CRADLEPOINT MBR1400

PRODUCT MANUAL

Mission-Critical Broadband Router

with **VPN Support**

ARC MBR1400 Series

Integrated Business Series Routers with 3G/4G

MBR1400LE-VZ
MBR1400LP-AT
MBR1400LP2-EU
MBR1400LP
MBR1400W

for additional information, visit:
knowledgebase.cradlepoint.com

Preface

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

Manual Revisions

Revision	Date	Description	Author
1.0	July 28, 2011	Initial release for Firmware version 3.2.4	Jeremy Cramer
1.1	Aug. 22, 2011	Updates for Firmware version 3.3.0	Jeremy Cramer
1.2	Jan. 20, 2012	Updates for Firmware version 3.4.1 and ARC versions	Jeremy Cramer
1.3	May 1, 2012	Updates for Firmware version 3.5.0	Jeremy Cramer
1.4	May 15, 2012	Updates for Firmware version 3.6.0	Jeremy Cramer
2.0	Dec. 28, 2012	Updates for Firmware version 4.1.1 and ARC MBR1400LP-AT	Jeremy Cramer
2.1	Feb. 25, 2013	Updates for Firmware version 4.2 and hardware version 2.0	Jeremy Cramer
2.2	Aug. 26, 2013	Updates for Firmware version 4.4	Jeremy Cramer
3.0	Nov. 19, 2013	Updates for Firmware version 5.0	Jeremy Cramer

Trademarks

`

Table of Contents

`

1 INTRODUCTION

1.1 Package Contents

- Cradlepoint Mission-Critical Broadband Router (MBR1400)
- AC power adapter (12V, 1.5A) WARNING: using a power adapter other than the one provided may damage the MBR1400 and will void the warranty
- Three 2.4 GHz high performance 802.11n antennas
- Mounting hardware
- CAT5 Ethernet cable
- Setup Guide
- ARC Series with integrated 3G/4G business-grade modem***
  - ARC MBR1400LE-VZ – 4G LTE / EVDO for Verizon
  - ARC MBR1400LP-AT – 4G LTE / HSPA+ for AT&T
  - ARC MBR1400LP2-EU – 4G LTE / HSPA+ for Europe
  - ARC MBR1400LP – 4G LTE / HSPA+ for Canada
  - ARC MBR1400W – 4G WiMAX for Sprint or CLEAR

  Discontinued:
  - MBR1400E-VZ – 3G EVDO for Verizon
  - MBR1400E-SP – 3G EVDO for Sprint

1.2 System Requirements

- At least one Internet source: a Cradlepoint 3G/4G business-grade modem, an Ethernet-based modem, a broadband data modem with active subscription (USB, ExpressCard), or WiFi as WAN.
- Windows 2000/XP/7, Mac OS X, or Linux computer (with WiFi adapter—802.11n recommended—for WiFi functionality).
- Internet Explorer v6.0 or higher, Firefox v2.0 or higher, Safari v1.0 or higher.

1.3 MBR1400 Overview

Cradlepoint's Mission-Critical Broadband Router (MBR1400) takes the power and flexibility of our industry leading router, and when combined with an active high-speed wireless broadband data connection, gets your business network online in no time. Cradlepoint's ARC Series includes an integrated 3G/4G business-grade modem, a seamless, worry-free solution to keep your business online.

Designed for small business, branch office, and retail locations – our business series router provides a secure primary or backup connection to the Internet. In addition to connection options for traditional wired networking solutions like cable, DSL, satellite, or T1, the most powerful feature of the MBR1400 is its ability to use Cradlepoint business-grade modems or USB or ExpressCard data modems to create instant networks anywhere you receive a broadband signal.

The MBR1400 features failover/failback, secure VPN, multiple encryption modes for maximum security, dual-band WiFi broadcast, private and public networks, WiFi as WAN, Modem Health Management, and remote management options with Cradlepoint Enterprise Cloud Manager for deployed units. Cradlepoint provides enterprise-grade performance, security, and the modem reliability businesses need to ensure continuous uptime. Create an instant network today with LTE, WiMAX, HSPA+, or any other wireless broadband technology.

ENTERPRISE PERFORMANCE

- Targeted for retail locations, branch offices, or small and medium-sized businesses
- Choose the ARC MBR1400 Series to include an integrated Cradlepoint business-grade modem
- Centralize the administration and monitoring of distributed routers using cloud-based WiPipe Central
- Load balance multiple data sources (data modems, wired data services, and WiFi as WAN)
- Compatible with Cisco, Juniper, and other industry-leading network hardware providers

ENHANCED WIFI

- Wireless "N" WiFi (802.11n, 802.11a + legacy 802.11b/g, 3x3 MIMO antenna system)
- Enhanced performance around walls and other obstructions
- Dual-band WiFi broadcast – either 2.4 GHz or 5.0 GHz
- Maximum security with both public and private networks

ADDITIONAL FEATURES

- Dual-band WiFi, 3x3 MIMO antenna subsystem, removable external antennas, up to four SSIDs
- Plug-and-play support for more than 120 broadband data modems, allowing for site-specific carrier/service selection for broadest deployment
- Up to 20 concurrent VPN endpoint sessions
- Compatible with Cisco, SonicWall, and other VPN termination systems
- Establish continuous uptime with optimum total cost of ownership for broad deployment
- Standardized platform and centralized remote management
- Simple to install, configure, and maintain with minimal impact on IT
- Virtual LAN capabilities
- Data Usage section that allows users to track and manage modem use relative to data plans
- NAT-less routing and VPN NAT traversal
- SNMP support
- USB-to-serial console passthrough support
- IP passthrough support
- Multicast Proxy support (requires hardware version 2.0)
- IPv6 support

LICENSABLE FEATURES – REQUIRE EXTENDED ENTERPRISE LICENSE

- OSPF, BGP, RIPv1 and RIPv2, VRRP, and STP (also requires hardware version 2.0)
- Site-to-site dynamic VPN with NHRP (also requires hardware version 2.0)
- NEMO (Network Mobility) / DMNR (Dynamic Mobile Network Routing for Verizon) (requires hardware version 2.0)
- Layer 2 Tunneling Protocol (L2TP)
- OpenVPN (SSL VPN)
- Seamless integration with Zscaler's secure web gateway.
- WPA2 Enterprise Authentication for WiFi as WAN

1.3.1 Cradlepoint Enterprise Cloud Manager

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

1.3.2 Captive Portal

The Captive Portal solution provided by Cradlepoint routers enables businesses to provide their customers with a public WiFi hotspot with access controls. The controls can be as simple as requiring acceptance of a terms of service agreement, while advanced features allow administrators to control and monitor usage, require login, direct users to specific web pages, provide revenue through services fees or paid advertising, and more.

1.4 Cradlepoint ARC MBR1400 Series

The Cradlepoint ARC MBR1400 Series includes a Cradlepoint 3G/4G business-grade modem with the MBR1400 and creates an effortless instant network from high-speed wireless broadband.

Cradlepoint integrated business-grade modems are specifically designed to provide the highest level of performance, reliability, and security for 24x7 business-critical applications. Antennas can be located and oriented to receive the highest signal strength. The ARC Series intelligently manages the coexistence between the mobile broadband signal and the WiFi broadcast of the router.

Choose from the following ARC MBR1400 Products:

- **MBR1400LE-VZ – 4G LTE/EVDO for Verizon**
- **MBR1400LP-AT – 4G LTE/HSPA+ for AT&T**
- **MBR1400LP2-EU – 4G LTE/HSPA+ for Europe**
- **MBR1400LP – 4G LTE/HSPA+ for Canada**
- **MBR1400W – 4G WiMAX for Sprint or CLEAR**

Discontinued:

- **MBR1400E-VZ – 3G EVDO for Verizon**
- **MBR1400E-SP – 3G EVDO for Sprint**

MBR1400LE-VZ **4G/3G 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 Band: LTE Band 13 (700 MHz)
CDMA EVDO Rev A/1xRTT (800/1,900 MHz)

Power: LTE 23 +/− 1 dBm, EVDO 24 +/− 1dBm (typical conducted)

Module: Sierra Wireless MC7750

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

GPS: standalone GPS support

Industry Standards & Certs: FCC, Verizon

Modem Part Number: MC200LE

MBR1400LP-AT 4G/3G LTE/HSPA+ for AT&T

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 17 (700MHz), Band 4 (AWS)
- UMTS/HSPA+ (850/1900/2100 MHz)
- EDGE/GPRS/GSM (850/900/1800/1900 MHz)

Module Power: LTE 23 +/− 1 dBm, UMTS 23 +/− 1 dBm (typical conducted)

Module: Sierra Wireless MC7700

Module Antennas: two SMA male (plug), 1 dBi (LTE), 2 dBi gain; finger tighten only; support for GPS on aux connection

GPS: standalone GPS support

Industry Standards & Certs: PTCRB, FCC, AT&T

Modem Part Number: MC200LP

MBR1400LP2-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 (800/900/1800/2100/2600 MHz)
- HSPA+/UMTS (900/2100 MHz)
- EDGE/GPRS/GSM (900/1800/1900 MHz)

Module Power: LTE 23 +/− 1 dBm, UMTS 23 +/− 1 dBm (typical conducted)

Module: Sierra Wireless MC7710

Module Antennas: two SMA male (plug), 1 dBi (LTE), 2 dBi (Cellular/PCS) gain; finger tighten only; support for GPS on aux connection

GPS: standalone GPS support

Industry Standards & Certs: CE, GCF-CC

Modem Part Number: MC200LP2

Cradlepoint products with the -EU SKUs enable and disable WiFi channels to comply with EU law. The -EU SKUs are required for use in Europe for products with 5 GHz WiFi, but these products are not legal for use in North America. See: http://en.wikipedia.org/wiki/List_of_WLAN_channels.

MBR1400LP	4G LTE/HSPA+ for Canada

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 17 (700MHz), Band 4 (AWS)
- UMTS/HSPA+ (850/1900/2100 MHz)
- EDGE/GPRS/GSM (850/900/1800/1900 MHz)

Module Power: LTE 23 +/− 1 dBm, UMTS 23 +/− 1 dBm (typical conducted)

Module: Sierra Wireless MC7700

Module Antennas: two SMA male (plug), 1 dBi (LTE), 2 dBi (Cellular/PCS) gain; finger tighten only; support for GPS on aux connections

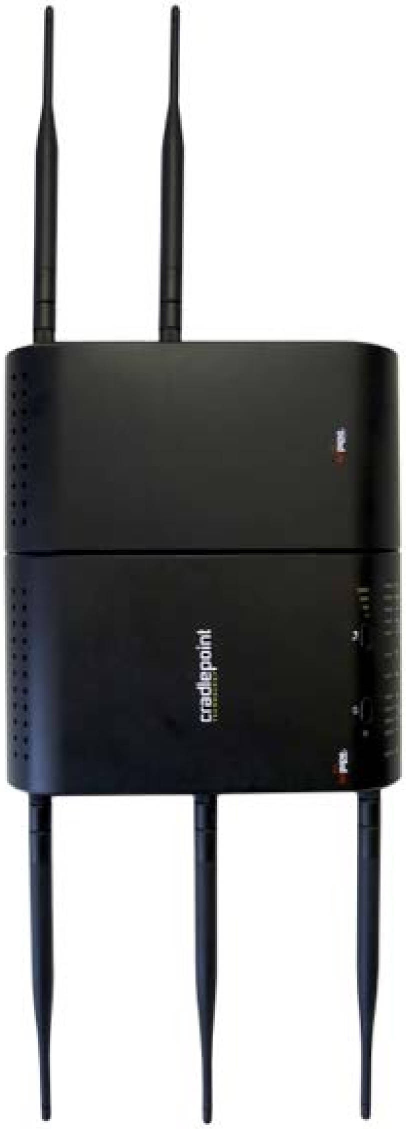
GPS: standalone GPS support

Industry Standards & Certs: PTCRB, FCC, IC

Modem Part Number: MC200LP

MBR1400W	**4G WiMAX for Sprint or CLEAR**
Technology: WiMAX 802.16e Wave 2	
Downlink Rates: 10Mbps peak, 6Mbps average	
Uplink Rates: 5 Mbps peak, 1.2 Mbps average	
Frequency Band: 2,500 MHz band	
Power: 23.5 +/− 0.5 dBm (RSU/CPE)	
Module: Beceem 250 chipset	
Module Antennas: two SMA male (plug), 5 dBi gain; finger tighten only; maximum torque spec is 7 kgf-cm	
GPS: no GPS support	
Industry Standards & Certs: FCC, Sprint, Clearwire	
Modem Part Number: MC100W	

For optimum performance, antennas on the MBR1400W-SP should be pointed in opposite directions as shown to the right. This will help prevent overlap with the 2.4 GHz WiFi band.



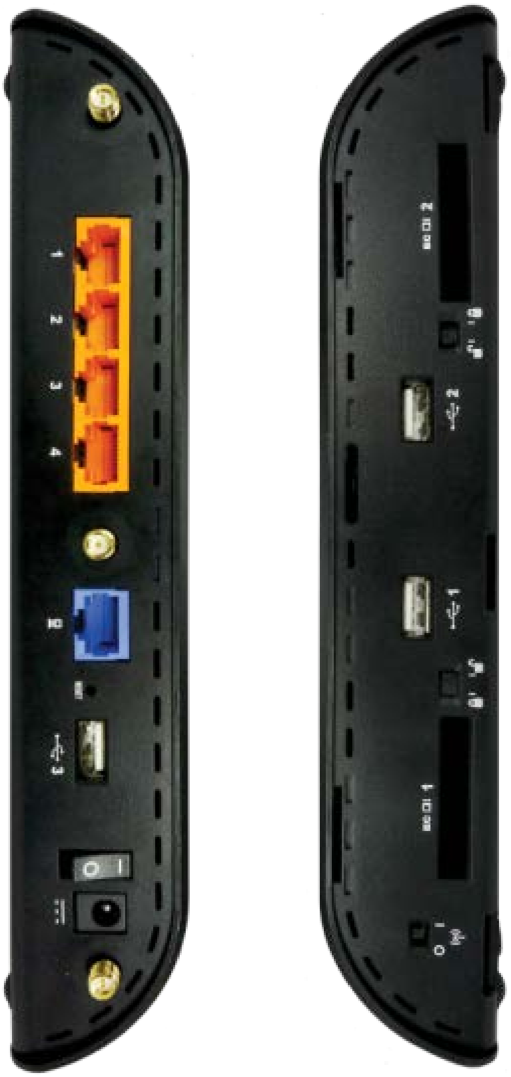
MBR1400E-VZ	3G EVDO for Verizon
Technology: EVDO Rev A	
Downlink Rates: 3.1 Mbps (theoretical)	
Uplink Rates: 1.8 Mbps (theoretical)	
Frequency Band: CDMA EVDO Rev A/1xRTT (800/1,900 MHz)	
Power: 24 +/− 0.5 dBm (typical conducted)	
Module: Sierra Wireless 5728v	
Module Antennas: two SMA male (plug), 2 dBi gain	
Industry Standards & Certs: modem model MC100E – Verizon IOT; FCC Part 15, 22 & 24, CDG Stages 1,2; IS-2000IA-98D/E, IS-134, IS-637B, IS-683A, IS-707A, IS-856, IS-866; JESD22-A114-B, JESD22-C101	
Modem Certification Model Number: MC100E **Modem Certification Part Number:** MC100E-VZ	

(MBR1400E-VZ has been discontinued.)

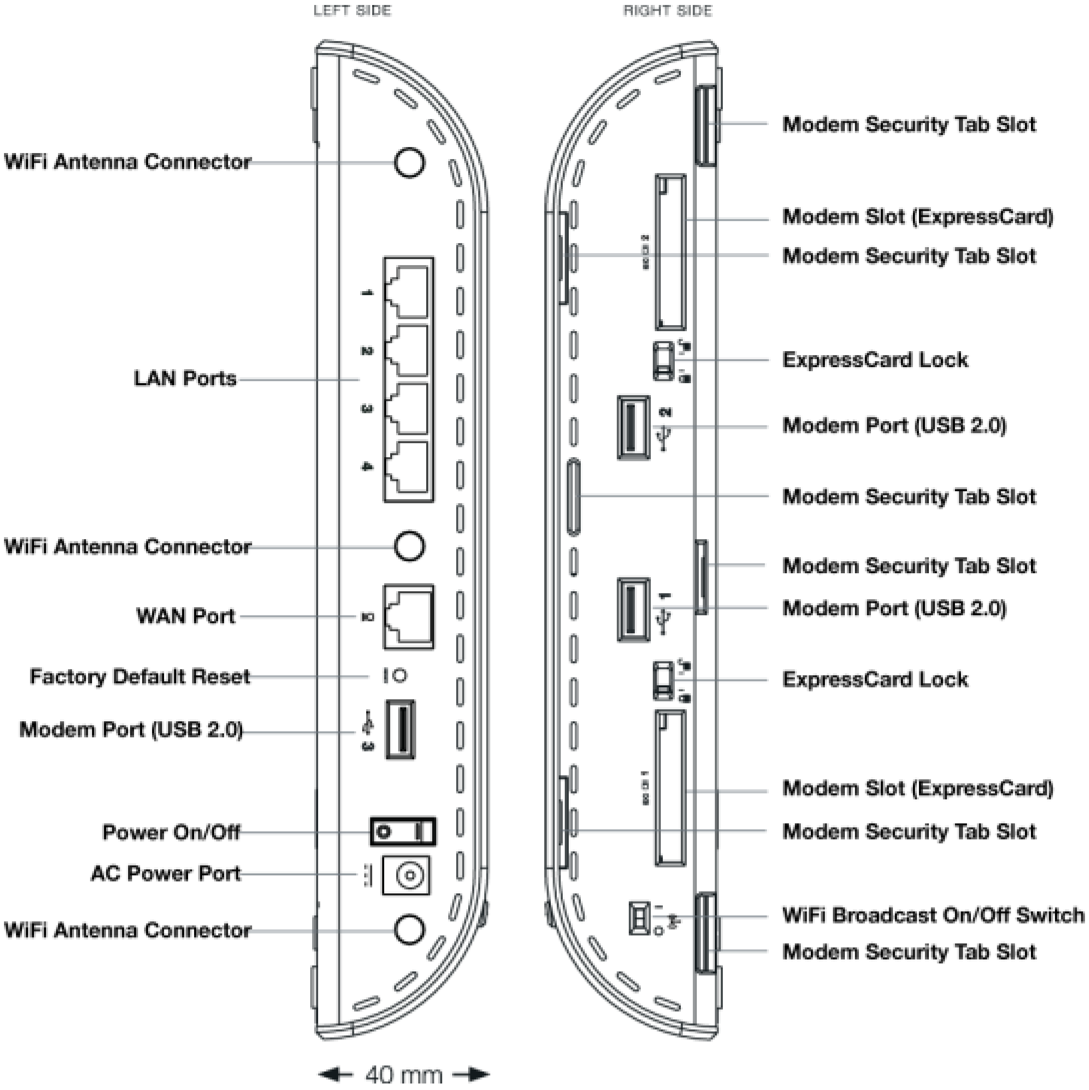
MBR1400E-SP	3G EVDO for Sprint
Technology: EVDO Rev A	
Downlink Rates: 3.1 Mbps (theoretical)	
Uplink Rates: 1.8 Mbps (theoretical)	
Frequency Band: CDMA Rev A/1xRTT (800/1,900 MHz)	
Power: 24 +/− 0.5 dBm (typical conducted)	
Module: Sierra Wireless 5728v	
Module Antennas: two SMA male (plug), 2 dBi gain	
Industry Standards & Certs: modem model MC100E – Sprint; FCC Part 15, 22 & 24, CDG Stages 1,2; IS-2000IA-98D/E, IS-134, IS-637B, IS-683A, IS-707A, IS-856, IS-866; JESD22-A114-B, JESD22-C101	
Modem Certification Model Number: MC100E **Modem Certification Part Number:** MC100E-SP	

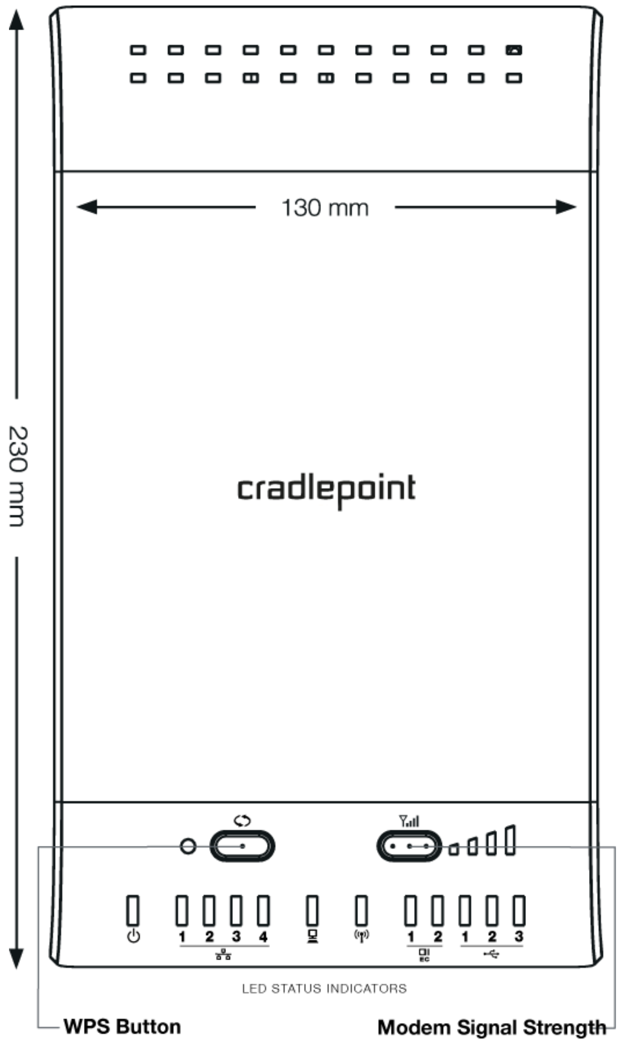
(MBR1400E-SP has been discontinued.)

2 HARDWARE OVERVIEW



2.1 Ports, Buttons, and Switches




130 mm
230 mm
cradlepoint
1 2 3 4
1 2 1 2 3
LED STATUS INDICATORS
WPS Button
Modem Signal Strength

LAN and WAN Ports: By default, the four orange ports are configured as LAN (Local Area Network) ports and the blue port is configured as a WAN (Wide Area Network—your Internet source) port. Any LAN port, however, can be reconfigured as a WAN port and vice versa.

Modem Ports: The MBR1400 has three USB 2.0 ports and two ExpressCard ports.

WiFi Antenna Connectors: Your router comes with three 2.4 GHz WiFi antennas (Reverse SMA). 5 GHz antennas are available as an accessory. The antennas are simple to attach and adjust for maximum WiFi broadcast. (Finger tight only.)

Factory Default Reset: You can return your router to factory default settings by pressing and holding the **Reset** button. This button is recessed, so it requires a pointed object such as a paper clip to press. Press and hold for 10 seconds to initiate reset.

WPS Button: WiFi Protected Setup. When you press the WPS button for five seconds, it allows you to use WPS for WiFi security. The LED will illuminate blue to indicate WPS status. Devices must support WPS in order to be configured by this method.

Power On/Off:

- I = On
- O = Off

WiFi Broadcast On/Off: You have the option to turn off the WiFi radio.

- I = On
- O = Off

3G/4G Modem Signal Strength Button: When pressed the bar LEDs indicate signal strength from the Cradlepoint business-grade modem or USB or ExpressCard modem. The signal strength is shown for 10 seconds if the modem does not support concurrent data connection and signal strength measurement. Tapping this button will toggle the Modem Signal Strength display on and off.

2.2 LEDs

WiFi PROTECTED SETUP STATUS

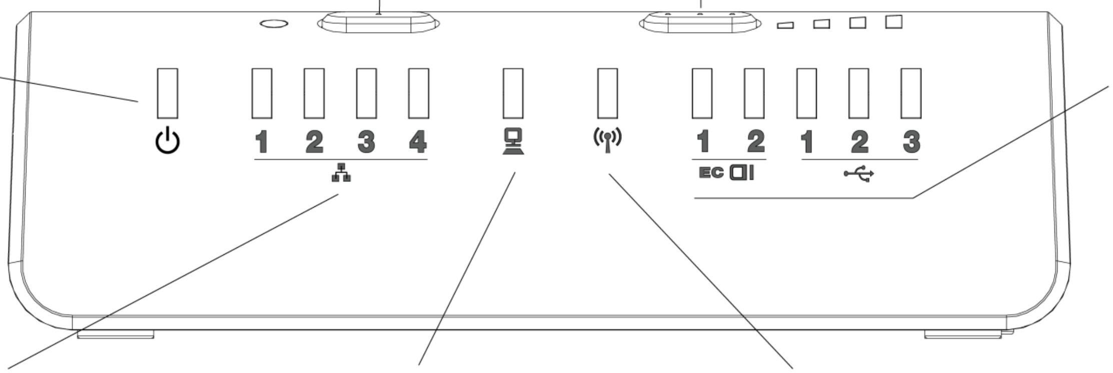
Blue	WPS is active
Blinking Blue	WPS setting in progress
No Light	WPS is not active

3G/4G MODEM SIGNAL STRENGTH

4 Blue Bars	Strong
3 Blue Bars	Good
2 Blue Bars	OK
1 Blue Bars	Weak
No Light	Indicator off, press button to activate

POWER STATUS

Green	On
No Light	Not receving power
Flashing Yellow	Attention: check router status page



3G/4G MODEM STATUS

Green	Connection active
Blinking Green	Establishing connectiion
Amber	Modem not active
Blinking Amber	Modem connection error
Blinking Red	Modem in process of resetting
No Light	Modem not connected

LAN STATUS (ports 1-4)

Blue	1000 Mbps connected
Blinking Blue	1000 Mbps activity
Green	10/100 Mbps connected
Blinking Green	10/100 Mbps activity
No Light	Cable disconnected or link failed

WAN STATUS

Blue	1000 Mbps connected
Blinking Blue	1000 Mbps activity
Green	10/100 Mbps connected
Blinking Green	10/100 Mbps activity
No Light	Cable disconnected or link failed

WiFi BROADCAST

Green	2.4 GHz WiFi is on and operating normally
Blue	5 GHz WiFi is on and operating normally
Blinking Red	Error with connection
No Light	WiFi is off

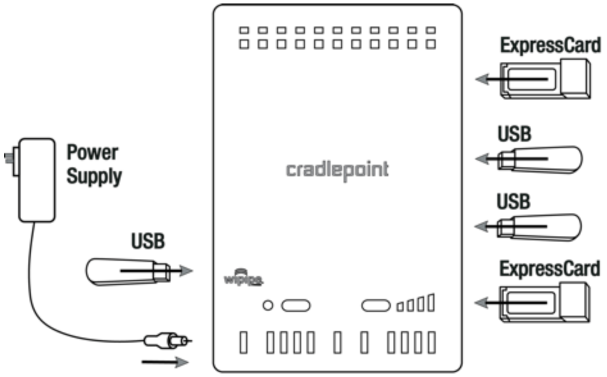
LAN and WAN LEDs: The default settings are shown. LAN ports can be reconfigured to function as WAN ports and vice versa; the LEDs will function accordingly.

3 QUICK START

3.1 Basic Setup

- Your router requires an Internet source. Attach a Cradlepoint business-grade modem, insert one or more supported USB or ExpressCard modem(s), connect a cable or DSL modem to the blue Ethernet WAN port, or connect to an available WiFi source. For failover/failback functionality, you will need at least two of these sources (for example: one Ethernet source and one USB modem).[1]
- Attach the three included WiFi antennas to the connectors for maximum WiFi broadcast. To attach, hold the antenna straight and twist the base of the antenna to connect, folding the joint if needed. Please note that 2.4 GHz antennas are provided. 5 GHz antennas are available as an accessory.
- Connect the 12v DC power adapter to the router and a power source. Flip the power switch to the ON position; this illuminates the green power status LED.

For full 3G/4G functionality, attach one (or more) of the following:



[1] This product requires a data modem with an active data plan for full functionality. Data modem only included with ARC models. See your 3G/4G service provider for details on coverage and data plan options.

- USB/ExpressCard modem(s)
- Integrated Cradlepoint business-grade modem

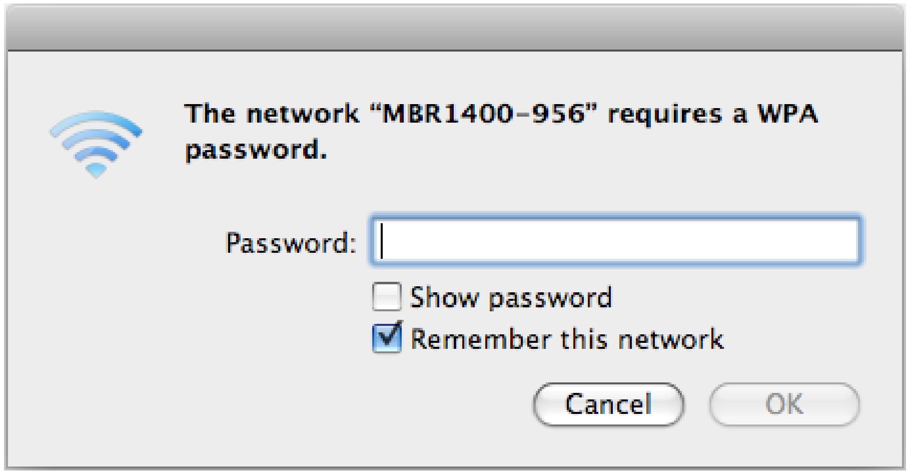
3.2 Connect to a Computer or other Device

3.2.1 Wireless Network Connection

1) Find the network. On a WiFi-enabled computer or device, open the window or dropdown menu that allows you to access wireless networks. The MBR1400 SSID will appear on the list: select this network.

2) Log in. Input the **Default Password** when prompted. The Default Password is provided on the product label found on the bottom of your router (this password is also the last eight digits of the router’s MAC address, which can be found on the product box or product label).

NOTE: If more than one MBR1400 wireless router is visible, find the correct unit by checking for its **SSID** (service set identifier; the unique name of the local network). The SSID can be found on the product label in the form MBR1400-xxx, where “xxx” is the last 3 digits of the router’s MAC address.

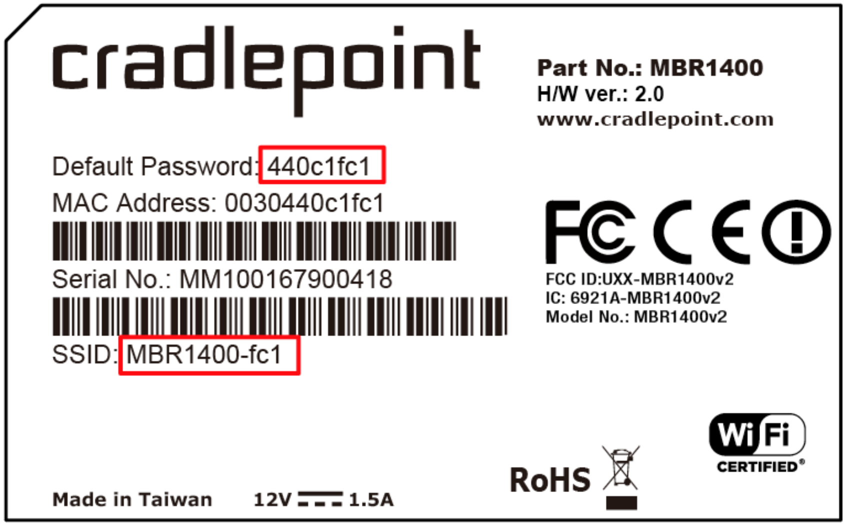


The network “MBR1400-956” requires a WPA password.

Password:

□ Show password

☑ Remember this network



cradlepoint

Part No.: MBR1400
H/W ver.: 2.0
www.cradlepoint.com

Default Password: 440c1fc1
MAC Address: 0030440c1fc1
Serial No.: MM100167900418
SSID: MBR1400-fc1

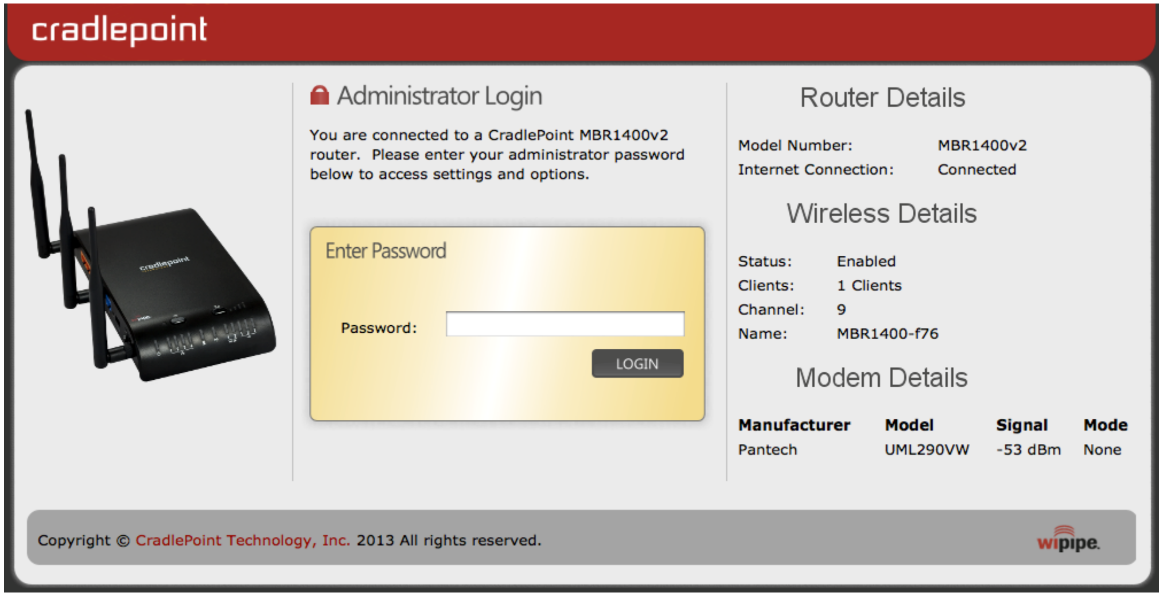
FCC ID:UXX-MBR1400v2
IC: 6921A-MBR1400v2
Model No.: MBR1400v2

Made in Taiwan 12V ⎓ 1.5A

3.2.2 Accessing the Administration Pages

For many users, the MBR1400 can be used immediately without any special configuration changes. If you would like to change your network name or password or configure any of the advanced features of the MBR1400, you will need to log into the administration pages:

- Access your router's **Administrator Login** screen by opening a web browser window and typing "cp/" (your router's default hostname) or the IP address "192.168.0.1" into the address bar.
- Enter your **Default Password**. This password can be found on the bottom of the MBR1400. Then click the **LOGIN** button.
- When you log in for the first time, the **First Time Setup Wizard** automatically appears. Follow the instructions given with the Wizard or see Getting Started – First Time Setup for more information about using the **First Time Setup Wizard**.



Administrator Login

You are connected to a CradlePoint MBR1400v2 router. Please enter your administrator password below to access settings and options.

Enter Password

Password:

Router Details

Model Number:	MBR1400v2
Internet Connection:	Connected

Wireless Details

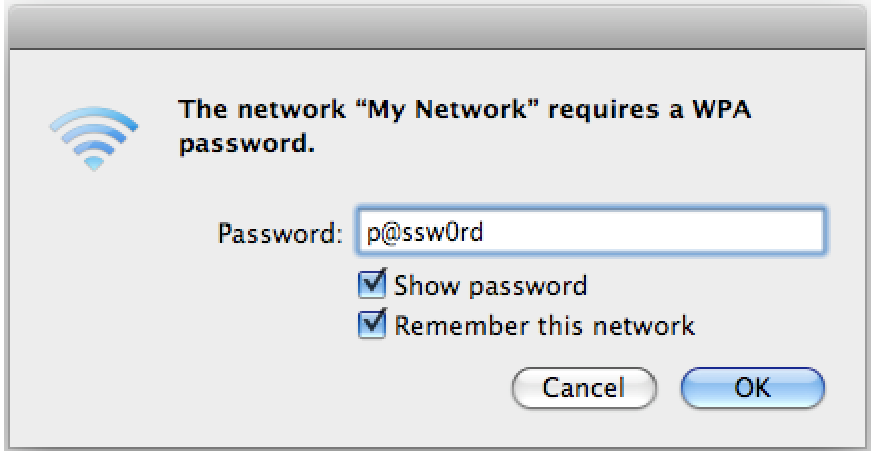
Status:	Enabled
Clients:	1 Clients
Channel:	9
Name:	MBR1400-f76

Modem Details

Manufacturer	Model	Signal	Mode
Pantech	UML290VW	-53 dBm	None

Copyright © CradlePoint Technology, Inc. 2013 All rights reserved.

3.2.3 Connect to the Internet



The network "My Network" requires a WPA password.

Password: p@ssw0rd

☑ Show password

☑ Remember this network

If you used the **First Time Setup Wizard**, you might have changed the "WiFi Network Name" or the "Security Mode" password. If so, you will need to reconnect to the MBR1400 network.

- **Find the network**. Look for your new personalized network name (or the default SSID of the form "MBR1400-xxx").
- **Log in** using your new personalized WiFi security password (or the Default Password found on the product label on the bottom of the router).

Your network should now be up and running, and users who have the security password can access the network on WiFi-enabled devices.

3.3 Common Problems

This section contains some of the most common issues faced by users of the MBR1400.

