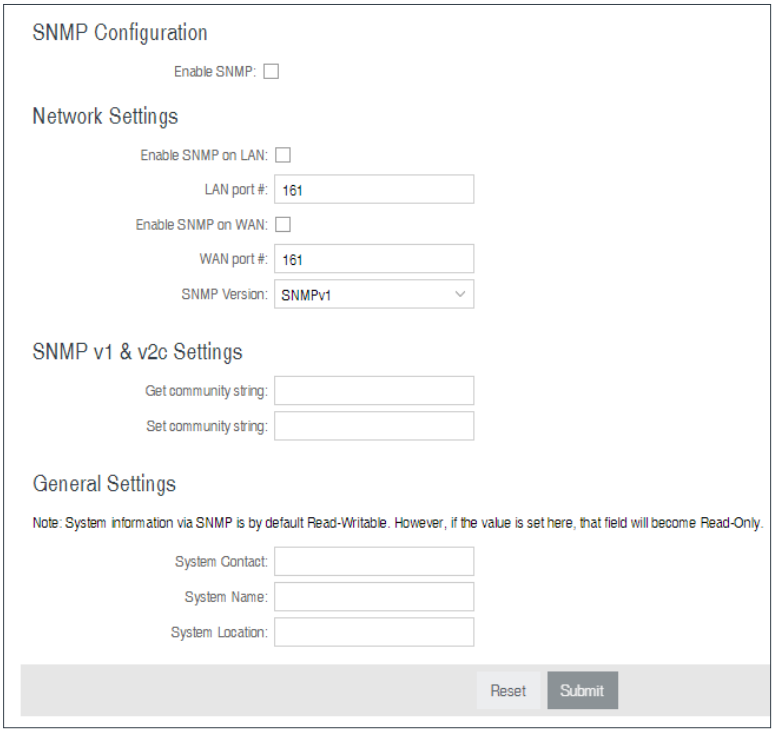


- **Enabled**: Enabling Telnet to Serial will start a Telnet server that passes its connection to the serial adapter. Enabling this service is not necessary when accessing serial through SSH.
- **LAN**: Enable serial redirector for LAN connections.
- **Authenticated LAN**: Enable serial redirector for 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)

SNMP CONFIGURATION

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

SNMP Configuration



- **Enable SNMP**: Selecting "Enable SNMP" will reveal the router's SNMP configuration options.

Network Settings

- **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)
- **SNMP Version**
  - **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.

SNMP v1 & v2c Settings

- **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."

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**
- **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)

General Settings

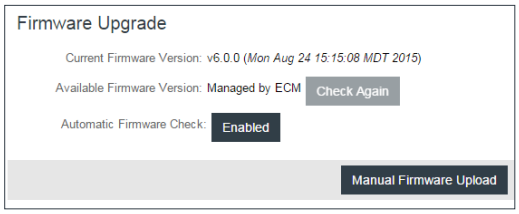
System information via SNMP is Read-Writable by default. However, if a value is set here, that field will become Read Only.

- **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.

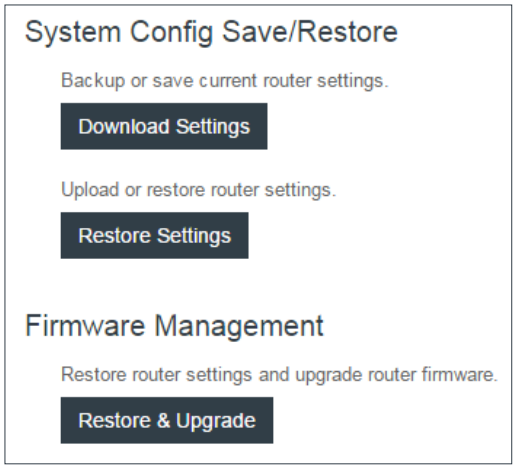
SYSTEM CONTROL

SYSTEM FIRMWARE

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 (cradlepoint.com/firmware) for information to decide if you should upgrade.



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 for the newest firmware.
Automatic Firmware Check: Automatically check for new firmware updates once daily.
Manual Firmware Upload: Upload the router firmware from an attached computer. (Go to **cradlepoint.com/firmware** to download the firmware.)



System Config Save/Restore
Download Settings: Click on "**Dowload Settings**" to save your current settings to a file on a computer.
Restore Settings: Click on "**Restore Settings**" to restore your previous settings from a file on a computer.