Please visit the Cradlepoint Knowledge Base at http://knowledgebase.Cradlepoint.com/ for more help and answers to your other questions.

3.3.1 You cannot connect to the Internet with a Cradlepoint business-grade modem

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

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

1. Log in to the MBR1400 administration pages (see Accessing the Administration Pages).
2. Select **Internet** from the top navigation bar and **Modem Settings** from the dropdown menu (**Internet → Modem Settings**).
3. Find and select the Cradlepoint modem.
4. Click Update/Activate.
5. Click Activate in the popup.

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

If you are still not online after activating the modem, go to knowledgebase.Cradlepoint.com for more information.

3.3.2 Your USB or ExpressCard modem does not work with the router

- If your USB data or ExpressCard is not working with the router, check the list of supported devices at http://www.Cradlepoint.com/modems to ensure you are using a supported device and carrier. The device you are using must be supported on the carrier network providing your cellular service or it's considered an unsupported device, even if it is supported on another carrier's network.

- Sometimes a USB data modem needs to be updated or have other configurations set correctly in order to make a connection through the router. If your USB modem has not been updated recently, it is recommended that you do so if it is having trouble connecting to the MBR1400. Insert your USB data modem into your PC and access the Internet using the software provided by your cellular carrier. Follow the directions provided to complete the update. Once you have updated your USB data modem, reconnect the cellular device to your Cradlepoint router and connect to the Internet.

- If you are using a WiMAX modem, you need to set the WiMAX Realm. This can be done in the administration pages. Log in using the hostname "cp/" or IP address "http://192.168.0.1" in your browser. Go to **Internet → Connection Manager**. In the **WAN Interfaces** section, select your modem and click "Edit." Select the **WiMAX Settings** tab and select/input your WiMAX Realm.

- Some wireless carriers provide more than one Access Point Name (APN) that a modem can connect to. If you wish to specify the APN, this can be done in the administration pages. Log in using the hostname "cp/" or IP address "http://192.168.0.1" in your browser. Go to **Internet → Connection Manager**. In the **WAN Interfaces** section, select your modem and click "Edit." Select the **SIM/APN Settings** tab. There is an Access Point Name field: Set the APN and click **Submit**. Some APN examples are **isp.cingular**, **ecp.tmobile.com**, and **vpn.com**. The modem must be removed and reinserted (or the router must be rebooted) for this change to take effect.

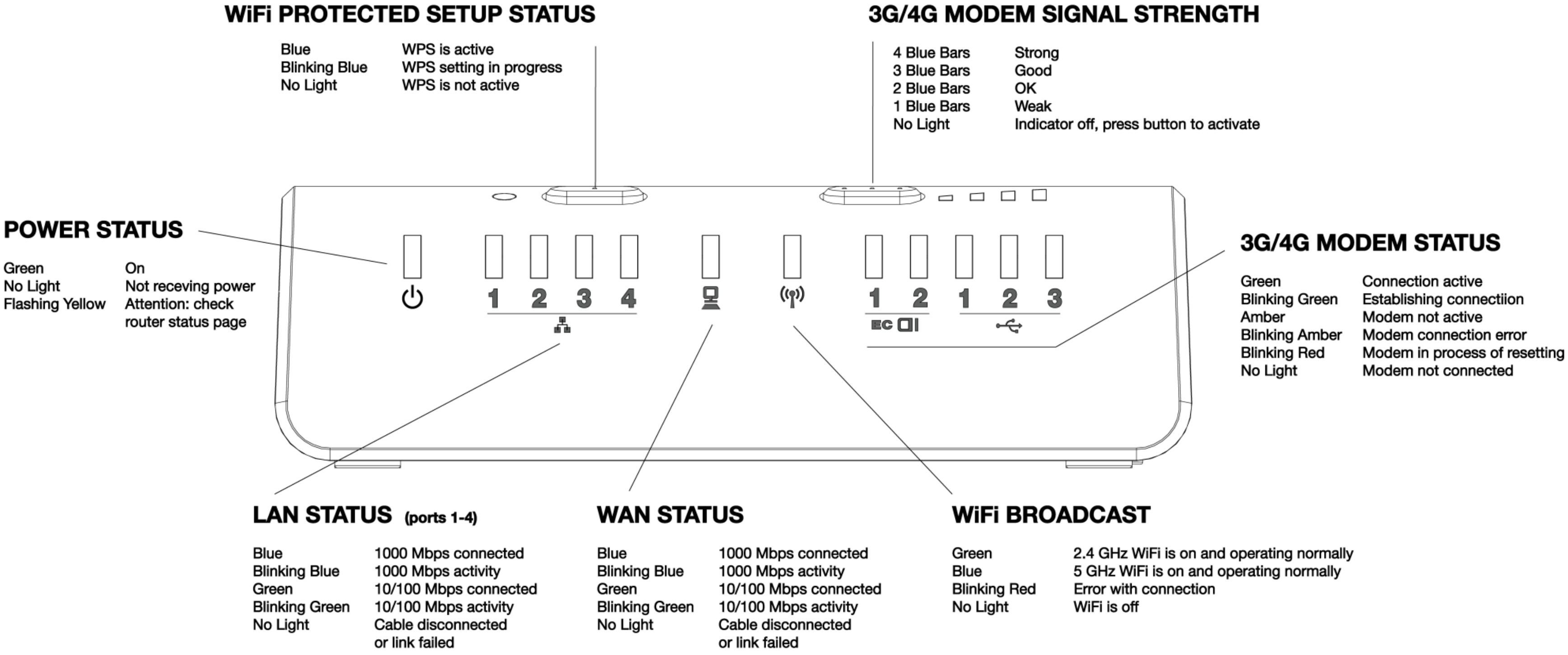
- If the above issues have been resolved and you can connect to the router but you cannot get Internet through it using your modem, you may need to upgrade the router firmware. Use your computer (you may need to plug your modem directly into your computer if you don't have another way to access the Internet) to download the latest firmware for the router at http://www.Cradlepoint.com/firmware/MBR1400. Then log into the router administration pages and manually upload the firmware. Go to **System Settings → System Software** and click on "Manual Firmware Upload".

If you are still not online after activating the modem, go to knowledgebase.Cradlepoint.com for more information.

3.3.3 You are connected to the router but cannot connect to the Internet

The status LEDs of your router will give you an indication whether or not a proper connection is being made. See the LED STATUS definitions below:

If the data modem LEDs are not illuminated, your modem is not connected and online. You may need to update firmware. Refer to the previous section, "Your USB or ExpressCard modem does not work with the router."



WiFi PROTECTED SETUP STATUS

Blue	WPS is active
Blinking Blue	WPS setting in progress
No Light	WPS is not active

3G/4G MODEM SIGNAL STRENGTH

4 Blue Bars	Strong
3 Blue Bars	Good
2 Blue Bars	OK
1 Blue Bars	Weak
No Light	Indicator off, press button to activate

POWER STATUS

Green	On
No Light	Not receving power
Flashing Yellow	Attention: check router status page

3G/4G MODEM STATUS

Green	Connection active
Blinking Green	Establishing connectiion
Amber	Modem not active
Blinking Amber	Modem connection error
Blinking Red	Modem in process of resetting
No Light	Modem not connected

LAN STATUS (ports 1-4)

Blue	1000 Mbps connected
Blinking Blue	1000 Mbps activity
Green	10/100 Mbps connected
Blinking Green	10/100 Mbps activity
No Light	Cable disconnected or link failed

WAN STATUS

Blue	1000 Mbps connected
Blinking Blue	1000 Mbps activity
Green	10/100 Mbps connected
Blinking Green	10/100 Mbps activity
No Light	Cable disconnected or link failed

WiFi BROADCAST

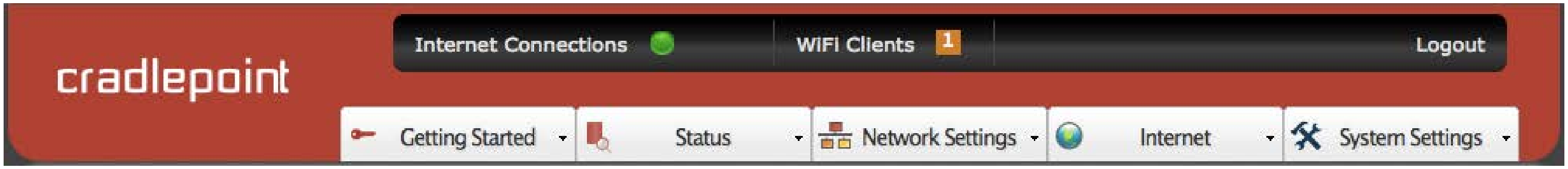
Green	2.4 GHz WiFi is on and operating normally
Blue	5 GHz WiFi is on and operating normally
Blinking Red	Error with connection
No Light	WiFi is off

If you are still not online after activating the modem, go to knowledgebase.Cradlepoint.com for more information.

4 WEB INTERFACE – ESSENTIALS

The MBR1400 has a browser-based interface for configuration and administration of all features. The interface is organized with 5 tabs at the top of the screen:

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

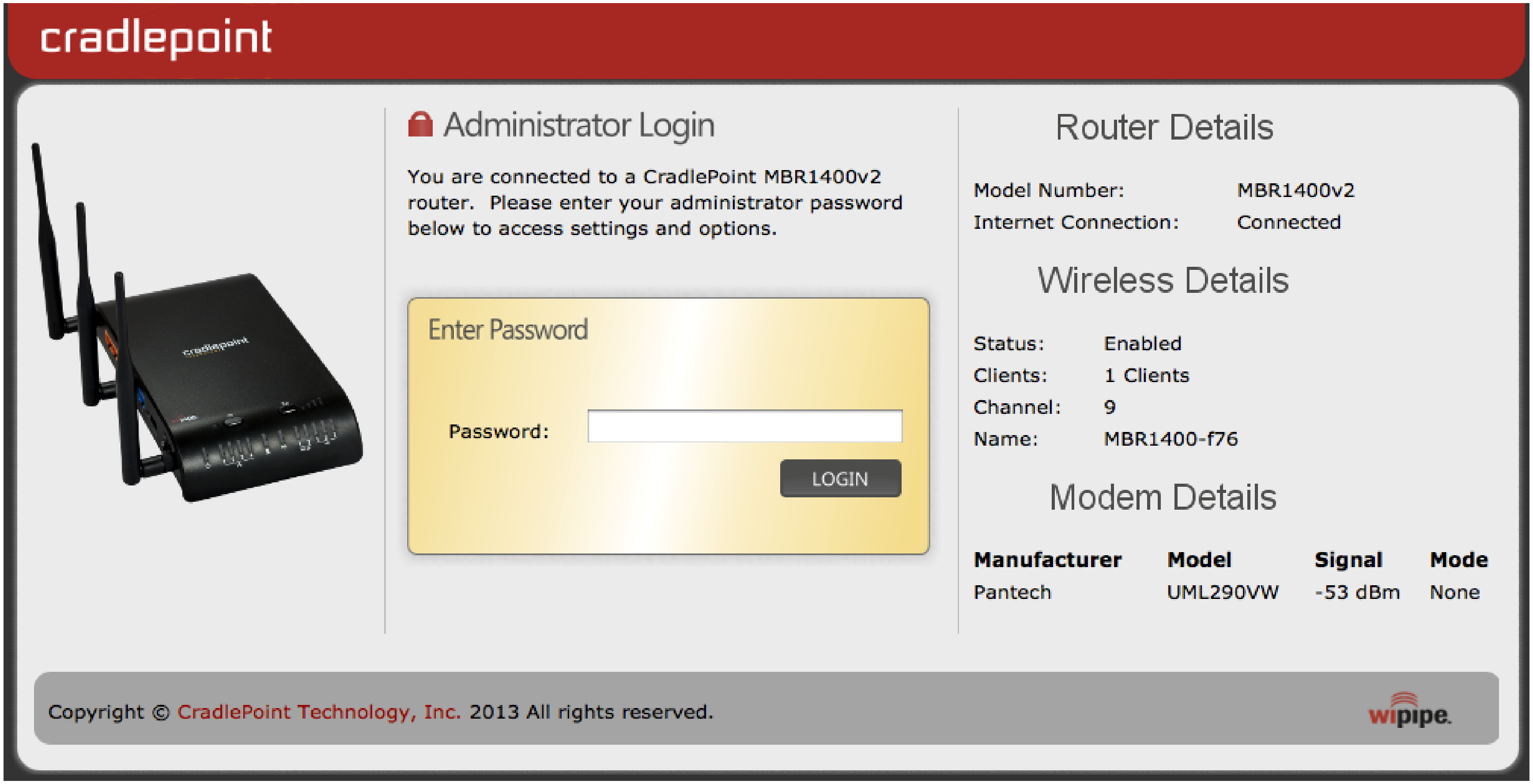


Web Interface – Essentials contains the following sections to help you more quickly and easily navigate these administration pages:

4.1 Administrator Login
4.2 Getting Started – First Time Setup Wizard
4.3 Quick Links
4.4 Configuration Pages
4.5 Enterprise Cloud Manager Registration
4.6 IP Passthrough Setup

4.1 Administrator Login

To access the administration pages, open a Web browser and type the hostname "cp/" or IP address "http://192.168.0.1" into the address bar. The Administrator Login page will appear.



Administrator Login

You are connected to a CradlePoint MBR1400v2 router. Please enter your administrator password below to access settings and options.

Enter Password

Password:

Router Details

Model Number:	MBR1400v2
Internet Connection:	Connected

Wireless Details

Status:	Enabled
Clients:	1 Clients
Channel:	9
Name:	MBR1400-f76

Modem Details

Manufacturer	Model	Signal	Mode
Pantech	UML290VW	-53 dBm	None

Copyright © CradlePoint Technology, Inc. 2013 All rights reserved.

Log in using your administrator password. Initially, this password can be found on the bottom of the MBR1400 unit as the **Default Password**. This password is also the last eight digits of the unit's MAC address.

You may have changed the administrator password during initial setup using the First Time Setup Wizard. Log in using your personalized administrator password.

If you have forgotten your personalized password, you can reset the MBR1400 to factory defaults. When you reset the router, the administrator password will revert back to the **Default Password**. Press and hold the **reset button** on the router unit until the lights flash (approximately 10-15 seconds). You can then log in using the **Default Password**.

4.1.1 Router Details

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

Router Details

- **Model Number:** MBR1400
- **Internet Connection:** Connected/Disconnected

Wireless Details

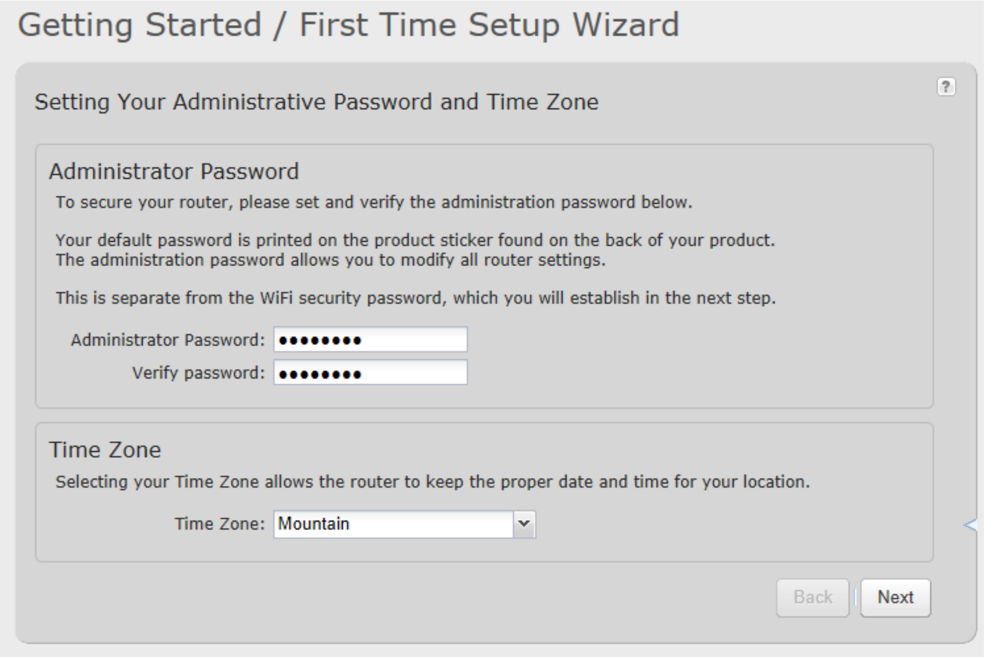
- **Status:** Enabled/Disabled
- **Clients:** The number of attached users
- **Channel:** The channel number
- **Name:** The name of the primary network (if you have more than one wireless network enabled, the additional network names will also be listed here)

Modem Details (if you have a business-grade/USB/ExpressCard data modem attached)

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

4.2 Getting Started – First Time Setup Wizard

The **First Time Setup Wizard** will help you customize the name of your wireless network, change passwords to something you choose, and establish an optimal WiFi security mode. The MBR1400 comes out of the box with a unique password at WPA1/WPA2 WiFi security level.



Getting Started / First Time Setup Wizard

Setting Your Administrative Password and Time Zone

Administrator Password

To secure your router, please set and verify the administration password below.

Your default password is printed on the product sticker found on the back of your product.
The administration password allows you to modify all router settings.

This is separate from the WiFi security password, which you will establish in the next step.

Administrator Password: ••••••••
Verify password: ••••••••

Time Zone

Selecting your Time Zone allows the router to keep the proper date and time for your location.

Time Zone: Mountain

1) Open a browser window and type "cp/" or "192.168.0.1" into the address bar. Press enter/return.

2) When prompted for your password, type the eight character **Default Password** found on the product label on the bottom of the MBR1400 (this is also the last 8 digits of the router's MAC address).

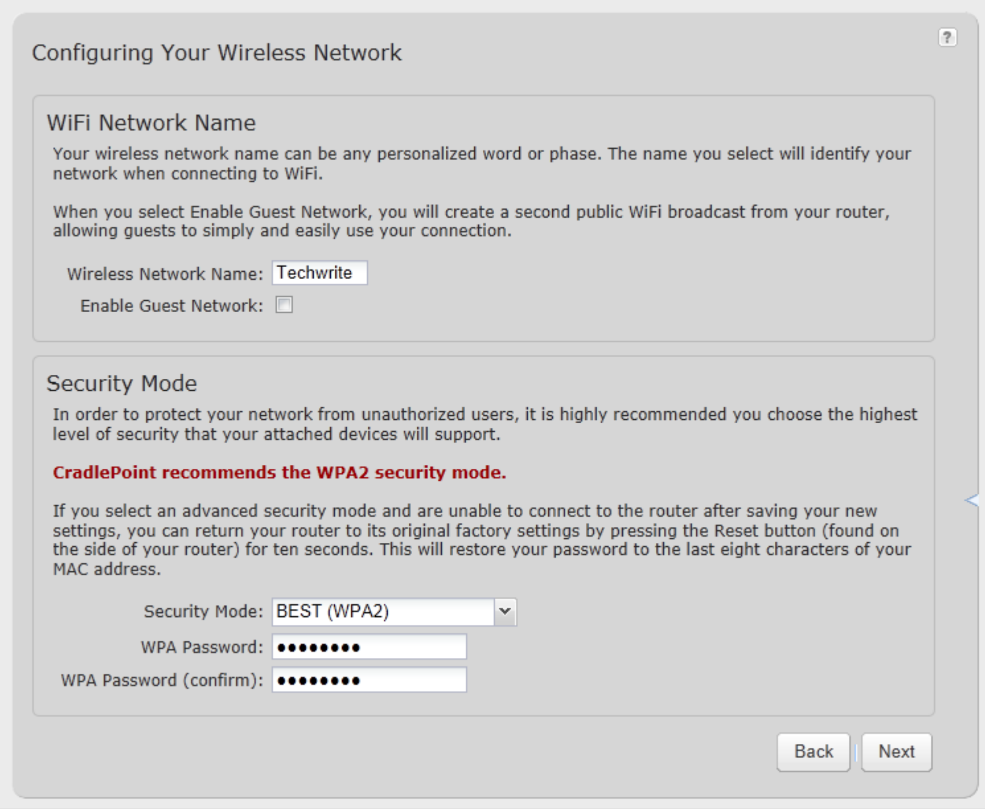
3) When you log in for the first time, you will be automatically directed to the **FIRST TIME SETUP WIZARD**. (Otherwise, go to **Getting Started → First Time Setup**).

4) Cradlepoint recommends that you change the router's **ADMINISTRATOR PASSWORD**, which is used to log in to the administration pages. The administrator password is separate from the WiFi security password, although initially the **Default Password** is used for both.

NOTE: If you plan to use your router in a PCI DSS compliant environment, do not use this setting. Use the "Advanced Security Mode" settings under the **Router Security** tab in **System Settings → Administration** instead.

5) You can select your **TIME ZONE** from a dropdown list. (This may be necessary to properly show time in your router log, but typically your router will automatically determine your time zone through your browser.) Click **NEXT**.

6) Cradlepoint recommends that you customize your WiFi network name. Type in your personalized network name here. You can also enable the Guest Network feature (for more configuration options, see **Network Settings → WiFi / Local Networks** and the Wireless (WiFi) Network Settings section of this manual).



Configuring Your Wireless Network

WiFi Network Name

Your wireless network name can be any personalized word or phase. The name you select will identify your network when connecting to WiFi.

When you select Enable Guest Network, you will create a second public WiFi broadcast from your router, allowing guests to simply and easily use your connection.

Wireless Network Name: Techwrite

Enable Guest Network: □

Security Mode

In order to protect your network from unauthorized users, it is highly recommended you choose the highest level of security that your attached devices will support.

CradlePoint recommends the WPA2 security mode.

If you select an advanced security mode and are unable to connect to the router after saving your new settings, you can return your router to its original factory settings by pressing the Reset button (found on the side of your router) for ten seconds. This will restore your password to the last eight characters of your MAC address.

Security Mode: BEST (WPA2)

WPA Password: ••••••••

WPA Password (confirm): ••••••••

Choose the **WIFI SECURITY MODE** that best fits your needs:

- **BEST (WPA2):** Select this option if your wireless adapters support WPA2-only mode. This will connect to most new devices and is the most secure, but may not connect to older devices or some handheld devices such as a PSP.
- **GOOD (WPA1 & WPA2):** Select this option if your wireless adapters support WPA or WPA2. This is the most compatible with modern devices and PCs.
- **POOR (WEP):** Select this option if your wireless adapters only support WEP. This should only be used if a legacy device that only supports WEP will be connected to the router. WEP is insecure and obsolete and is only supported in the router for legacy reasons. The router cannot use 802.11n modes if WEP is enabled; WiFi performance and range will be limited.
- **NONE (OPEN):** Select this option if you do not want to activate any security features.

Cradlepoint recommends BEST (WPA2) WiFi security. Try this option first and switch only if you have a device that is incompatible with WPA2.

Choose a personalized **WPA PASSWORD** or **WEP KEY**. This password will be used to connect devices to the router's WiFi broadcast once the security settings have been saved.

- **WPA Password:** The WPA Password must be between 8 and 64 characters long. A combination of upper and lower case letters along with numbers and special characters is recommended to prevent hackers from gaining access to your network.
- **WEP Key:** A WEP Key must be either a hexadecimal value of 5 or 13 characters or a text value of 10 or 26 characters.

Click **NEXT**.

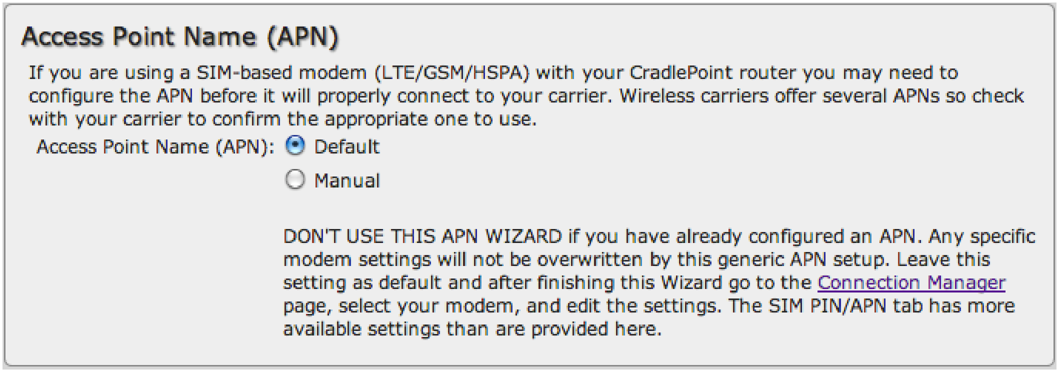
7) **Configuring Your Access Point Name (APN)**:

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

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

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

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



Access Point Name (APN)

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

Access Point Name (APN): ● Default

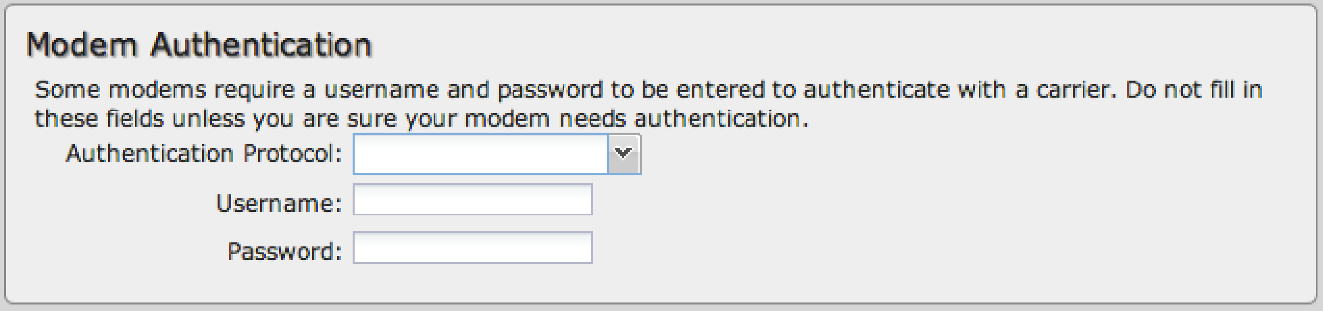
○ Manual

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

8) **Modem Authentication**:

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

- **Authentication Protocol** – Set this only if your service provider requires a specific protocol and the **Auto** option chooses the wrong one. Select from:
    - **Auto**
    - **Pap**
    - **Chap**
- **Username**
- **Password**



Modem Authentication

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

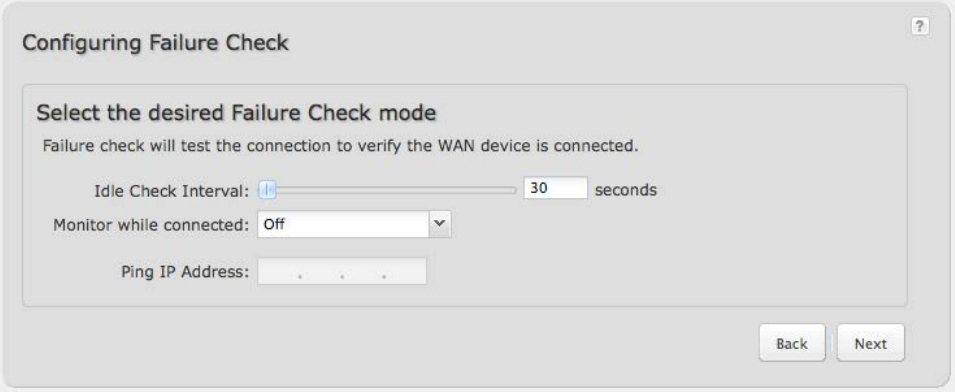
Authentication Protocol:

Username:

Password:

9) <u>Configuring Failure Check</u>:

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



Configuring Failure Check

Select the desired Failure Check mode

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

Idle Check Interval: 30 seconds

Monitor while connected: Off

Ping IP Address: . . .

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

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

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

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

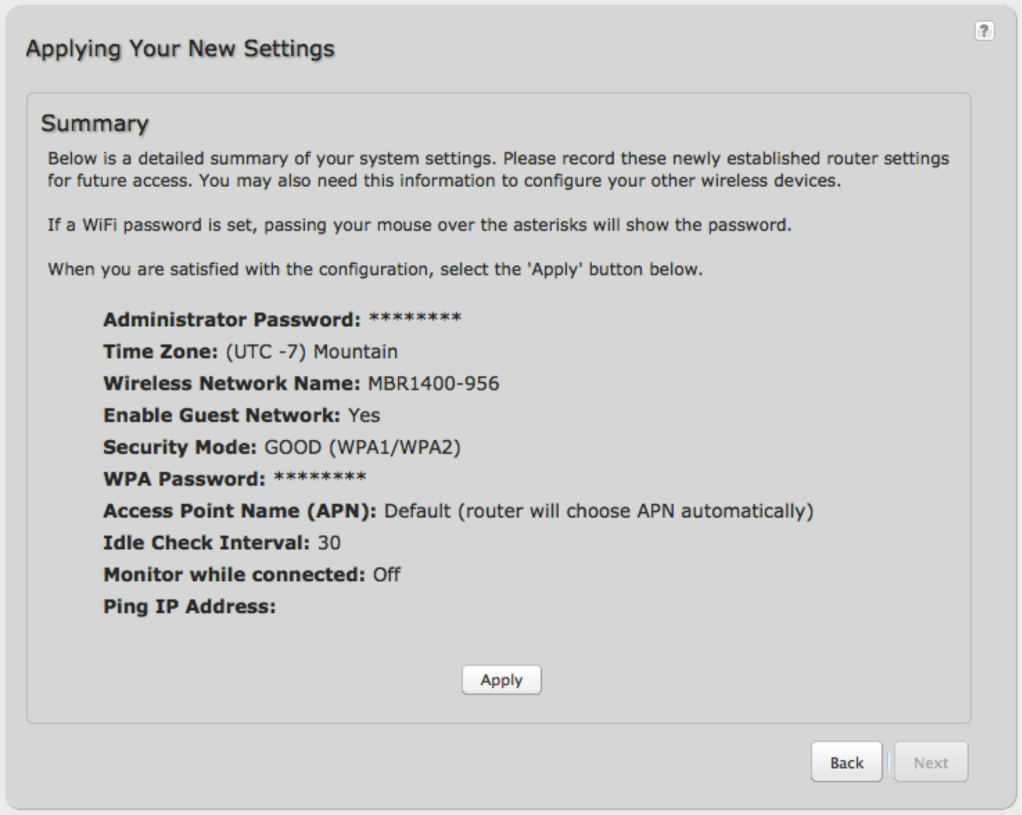
Click **NEXT**.

10) Review the details and record your wireless network name, administrative password, and WPA password (or WEP key). Move your mouse over your WiFi password to reveal it.

Please record these settings for future access. You may need this information to configure other wireless devices.

NOTE: If you are currently using the MBR1400 WiFi network, reconnect your devices to the network using the new wireless network name and security password.

Click **APPLY** to save the settings and update them to your router.



Applying Your New Settings

Summary

Below is a detailed summary of your system settings. Please record these newly established router settings for future access. You may also need this information to configure your other wireless devices.

If a WiFi password is set, passing your mouse over the asterisks will show the password.

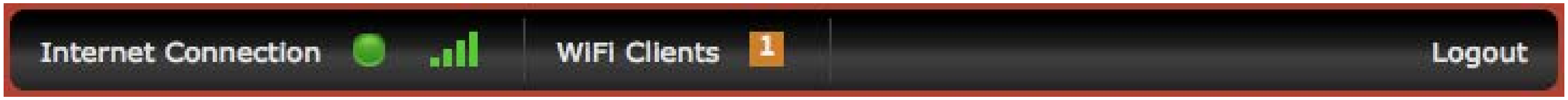
When you are satisfied with the configuration, select the 'Apply' button below.

Administrator Password: ********
Time Zone: (UTC -7) Mountain
Wireless Network Name: MBR1400-956
Enable Guest Network: Yes
Security Mode: GOOD (WPA1/WPA2)
WPA Password: ********
Access Point Name (APN): Default (router will choose APN automatically)
Idle Check Interval: 30
Monitor while connected: Off
Ping IP Address:

4.3 Quick Links

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

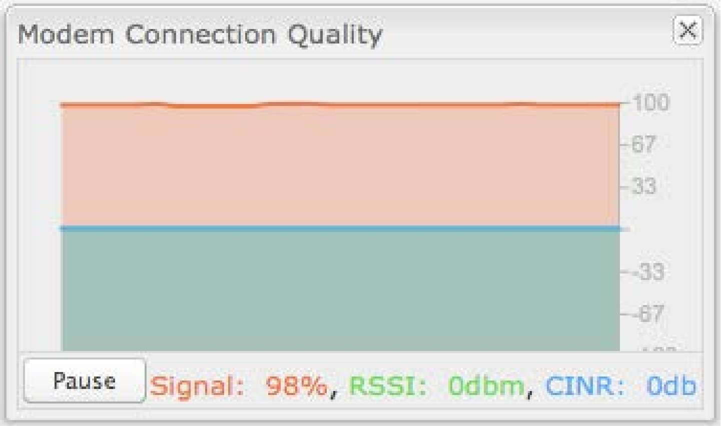
The black bar across the top provides quick access to important information and controls.



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

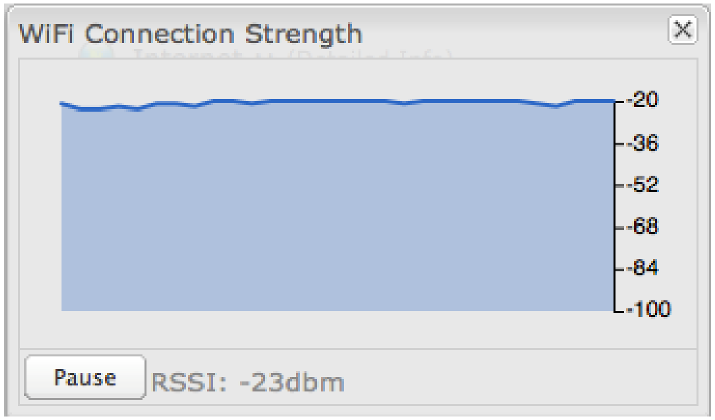
Click on this green dot to link to **Internet → Connection Manager** where you can manage your WAN interfaces.

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



Signal: 98%, RSSI: 0dbm, CINR: 0db

WiFi Clients Click to view a signal strength indicator for your network, "WiFi Connection Strength".



RSSI: -23dbm

1 The number listed in the orange block shows the number of attached clients. Click this to go to the Client List page (**Status → Client List**).

Logout Click to log out of the administration pages.

4.4 Configuration Pages

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

Getting Started	Status	Network Settings	Internet	System Settings
Enterprise Cloud Manager Registration First Time Setup IP Passthrough Setup WiFi Protected Setup	Client List CP Connect Dashboard GPS GRE Tunnels Hotspot Clients Internet Connections Routing Statistics System Logs VPN Tunnels WiPipe QoS	Content Filtering DHCP Server DNS Firewall MAC Filter / Logging Routing Routing Protocols WiFi / Local Networks WiPipe QoS	Connection Manager CP Connect Client Data Usage Data Usage GRE Tunnels L2TP Tunnels Network Mobility (NEMO) NHRP Interfaces OpenVPN Tunnels VPN Tunnels WiFi as WAN / Bridge WAN Affinity / Load Balancing	Administration Device Alerts Enterprise Cloud Manager Feature Licenses Hotspot Services Serial Redirector SNMP Configuration System Control System Software

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

Network Settings – Provides configuration options for the networks, or LAN, created by your router. For example, enable a guest WiFi network (**WiFi / Local Networks**), set up rules to filter websites (**Content Filtering**), or create a traffic-shaping rule to set bandwidth priorities (**WiPipe QoS**).

Internet – Provides configuration options for the Internet sources, or WAN, used by the router. For example, you can set up a rule to track how much data you are using per month on a modem (**Data Usage**), set WiFi to be an Internet source (**WiFi as WAN / Bridge**), or set the failover order for your Internet sources (**Connection Manager**).

System Settings – Provides broad administrative controls. For example, you can set up a Terms of Use page for your guest network (**Hotspot Services**), enable remote management of the router (**Administration**), or upgrade firmware (**System Software**).

4.4.1 Network Settings vs. Internet

When using the Web interface, it will be important to pay attention to the difference between the **Internet source** for your MBR1400 and the **network** created by the MBR1400. The **"Internet"** tab broadly refers to the router's source of Internet, while the **"Network Settings"** tab broadly refers to the network created by the router.

Internet tab	**Network Settings** tab
Internet "input" Source for MBR1400 WAN (Wide Area Network)	Internet "output" Network created by MBR1400 LAN (Local Area Network)

Examples:

- If you want to change the content filtering settings for the network created by the MBR1400, go to the **Network Settings** tab.
- If you have multiple Internet sources (such as a Cradlepoint business-grade modem and an Ethernet connection) for which you would like to set priority levels, go to the **Internet** tab.

4.5 Enterprise Cloud Manager Registration

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

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

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

4.6 IP Passthrough Setup

You can quickly enable IP passthrough with the IP Passthrough Setup Wizard available under **Getting Started → 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.

Using this function requires many changes to your router configuration. The IP Passthrough Setup Wizard will automatically make these changes for you: simply read through the wizard and select **Enable IP Passthrough** on the second page. For further configuration options, see **Network Settings → WiFi / Local Networks**.

Review the list of changes to ensure they are compatible with your router needs:

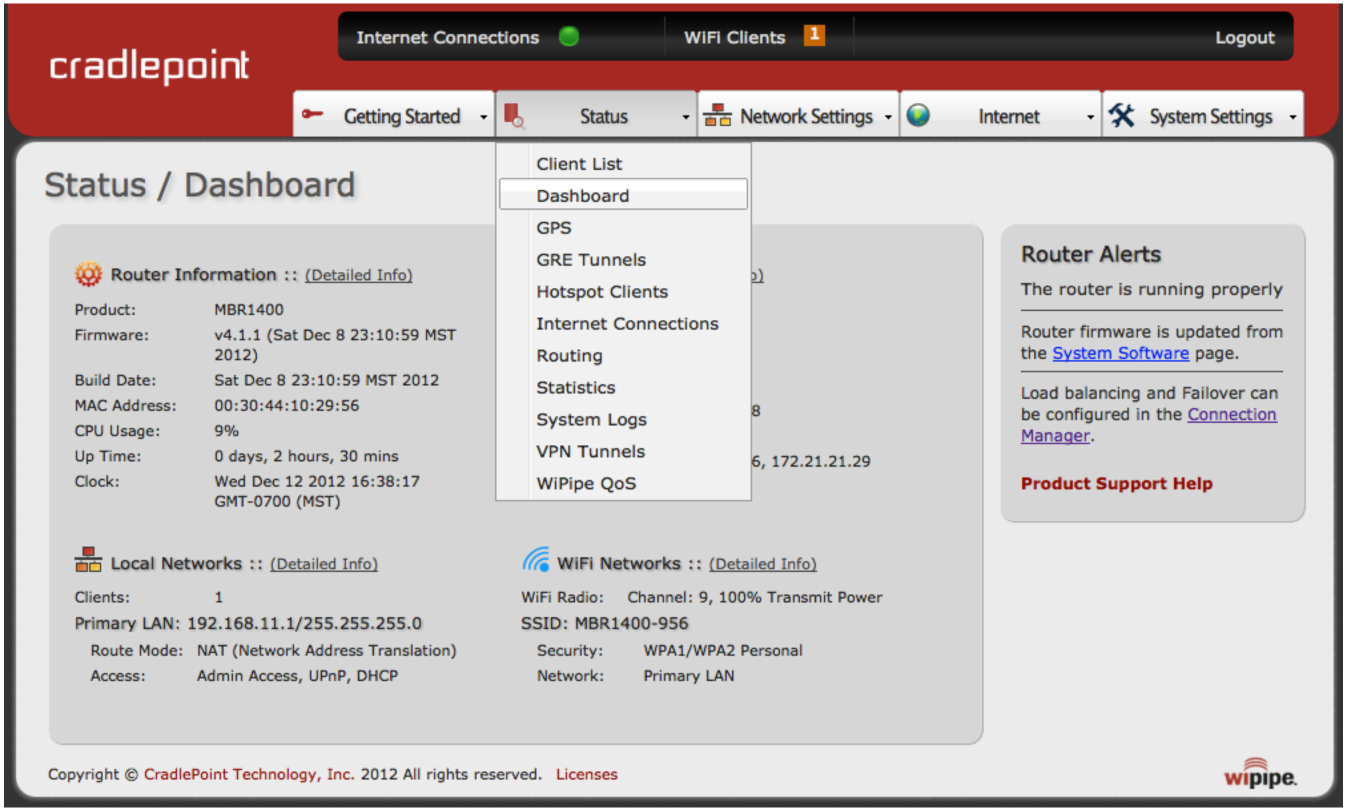
- All Ethernet ports will be set to LAN (i.e. you cannot use Ethernet as an Internet source for your router).
- All WAN devices will have Load Balance disabled and the highest priority device will be used.
- All network groups except the primary network group will be removed.
- All wireless interfaces will be removed from the primary network group. (It is possible to have a wireless interface associated with another network.)
- All router-based VPN and GRE services will be disabled.
- The Routing Mode will be set to IP Passthrough. (**Network Settings → Local Networks** in the “Local Network Editor” under “IP Settings”)
- The Subnet Selection Mode will be set to "Automatically Create Subnet". (**Network Settings → Local Networks** in the “Local Network Editor” under “IP Settings” – this shows once IP Passthrough is set as the Routing Mode)

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

5 STATUS

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

- Client List
- CP Connect
- Dashboard
- GPS
- GRE Tunnels
- Hotspot Clients
- Internet Connections
- Routing
- Statistics
- System Logs
- VPN Tunnels
- WiPipe QoS



Status / Dashboard

Router Information :: (Detailed Info)

Product: MBR1400
Firmware: v4.1.1 (Sat Dec 8 23:10:59 MST 2012)
Build Date: Sat Dec 8 23:10:59 MST 2012
MAC Address: 00:30:44:10:29:56
CPU Usage: 9%
Up Time: 0 days, 2 hours, 30 mins
Clock: Wed Dec 12 2012 16:38:17 GMT-0700 (MST)

Local Networks :: (Detailed Info)

Clients: 1
Primary LAN: 192.168.11.1/255.255.255.0
Route Mode: NAT (Network Address Translation)
Access: Admin Access, UPnP, DHCP

WiFi Networks :: (Detailed Info)

WiFi Radio: Channel: 9, 100% Transmit Power
SSID: MBR1400-956
Security: WPA1/WPA2 Personal
Network: Primary LAN

Router Alerts

The router is running properly

Router firmware is updated from the System Software page.

Load balancing and Failover can be configured in the Connection Manager.

Product Support Help

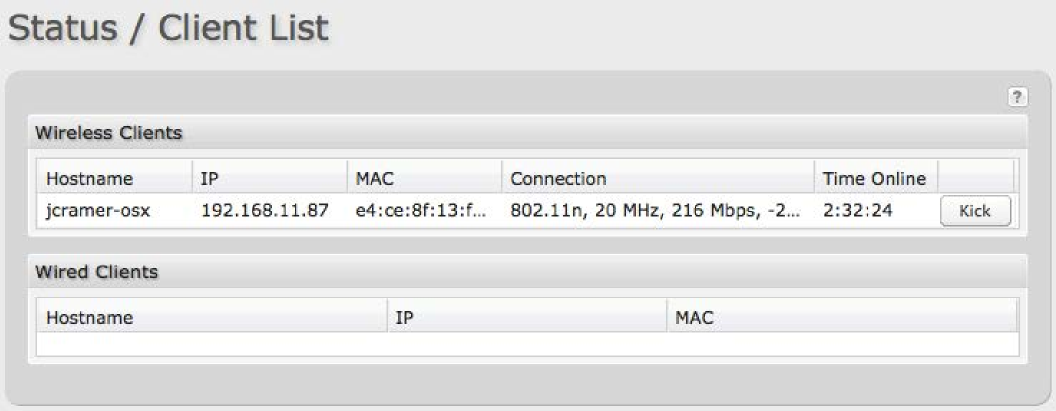
Copyright © CradlePoint Technology, Inc. 2012 All rights reserved. Licenses

5.1 Client List

The Client List displays the specifications of each device connected to your router, including **Wireless** and **Wired** clients.

Wireless Clients. For each device using a wireless connection to your MBR1400, the following information is displayed: **Hostname**, **IP**, **MAC**, **Connection**, and **Time Online**.

Wired Clients. For each device using a wired connection to your MBR1400, the following information is displayed: **Hostname**, **IP**, and **MAC**.



Status / Client List

Wireless Clients

Hostname	IP	MAC	Connection	Time Online	
jcramer-osx	192.168.11.87	e4:ce:8f:13:f...	802.11n, 20 MHz, 216 Mbps, -2...	2:32:24	Kick

Wired Clients

Hostname	IP	MAC

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

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

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

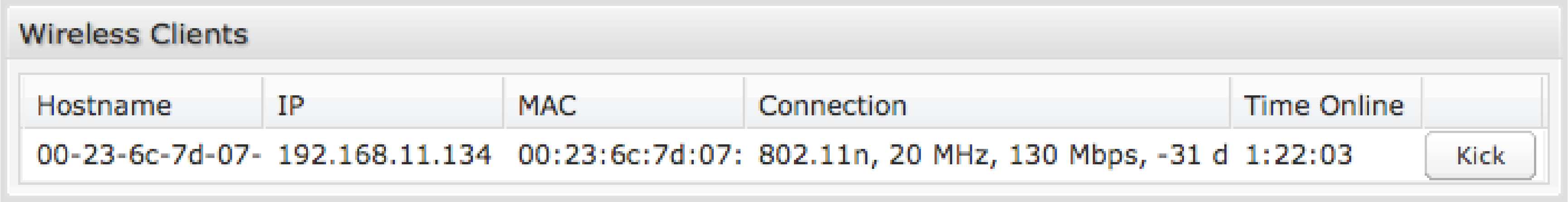
Connection: Summary of the wireless connection. For example: **802.11n, 20 MHz, 130 Mbps, -26 dBm**

- **802.11n:** The transmission standard being used by the client. Possible values include 802.11a, 802.11b, 802.11g, and 802.11n. 802.11n is the newest and best standard, but some older devices may not support it.
- **20 MHz:** This is the channel width that defines the theoretical data rate (in megahertz) that the attached computer or device can send to or receive from the router. The channel width is set in **Network Settings → WiFi / Local Networks**. Typically this will be 20 MHz, but 40 MHz is possible if the router is set to use two adjacent 20 MHz channels. A wider channel can mean better performance, but not if there is too much interference. Even if 40 MHz is set in the WiFi Channel Width, the router may still fall back to 20 MHz if interference is found.
- **130 Mbps:** The transmit rate (in megabits per second) currently used to transmit packets from the router to the client. This rate changes automatically to match environmental conditions. Distance from the router, interference, etc can impact this value. Higher values indicate better performance. Devices can still function in the network with as little as 1 Mbps.

- **-26 dBm:** A relative measure of wireless signal quality (decibels relative to one milliwatt). This expresses theoretical best quality. The value is given as a negative exponent: -20 is a very good value while -80 is relatively poor. Signal quality can be reduced by distance, by interference from other radio-frequency sources (such as cordless telephones or neighboring wireless networks), and by obstacles between the router and the wireless device.

Time Online: Simply the amount of time the device has been connected to the router.

Kick: Click on this button to disconnect a client.

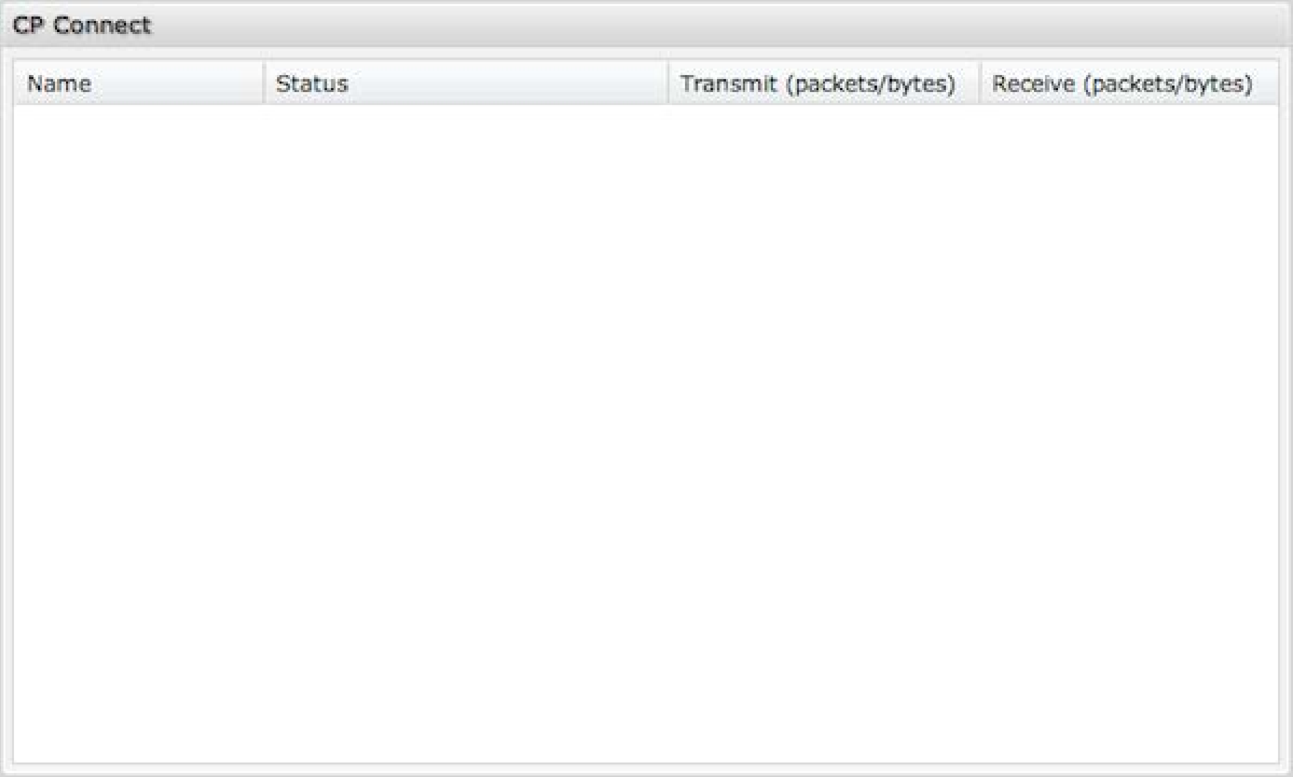


Wireless Clients

Hostname	IP	MAC	Connection	Time Online	
00-23-6c-7d-07-	192.168.11.134	00:23:6c:7d:07:	802.11n, 20 MHz, 130 Mbps, -31 d	1:22:03	Kick

5.2 CP Connect

View the status of configured CP Connect tunnels.



CP Connect

Name	Status	Transmit (packets/bytes)	Receive (packets/bytes)

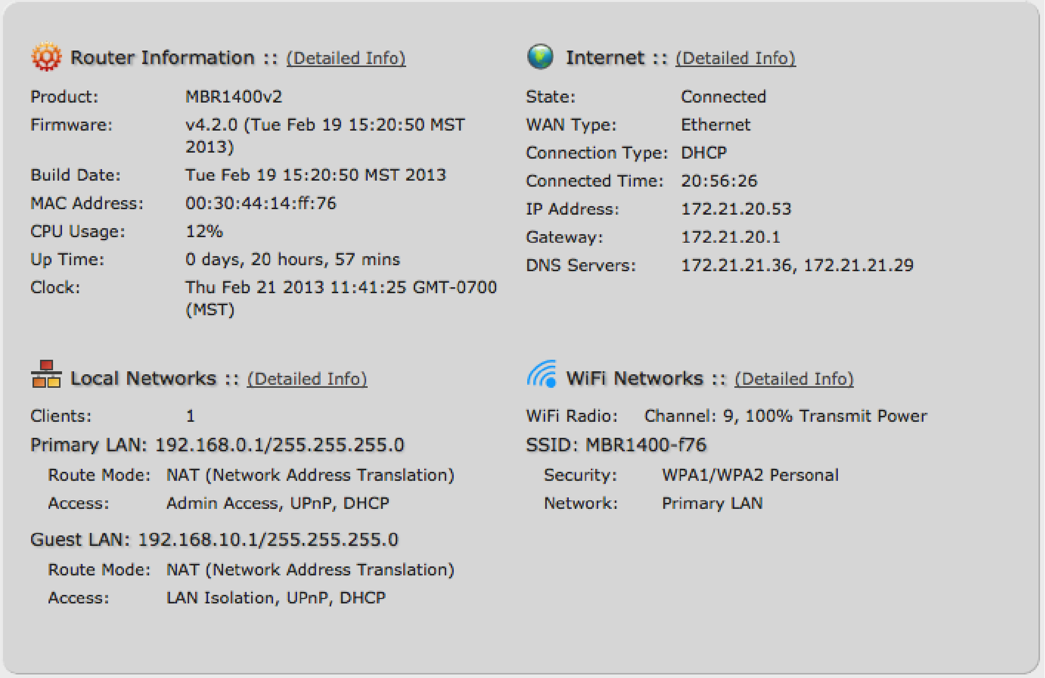
To set up or edit a CP Connect tunnel, go to **Internet → VPN Tunnels**.

NOTE: CP Connect requires a feature license. Go to System **Settings → Feature Licenses** to enable this feature.

5.3 Dashboard

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

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



Router Information :: Detailed Info

Product: MBR1400v2
Firmware: v4.2.0 (Tue Feb 19 15:20:50 MST 2013)
Build Date: Tue Feb 19 15:20:50 MST 2013
MAC Address: 00:30:44:14:ff:76
CPU Usage: 12%
Up Time: 0 days, 20 hours, 57 mins
Clock: Thu Feb 21 2013 11:41:25 GMT-0700 (MST)

Internet :: Detailed Info

State: Connected
WAN Type: Ethernet
Connection Type: DHCP
Connected Time: 20:56:26
IP Address: 172.21.20.53
Gateway: 172.21.20.1
DNS Servers: 172.21.21.36, 172.21.21.29

Local Networks :: Detailed Info

Clients: 1
Primary LAN: 192.168.0.1/255.255.255.0
Route Mode: NAT (Network Address Translation)
Access: Admin Access, UPnP, DHCP
Guest LAN: 192.168.10.1/255.255.255.0
Route Mode: NAT (Network Address Translation)
Access: LAN Isolation, UPnP, DHCP

WiFi Networks :: Detailed Info

WiFi Radio: Channel: 9, 100% Transmit Power
SSID: MBR1400-f76
Security: WPA1/WPA2 Personal
Network: Primary LAN

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

Router Information

- **System Settings → Administration**

Internet

- **Internet → Connection Manager**

Local Networks

- **Network Settings → WiFi / Local Networks**

WiFi Networks

- **Network Settings → WiFi / Local Networks**

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

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

- **Product:** MBR1400 or MBR1400v2
- **Firmware**: Gives the number of the current firmware version
- **Build Date:** Year-month-day-hours-minutes-seconds for the most recent firmware upgrade
- **MAC Address:** The router’s unique identifier
- **CPU Usage:** Expressed as a percentage
- **Up Time:** Total time for current session
- **Clock:** Current local date and time

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

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

- **State:** Connected/Disconnected
- **Signal Strength:** Expressed as a percentage (Signal Strength is not included if Ethernet is the WAN type)
- **WAN Type:** Ethernet, Modem, or WiFi as WAN
- **Connection Type:** Possibilities include: DHCP (for Ethernet), HSPA, LTE, WiMAX, etc.
- **Connected Time:** The time the current Internet source (WAN) has been connected
- **IP Address**
- **Gateway**
- **DNS Servers**

For configuration options, see **Internet → Connection Manager**.
The IP address and gateway describe your active WAN source.
For DNS server configuration options, see **Network Settings → DNS**.

Local Networks: **"**Detailed Info" links to **Network Settings → WiFi / Local Networks**.

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

For each network, the following information is displayed:

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

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

WiFi Networks: **"**Detailed Info" links to **Network Settings → WiFi / Local Networks**.

- **WiFi Radio: Channel:** 1-11 for 2.4 GHz; 36, 40, 44, 48, 149, 153, 157, 161, or 165 for 5 GHz; **Transmit Power** (expressed as a percentage)

For each WiFi network, the following information is displayed:

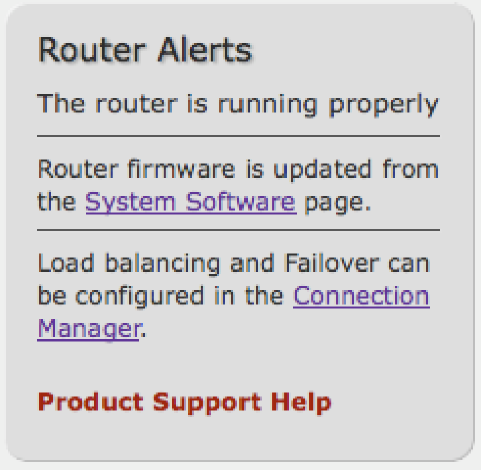
- **SSID:** Service Set Identifier, an identifier for a wireless network
    - **Security:** WPA2/WPA1/WEP Personal/Enterprise or Open; Isolated Clients
    - **Network:** The name of the local network

To configure WiFi network settings see **Network Settings → WiFi / Local Networks**.

5.3.1 Router Alerts

On the right side of the **Dashboard** page is a brief set of “**Router Alerts**” that state basic information such as whether the router is running properly. This will inform you about the availability of new firmware, for example.

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



Router Alerts

The router is running properly

Router firmware is updated from the System Software page.

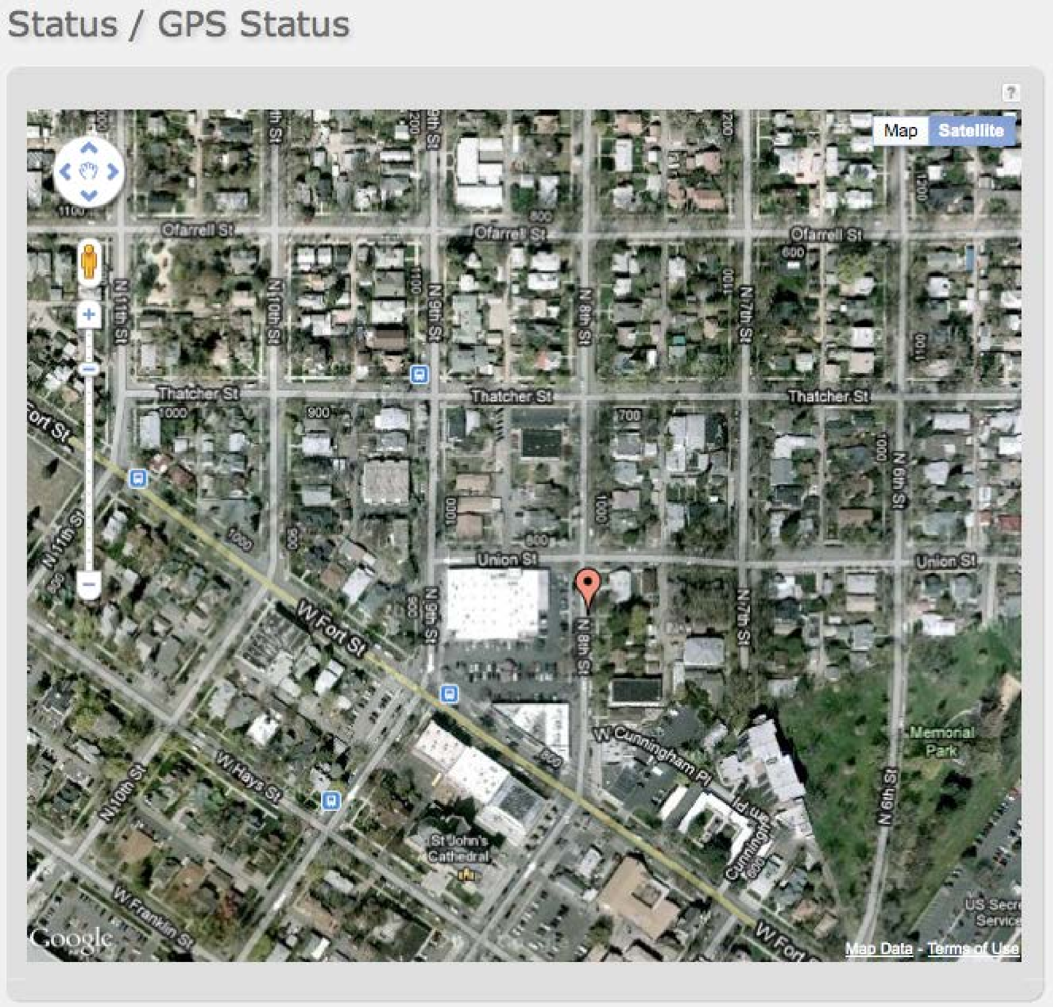
Load balancing and Failover can be configured in the Connection Manager.

Product Support Help

5.4 GPS

If GPS support is enabled and a modem capable of providing GPS coordinates is connected, this page shows a graphical view of your router's location. See the GPS section in **System Settings → Administration** to enable GPS support.

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



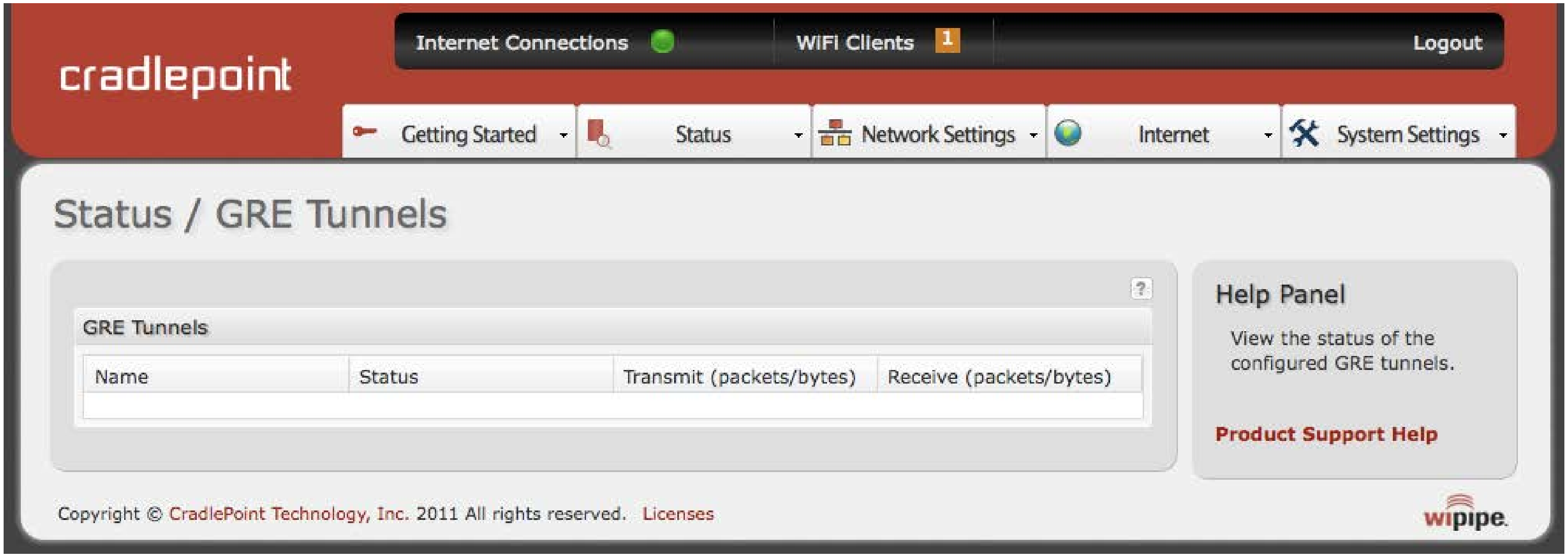
Status / GPS Status

5.5 GRE Tunnels

View the status of configured GRE Tunnels. To set up or edit a GRE tunnel, go to **Internet → GRE Tunnels**.

Included information:

- Name
- Status
- Transmit (packets/bytes)
- Receive (packets/bytes)



Status / GRE Tunnels

GRE Tunnels

Name	Status	Transmit (packets/bytes)	Receive (packets/bytes)

Help Panel

View the status of the configured GRE tunnels.

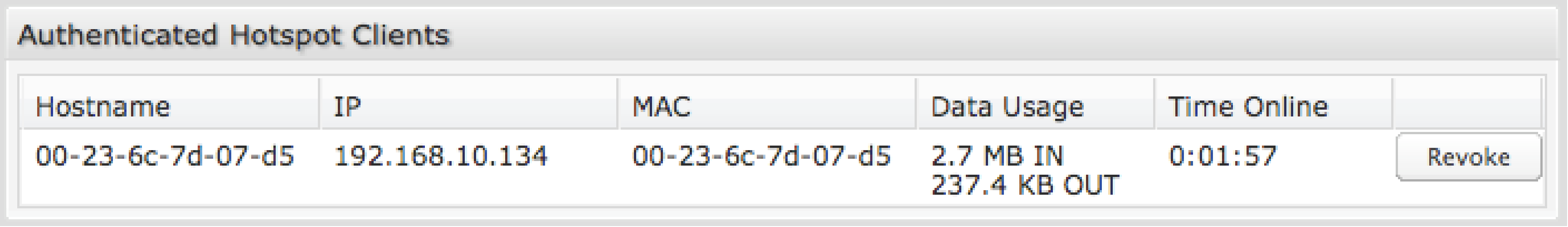
Product Support Help

Copyright © CradlePoint Technology, Inc. 2011 All rights reserved. Licenses

5.6 Hotspot Clients

View the status of the clients that have logged in through the Hotspot/Captive Portal. View:

- Hostname
- IP address
- MAC address
- Data Usage (both IN and OUT)
- Time Online



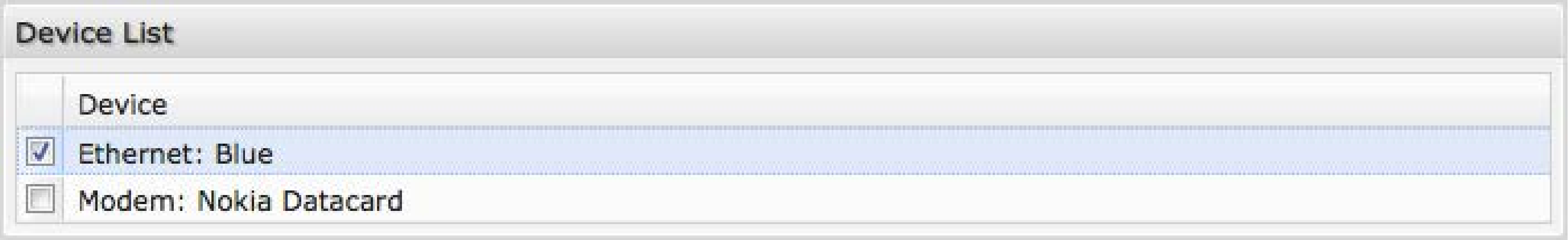
Authenticated Hotspot Clients

Hostname	IP	MAC	Data Usage	Time Online	
00-23-6c-7d-07-d5	192.168.10.134	00-23-6c-7d-07-d5	2.7 MB IN 237.4 KB OUT	0:01:57	Revoke

You may revoke a client's access to the Internet by clicking the 'Revoke' button.

5.7 Internet Connections

The Internet Connections submenu option provides a list of attached WAN devices used as the Internet source for the MBR1400. Select one of these devices to see detailed information about that particular device.



Device List

	Device
☑	Ethernet: Blue
□	Modem: Nokia Datacard

For each type of device, different information will be included in the **Device Information** section. Possible devices include:

- Ethernet
- LTE Modem
- HSPA+ Modem
- WiMAX Modem
- GSM Modem
- EVDO Modem
- WiFi as WAN

Depending on the device, possible information will be in the following sections: Diagnostics, General Information, IP Information, and Statistics. For modems, the Diagnostics section provides specific information about how the modem is communicating with its carrier.

5.7.1 Ethernet

General Information

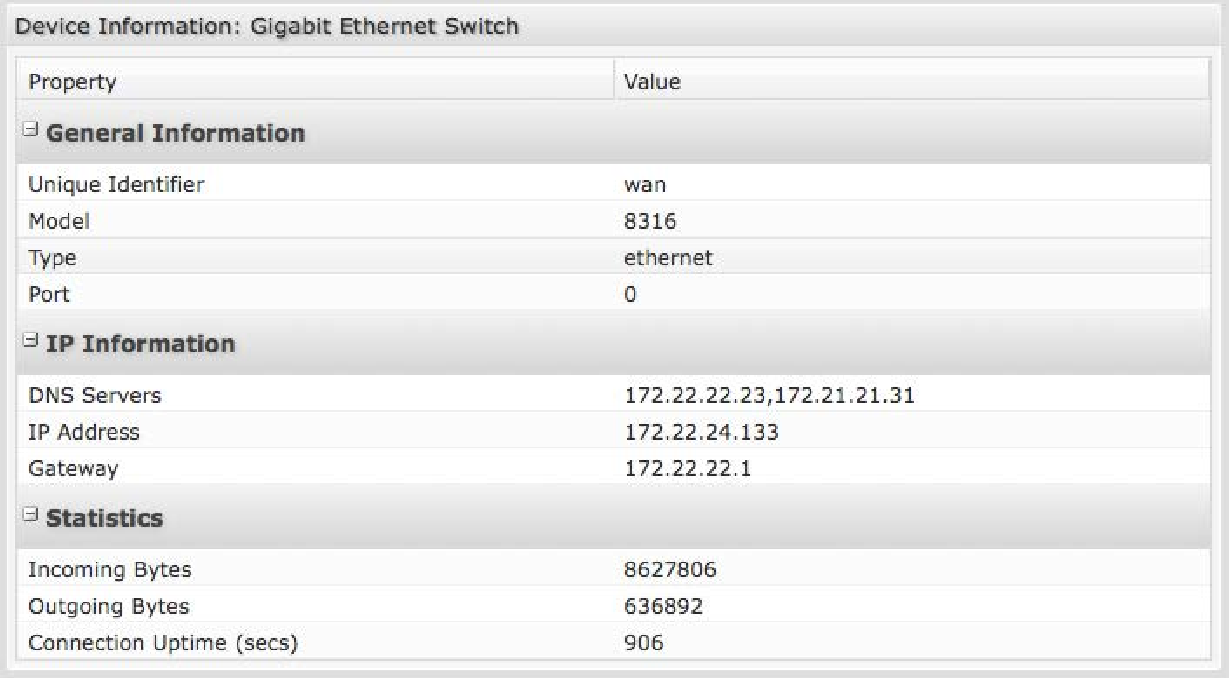
- **Unique Identifier** *wan*
- **Model**
- **Type** *ethernet*
- **Port**

IP Information

- **DNS Servers**
- **IP Address**
- **Gateway**

Statistics

- **Incoming Bytes**
- **Outgoing Bytes**
- **Connection Uptime (secs)**



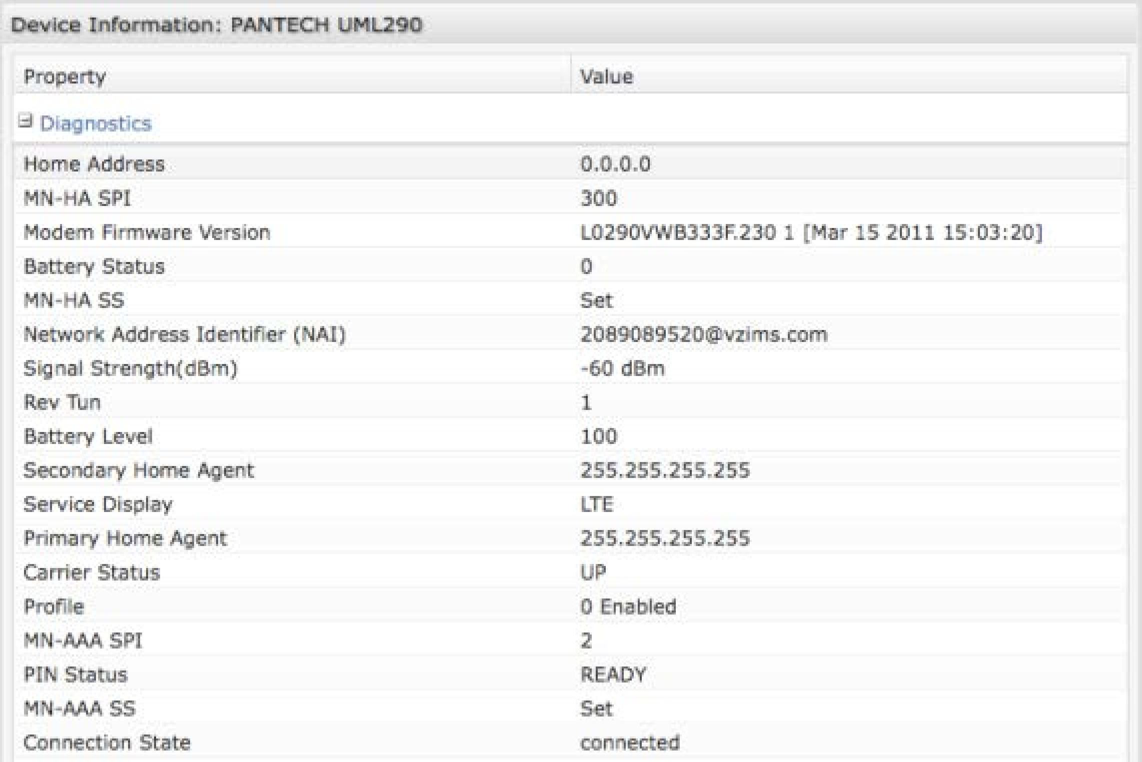
Device Information: Gigabit Ethernet Switch

Property	Value
⊟ **General Information**	
Unique Identifier	wan
Model	8316
Type	ethernet
Port	0
⊟ **IP Information**	
DNS Servers	172.22.22.23,172.21.21.31
IP Address	172.22.24.133
Gateway	172.22.22.1
⊟ **Statistics**	
Incoming Bytes	8627806
Outgoing Bytes	636892
Connection Uptime (secs)	906

5.7.2 LTE Modem (PANTECH UML290)

Diagnostics

- **Home Address**
- **MN-HA SPI**
- **Modem Firmware Version**
- **Battery Status**
- **MN-HA SS**
- **Network Address Identifier (NAI)**
- **Signal Strength(dBm)**
- **Rev Tun**
- **Battery Level**
- **Secondary Home Agent**
- **Service Display** *LTE*
- **Primary Home Agent**
- **Carrier Status**
- **Profile**
- **MN-AAA SPI**
- **PIN Status**
- **MN-AAA SS**
- **Connection State** (connected, idle, etc.)