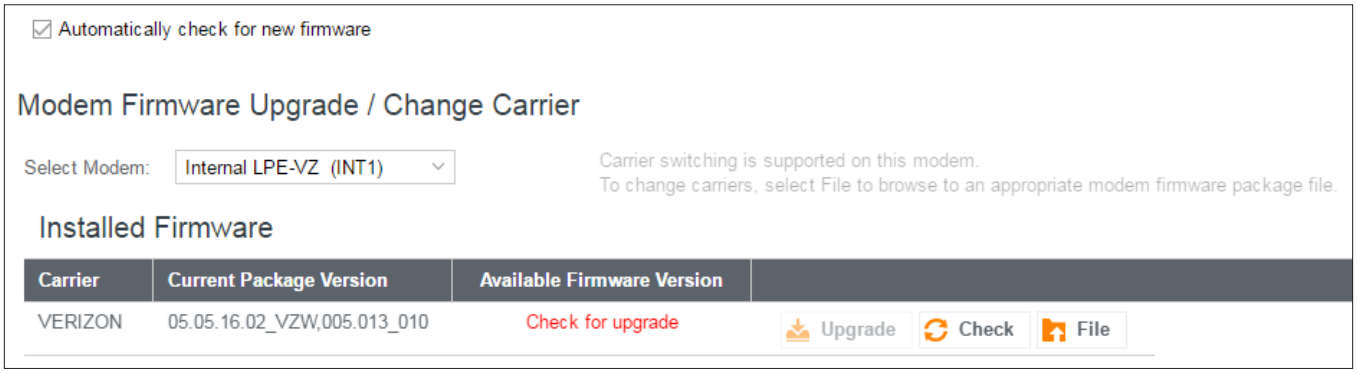
Firmware Management
Load new firmware and restore your previous settings from a file on a computer without rebooting between steps.

MODEM FIRMWARE

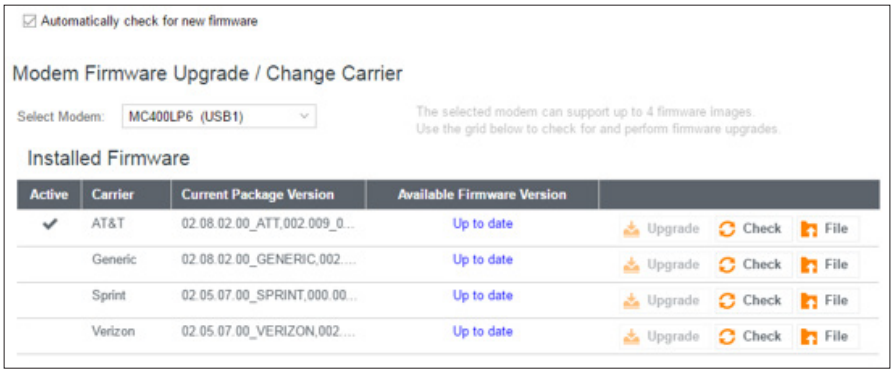
This allows the administrator to load new firmware onto Cradlepoint modems attached to the router. Note that modem firmware is separate from router firmware. New modem firmware may be necessary to update the module due to carrier updates or defect resolution. If you are happy with the operation of the modem, you may not want to upgrade just because a new version is available. Please check the modem firmware release notes for information to decide if you should upgrade or not.

Most Cradlepoint modems contain a single firmware image that can be Checked, Updated or manually updated. With some modems (such as LPE), you have the ability to change the firmware to support a different carrier image. With other select modems (such as LP6), more than one modem firmware image may be locally stored within the device's memory.

You must first select the Cradlepoint modem you would like to update. Once selected, the appropriate modem firmware update options will display.



For modems supporting manual carrier switching (such as LPE), select **File** to browse to an appropriate, different modem firmware package file to load into the modem's memory.



Firmware updates can be performed on any firmware line item using the **Check/Upgrade** or **File** (manual) process.