Device Information: PANTECH UML290

Property	Value
⊟ Diagnostics	
Home Address	0.0.0.0
MN-HA SPI	300
Modem Firmware Version	L0290VWB333F.230 1 [Mar 15 2011 15:03:20]
Battery Status	0
MN-HA SS	Set
Network Address Identifier (NAI)	2089089520@vzims.com
Signal Strength(dBm)	-60 dBm
Rev Tun	1
Battery Level	100
Secondary Home Agent	255.255.255.255
Service Display	LTE
Primary Home Agent	255.255.255.255
Carrier Status	UP
Profile	0 Enabled
MN-AAA SPI	2
PIN Status	READY
MN-AAA SS	Set
Connection State	connected

General Information

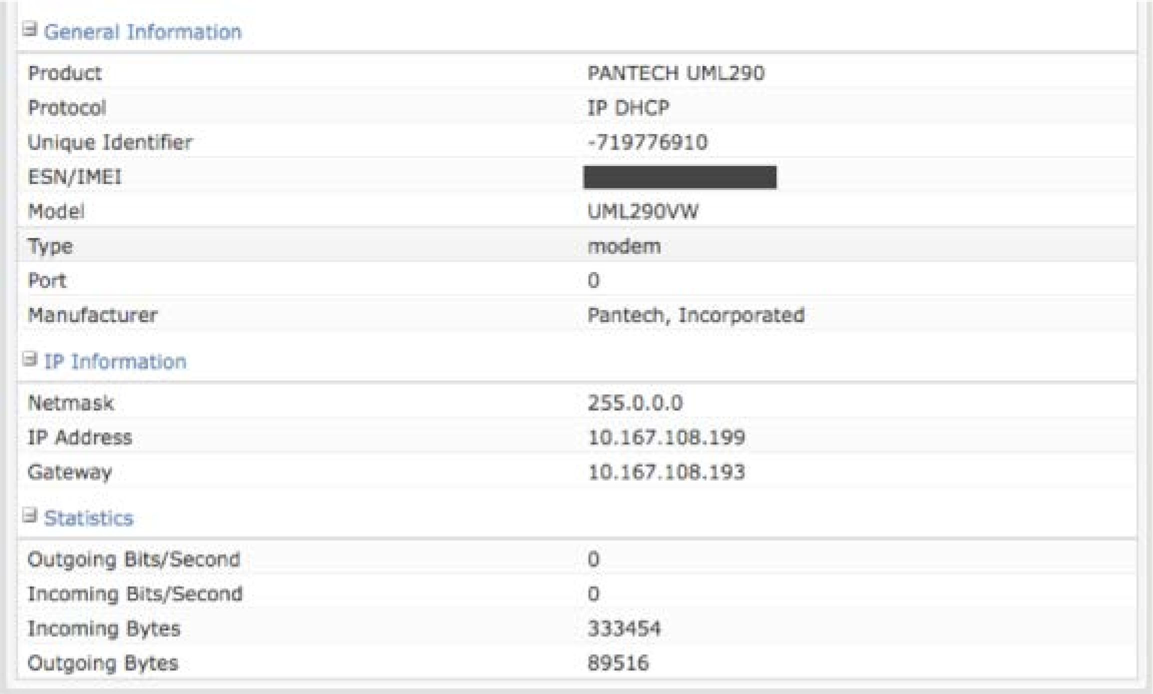
- **Product** *PANTECH UML290*
- **Protocol** *IP DHCP*
- **Unique Identifier**
- **ESN/IMEI**
- **Model** *UML290VW*
- **Type** *modem*
- **Port**
- **Manufacturer** *Pantech, Incorporated*

IP Information

- **Netmask**
- **IP Address**
- **Gateway**

Statistics

- **Outgoing Bits/Second**
- **Incoming Bits/Second**
- **Incoming Bytes**
- **Outgoing Bytes**



⊟ General Information

Product	PANTECH UML290
Protocol	IP DHCP
Unique Identifier	-719776910
ESN/IMEI	[redacted]
Model	UML290VW
Type	modem
Port	0
Manufacturer	Pantech, Incorporated

⊟ IP Information

Netmask	255.0.0.0
IP Address	10.167.108.199
Gateway	10.167.108.193

⊟ Statistics

Outgoing Bits/Second	0
Incoming Bits/Second	0
Incoming Bytes	333454
Outgoing Bytes	89516

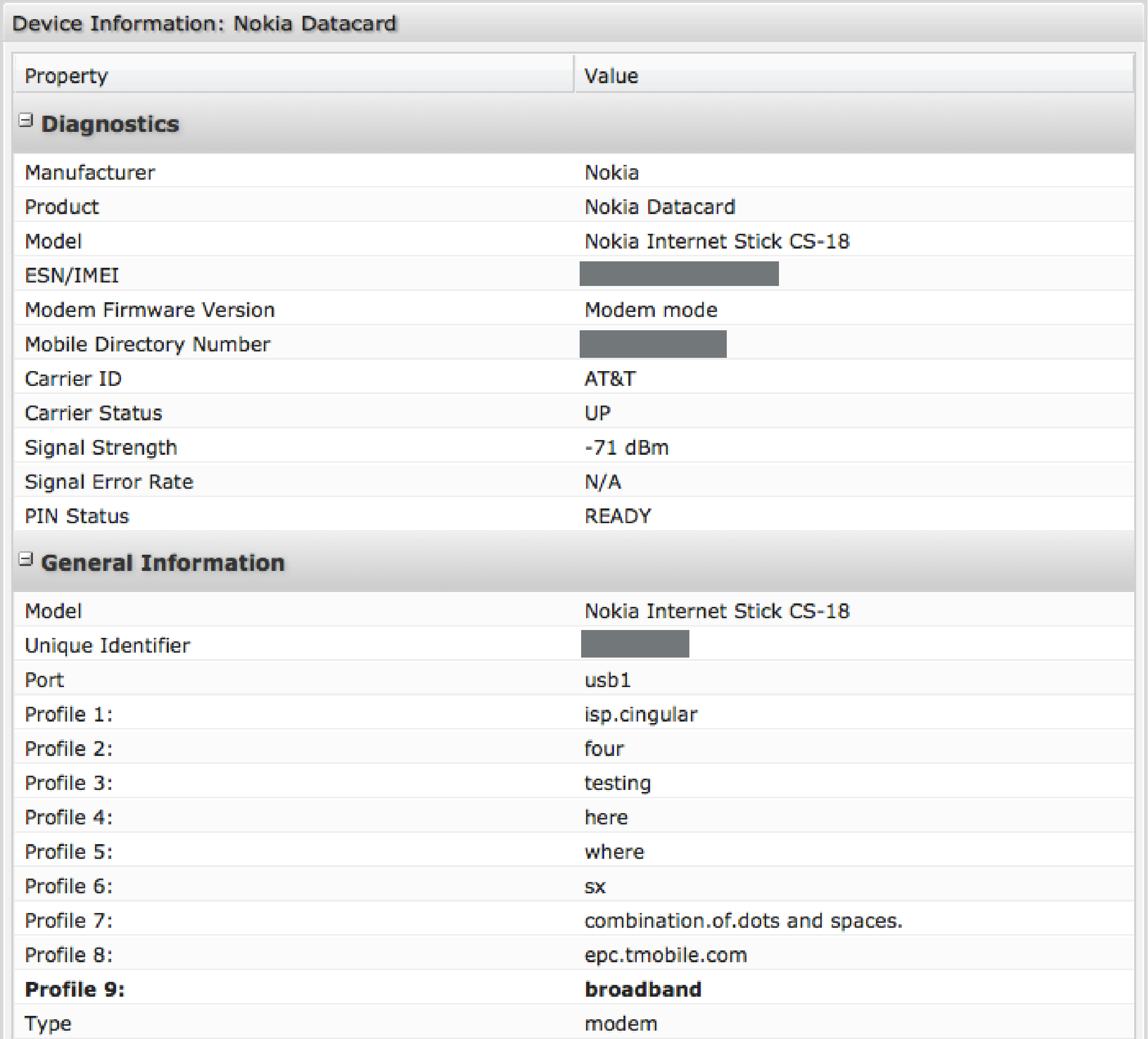
5.7.3 HSPA+ Modem (Nokia Datacard)

Diagnostics

- **Manufacturer** *Nokia*
- **Product** *Nokia Datacard*
- **Model** *Nokia Internet Stick CS-18*
- **ESN/IMEI**
- **Modem Firmware Version**
- **Mobile Directory Number**
- **Carrier ID** *AT&T*
- **Carrier Status**
- **Signal Strength**
- **Signal Error Rate**
- **PIN Status**

General Information

- **Model** *Nokia Internet Stick CS-18*
- **Unique Identifier**
- **Port**
- **Profiles 1-9**
- **Type** *modem*



Device Information: Nokia Datacard

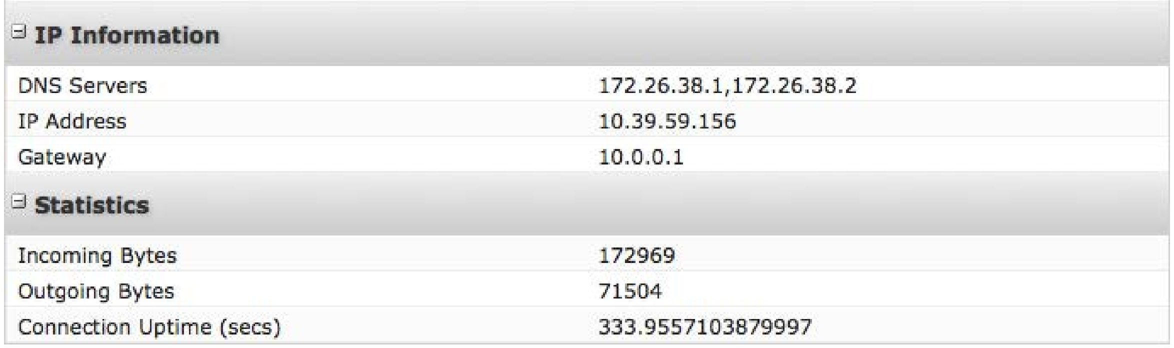
Property	Value
⊟ **Diagnostics**	
Manufacturer	Nokia
Product	Nokia Datacard
Model	Nokia Internet Stick CS-18
ESN/IMEI	[redacted]
Modem Firmware Version	Modem mode
Mobile Directory Number	[redacted]
Carrier ID	AT&T
Carrier Status	UP
Signal Strength	-71 dBm
Signal Error Rate	N/A
PIN Status	READY
⊟ **General Information**	
Model	Nokia Internet Stick CS-18
Unique Identifier	[redacted]
Port	usb1
Profile 1:	isp.cingular
Profile 2:	four
Profile 3:	testing
Profile 4:	here
Profile 5:	where
Profile 6:	sx
Profile 7:	combination.of.dots and spaces.
Profile 8:	epc.tmobile.com
Profile 9:	**broadband**
Type	modem

IP Information

- **DNS Servers**
- **IP Address**
- **Gateway**

Statistics

- **Incoming Bytes**
- **Outgoing Bytes**
- **Connection Uptime (secs)**



⊟ **IP Information**

DNS Servers	172.26.38.1,172.26.38.2
IP Address	10.39.59.156
Gateway	10.0.0.1

⊟ **Statistics**

Incoming Bytes	172969
Outgoing Bytes	71504
Connection Uptime (secs)	333.9557103879997

5.7.4 WiMAX Modem (U300 – 4G)

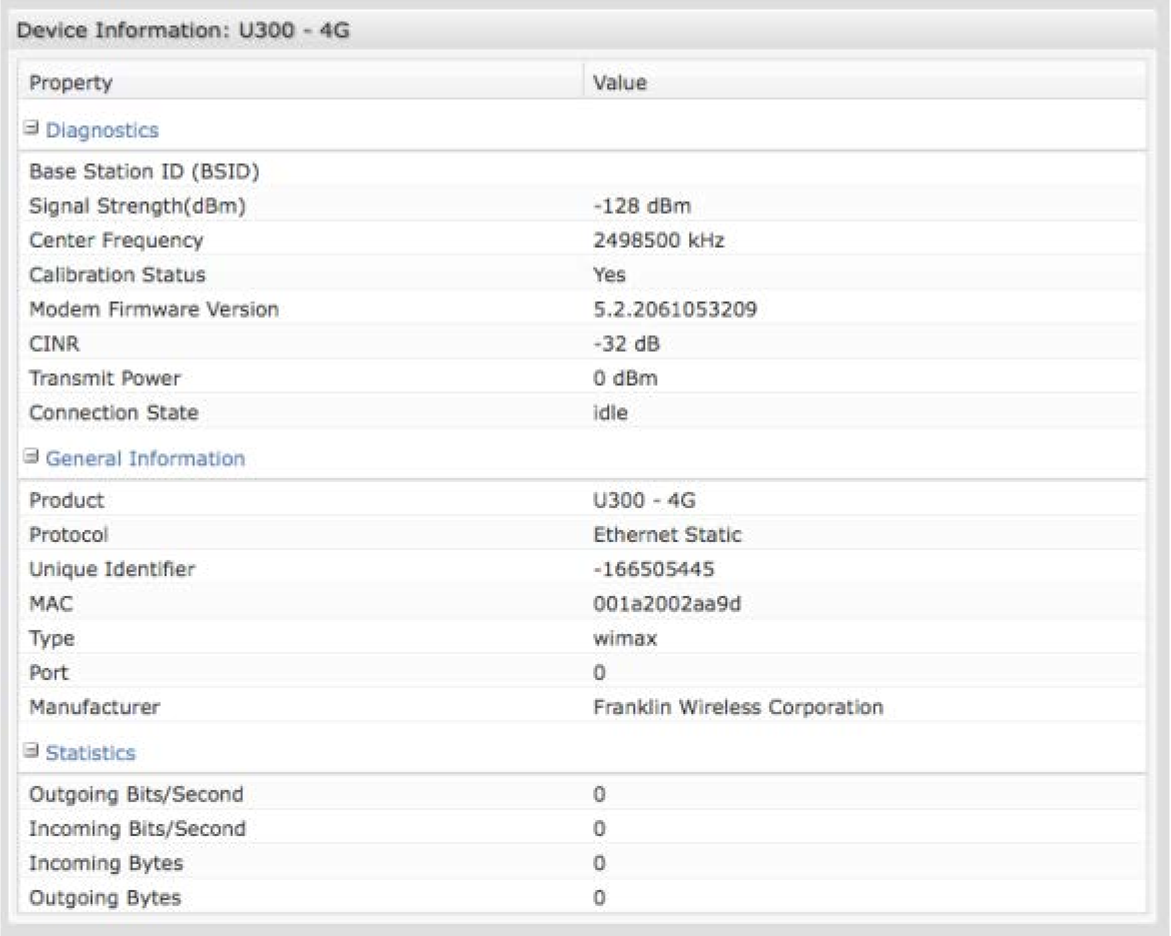
Diagnostics

For a WiMAX modem, the CINR and Signal Strength values are important as they show how strong the signal is and that has significant effects on how much data the router can download or send. You can place the router in different locations to see where you get better signal. You can also see a LED display of the current signal strength. Pressing the router's Signal Strength button will toggle the LED display on and off.

- **Base Station ID (BSID)**
- **Signal Strength(dBm)**
- **Center Frequency**
- **Calibration Status**—Don't worry if this says the modem is not calibrated.
- **Modem Firmware Version**
- **CINR**
- **Connection State** (connected, idle, etc.)

General Information

- **Product** *U300 – 4G*
- **Protocol** *Ethernet Static*
- **Unique Identifier**
- **MAC**



Device Information: U300 - 4G

Property	Value
⊟ Diagnostics	
Base Station ID (BSID)	
Signal Strength(dBm)	-128 dBm
Center Frequency	2498500 kHz
Calibration Status	Yes
Modem Firmware Version	5.2.2061053209
CINR	-32 dB
Transmit Power	0 dBm
Connection State	idle
⊟ General Information	
Product	U300 - 4G
Protocol	Ethernet Static
Unique Identifier	-166505445
MAC	001a2002aa9d
Type	wimax
Port	0
Manufacturer	Franklin Wireless Corporation
⊟ Statistics	
Outgoing Bits/Second	0
Incoming Bits/Second	0
Incoming Bytes	0
Outgoing Bytes	0

- **Type** *WiMAX*
- **Port**
- **Manufacturer** *Franklin Wireless Corporation*

Statistics

- **Outgoing Bits/Second**
- **Incoming Bits/Second**
- **Incoming Bytes**
- **Outgoing Bytes**

5.7.5 GSM Modem (Nokia Datacard)

Diagnostics

- **Signal Error Rate**
- **Modem Firmware Version**
- **Battery Status**
- **Battery Level**
- **Carrier Status**
- **Signal Strength(dBm)**
- **PIN Status**
- **Connection State** (connected, idle, etc.)

General Information

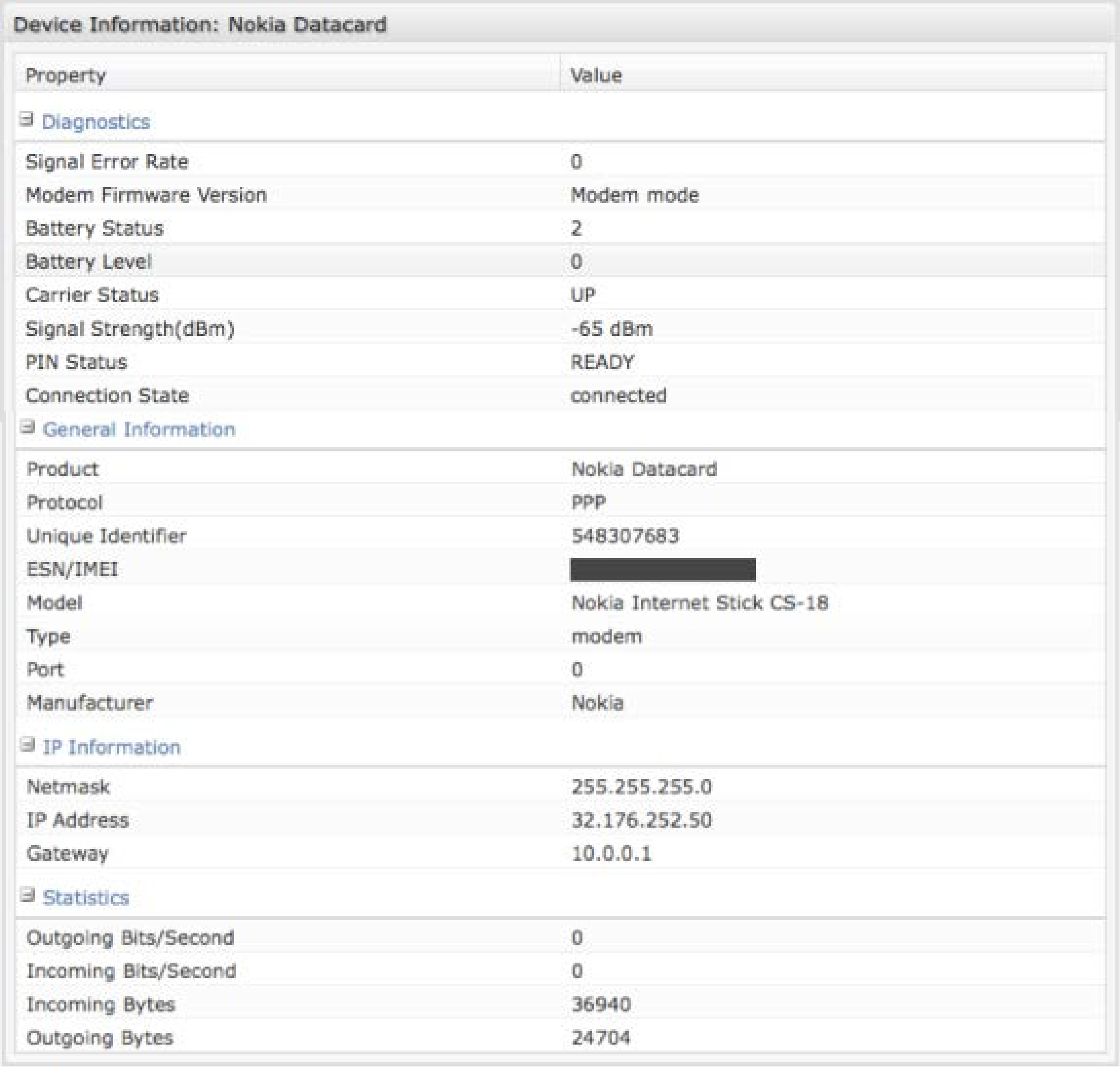
- **Product** *Nokia Datacard*
- **Protocol** *PPP*
- **Unique Identifier**
- **ESN/IMEI**
- **Model** *Nokia Internet Stick CS-18*
- **Type** *modem*
- **Port**
- **Manufacturer** *Nokia*

IP Information

- **Netmask**
- **IP Address**
- **Gateway**

Statistics

- **Outgoing Bits/Second**
- **Incoming Bits/Second**



Device Information: Nokia Datacard

Property	Value
⊟ Diagnostics	
Signal Error Rate	0
Modem Firmware Version	Modem mode
Battery Status	2
Battery Level	0
Carrier Status	UP
Signal Strength(dBm)	-65 dBm
PIN Status	READY
Connection State	connected
⊟ General Information	
Product	Nokia Datacard
Protocol	PPP
Unique Identifier	548307683
ESN/IMEI	[redacted]
Model	Nokia Internet Stick CS-18
Type	modem
Port	0
Manufacturer	Nokia
⊟ IP Information	
Netmask	255.255.255.0
IP Address	32.176.252.50
Gateway	10.0.0.1
⊟ Statistics	
Outgoing Bits/Second	0
Incoming Bits/Second	0
Incoming Bytes	36940
Outgoing Bytes	24704

- **Incoming Bytes**
- **Outgoing Bytes**

5.7.6 EVDO Modem: (MC760 Comcast)

Diagnostics

- **Modem Firmware Version**
- **PRL Version**
- **Service Display** *EVDO*
- **Carrier Status**
- **Signal Strength(dBm)**
- **Connection Type** *CDMA*
- **Connection State** (connected, idle, etc.)

General Information

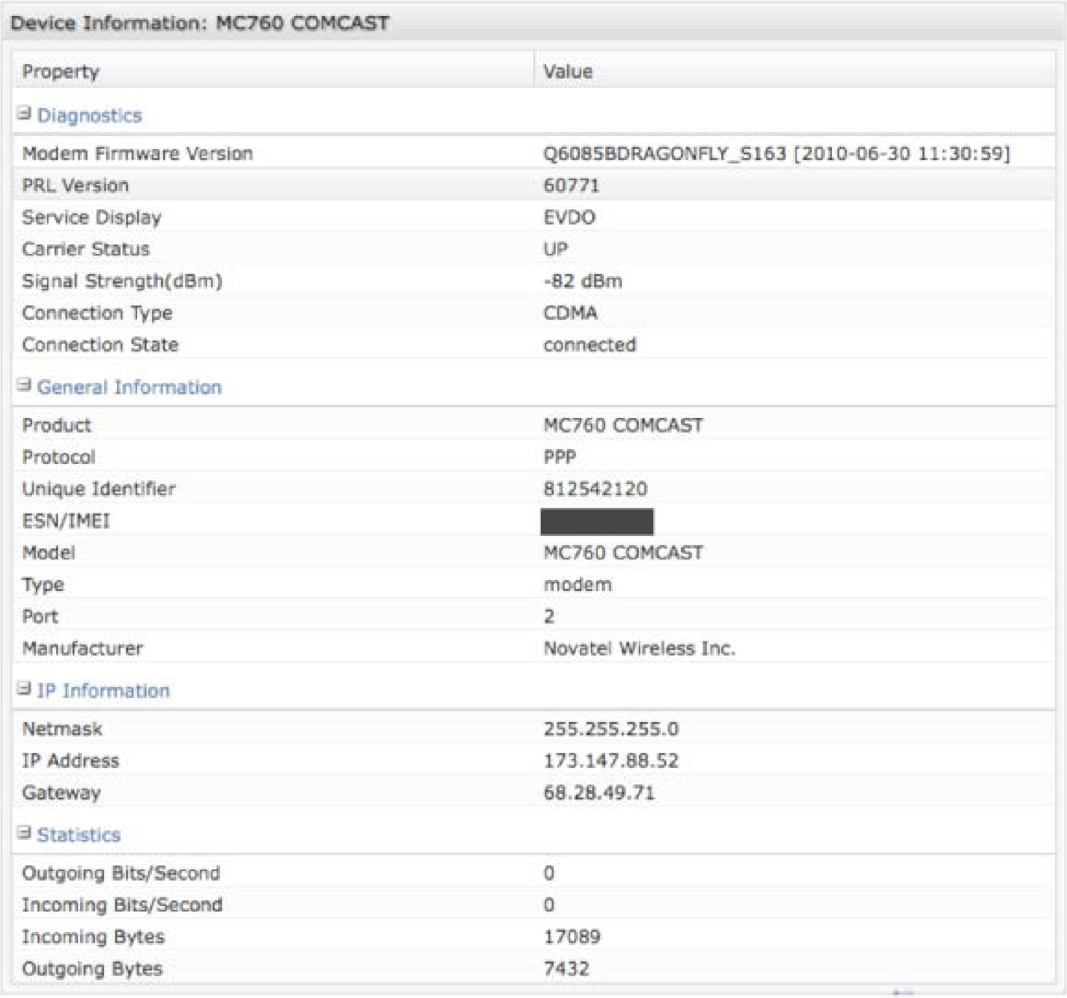
- **Product** *MC769 COMCAST*
- **Protocol** *PPP*
- **Unique Identifier**
- **ESN/IMEI**
- **Model** *MC760 COMCAST*
- **Type** *modem*
- **Port**
- **Manufacturer** *Novatel Wireless Inc.*

IP Information

- **Netmask**
- **IP Address**
- **Gateway**

Statistics

- **Outgoing Bits/Second**
- **Incoming Bits/Second**
- **Incoming Bytes**
- **Outgoing Bytes**



Device Information: MC760 COMCAST

Property	Value
⊟ Diagnostics	
Modem Firmware Version	Q6085BDRAGONFLY_S163 [2010-06-30 11:30:59]
PRL Version	60771
Service Display	EVDO
Carrier Status	UP
Signal Strength(dBm)	-82 dBm
Connection Type	CDMA
Connection State	connected
⊟ General Information	
Product	MC760 COMCAST
Protocol	PPP
Unique Identifier	812542120
ESN/IMEI	[redacted]
Model	MC760 COMCAST
Type	modem
Port	2
Manufacturer	Novatel Wireless Inc.
⊟ IP Information	
Netmask	255.255.255.0
IP Address	173.147.88.52
Gateway	68.28.49.71
⊟ Statistics	
Outgoing Bits/Second	0
Incoming Bits/Second	0
Incoming Bytes	17089
Outgoing Bytes	7432

5.7.7 WiFi as WAN

Diagnostics

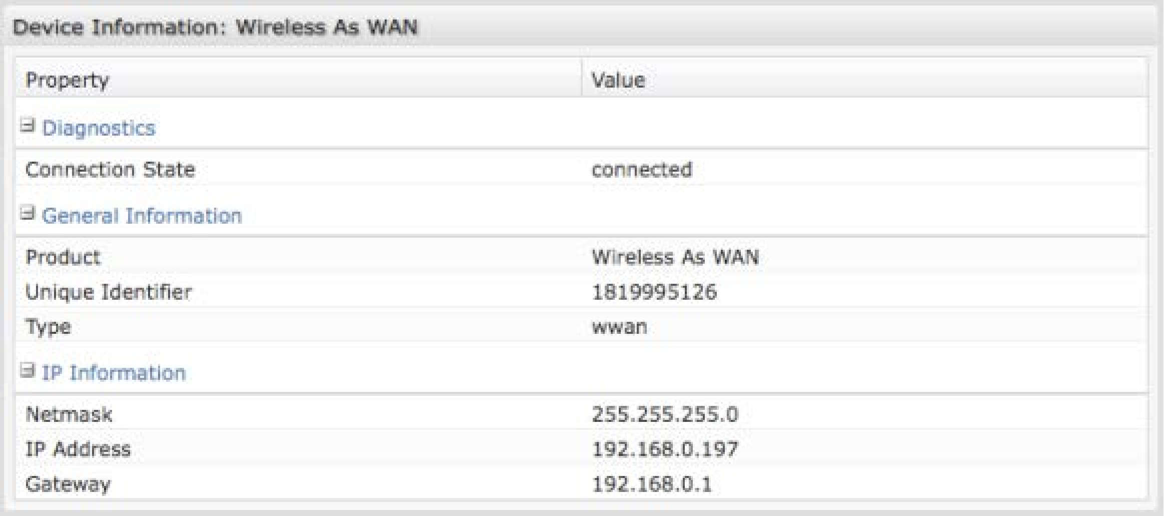
- **Connection State** (connected, idle, etc.)

General Information

- **Product** *Wireless As WAN*
- **Unique Identifier**
- **Type** *wwan*

IP Information

- **Netmask**
- **IP Address**
- **Gateway**

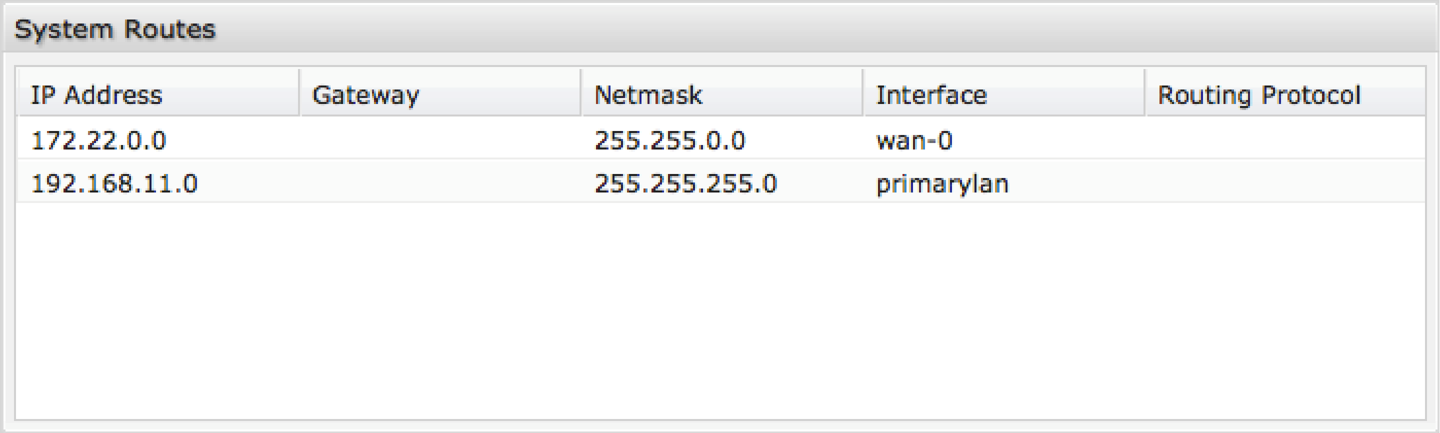


Device Information: Wireless As WAN

Property	Value
⊟ Diagnostics	
Connection State	connected
⊟ General Information	
Product	Wireless As WAN
Unique Identifier	1819995126
Type	wwan
⊟ IP Information	
Netmask	255.255.255.0
IP Address	192.168.0.197
Gateway	192.168.0.1

5.8 Routing

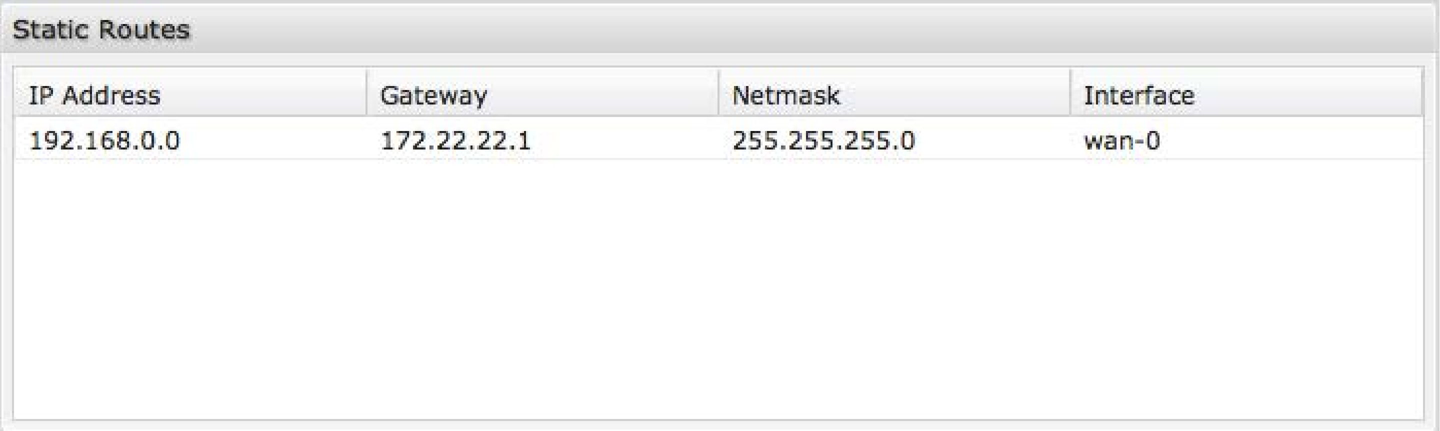
System Routes displays routes associated with networks connected to the router as well as routes learned from routing protocols (such as RIP or BGP).



System Routes

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

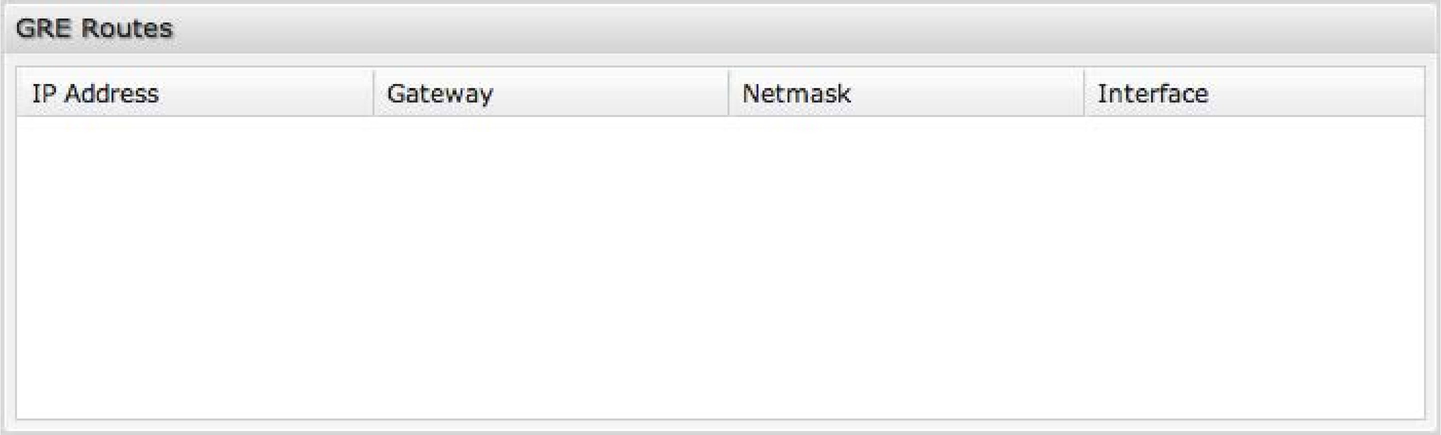
Static Routes displays user-specified routes configured in **Network Settings → Routing**.



Static Routes

IP Address	Gateway	Netmask	Interface
192.168.0.0	172.22.22.1	255.255.255.0	wan-0

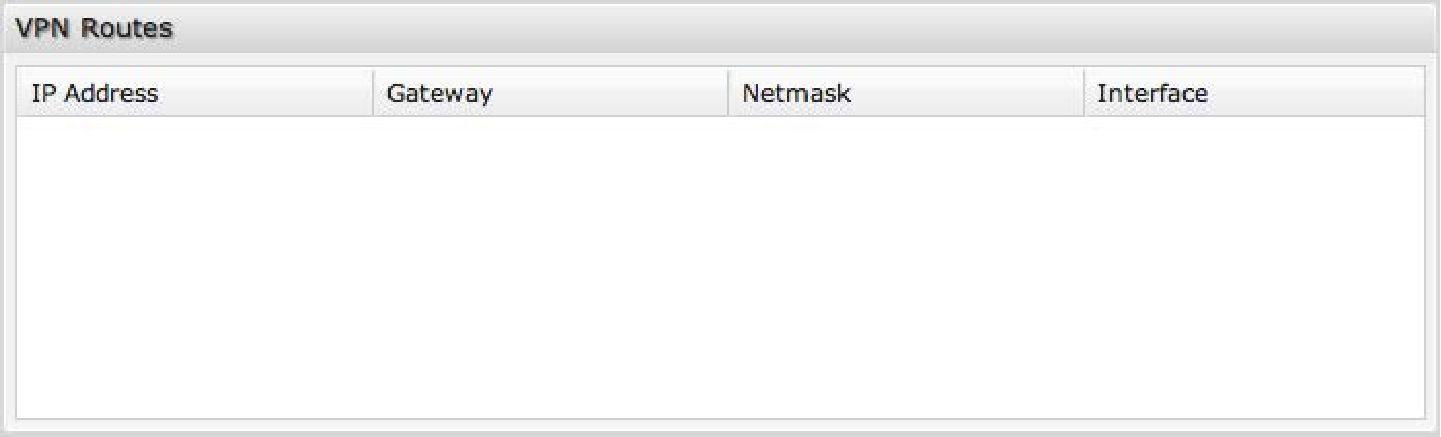
GRE Routes displays user-specified routes configured in **Internet → GRE Tunnels**.



GRE Routes

IP Address	Gateway	Netmask	Interface

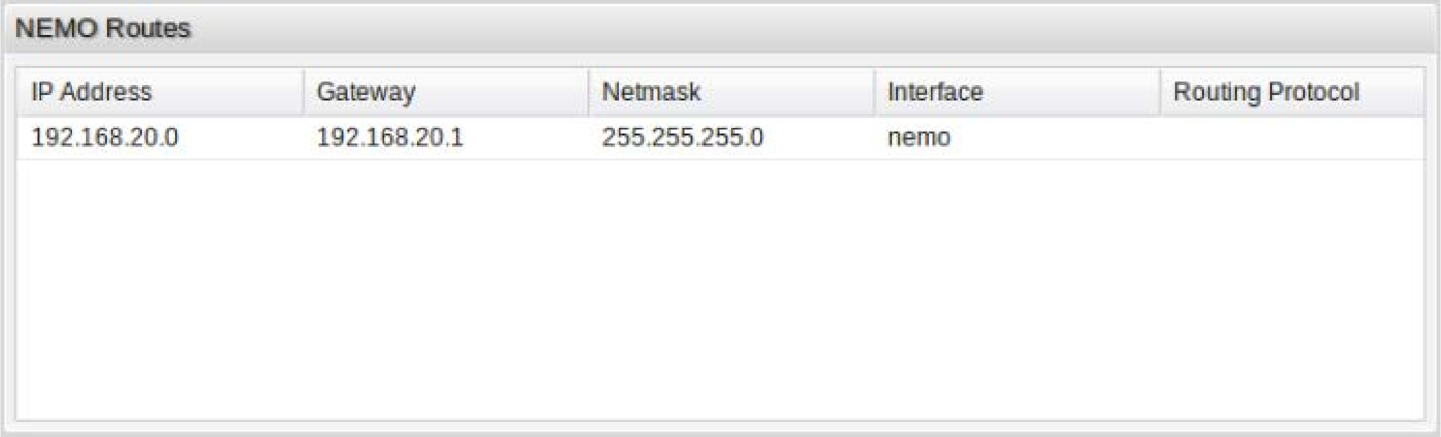
VPN Routes displays user-specified routes configured in **Internet → VPN Tunnels**.



VPN Routes

IP Address	Gateway	Netmask	Interface

NEMO Routes displays user-specified routes configured in **Internet → Network Mobility (NEMO)**.

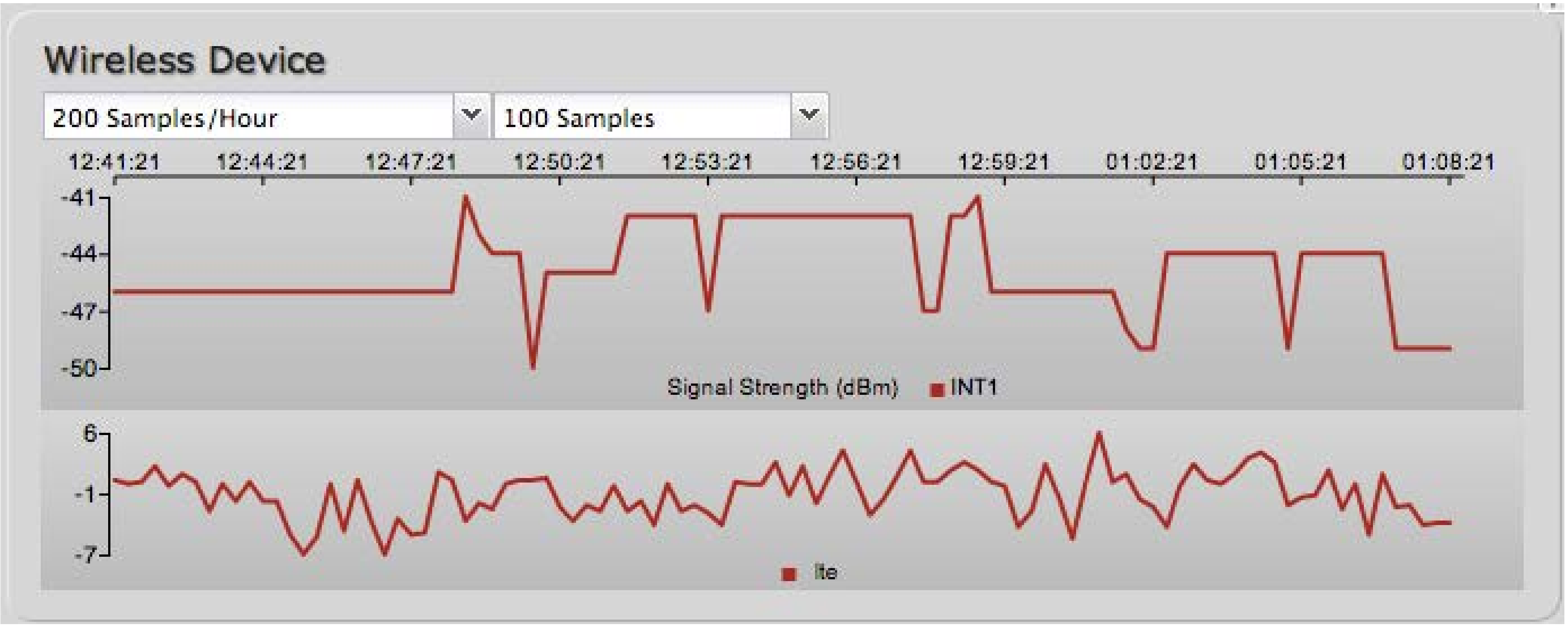


NEMO Routes

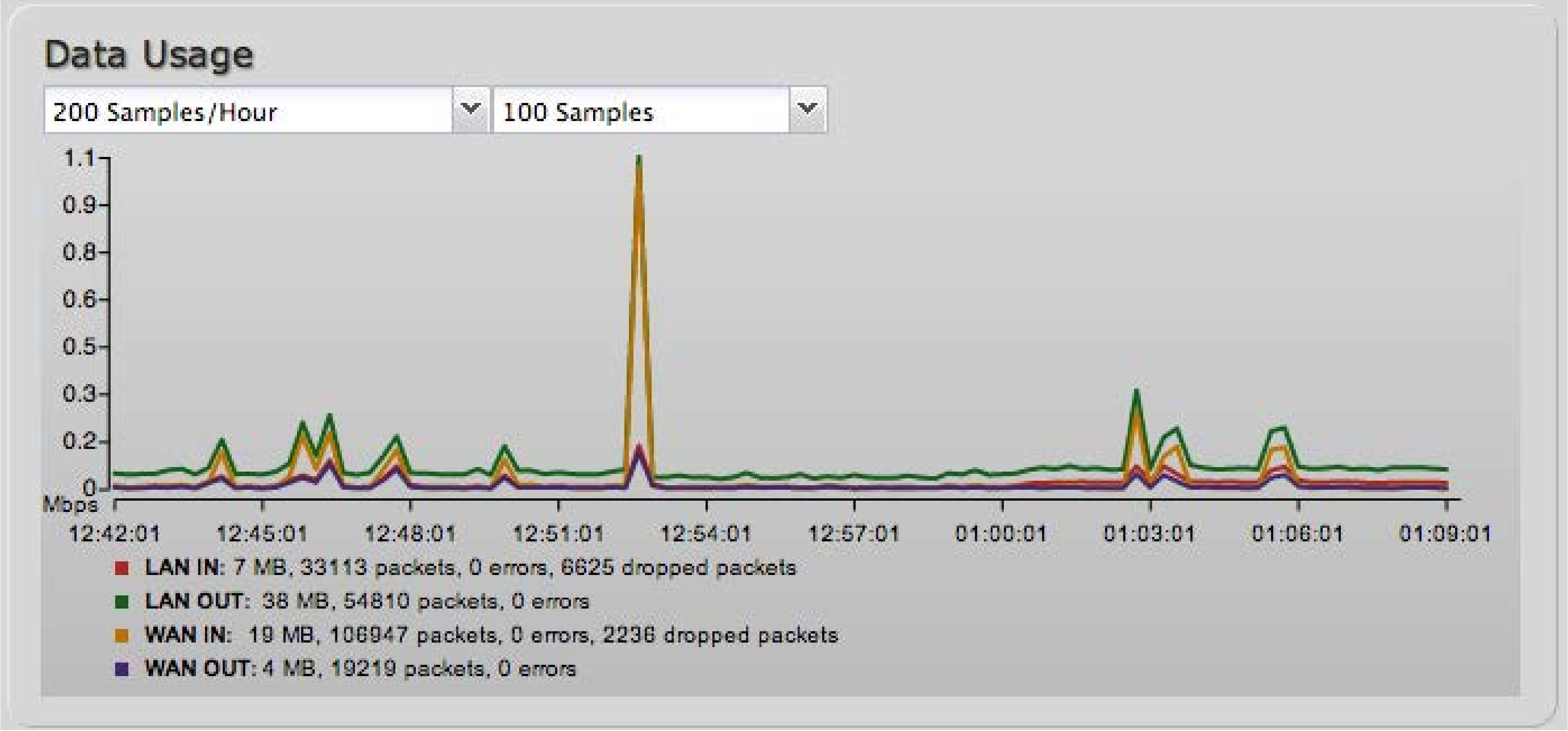
IP Address	Gateway	Netmask	Interface	Routing Protocol
192.168.20.0	192.168.20.1	255.255.255.0	nemo	

5.9 Statistics

The Statistics submenu option displays basic traffic statistics.



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



Data Usage

200 Samples/Hour

100 Samples

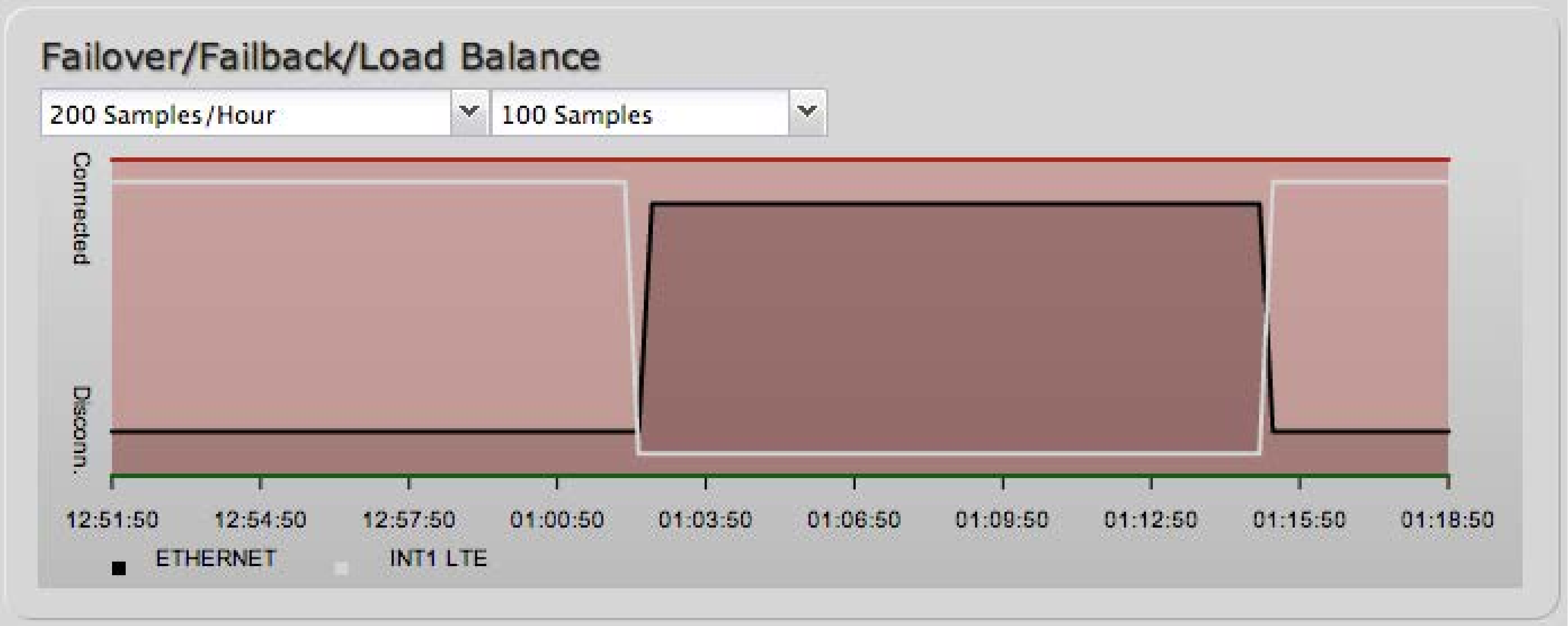
🟥 **LAN IN:** 7 MB, 33113 packets, 0 errors, 6625 dropped packets

🟩 **LAN OUT:** 38 MB, 54810 packets, 0 errors

🟧 **WAN IN:** 19 MB, 106947 packets, 0 errors, 2236 dropped packets

🟪 **WAN OUT:** 4 MB, 19219 packets, 0 errors

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



Failover/Failback/Load Balance

200 Samples/Hour

100 Samples

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

5.10 System Logs

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

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

Update: Click to check for new router messages.

Clear Log: Clear the log file.

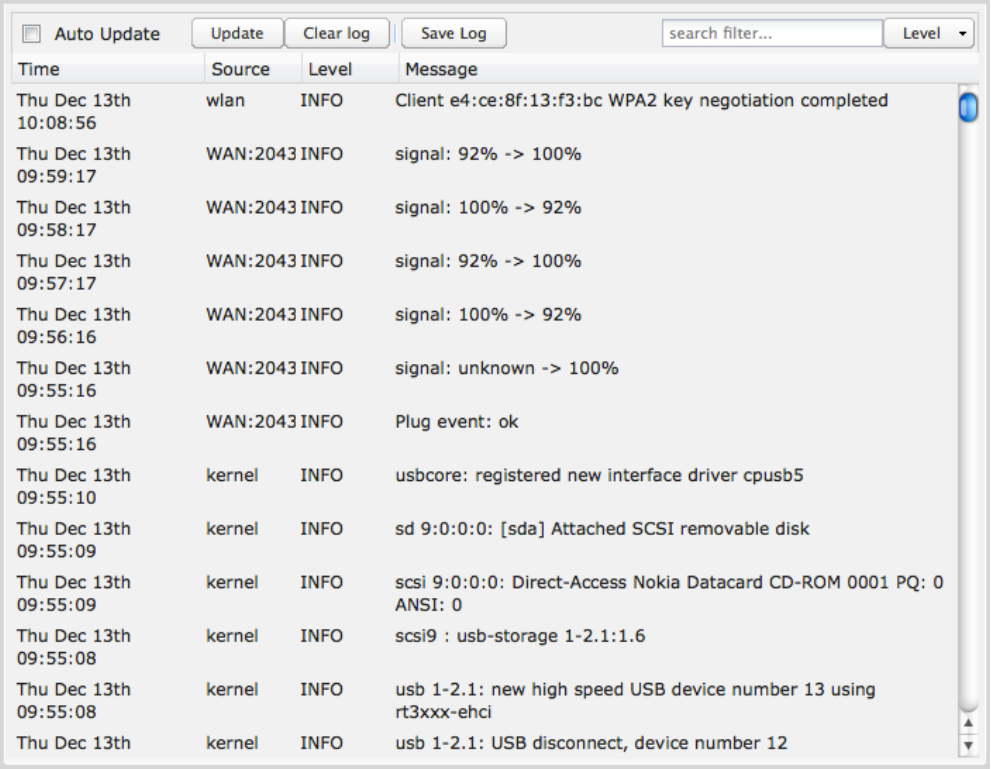
Save Log: This will open a dialog in your browser that will allow you to save the router's log to your computer.

Search: Enter keywords to find specific events.

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

- Critical
- Error
- Warning
- Info

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



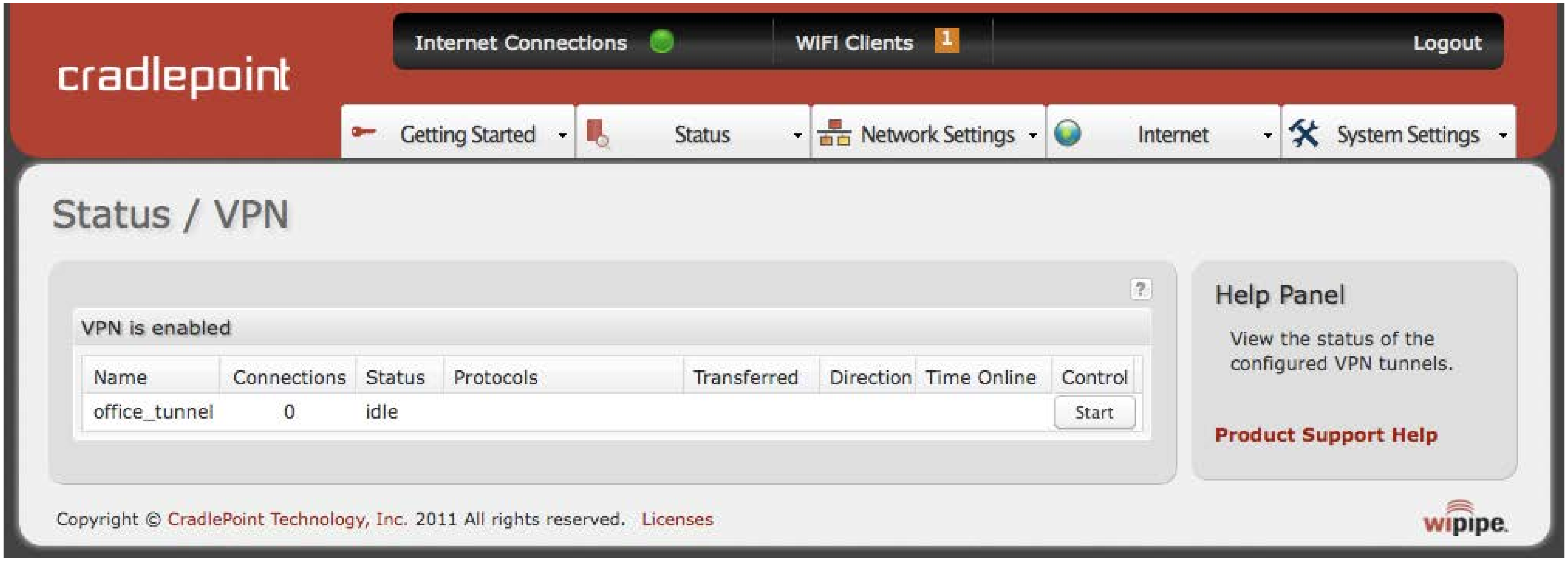
Time	Source	Level	Message
Thu Dec 13th 10:08:56	wlan	INFO	Client e4:ce:8f:13:f3:bc WPA2 key negotiation completed
Thu Dec 13th 09:59:17	WAN:2043	INFO	signal: 92% -> 100%
Thu Dec 13th 09:58:17	WAN:2043	INFO	signal: 100% -> 92%
Thu Dec 13th 09:57:17	WAN:2043	INFO	signal: 92% -> 100%
Thu Dec 13th 09:56:16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

5.11 VPN Tunnels

View the status of configured VPN tunnels. To set up or edit a VPN tunnel, go to **Internet → VPN Tunnels**.

Included information:

- Name
- Connections
- Status
- Protocols
- Transferred
- Direction
- Time Online
- Control



Status / VPN

VPN is enabled

Name	Connections	Status	Protocols	Transferred	Direction	Time Online	Control
office_tunnel	0	idle					Start

Help Panel

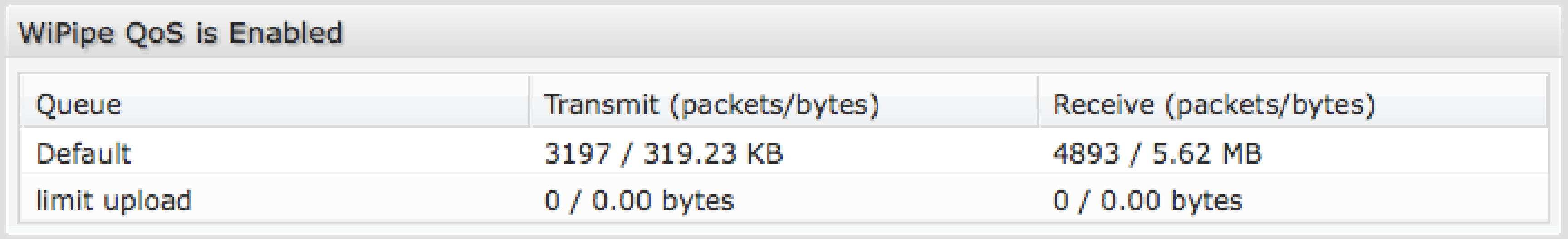
View the status of the configured VPN tunnels.

Product Support Help

Copyright © CradlePoint Technology, Inc. 2011 All rights reserved. Licenses

5.12 WiPipe QoS

View the breakdown of packets and bytes sent and received associated with each WiPipe QoS rule.



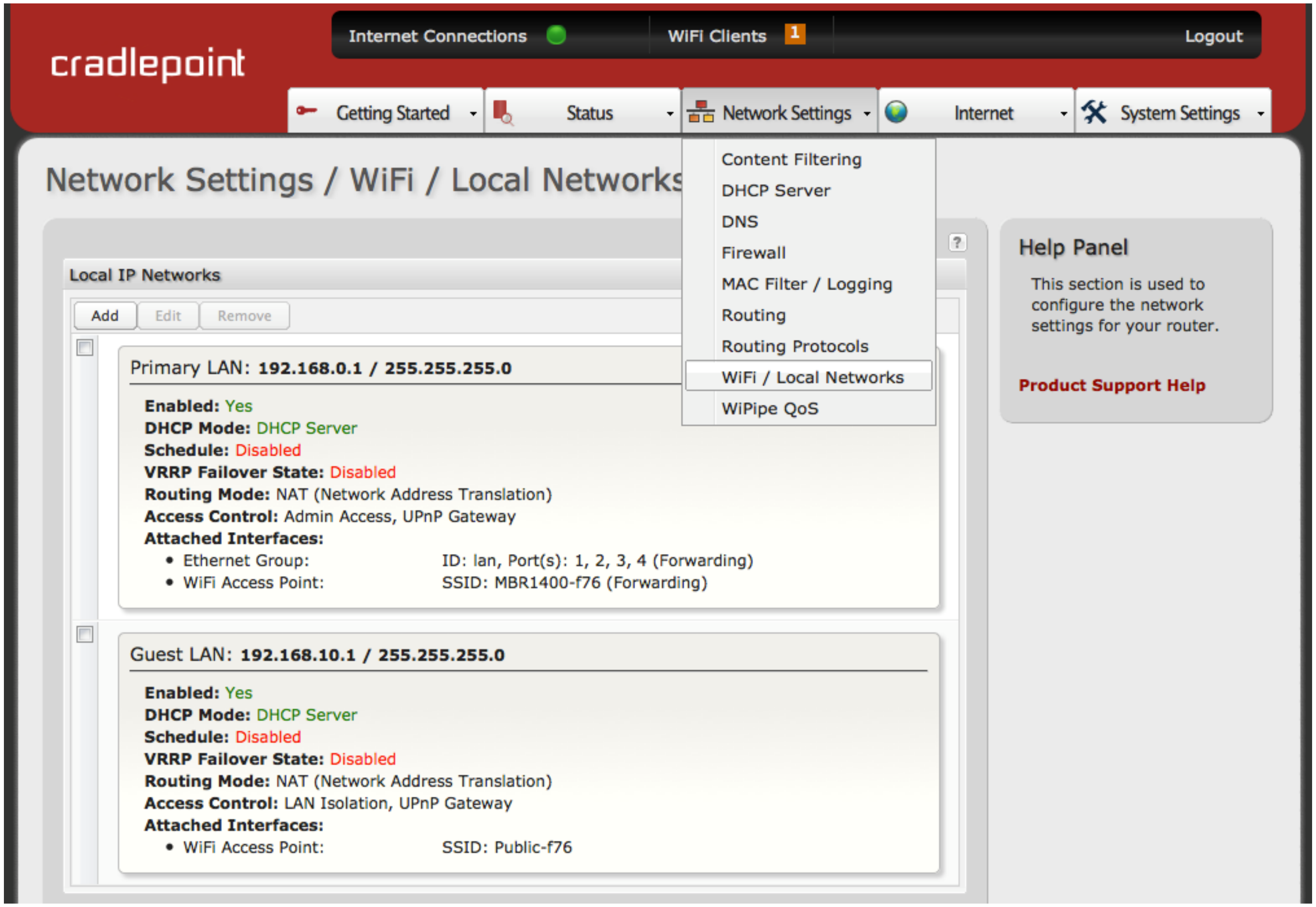
WiPipe QoS is Enabled

Queue	Transmit (packets/bytes)	Receive (packets/bytes)
Default	3197 / 319.23 KB	4893 / 5.62 MB
limit upload	0 / 0.00 bytes	0 / 0.00 bytes

6 NETWORK SETTINGS

The Network Settings tab provides access to these submenu options for administering the following functions/tasks, which all relate to managing the LAN (Local Area Networks).

- Content Filtering
- DHCP Server
- DNS
- Firewall
- MAC Filter / Logging
- Routing
- Routing Protocols
- WiFi / Local Networks
- WiPipe QoS



Network Settings / WiFi / Local Networks

Local IP Networks

Primary LAN: 192.168.0.1 / 255.255.255.0

Enabled: Yes
DHCP Mode: DHCP Server
Schedule: Disabled
VRRP Failover State: Disabled
Routing Mode: NAT (Network Address Translation)
Access Control: Admin Access, UPnP Gateway
Attached Interfaces:

- Ethernet Group: ID: lan, Port(s): 1, 2, 3, 4 (Forwarding)
- WiFi Access Point: SSID: MBR1400-f76 (Forwarding)

Guest LAN: 192.168.10.1 / 255.255.255.0

Enabled: Yes
DHCP Mode: DHCP Server
Schedule: Disabled
VRRP Failover State: Disabled
Routing Mode: NAT (Network Address Translation)
Access Control: LAN Isolation, UPnP Gateway
Attached Interfaces:

- WiFi Access Point: SSID: Public-f76

Help Panel

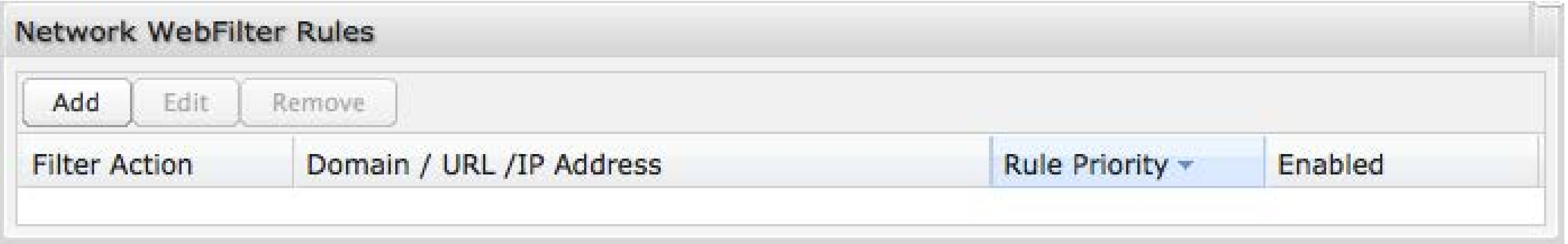
This section is used to configure the network settings for your router.

Product Support Help

6.1 Content Filtering

You have two main options for filtering content in a network created by your MBR1400.

1) **WebFilter Rules:** Create a list of websites that will be either disallowed or allowed. Customize the filter settings for each network and/or each MAC address. (These rules will not block HTTPS websites.)
2) **Cloud Based Filtering/Security:** Allows several options for filtering and security using third-party services:
   - **Umbrella** by **OpenDNS**
   - **Zscaler**



Network WebFilter Rules

Filter Action	Domain / URL /IP Address	Rule Priority	Enabled

6.1.1 Network WebFilter Rules

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

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

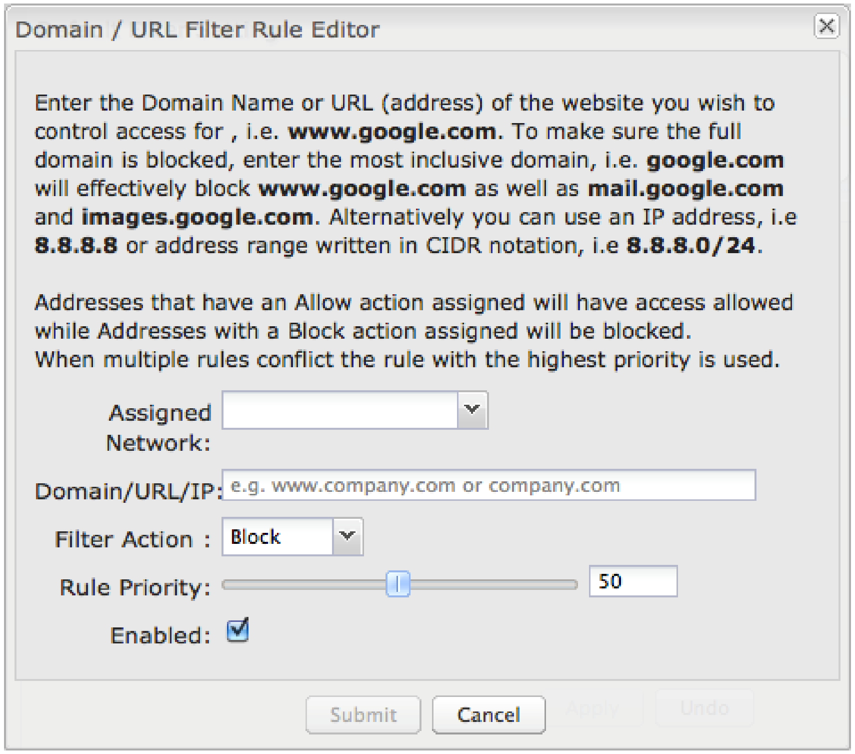
When creating rules keep in mind that some sites use multiple domains, so each domain may need a rule added to produce the desired behavior.

NOTE: Websites that use HTTPS will not be blocked by these rules. You will need to use OpenDNS to block HTTPS websites.

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

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

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



Domain / URL Filter Rule Editor

Enter the Domain Name or URL (address) of the website you wish to control access for , i.e. **www.google.com**. To make sure the full domain is blocked, enter the most inclusive domain, i.e. **google.com** will effectively block **www.google.com** as well as **mail.google.com** and **images.google.com**. Alternatively you can use an IP address, i.e **8.8.8.8** or address range written in CIDR notation, i.e **8.8.8.0/24**.

Addresses that have an Allow action assigned will have access allowed while Addresses with a Block action assigned will be blocked.
When multiple rules conflict the rule with the highest priority is used.

Assigned Network:

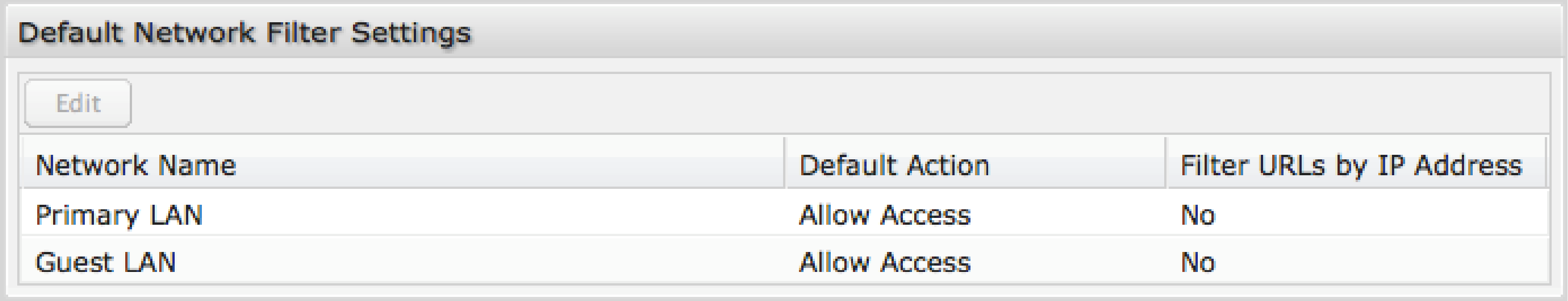
Domain/URL/IP: e.g. www.company.com or company.com

Filter Action : Block

Rule Priority: 50

Enabled: ☑

6.1.2 Default Filter Settings



Default Network Filter Settings

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

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

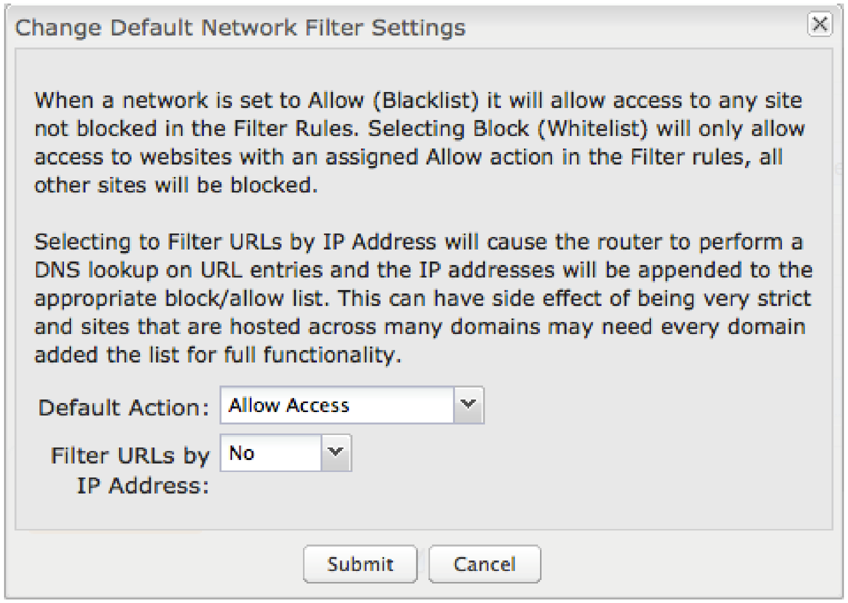
Default Action: Select from the following dropdown options:

- Allow Access (default)
- Block Access

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

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

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



Change Default Network Filter Settings

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

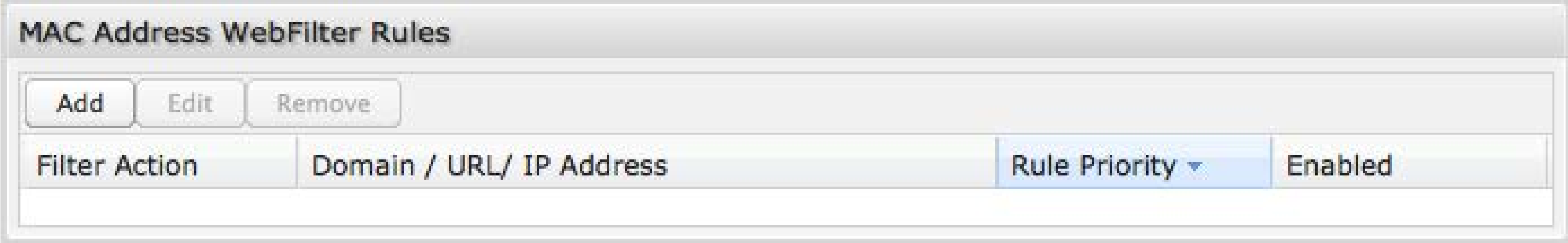
Selecting to Filter URLs by IP Address will cause the router to perform a DNS lookup on URL entries and the IP addresses will be appended to the appropriate block/allow list. This can have side effect of being very strict and sites that are hosted across many domains may need every domain added the list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

Default Action: Allow Access

Filter URLs by IP Address: No

6.1.3 MAC Address WebFilter Rules

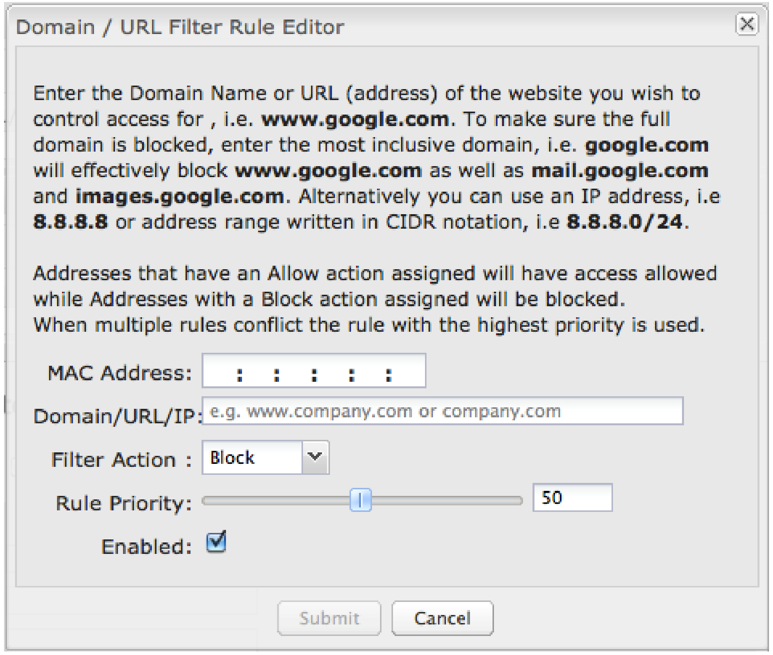
MAC Address WebFilter Rules allow you to control access from a specific MAC address to external domains or websites.