The following actions are available to be configured:

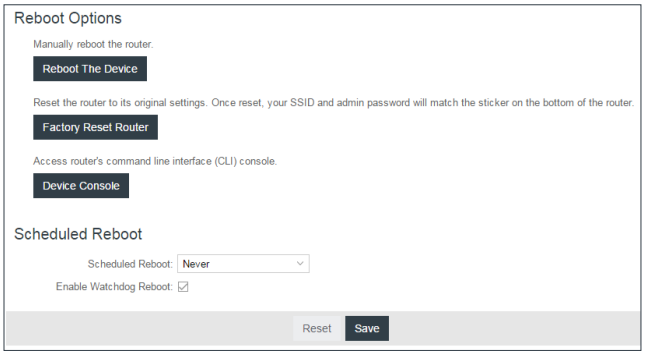
- **Automatically check for new firmware:** Click the checkbox to indicate whether the system is to automatically check for available modem firmware updates. When enabled, the system checks once a day. This global setting applies to all modems connected to the router.
- **Select Modem:** Select the appropriate modem which you would like to update. Note that dual SIM devices are listed as a single modem.

In the Installed Firmware grid, you will see the following columns:

- **Active (Multi-firmware modems only):** Indicates which carrier package is currently active on the modem. *Note: You cannot select the active image. On multi-firmware modems, the carrier firmware is selected automatically.*
- **Carrier:** Displays the carrier supported by the modem firmware. For carriers not otherwise available, "Generic" will be displayed.
- **Current Package Version:** Displays the current firmware package version loaded on the modem.
- **Available Firmware Version:** Displays the firmware version available for upgrade or indicates status of the current firmware. If new firmware is available, the available upgrade version is displayed.
- **Upgrade:** Click this button to download the Available Firmware Version file and perform this over-the-air upgrade. If a connection error occurs, it is possible that HTTPS is blocked for the upgrade check. Enable Allow HTTP Firmware Check in **SYSTEM > System Control >System Firmware** to address this issue.
- **Check:** Click this button to refresh or update the Available Firmware Version status column.
- **File:** Click this button to manually upload a modem firmware file. Type the path/file or click Select Firmware File to browse to the local file location. Once entered, click Begin Firmware Upgrade. *Note: For modems which support manual carrier switching, find the appropriate modem firmware package file via ECM or the Cradlepoint portal.*

DEVICE OPTIONS

Reboot Options



- **Reboot the Device**: Manually restart the router.
- **Factory Reset Router**: Reset the router to its original settings. Once reset your SSID and admin password will match the sticker on the bottom of the router.
- **Device Console**: Access router's command line interface (CLI) console.

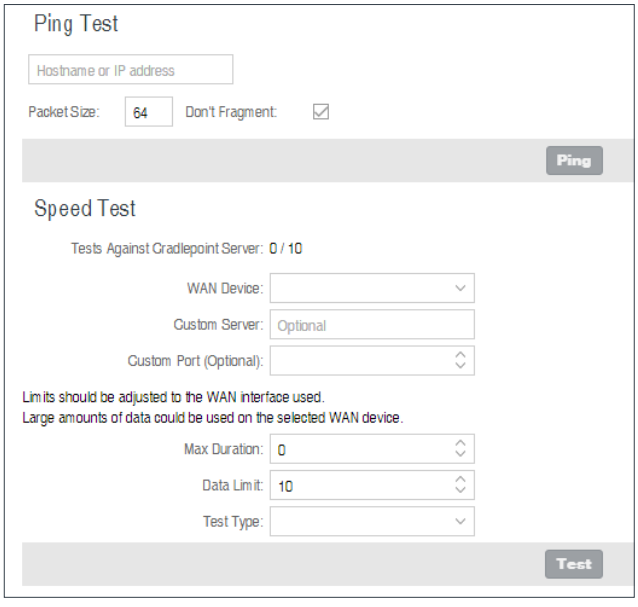
Scheduled Reboot

- **Scheduled Reboot**: Router will restart at user-specified time.
- **Enable Watchdog Reboot**: Router will restart when it determines an unrecoverable error condition has occurred.