MAC Address WebFilter Rules

Filter Action	Domain / URL/ IP Address	Rule Priority ▾	Enabled

The settings for the **MAC Address WebFilter Rules** section match those for the **Network WebFilter Rules**, except that you must assign a MAC address instead of a network to each rule.

See the **Network WebFilter Rules** section for more configuration details.


Domain / URL Filter Rule Editor

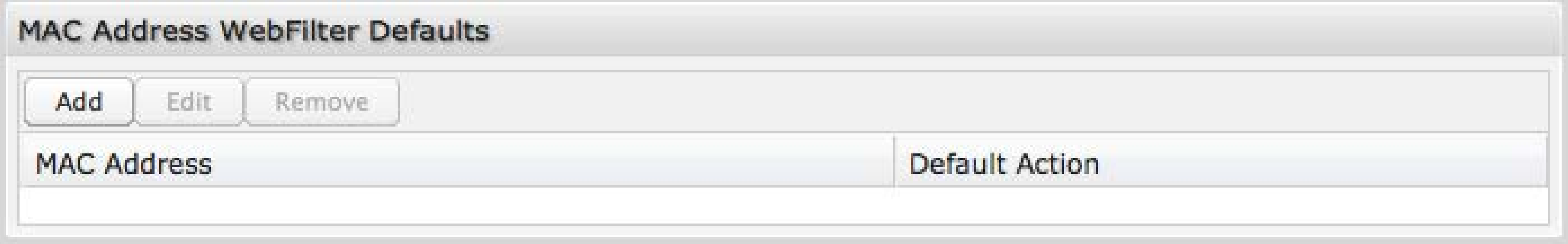
Enter the Domain Name or URL (address) of the website you wish to control access for , i.e. **www.google.com**. To make sure the full domain is blocked, enter the most inclusive domain, i.e. **google.com** will effectively block **www.google.com** as well as **mail.google.com** and **images.google.com**. Alternatively you can use an IP address, i.e **8.8.8.8** or address range written in CIDR notation, i.e **8.8.8.0/24**.

Addresses that have an Allow action assigned will have access allowed while Addresses with a Block action assigned will be blocked.
When multiple rules conflict the rule with the highest priority is used.

MAC Address: : : : : :
Domain/URL/IP: e.g. www.company.com or company.com
Filter Action : Block
Rule Priority: 50
Enabled: ☑

6.1.4 MAC Address WebFilter Defaults

Use **MAC Address WebFilter Defaults** together with **MAC Address WebFilter Rules** to control website access for specific MAC addresses. By default, each MAC address is allowed website access. Click Add/Edit to change this setting for a MAC address.


MAC Address WebFilter Defaults

MAC Address	Default Action

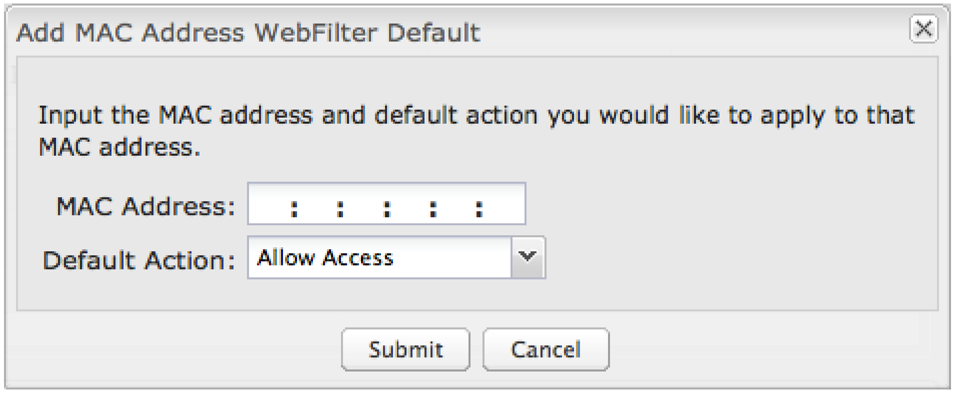
Input the **MAC address** and **default action** you would like to apply to that MAC address.

Default Action: Select from the following dropdown options:

- Allow Access (default)
- Block Access

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

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


Add MAC Address WebFilter Default

Input the MAC address and default action you would like to apply to that MAC address.

MAC Address: : : : : :

Default Action: Allow Access

6.1.5 Cloud Based Filtering/Security

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

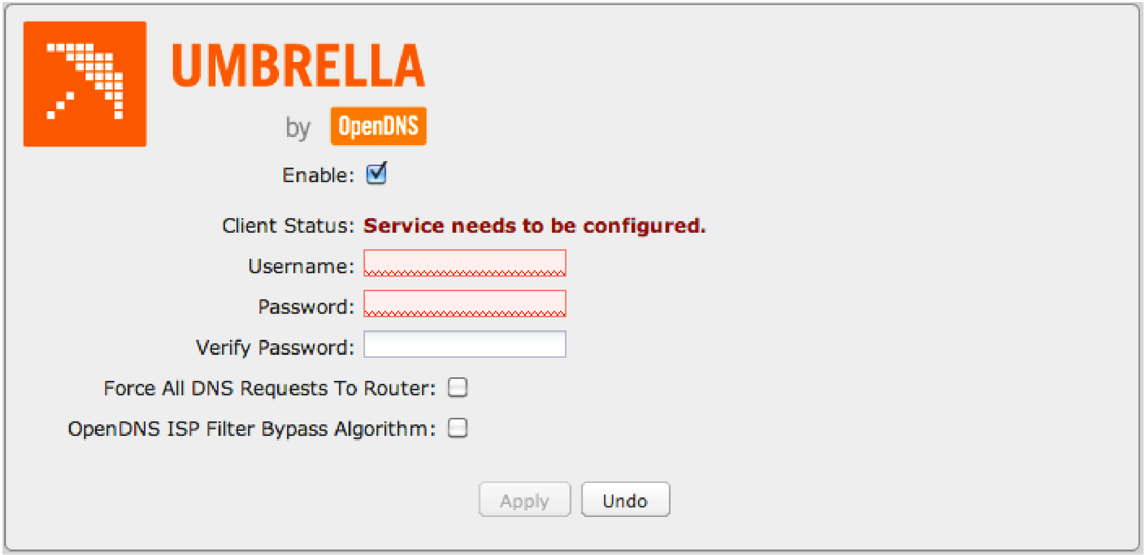
- **Umbrella** by **OpenDNS**
- **Zscaler**

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.

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 the client might have their own DNS servers statically set.



Enable: ☑

Client Status: **Service needs to be configured.**

Username:

Password:

Verify Password:

Force All DNS Requests To Router: □

OpenDNS ISP Filter Bypass Algorithm: □

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.

Zscaler

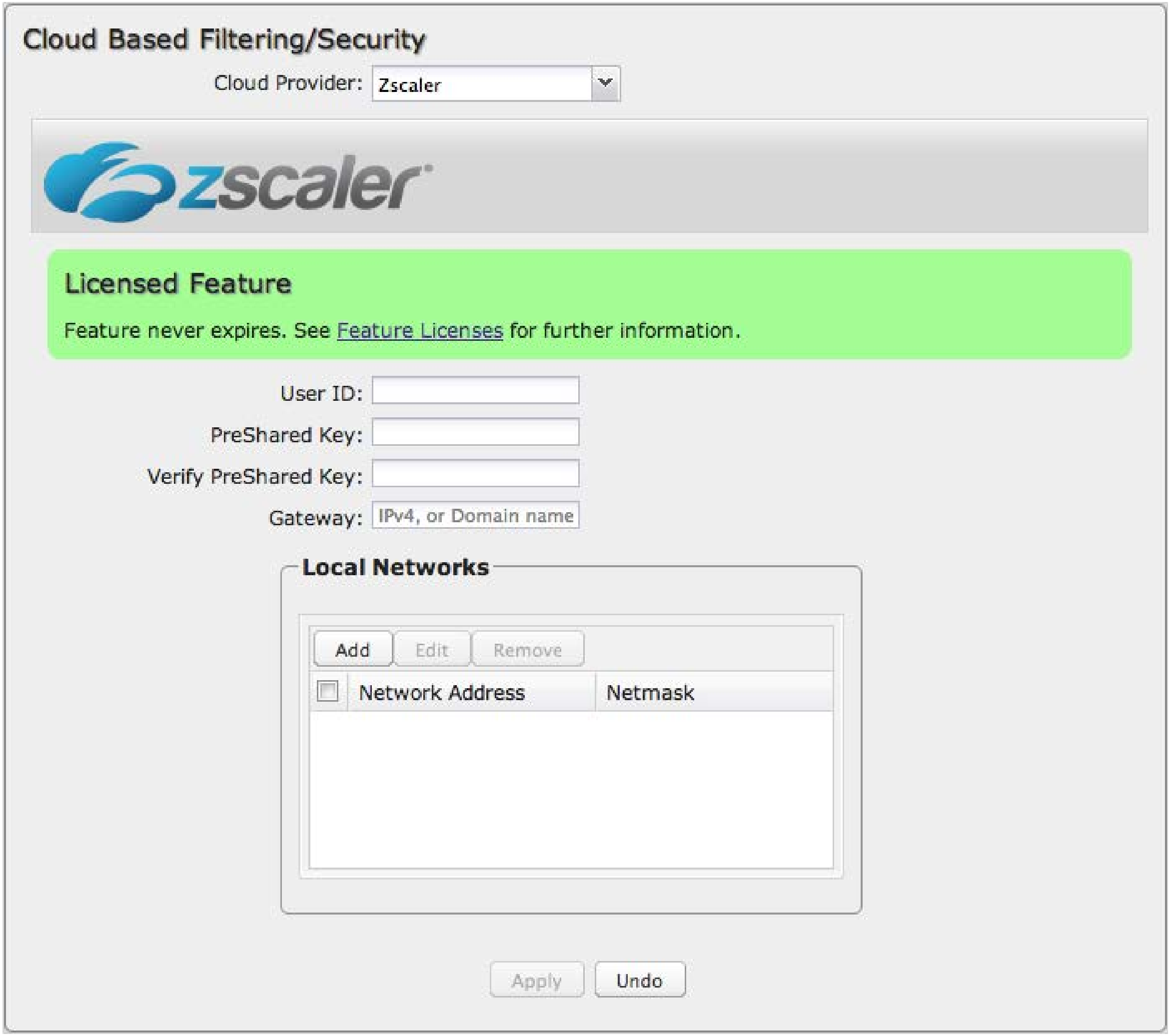
Zscaler (http://www.zscaler.com) is a cloud based web filtering and security provider that offers several plan options. Depending on your Zscaler implementation, this could include:

- Global Cloud Platform

- Real-Time Reporting
- Behavioral Analysis
- URL Filtering
- Advanced Threat Protection
- Inline Anti-Virus & Anti-Spyware
- Web 2.0 Control
- Data Loss Prevention
- Bandwidth Management
- Web Access Control
- And more…

NOTE: Zscaler requires a feature license. Go to System **Settings → Feature Licenses** to enable this feature.

Enter your Zscaler account information to enable these settings. Input local network information (Network Address and Netmask) to assign your Zscaler implementation to one or more local network(s).



Cloud Based Filtering/Security

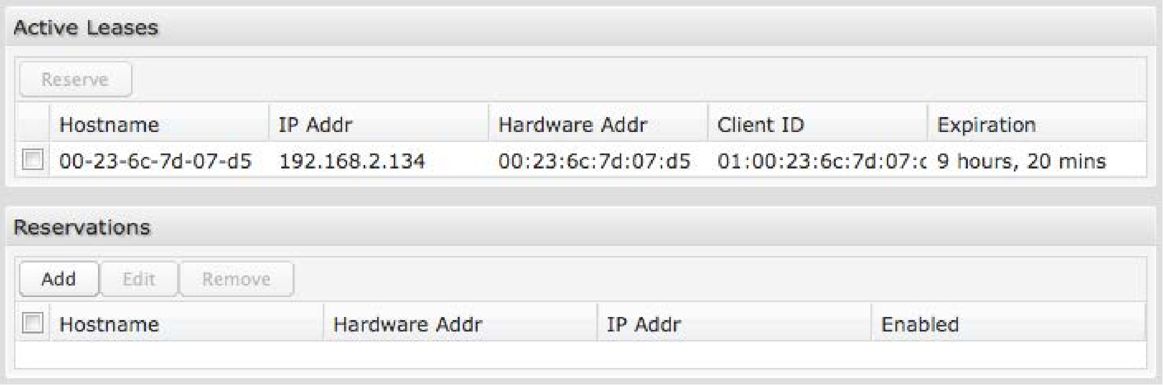
Cloud Provider: Zscaler

Licensed Feature

Feature never expires. See Feature Licenses for further information.

6.2 DHCP Server

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



Active Leases

Reserve

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

Reservations

Add Edit Remove

□	Hostname	Hardware Addr	IP Addr	Enabled

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**.

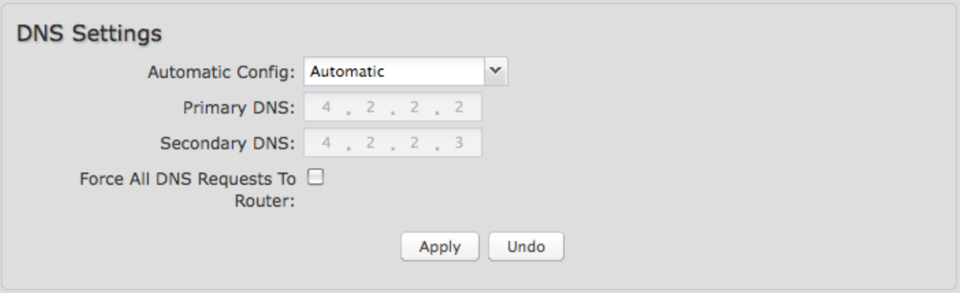
6.3 DNS

DNS, or Domain Name System, is a naming system that translates between domain names (www.Cradlepoint.com, for example) and Internet IP addresses (206.207.82.197). A DNS server acts as an Internet phone book, translating between names that make sense to people and the more complex numerical identifiers. The DNS page for the MBR1400 has these distinct functions:

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

6.3.1 DNS Settings

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



DNS Settings

Automatic Config: Automatic

Primary DNS: 4 . 2 . 2 . 2

Secondary DNS: 4 . 2 . 2 . 3

Force All DNS Requests To Router: □

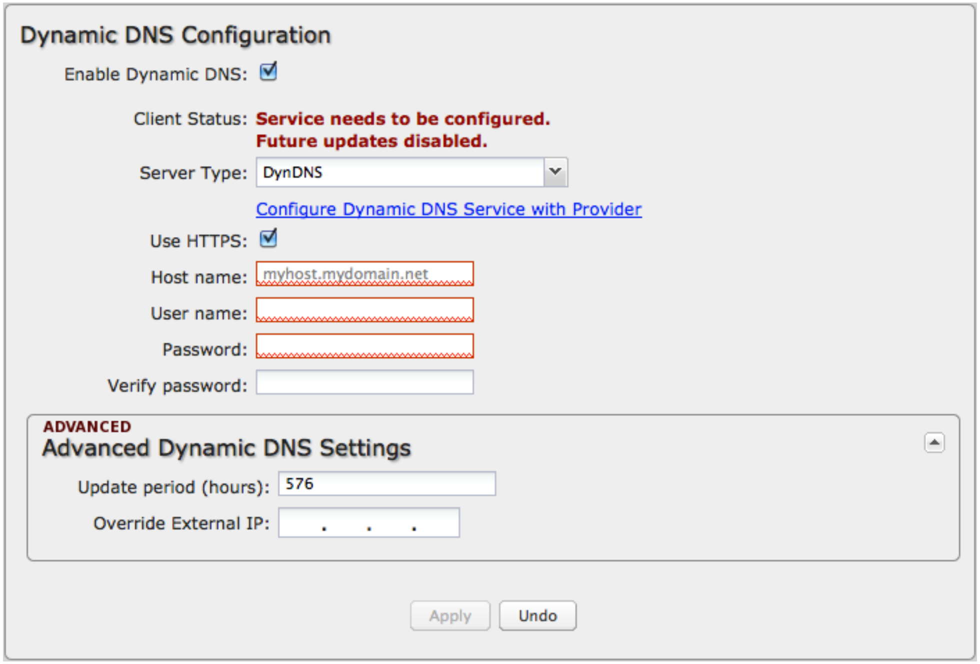
Automatic Config: Automatic or Static (default: Automatic). Switching to “Static” enables you to set specific DNS servers in the **Primary DNS** and **Secondary DNS** fields.

Primary DNS and **Secondary DNS:** If you choose to specify your DNS servers, 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.

6.3.2 Dynamic DNS Configuration

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



Dynamic DNS Configuration

Enable Dynamic DNS: ☑

Client Status: **Service needs to be configured.**
Future updates disabled.

Server Type: DynDNS

Configure Dynamic DNS Service with Provider

Use HTTPS: ☑

Host name: myhost.mydomain.net

User name:

Password:

Verify password:

ADVANCED

Advanced Dynamic DNS Settings

Update period (hours): 576

Override External IP: . . .

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

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

- 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 could be disabled if not compatible with the server.

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

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

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

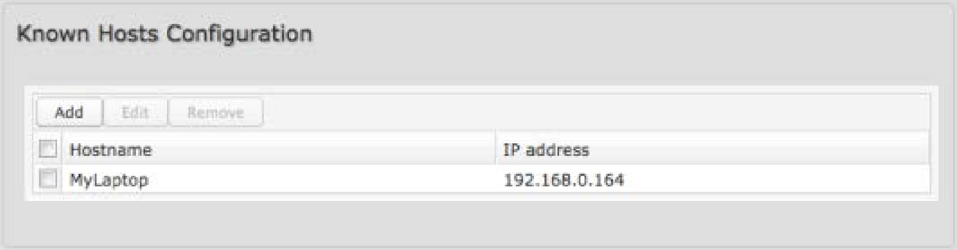
6.3.3 Advanced Dynamic DNS Settings

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

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

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

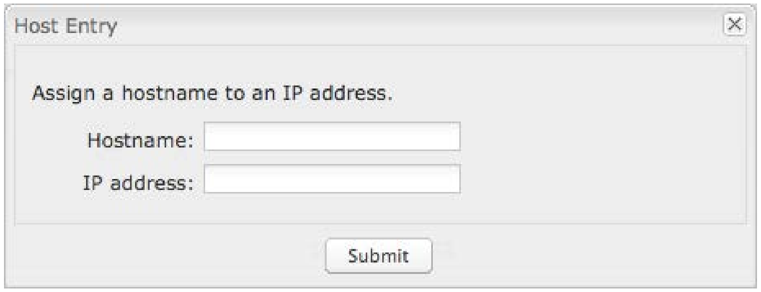
6.3.4 Known Hosts Configuration



☐	Hostname	IP address
☐	MyLaptop	192.168.0.164

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.



Assign a hostname to an IP address.

Hostname:

IP address:

Fill in the following fields:

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

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

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

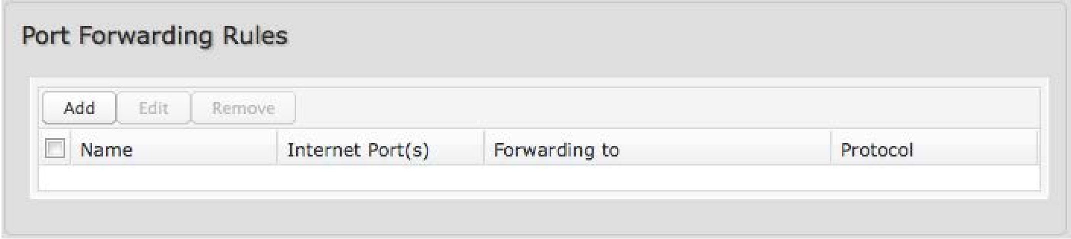
6.4 Firewall

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

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

6.4.1 Port Forwarding Rules

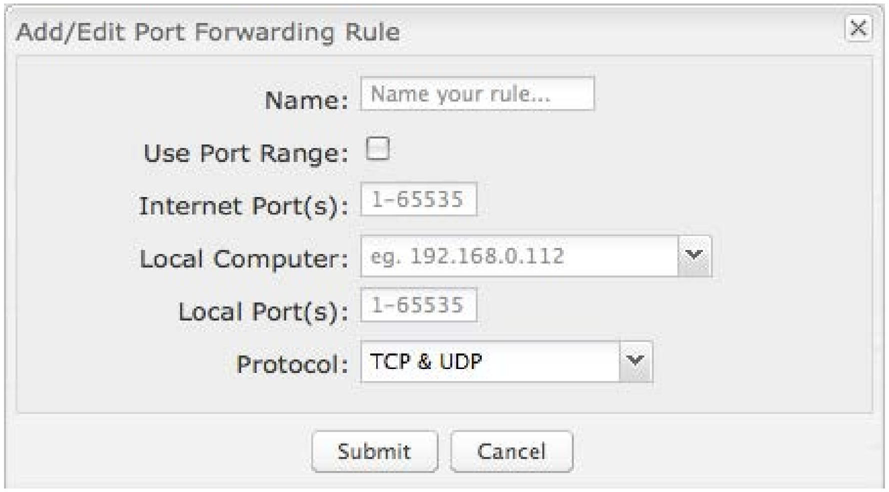
A port forwarding rule allows traffic from the Internet to reach a computer on the inside of your network. For example, a port forwarding rule might be used to run a Web server.


Port Forwarding Rules

□ Name	Internet Port(s)	Forwarding to	Protocol

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

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


Add/Edit Port Forwarding Rule

Name: Name your rule...

Use Port Range: □

Internet Port(s): 1-65535

Local Computer: eg. 192.168.0.112

Local Port(s): 1-65535

Protocol: TCP & UDP

Add/Edit Port Forwarding Rule

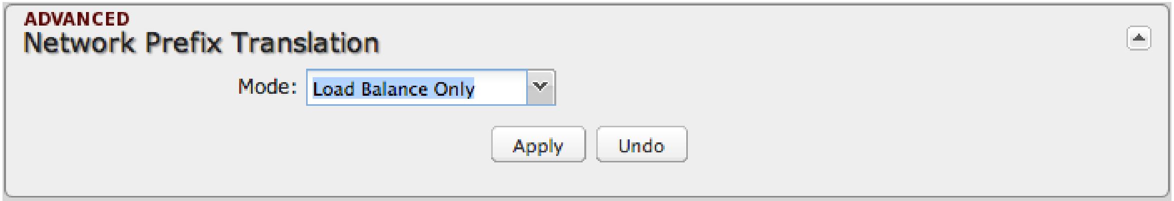
- **Name:** Name your rule.
- **Use Port Range:** Changes the selection options to allow you to input a range of ports (if desired).
- **Internet Port(s):** The port number(s) as you want it defined on the Internet. Typically these will be the same as the local port numbers, but they do not have to be.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

- **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 **Submit** to save your completed port forwarding rule.

6.4.2 Network Prefix Translation (Advanced)

Network Prefix Translation is used in IPv6 networks to translate one IPv6 prefix to another. IPv6 prefix translation is an experimental specification (RFC 6296) trying to achieve address independence similar to NAT in IPv4. Unlike NAT, however, NPT is stateless and preserves the IPv6 principle that each device has a routable public address. 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.



ADVANCED
Network Prefix Translation

Mode: Load Balance Only

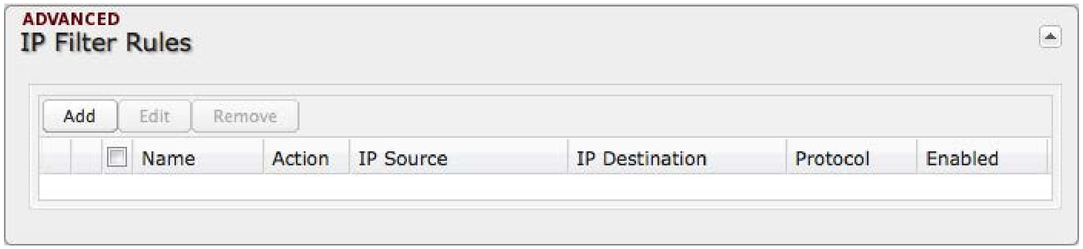
Mode:

- **None** – No translation is performed
- **Load Balance Only** – (Default) Only translate networks when actively load balancing
- **First** – Use the first IPv6 prefix found
- **Static** – Always use a static IPv6 translation (input the prefix here)

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

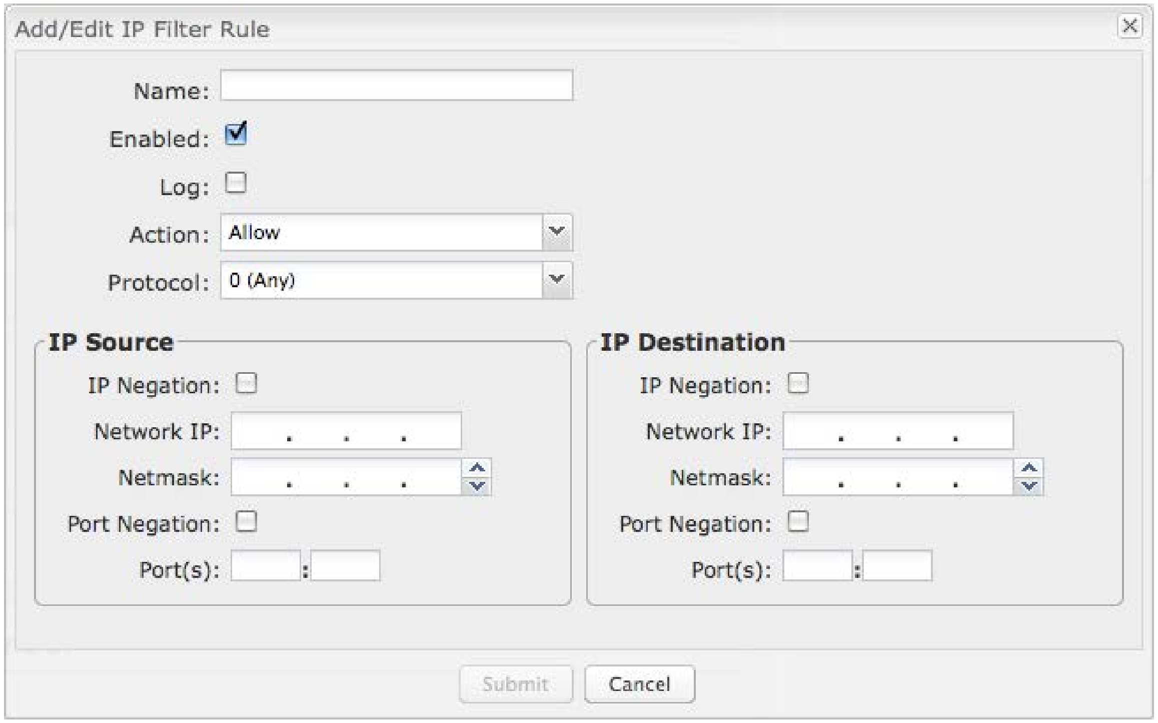
6.4.3 IP Filter Rules (Advanced)

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



□	Name	Action	IP Source	IP Destination	Protocol	Enabled

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



Name:
Enabled: ☑
Log: □
Action: Allow
Protocol: 0 (Any)

IP Source
IP Negation: □
Network IP: . . .
Netmask: . . .
Port Negation: □
Port(s): :

IP Destination
IP Negation: □
Network IP: . . .
Netmask: . . .
Port Negation: □
Port(s): :

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

IP Source / IP Destination

- **IP Negation:** Match on any IP address that is NOT in the specified IP network range.
- **Network IP:** Optional field to specify a matching network IP address for this rule to match against.
- **Netmask:** Use this to define a subnet size this rule will match against.

- **Port Negation:** Match on any port that is NOT in the specified port range.
- **Port(s):** Use for a single port or a range of ports. Fill in the left side for a single port.

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

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

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

Add IP Filter Rule

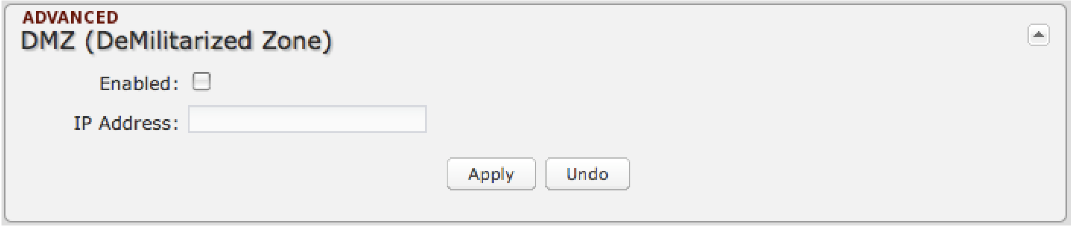
- **Name:** No more Johnny
- **Enabled:** Selected
- **Action:** Deny
- **Protocol:** Any

IP Source

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

6.4.4 DMZ: DeMilitarized Zone (Advanced)

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



Enabled: □

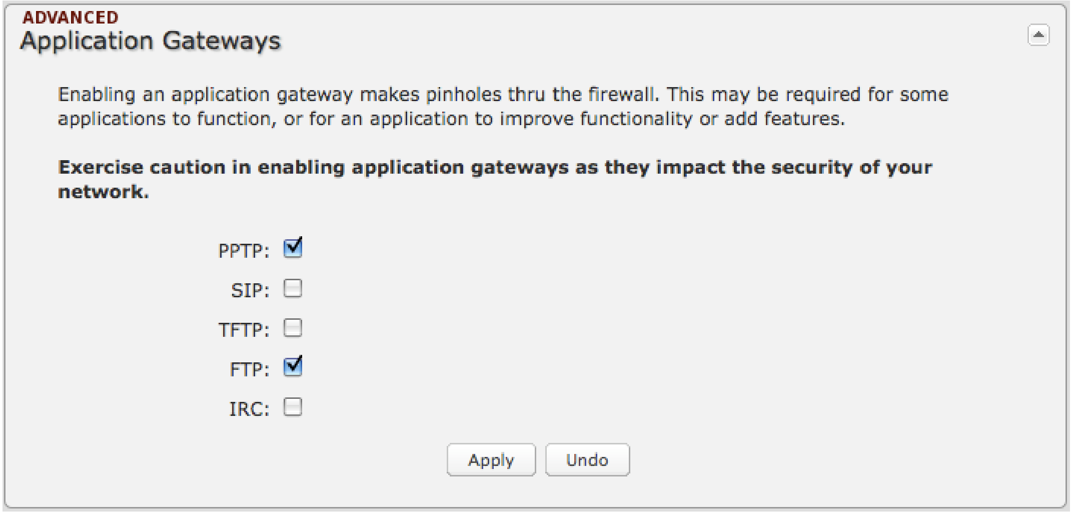
IP Address:

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

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

6.4.5 Application Gateways (Advanced)

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



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

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

PPTP: ☑

SIP: □

TFTP: □

FTP: ☑

IRC: □

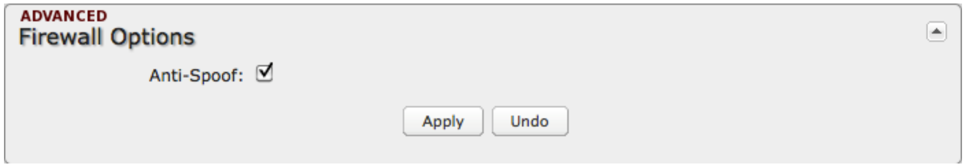
Exercise caution in enabling application gateways as they impact the security of your network.

Enable any of the following types of application gateways:

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

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

6.4.6 Firewall Options (Advanced)

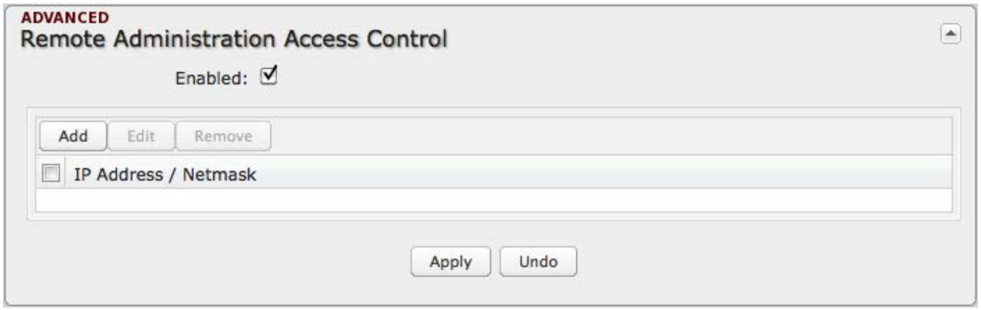

ADVANCED
Firewall Options
Anti-Spoof: ☑

Anti-Spoof: Anti-Spoof checks help protect against malicious users faking the source address in packets they transmit in order to either hide themselves or to impersonate someone else. Once the user has spoofed their address they can launch a network attack without revealing the true source of the attack or attempt to gain access to network services that are restricted to certain addresses.

6.4.7 Remote Administration Access Control (Advanced)

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

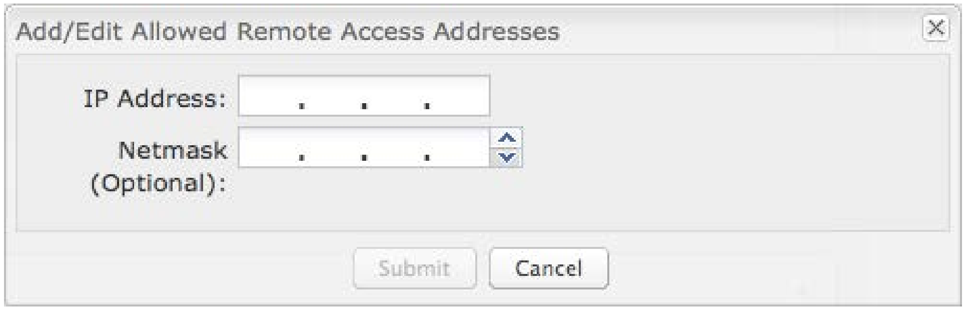
The services affected by this include remote HTTP, HTTPS, SNMP, and SSH configuration tools. This does not restrict access to LAN-based administration, i.e. devices within your network still have administration access. The individual remote administration services can be enabled under **System Settings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


ADVANCED
Remote Administration Access Control
Enabled: ☑

Add/Edit Allowed Remote Access Addresses

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

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



Add/Edit Allowed Remote Access Addresses

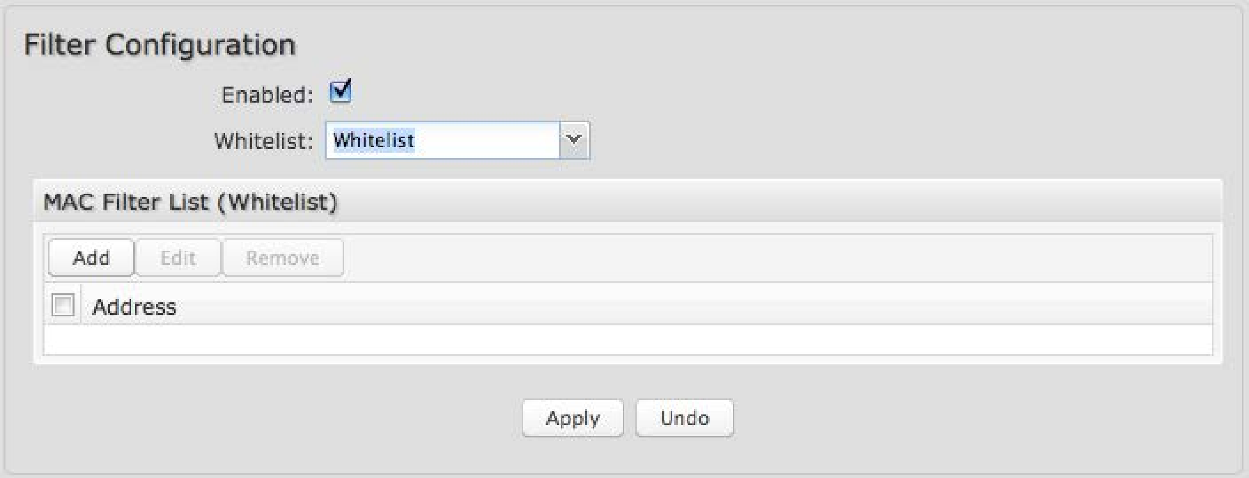
IP Address: . . .

Netmask (Optional): . . .

6.5 MAC Filter / Logging

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

6.5.1 Filter Configuration



Filter Configuration

Enabled: ☑

Whitelist: Whitelist

MAC Filter List (Whitelist)

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

Enabled: Click to allow MAC Filter options.

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

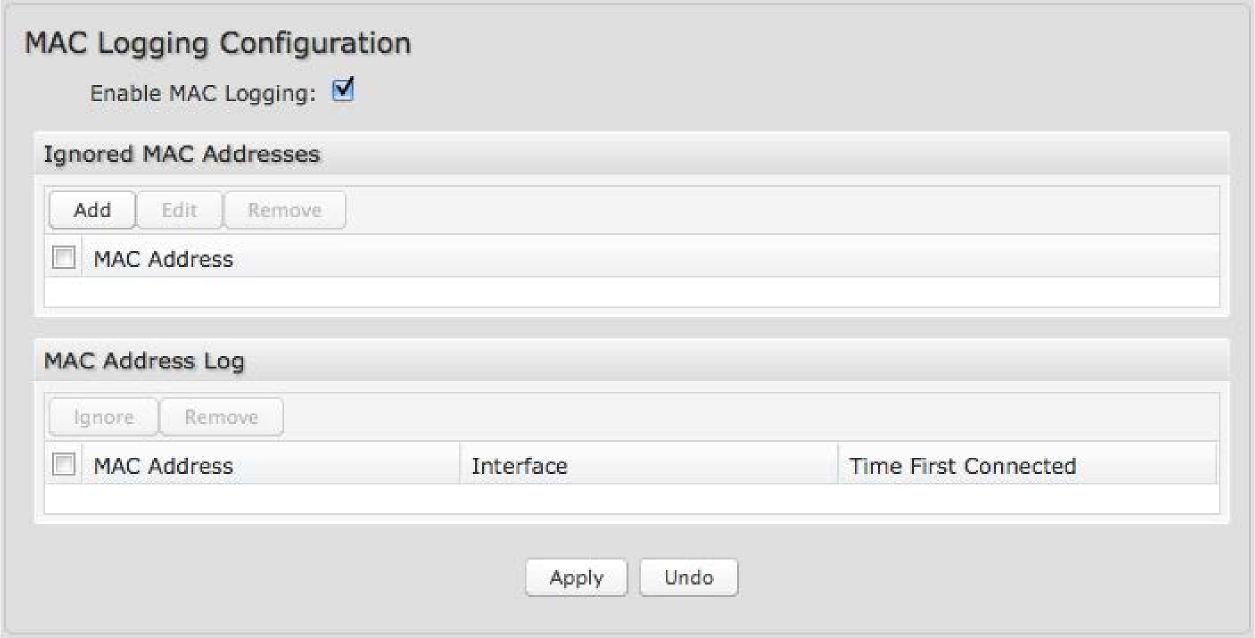
MAC Filter List (Whitelist or Blacklist): Add devices to either your whitelist or blacklist simply by inputting each device’s MAC address.

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

6.5.2 MAC Logging Configuration

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

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


MAC Logging Configuration

Enable MAC Logging: ☑

Ignored MAC Addresses

□ MAC Address

MAC Address Log

□ MAC Address	Interface	Time First Connected

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.

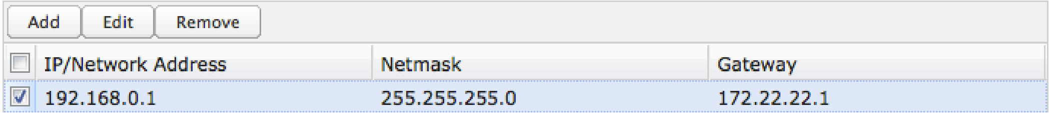
MAC Address Log: This shows the last 64 MAC addresses that have connected to the router, as well as which interface was used to connect. The time/date that is logged is the time of the first connection. The page may need to be refreshed to show the most recent log entries.

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

6.6 Routing

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

Static routes are unnecessary for most users. They are typically only 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.

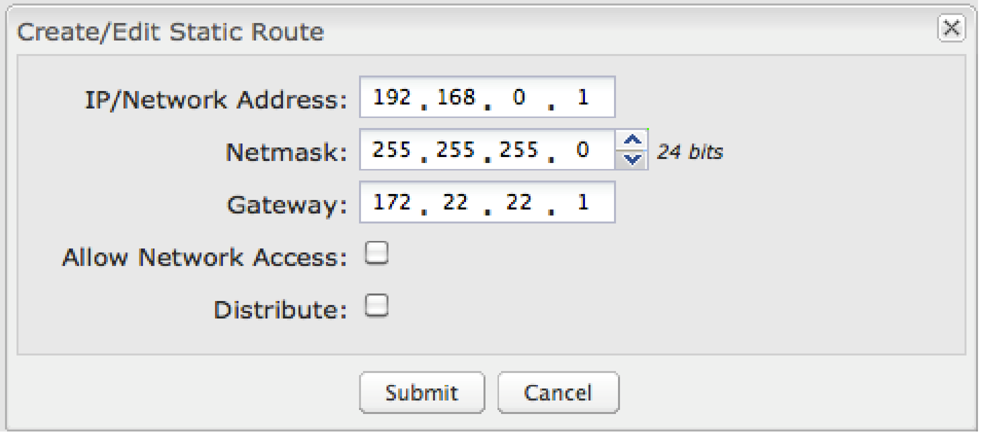


□	IP/Network Address	Netmask	Gateway
☑	192.168.0.1	255.255.255.0	172.22.22.1

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

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

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



IP/Network Address: 192 . 168 . 0 . 1

Netmask: 255 . 255 . 255 . 0 *24 bits*

Gateway: 172 . 22 . 22 . 1

Allow Network Access: □

Distribute: □

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

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

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

Distribute: Allow this static route to be distributed via a routing protocol (**Network Settings → Routing Protocols**).

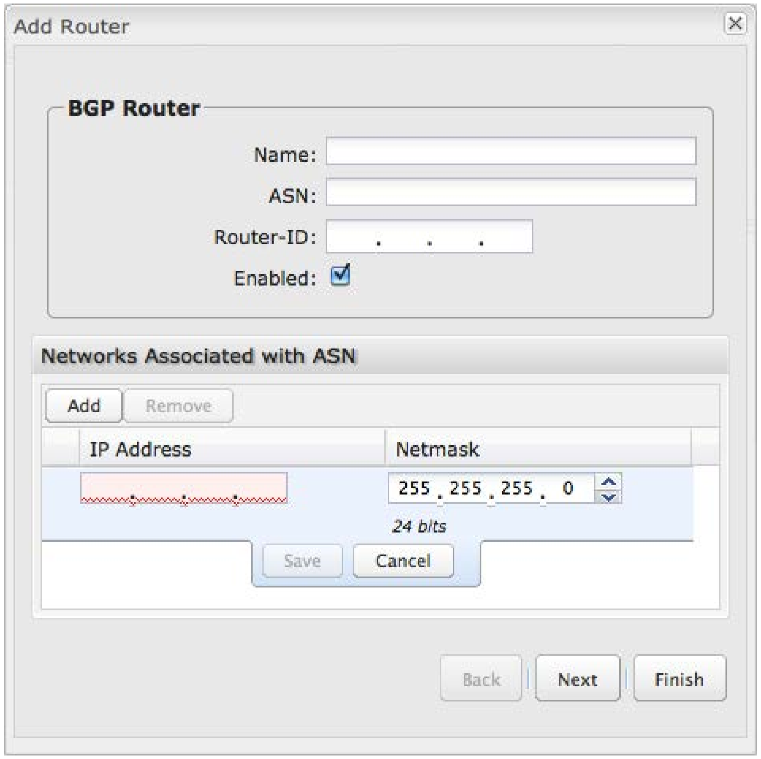
6.7 *Routing Protocols*

NOTE: Routing Protocols require a feature license. Go to System **Settings → Feature Licenses** to enable these features. These protocols also require hardware version 2.0.

A routing protocol is a protocol that specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms choose the route. Each router has a prior knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network.

Choose from the following tabs to configure routing protocols:

- BGP Routing
- OSPF Routing
- RIP Routing
- RIPNG Routing
- Route Maps and Filters



Enabled: ☑

Netmask: 255 . 255 . 255 . 0

24 bits

6.7.1 BGP Routing

The latest version of BGP (Border Gateway Protocol) is version 4. BGP-4 is one of the Exterior Gateway Protocols and de facto standard of Inter Domain routing protocol. BGP-4 is described in RFC1771, A Border Gateway Protocol 4 (BGP-4). BGP is a distance vector routing protocol, and the AS-Path framework provides distance vector metric and loop detection to BGP. RFC1930.

BGP Editor

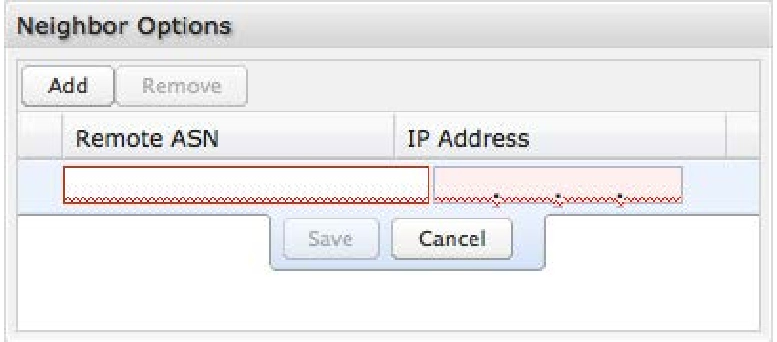
- **Name**: Unique name of the policy.
- **ASN**: The AS (Autonomous System) number is one of the essential elements of BGP.
- **Router-ID**: This sets the router-ID of the BGP process. The router-ID may be an IP address of the router, but need not be - it can be

any arbitrary 32bit number. However it MUST be unique within the entire BGP domain to the BGP speaker - bad things will happen if multiple BGP speakers are configured with the same router-ID.

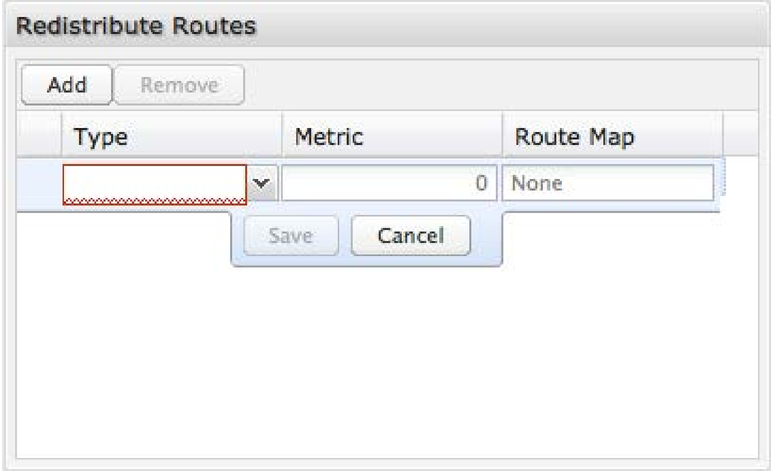
- **Enabled**: Click to enable/disable the policy. (Default: enabled.)

Networks Associated with ASN: Use the IP address and netmask to assign networks to this ASN.

Neighbor Options: Creates a new neighbor identified by remote ASN and IP address.



Redistribute Routes: Redistribute routes of the specified protocol or kind into BGP, with the metric type and metric set if specified, filtering the routes using the given route map if specified. Redistributed routes may also be filtered with distribute lists.



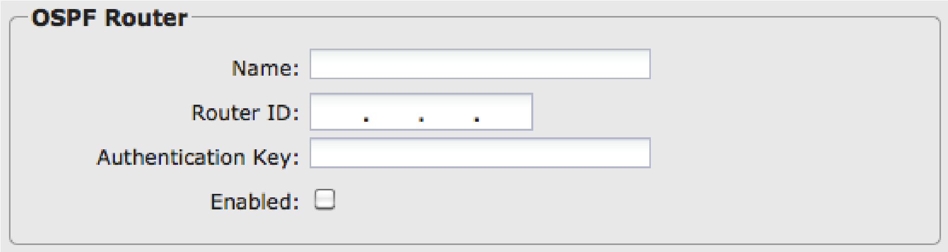
- **Type**: The type is the source of the route. Select from: Main, Connected, Static, RIP, and OSPF.
- **Metric:** Numerical priority of the route.
- **Route Map**: Route maps provide a means to filter and/or apply actions to routes, allowing policies to be applied to routes.

6.7.2 OSPF Routing

OSPF (Open Shortest Path First) version 2 is a routing protocol described in RFC2328, OSPF Version 2. OSPF is an IGP (Interior Gateway Protocol). Compared with RIP, OSPF can provide more scalable network support and faster convergence times. OSPF is widely used in large networks such as ISP (Internet Service Provider) backbone and enterprise networks.

OSPF Editor

- **Name**: Unique name of the policy.
- **Router ID**: This sets the router-ID of the OSPF process. The router-ID may be an IP address of the router, but need not be – it can be any arbitrary 32bit number. However it MUST be unique within the entire OSPF domain to the OSPF speaker - bad things will happen if multiple OSPF speakers are configured with the same router-ID.
- **Authentication Key**: Set OSPF authentication key to a simple password. After setting authentication key, all OSPF packets are authenticated. The authentication key has a maximum length of eight characters.
- **Enabled**: Click to enable/disable the policy. (Default: enabled.)



OSPF Router

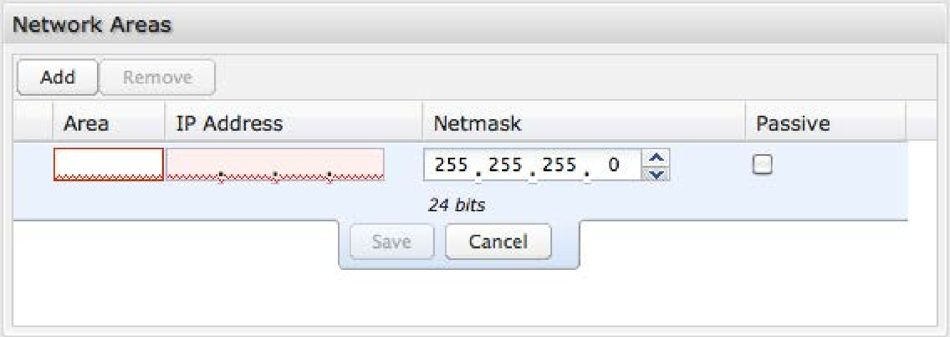
Name:

Router ID: . . .

Authentication Key:

Enabled: □

Network Areas: Areas are identified by an ID number. As of 4.1.1, Cradlepoint only supports area 0. Use the IP address and netmask fields to associate a network with this policy. Also, choose whether to select **Passive** (active by default). Passive areas do not advertise.

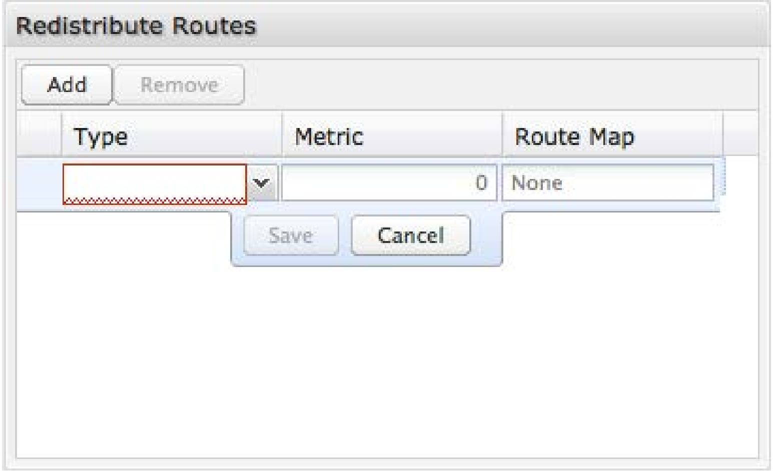


Network Areas

Area	IP Address	Netmask	Passive
	. . .	255 . 255 . 255 . 0 24 bits	□

Redistribute Routes: Redistribute routes of the specified protocol or kind into BGP, with the metric type and metric set (if specified), filtering the routes using the given route map (if specified). Redistributed routes may also be filtered with distribute lists.

- **Type**: The type is the source of the route. Select from: Main, Connected, Static, RIP, OSPF.
- **Metric:** Numerical priority of the route.
- **Route Map**: Route maps provide a means to filter and/or apply actions to routes, allowing policies to be applied to routes.

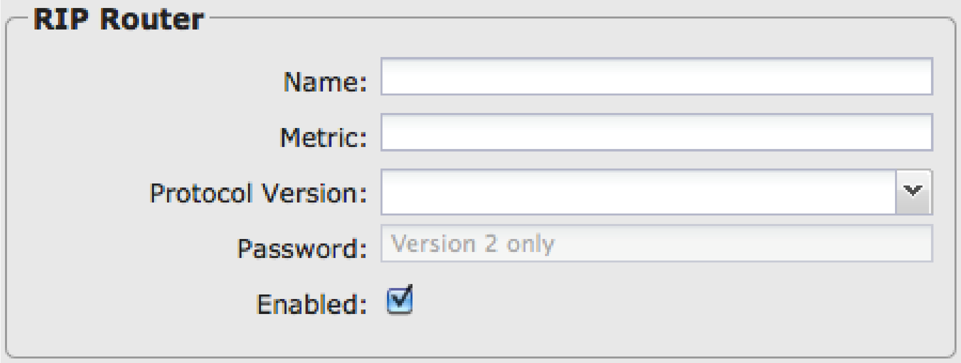


6.7.3 RIP Routing

RIP (Routing Information Protocol) is a widely deployed interior gateway protocol. RIP is a distance-vector protocol based on the Bellman-Ford algorithms. As a distance-vector protocol, RIP sends updates from one router to its neighbors periodically, allowing the convergence to a known topology. In each update, the distance to any given network will be broadcast to its neighboring router. The router supports RIP version 2 as described in RFC2453 and RIP version 1 as described in RFC1058.

RIP Editor

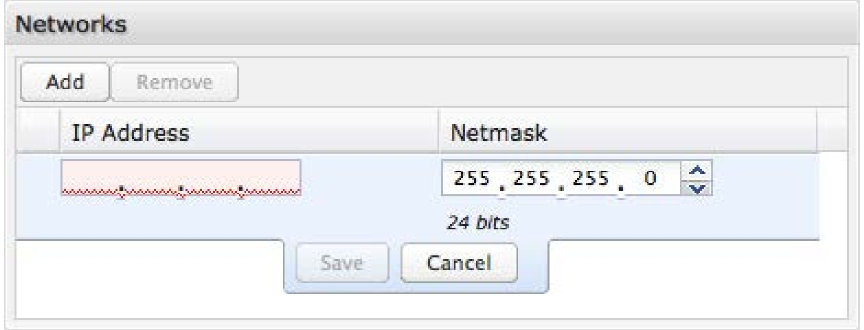
- **Name**: Unique name of the policy.
- **Metric**: RIP metric is a value for distance for the network. Usually RIP increments the metric when the network information is received. The metric for redistributed routes is set to 1.
- **Protocol Version**: RIP can be configured to send either Version 1 or Version 2 packets. The default is to send RIPv2 while accepting both RIPv1 and



Enabled: ☑

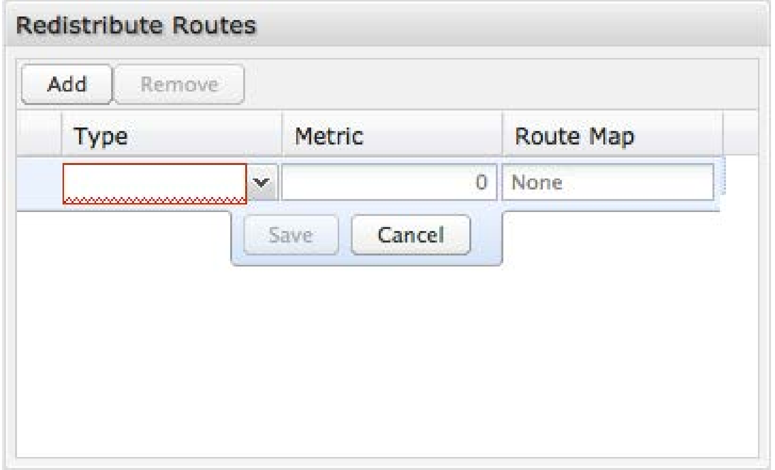
RIPv2 (and replying with packets of the appropriate version for REQUESTS / triggered updates).

- **Password**: RIPv2 allows packets to be authenticated via either an insecure plain text password, included with the packet, or a more secure MD5 based HMAC (keyed-Hashing for Message AuthentiCation). RIPv1 cannot be authenticated at all, so when authentication is configured RIP will discard routing updates received via RIPv1 packets.
- **Enabled**: Click to enable/disable the policy. (Default: enabled.)



Networks: Set the RIP-enabled interfaces by network. RIP is enabled on the interfaces that have addresses within the network range.

Neighbors: When a neighbor doesn't understand multicast, this command is used to specify neighbors. In some cases, not all routers will be able to understand multicasting, where packets are sent to a network or a group of addresses. In a situation where a neighbor cannot process multicast packets, it is necessary to establish a direct link between routers. The neighbor command allows the network administrator to specify a router as a RIP neighbor. The no neighbor a.b.c.d command will disable the RIP neighbor. Assign a neighbor by inputting an IP address.



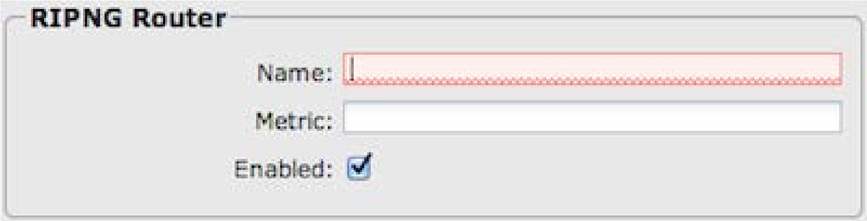
Redistribute Routes: Redistribute routes of the specified protocol or kind into BGP, with the metric type and metric set (if specified), filtering the routes using the given route map (if specified). Redistributed routes may also be filtered with distribute lists.

- **Type**: The type is the source of the route. Select from: Main, Connected, Static, RIP, OSPF.
- **Metric:** Numerical priority of the route.
- **Route Map**: Route maps provide a means to filter and/or apply actions to routes, allowing policies to be applied to routes.

6.7.4 RIPNG Routing

RIP (Routing Information Protocol) RIPng (RIP next generation) extends RIPv2 to support IPv6. See RIPng on Wikipedia and RFC 2080 for details.

RIPNG Editor

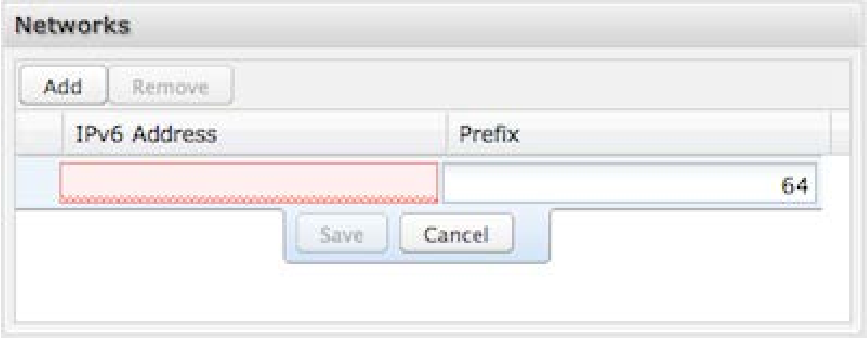

RIPNG Router

Name:

Metric:

Enabled: ☑

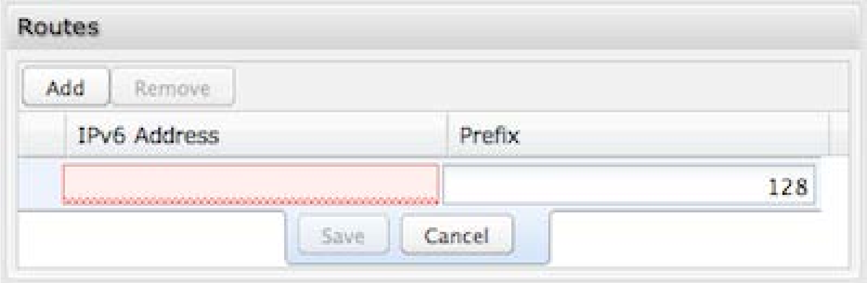
- **Name**: Unique name of the policy.
- **Metric**: RIPng metric is a value for distance for the network. Usually RIP increments the metric when the network information is received. The metric for redistributed routes is set to 1.
- **Enabled**: Click to enable/disable the policy. (Default: enabled.)


Networks

IPv6 Address	Prefix
	64

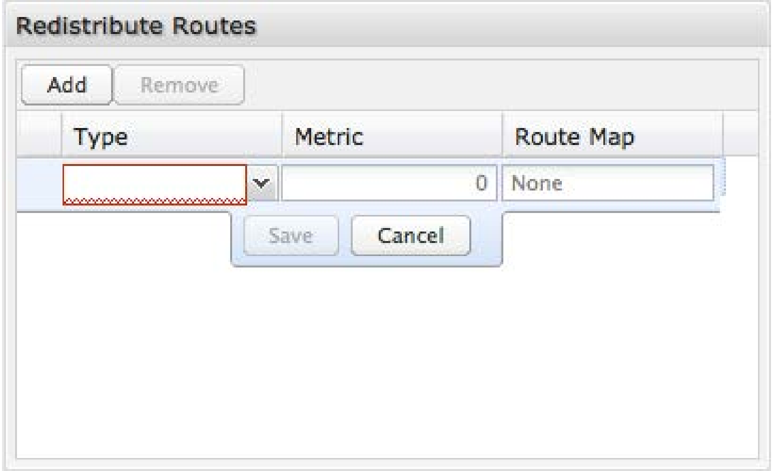
Networks: Set the RIPng-enabled interfaces by network using IPv6 addresses. RIPng is enabled on the interfaces that have addresses within the network range.

Routes: Set RIPng static routing announcement of specified network address.



Redistribute Routes: Redistribute routes of the specified protocol or kind into BGP, with the metric type and metric set (if specified), filtering the routes using the given route map (if specified). Redistributed routes may also be filtered with distribute lists.

- **Type**: The type is the source of the route. Select from: Main, Connected, Static, RIP, OSPF.
- **Metric:** Numerical priority of the route.
- **Route Map**: Route maps provide a means to filter and/or apply actions to routes, allowing policies to be applied to routes.



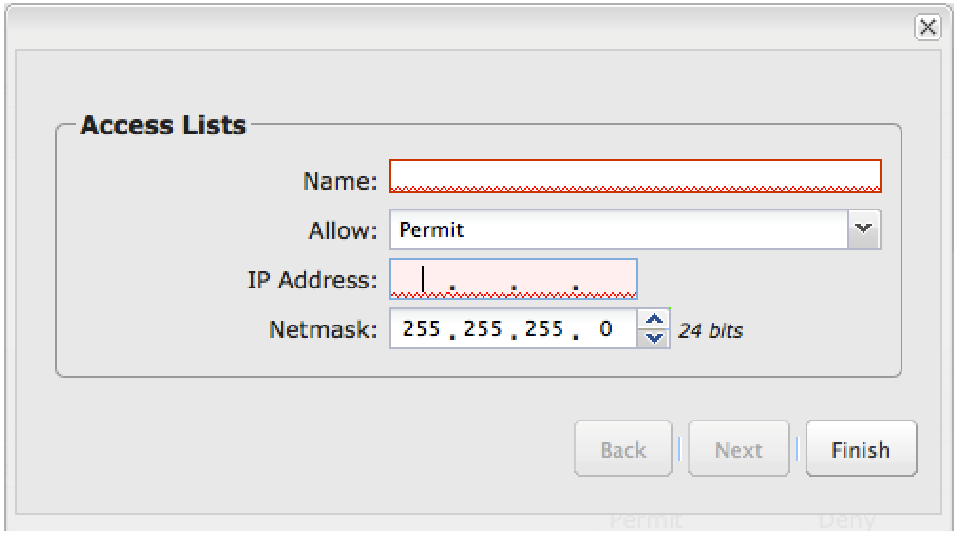
6.7.5 Route Maps and Filters

Access Lists

This option provides for basic filtering based on IP addresses and netmasks.

Click **Add** to create a filtering rule.

Name: Choose a unique name.
Allow: Select "Permit" or "Deny".
IP Address: Input the IP addresses that you want permitted or denied.
Netmask: Use this along with "IP Address" to specify a range of IP Addresses associated with this Access Lists rule.



Access Lists

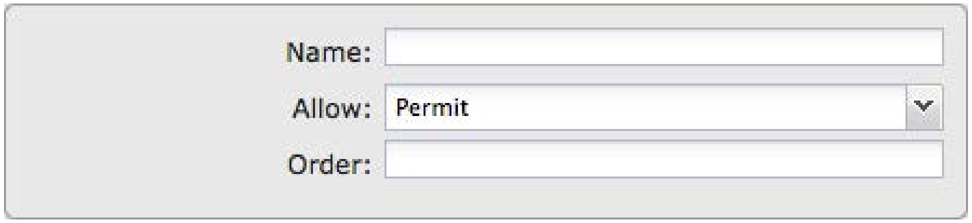
Name:
Allow: Permit
IP Address: . . .
Netmask: 255 . 255 . 255 . 0 24 bits

Route Map

Route maps provide a means to filter and/or apply actions to routes, allowing policies to be applied to routes. Route maps define rules for transferring between different routing protocols. Each statement in a route map is ordered. Once there is a match to a statement, the statement is executed and the scan terminates.

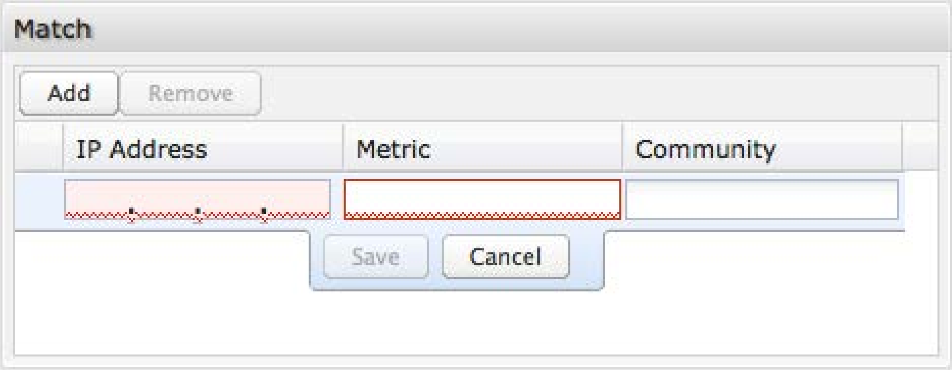
Click **Add** to create a new route map.

- **Name:** Choose a unique name.
- **Allow:** Select "Permit" or "Deny".
- **Order:** Input a number to set the order of this policy.



Name:
Allow: Permit
Order:

Match and **Set**: Both of these have the following configuration options:



- **IP address**: Input an IP address with this policy.
- **Metric**: Numerical priority of the route.
- **Community**: The BGP community list is a user-defined BGP communities attribute list. The BGP community list can be used for matching or manipulating BGP communities attribute in updates.The community attributes are a 32-bit number that also has some aliases.
    - **internet**: alias for well-known communities value 0
    - **no-export**: alias for well-known communities value NO_EXPORT (0xffffff01)
    - **no-advertise**: alias for well-known communities value NO_ADVERTISE (0xffffff02)
    - **local-AS**: alias for well-known communities value NO_EXPORT_SUBCONFED (0xffffff03)

Match: This specifies the policy implied if the `Matching Conditions' are met or not met, and which actions of the route map are to be taken, if any. The two possibilities are:

1. Permit: If the entry matches, then carry out the `Set Actions'. Then finish processing the route map, permitting the route, unless an `Exit Action' indicates otherwise.
2. Deny: If the entry matches, then finish processing the route-map and deny the route (return `deny').

Set: A route-map entry may, optionally, specify one or more `Set Actions' to set or modify attributes of the route.

6.8 WiFi / Local Networks

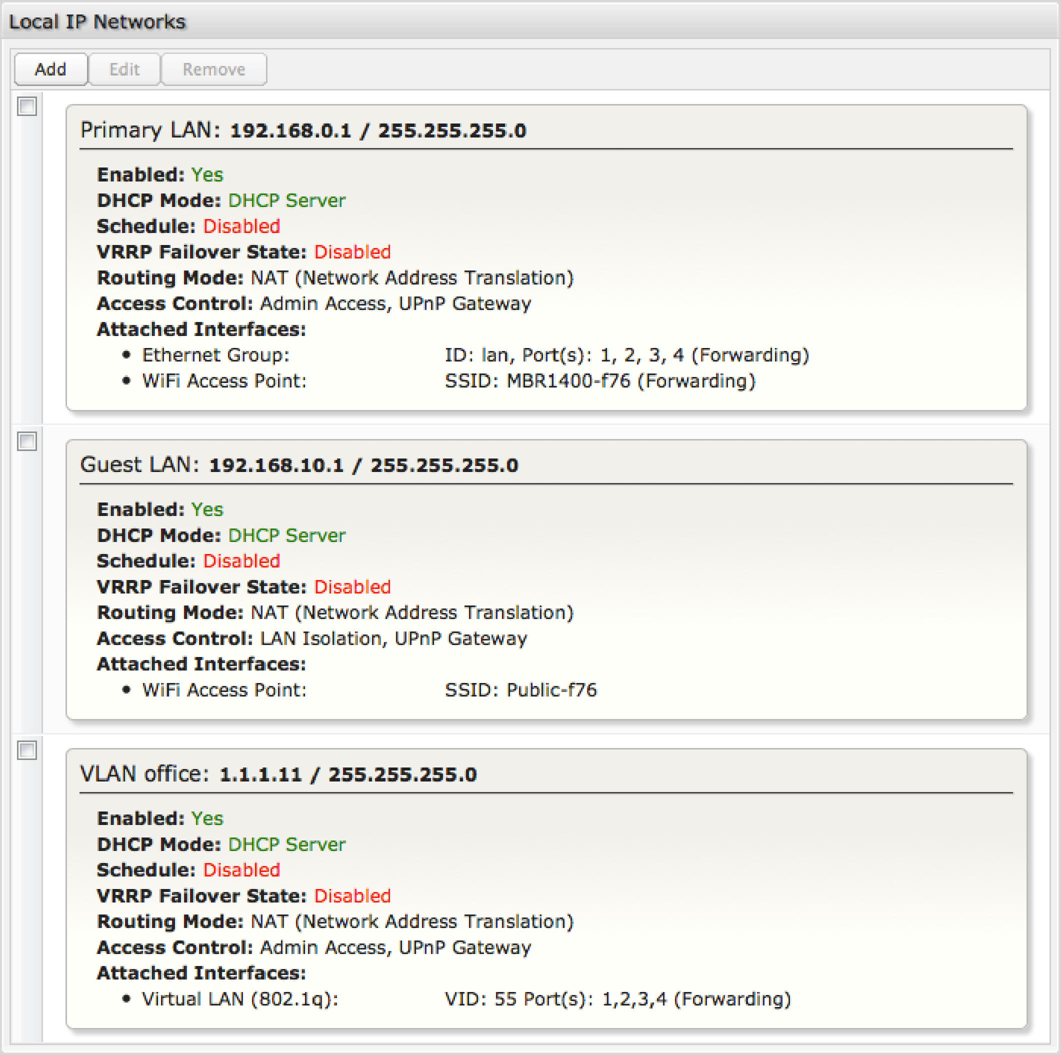
This section is used to configure the settings for networks created by your router (LAN). Note that changes made in this section may also need to be duplicated on wireless devices that you want to connect to your wireless network.

For example, if you change a wireless LAN's IP address, devices within that network will lose connection. They will have to reconnect to the network.

The user can set up multiple networks on the MBR1400, each with its own unique configuration and its own selection of interfaces. Each local network can be attached to any of the following types of interfaces:

- WiFi
- Ethernet
- VLAN

For example, one network might be just an isolated WiFi hotspot for guests, while another might be the main network with administrative access, an Ethernet port, a password-protected WiFi SSID, and a VLAN interface.