DIAGNOSTICS

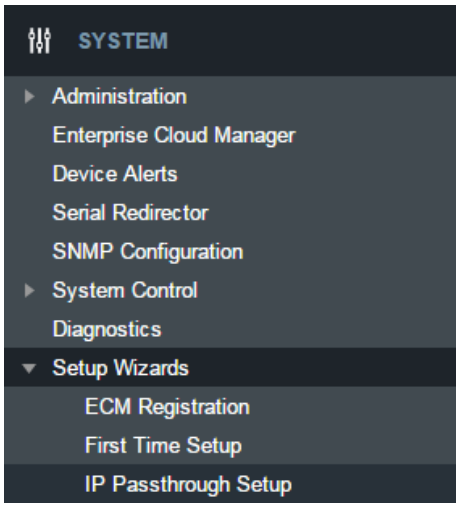
Ping Test

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



Speed Test

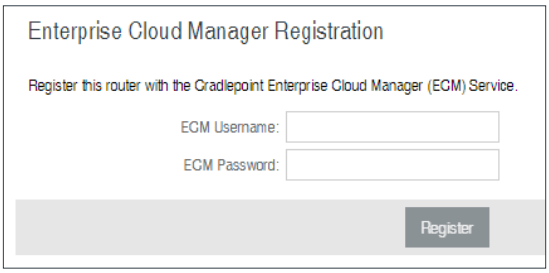
- **Tests Against Cradlepoint Server** - Up to ten speed tests are permitted against a Cradlepoint server.
- **WAN Device** - The WAN Device that is selected will have the test run on it. If no device is selected then the highest priority connected device will be used.
- **Custom Server** - Type the Hostname or IP address of the server to which you wish to perform a test. If left empty the test will be done to a Cradlepoint server.
- **Custom Port (Optional)** - The port to which the test is directed.
- **Max Duration** - The Max Duration is the Maximum amount of time for which the test should be run. The test may finish sooner if sufficient data is collected.
- **Data Limit** - The Data Limit is the limit of how much data will be transferred while measuring the connection speed; this should be limited to reduce the expense of a speed test. Setting the limit to 0 will cause the test to run until enough data is collected or the duration limit is met.
- **Test Type** - Select the type of test you would like to run. TCP Upload will test speed going to the server, TCP Download will test speed coming to the client, and UDP will measure the speed going to the server.



SETUP WIZARDS

ECM REGISTRATION

To register the router with Cradlepoint ECM you must first have an account. If you need to create an account you can signup at **cradlepoint.com**.



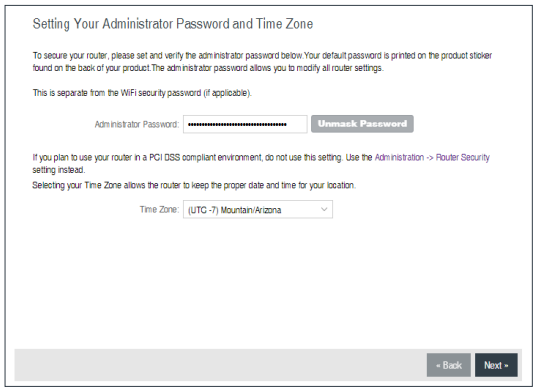
Once you've created an account, or if you already have one, you can enter your ECM username and password to register the router.

FIRST TIME SETUP

Administrator Password and Time Zone

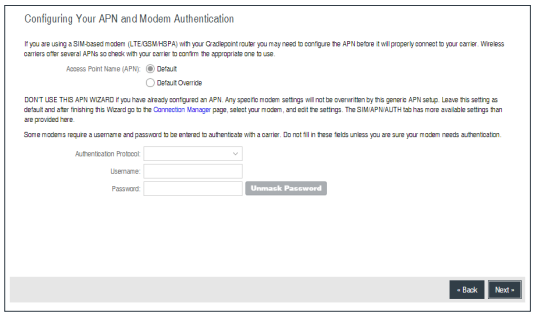
Enter a password for the administrator who will have full access to the router's management interface.

You can use the default password on the back of your product, or you can create a custom Administrator Password.



Configuring Your APN and Modem Authentication

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. You can use the default password on the back of your product, or you can create a custom Administrator Password.



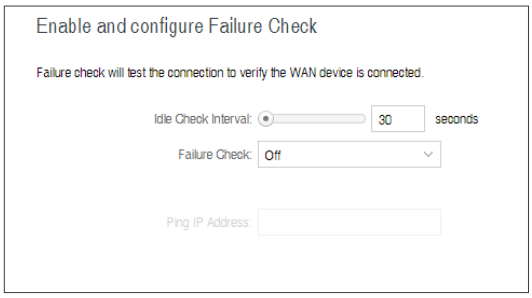
NOTE: *DO NOT USE THIS APN WIZARD* if you have already configured an APN. Any specific modem settings will not be overwritten by this generic APN setup. Leave this setting as default and after finishing this Wizard go to the **CONNECTION MANAGER** page, select your modem, and edit the settings. The SIM PIN/APN tab has more available settings than are provided here.

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

- Authentication Protocol
- Username
- Password

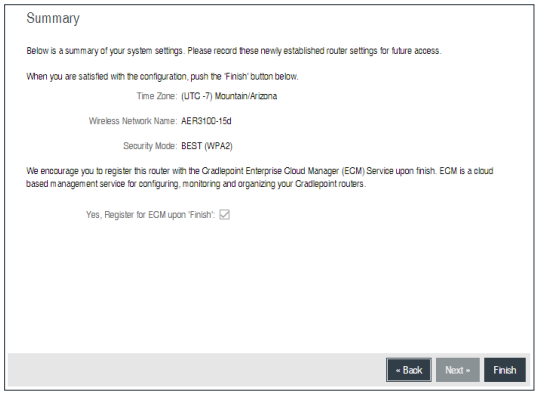
Enable and Configure Failure Check

Failure check will test the connection to verify the WAN device is connected.



- **Idle Check Interval**: Set the number of seconds the router will wait between checks to see if the WAN is still available.

- **Failure Check**:
  - **Off**: Once the link is established the router takes no action to verify that it is still up.
  - **On**: Modems will be set to use the Passive DNS failure check type. Ethernet connections will be set to use Active Ping.
- **Ping IP Address**: This IP address 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.

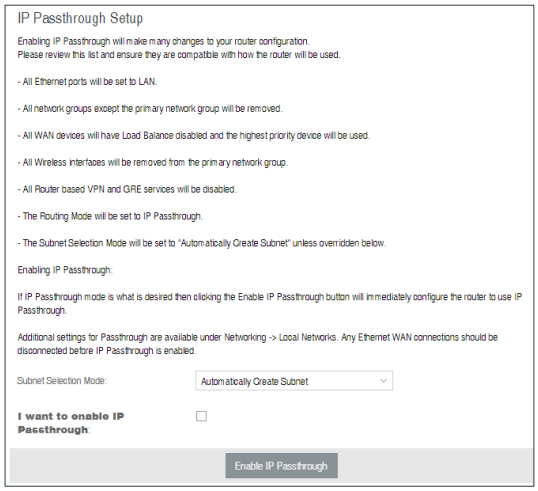


Summary
Review your settings and click **Finish** to exit or **Back** to edit.

IP PASSTHROUGH SETUP

IP passthrough takes a 3G/4G WAN data source (USB, ExpressCard, or Cradlepoint business-grade modem) and passes the IP address through to Ethernet LAN.

Enabling IP passthrough will make many changes to your router configuration. Please review this list and ensure they are compatible with how the router will be used.



- All Ethernet ports will be set to LAN
- All network groups except the primary network group will be removed
- All WAN devices will have Load Balance disabled and the highest priority device will be used
- All Router based VPN and GRE services will be disabled
- The Routing Mode will be set to IP Passthrough
- The Subnet Selection Mode will be set to "Automatically Create Subnet" unless overridden via the **Subnet Selection Mode** dropdown

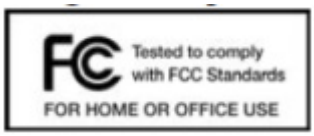
Any Ethernet WAN connections should be disconnected before IP passthrough is enabled.

APPENDIX

SAFETY, REGULATORY, AND WARRANTY GUIDE

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 and 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.

Purchaser agrees to indemnify Cradlepoint against any liability or damages caused to third parties as a result of Purchaser's misuse or misapplication of the Cradlepoint product.

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.

WARRANTY INFORMATION

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.

LIMITATION OF CRADLEPOINT LIABILITY

The information contained in this Safety, Regulatory, and Warranty 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; OR (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 THE DEVICE, REGARDLESS OF THE NUMBER OF EVENTS, OCCURRENCES, OR CLAIMS GIVING RISE TO LIABILITY, EXCEED THE PRICE PAID BY THE ORIGINAL PURCHASER OF THE DEVICE.

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, contact Cradlepoint at **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 **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.

ROUTER COMMUNICATION/DATA USAGE

The factory default configuration of the router is set to communicate with Cradlepoint and other resources at regular intervals to access the latest firmware and modem updates, clock synchronization (NTP), and Enterprise Cloud Manager (ECM) membership. Such communication may result in data usage and applicable charges regardless of whether the router uses a wired or wireless Internet connection. To avoid such data usage and potential charges, consult the following Knowledge Base article:

http://knowledgebase.cradlepoint.com/articles/support/router-communication-data-usage