□ Primary LAN: **192.168.0.1 / 255.255.255.0**

Enabled: Yes
DHCP Mode: DHCP Server
Schedule: Disabled
VRRP Failover State: Disabled
Routing Mode: NAT (Network Address Translation)
Access Control: Admin Access, UPnP Gateway
Attached Interfaces:

- Ethernet Group: ID: lan, Port(s): 1, 2, 3, 4 (Forwarding)
- WiFi Access Point: SSID: MBR1400-f76 (Forwarding)

□ Guest LAN: **192.168.10.1 / 255.255.255.0**

Enabled: Yes
DHCP Mode: DHCP Server
Schedule: Disabled
VRRP Failover State: Disabled
Routing Mode: NAT (Network Address Translation)
Access Control: LAN Isolation, UPnP Gateway
Attached Interfaces:

- WiFi Access Point: SSID: Public-f76

□ VLAN office: **1.1.1.11 / 255.255.255.0**

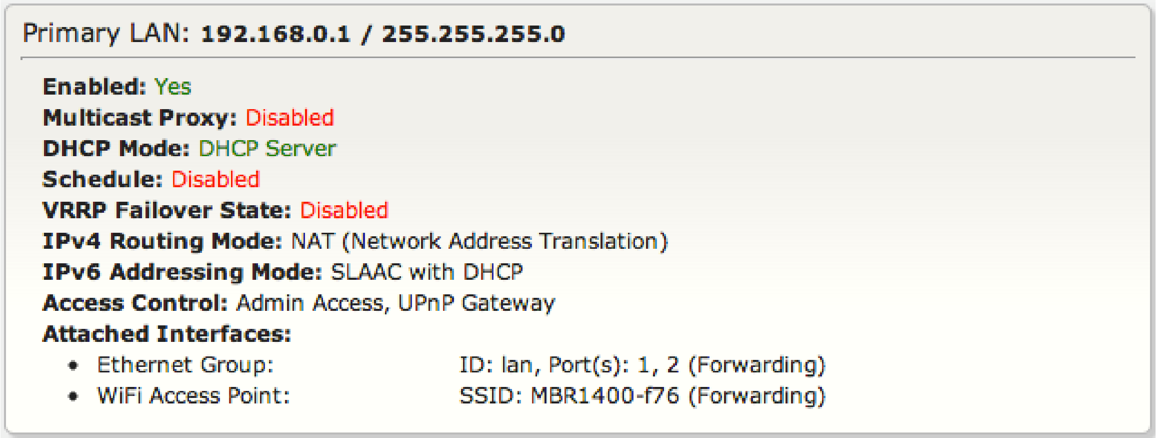
Enabled: Yes
DHCP Mode: DHCP Server
Schedule: Disabled
VRRP Failover State: Disabled
Routing Mode: NAT (Network Address Translation)
Access Control: Admin Access, UPnP Gateway
Attached Interfaces:

- Virtual LAN (802.1q): VID: 55 Port(s): 1,2,3,4 (Forwarding)

6.8.1 Local IP Networks

Local IP Networks displays the following information for each network:

- **Network Name** and **IP address/Netmask** (along the top bar)
- **Enabled:** Yes/No
- **Multicast Proxy** (Enabled/Disabled)
- **DHCP Server** (Enabled/Disabled)
- **Schedule** (Enabled/Disabled – See the Schedule tab in the Local Network Editor)
- **VRRP Failover State** (Disabled, Backup, or Master)
- **IPv4 Routing Mode** (NAT, Standard, IP Passthrough, Hotspot, 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, WiFi, VLAN)



Primary LAN: **192.168.0.1 / 255.255.255.0**

Enabled: Yes
Multicast Proxy: Disabled
DHCP Mode: DHCP Server
Schedule: Disabled
VRRP Failover State: Disabled
IPv4 Routing Mode: NAT (Network Address Translation)
IPv6 Addressing Mode: SLAAC with DHCP
Access Control: Admin Access, UPnP Gateway
Attached Interfaces:

- Ethernet Group: ID: lan, Port(s): 1, 2 (Forwarding)
- WiFi Access Point: SSID: MBR1400-f76 (Forwarding)

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

HotSpot (Captive Portal)

When you set a network as a “Hotspot” under **Routing Mode**, you will also need to:

1) Configure hotspot settings under **System Settings → Hotspot Services**. Click on **Configure** to link to that page.
2) If you want a hotspot that includes WiFi, set one of your WiFi interfaces to “Open” for its Security Mode and attach this interface to your hotspot network. Otherwise guests will need to know the password to connect to the WiFi network even before viewing a Terms of Service page (or other hotspot options). Also, make sure your WiFi interface is “Enabled”.

6.8.2 Local Network Editor

Click **Add** or select a network and click **Edit** to open the **Local Network Editor** to make configure a LAN. The **Local Network Editor** contains the following tabs: General Settings, IPv4 Settings, IPv6 Settings, Interfaces, Access Control, IPv4 DHCP, IPv6 Addressing, Multicast Proxy, Schedule, VRRP, STP, and Wired 802.1X.

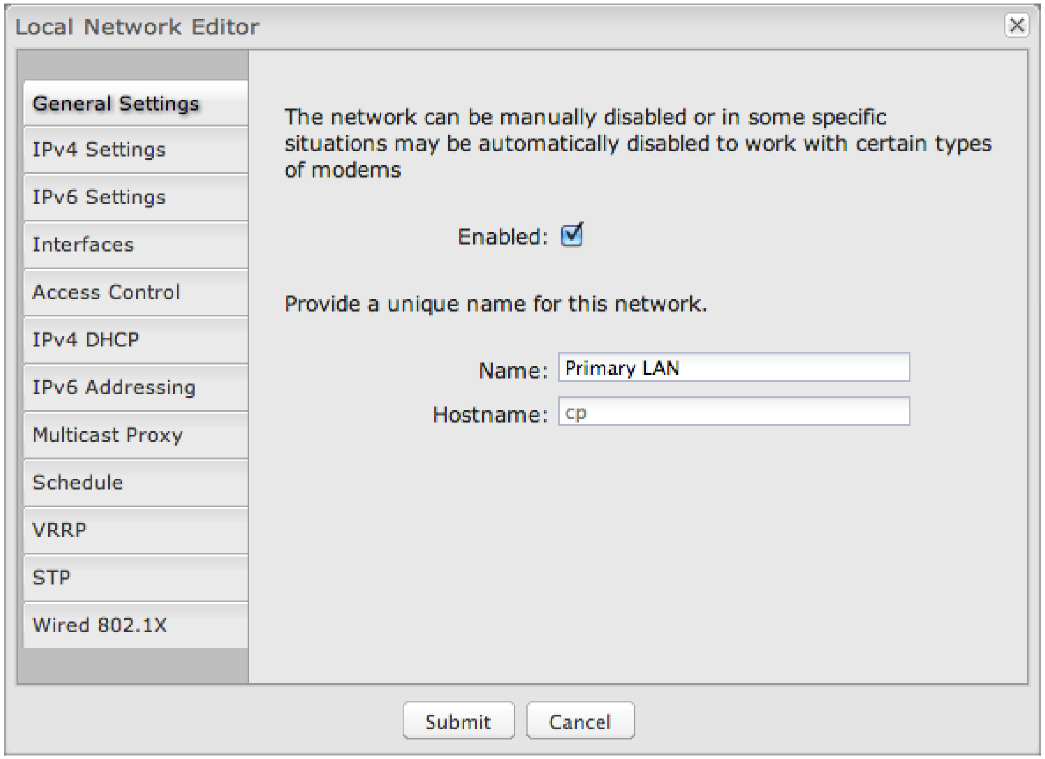
General Settings:

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

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

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

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



The network can be manually disabled or in some specific situations may be automatically disabled to work with certain types of modems

Enabled: ☑

Provide a unique name for this network.

Name: Primary LAN

Hostname: cp

IPv4 Settings:

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

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

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

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

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

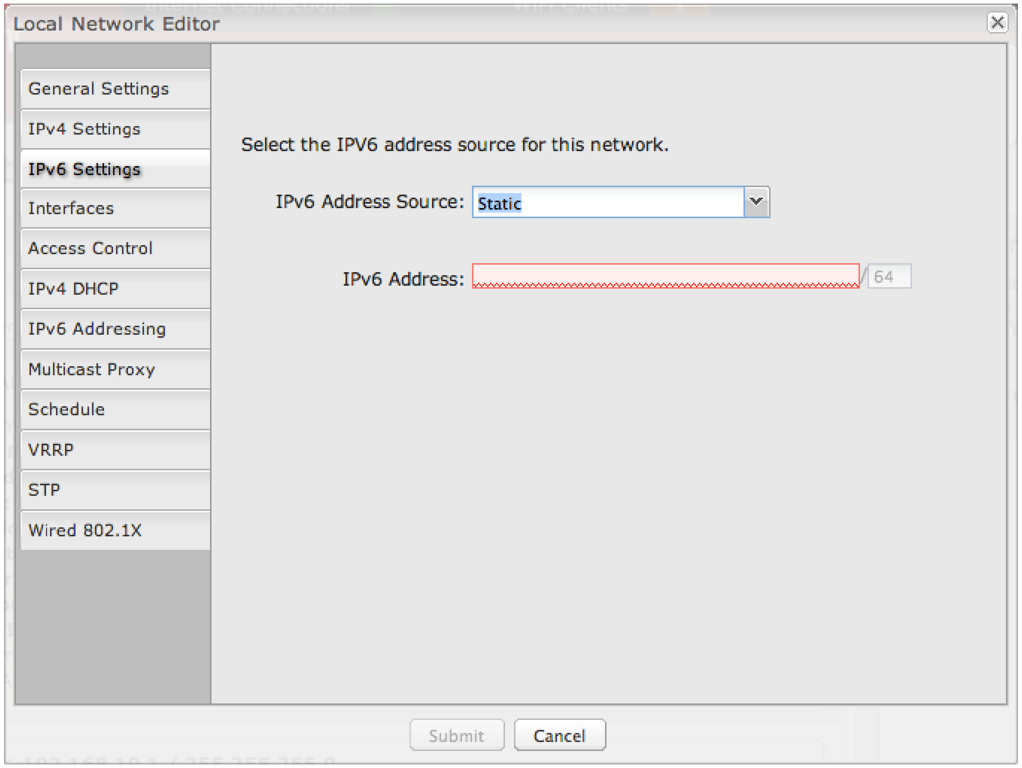
IPv4 Routing Mode: (Default: NAT) Each network can use a unique routing mode to connect to the Internet and other local networks. NAT is desirable for most configurations. Select from the following options in the dropdown list:

- **NAT:** Network Address Translation hides private IP addresses behind the router's IP address. This is the simplest and most common choice for users, because NAT does the translation work for you.
- **Standard:** NAT-less routing. If you select **Standard**, you must separately configure your IP addresses so that they will be publically accessible. Typically you will not select this option unless you have a specific reason to bypass NAT.
- **IP Passthrough:** IP Passthrough passes the IP address given by a cellular modem (WAN) through the router to Ethernet (LAN). All Ethernet ports must be in LAN mode (or disabled) and Hotspot, VPN, and GRE must be disabled. Any wireless interfaces must be removed from this network in order to enable IP Passthrough. The easiest way to enable IP Passthrough mode is with the **IP Passthrough Setup Wizard** (see **Getting Started → IP Passthrough Setup**).
- **Hotspot:** Provide Hotspot Services on this network, requiring Terms of Service or RADIUS/UAM authentication before WAN access will occur on both wireless and wired LAN connections. To enable a Hotspot you must also configure your Hotspot settings under **System Settings → Hotspot Services**.
- **Disabled:** Disable this network.

IPv6 Settings:

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

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



Select the IPV6 address source for this network.

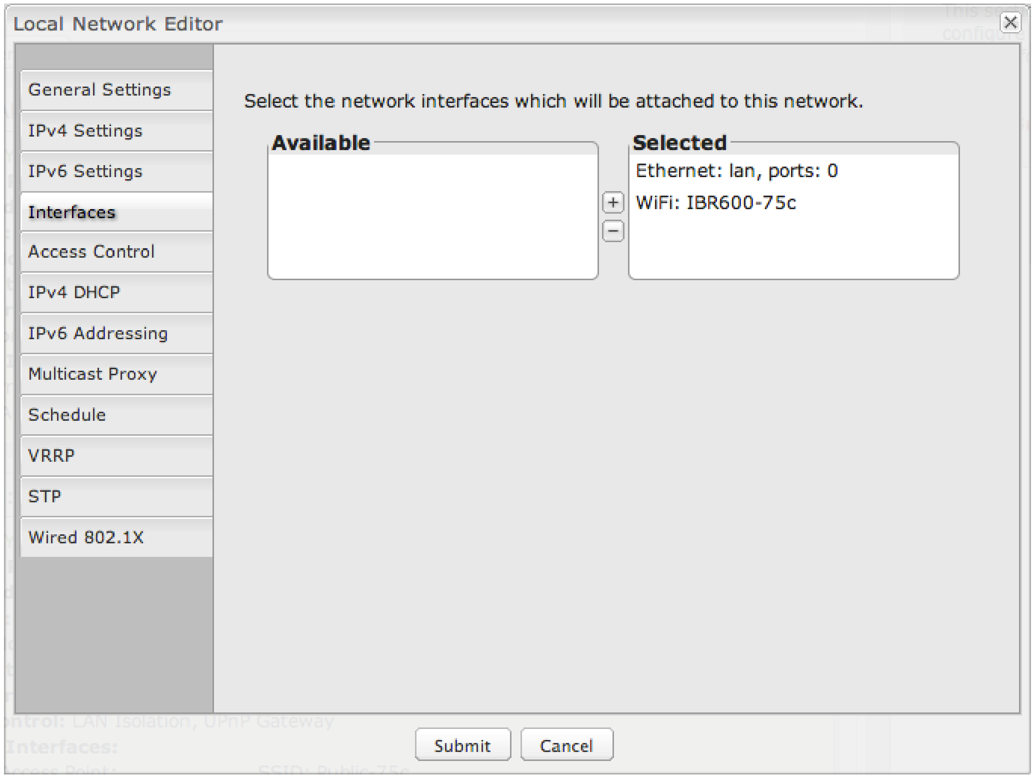
IPv6 Address Source: Static

IPv6 Address: / 64

Interfaces:

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

If you want more interface options, you must configure additional WiFi, Ethernet ports, and VLAN interfaces separately. See the **Local Network Interfaces** section below (on this same administration page: **Network Settings → WiFi / Local Networks**).



Select the network interfaces which will be attached to this network.

Available

Selected

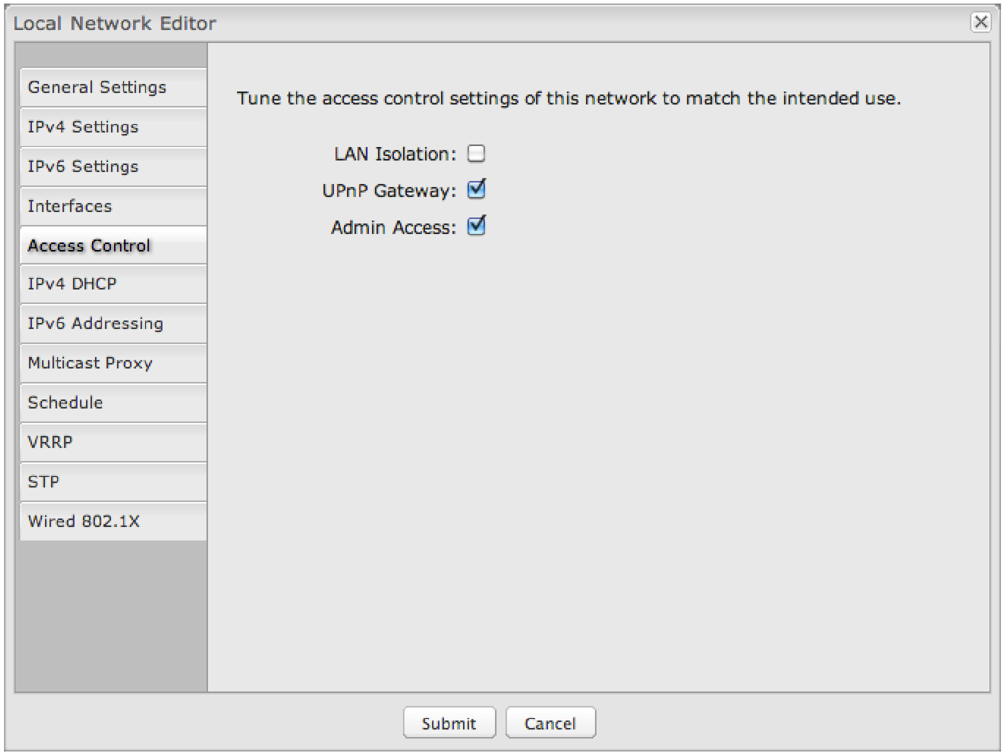
Ethernet: lan, ports: 0

WiFi: IBR600-75c

Access Control:

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

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



Tune the access control settings of this network to match the intended use.

LAN Isolation: □
UPnP Gateway: ☑
Admin Access: ☑

IPv4 DHCP:

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

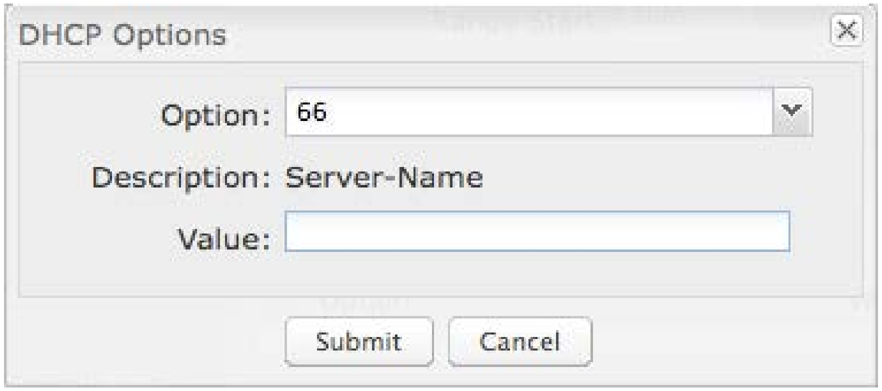
DHCP Server: (Default: Enabled) When the DHCP server is enabled, users of your network will be able to automatically connect to the Internet without any special configuration. **It is recommended that you leave this enabled.** Disabling the DHCP server is only recommended if you have another DHCP server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

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

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

Lease Time: [Default: 720 minutes (12 hours)] 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: Input a custom DHCP option by first clicking the **Custom Options** field to enable it and then clicking “Add” at the top of the table that appears. There are close to 200 possible DHCP options available. One of the more common uses is to assign a VoIP phone server using option 66 (Server name).



DHCP Options

Option: 66

Description: Server-Name

Value:

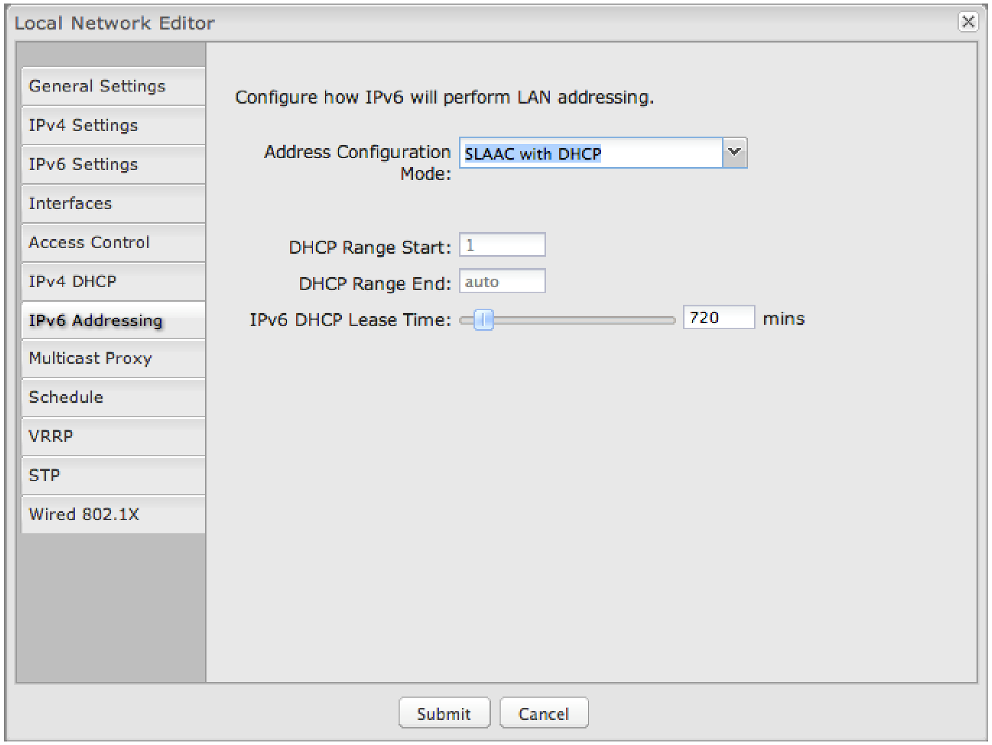
- **Option:** Select an option from the dropdown list or manually enter the number of an option. A complete list of options is available from IANA.
- **Value:** Generally this field should be a string, IP address, or numeric value. Some fields can accept both IP addresses and hostnames – in these cases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

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

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

IPv6 Addressing:

Address Configuration Mode:



Configure how IPv6 will perform LAN addressing.

Address Configuration Mode: SLAAC with DHCP

DHCP Range Start: 1

DHCP Range End: auto

IPv6 DHCP Lease Time: 720 mins

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

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

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

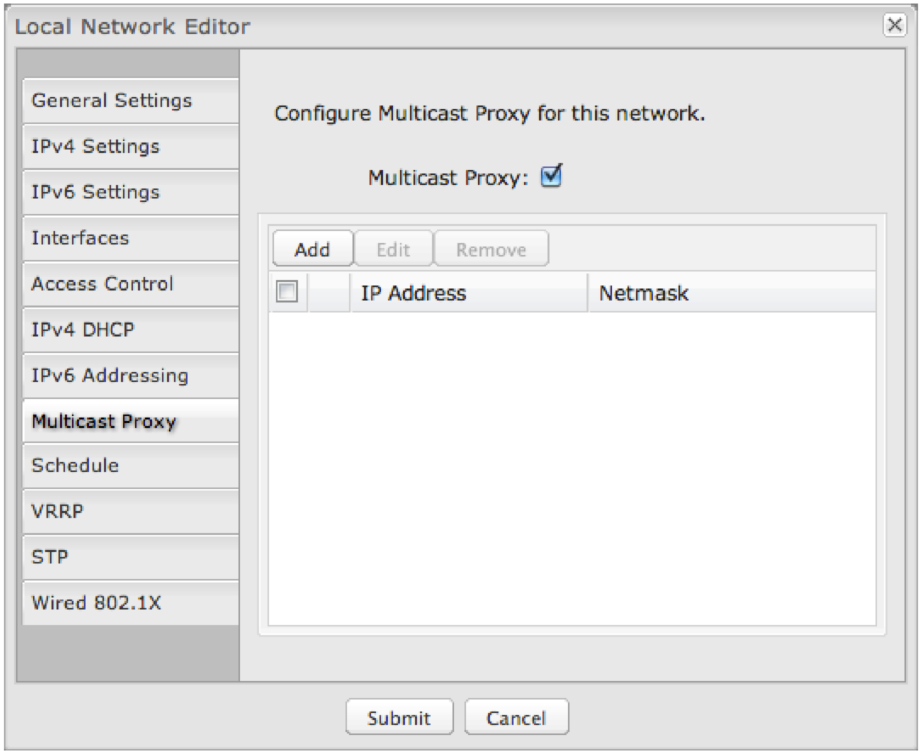
Disable SLAAC and DHCP – Disable both IPv6 address configuration modes.

Multicast Proxy:

IGMP (Internet Group Management Protocol) multicast proxy allows a single packet to reroute to multiple destinations (see the Wikipedia explanation of multicast). This may be used for IPTV, for example.

Multicast Proxy: Select to enable IGMP proxy support to allow multicast streams to flow across this network.

By default, enabling multicast proxy enables a multicast connection with devices within the LAN. In rare cases, additional IP address ranges need access to the multicast streams. Click **Add** and input the **IP Address** and **Netmask** for an additional IP address range.

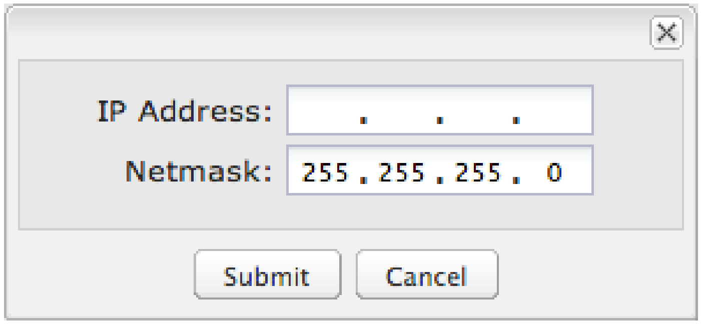


Local Network Editor

Configure Multicast Proxy for this network.

Multicast Proxy: ☑

☐	IP Address	Netmask



IP Address: . . .

Netmask: 255 . 255 . 255 . 0

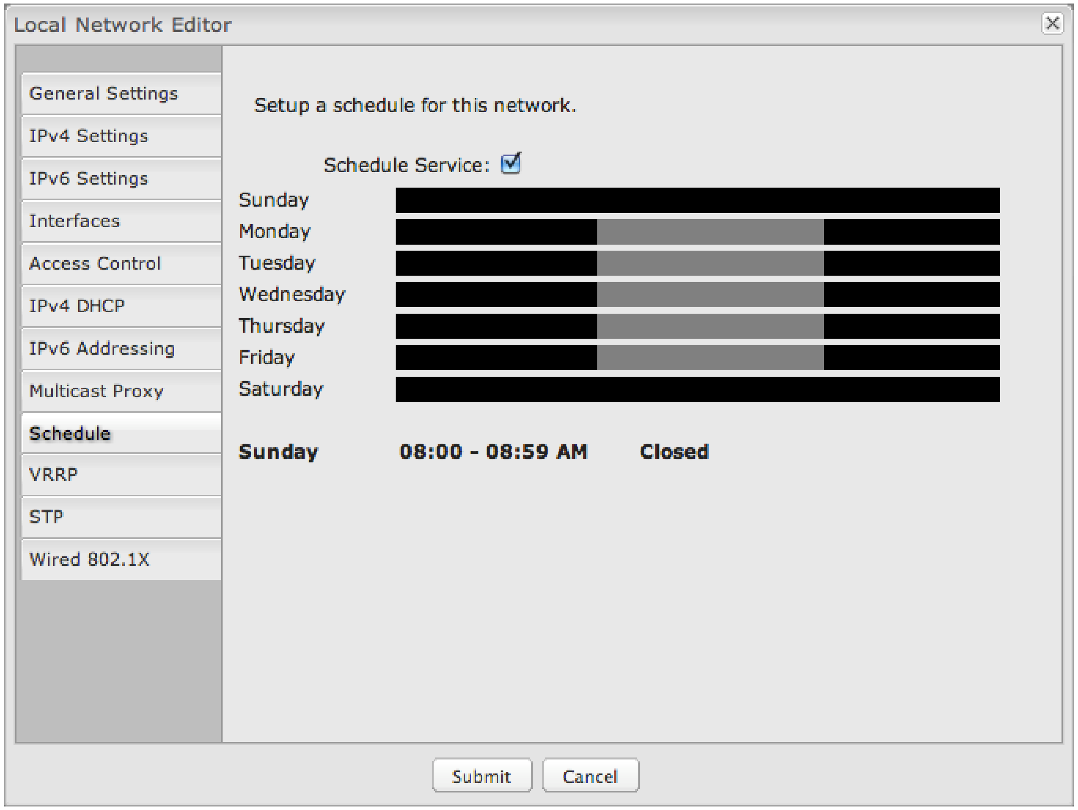
Schedule:

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

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

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

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



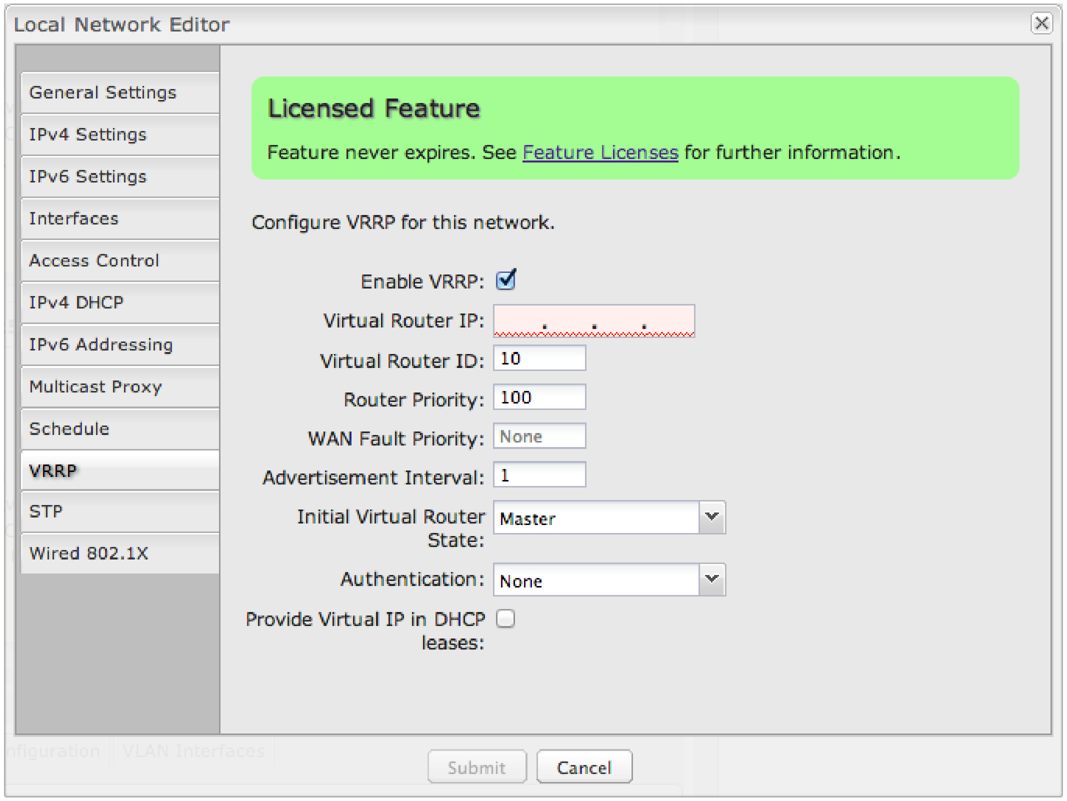
Setup a schedule for this network.

Schedule Service: ☑

Sunday 08:00 - 08:59 AM Closed

VRRP:

NOTE: VRRP requires a feature license. Go to **System Settings → Feature Licenses** to enable this feature. VRRP also requires hardware version 2.0.



Local Network Editor

Licensed Feature

Feature never expires. See Feature Licenses for further information.

Configure VRRP for this network.

Enable VRRP: ☑

Virtual Router IP: . . .

Virtual Router ID: 10

Router Priority: 100

WAN Fault Priority: None

Advertisement Interval: 1

Initial Virtual Router State: Master

Authentication: None

Provide Virtual IP in DHCP leases: □

VRRP (Virtual Router Redundancy Protocol) allows you to associate multiple routers with one LAN so that if the primary physical router fails, the LAN will keep the same settings via the virtual router.

Enable VRRP: Select to enable VRRP configuration options.

Virtual Router IP: IP address of the virtual router. This must be distinct from the IP address of any physical router associated with the virtual router.

Virtual Router ID: Identifying number of the virtual router. (Range: 1-255)

Router Priority: Failover priority level of this physical router. The physical router with the highest priority number will have primary ownership of the virtual router. (Range: 1-254)

WAN Fault Priority: This optional value sets the failover priority of this router when no WAN connection is available. If the value matches the normal router priority, WAN connection state will not be considered. If the value is empty (the default), the router will always give up ownership of the virtual IP and let a new master take over when no WAN connection is available.

Advertisement Interval: Sets the amount of time (in seconds) between VRRP advertisements, which communicate the router status. The default of 1 second is standard.

Initial Virtual Router State: This controls the initial VRRP failover state for this physical router: choose **Master** or **Backup**. This sets up the virtual router association more quickly than the **Router Priority** level, but the **Router Priority** assignment will eventually overrule this if there is a discrepancy.

Authentication: VRRP Authentication Method. This is for legacy purposes: VRRP Authentication has been deprecated as of RFC 3768. Select **None** or **Simple**. If you select **Simple**, input a VRRP group password.

Provide Virtual IP in DHCP leases: Select this to automatically set the DHCP default gateway address and DNS server address to the virtual IP in DHCP leases provided on this network.

STP:

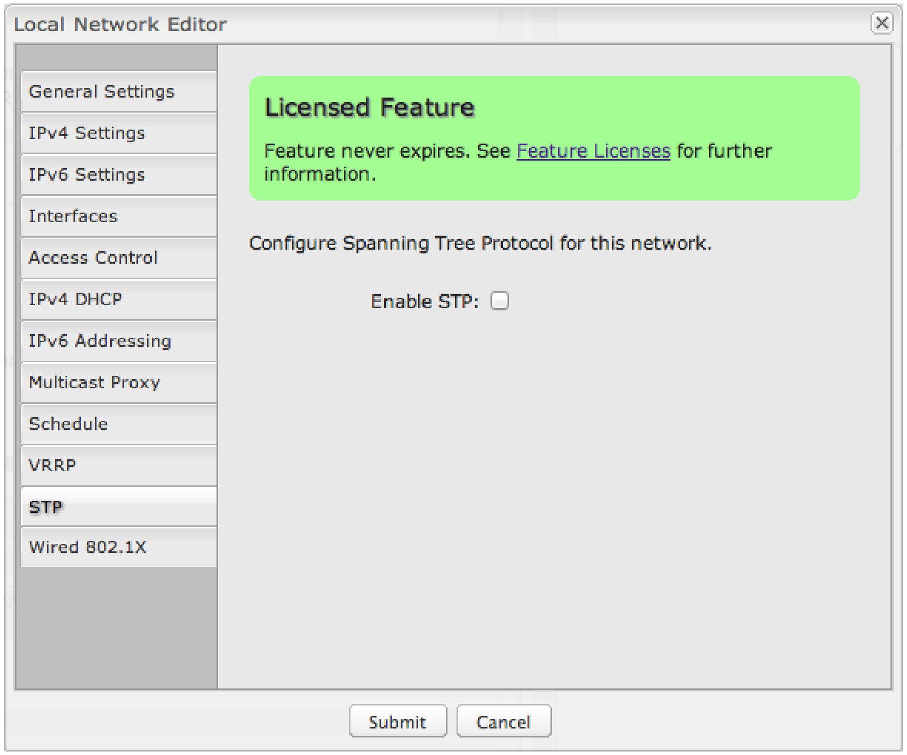
NOTE: STP requires a feature license. Go to **System Settings → Feature Licenses** to enable this feature. STP also requires hardware version 2.0.

NOTE: STP requires a feature license. Go to

Spanning Tree Protocol (STP) allows a network design to include redundant paths while preventing broadcast radiation from bridge loops.

Enable STP: Enable Spanning Tree Protocol loop detection.

Bridge Priority: Set the priority of the bridge. When determining the root bridge of the spanning tree topology, the bridge priority is compared first. The bridge with the lowest priority value will win. If you want this router to be the root bridge, then set it to a value less than the default of 32768. A valid priority value is between 0 and 65535.



Licensed Feature

Feature never expires. See Feature Licenses for further information.

Configure Spanning Tree Protocol for this network.

Enable STP: □

Wired 802.1X: (requires hardware version 2.0)

This allows you to configure an authentication server that will accept authentication requests from devices attached to wired Ethernet ports. IEEE 802.1X defines the encapsulations of the Extensible Authentication Protocol (EAP).

Click **Enable 802.1X** to require IEEE 802.1X authorization for the Ethernet ports associated with this network.

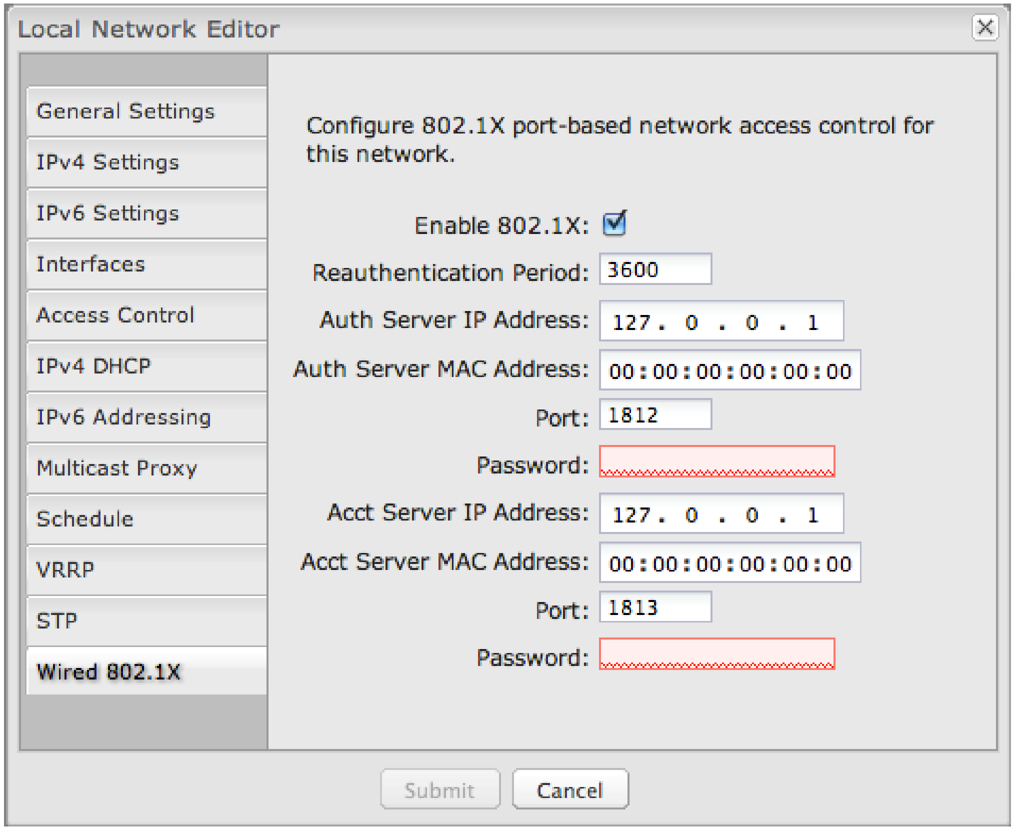
Reauthentication Period: EAP re-authentication period in seconds.

Authentication settings

- **Auth Server IP Address:** This is the IP address of the connected RADIUS server.
- **Auth Server MAC Address:** This is the hardware address of the connected RADIUS server's interface.
  NOTE: If you don't know the MAC address for the RADIUS server, enter 00:00:00:00:00:00 and the service will *try* to find the MAC address from the given IP address.
- **Port:** 1812 is common for the authentication port.
- **Password:** Assigned by the RADIUS server.

Accounting settings: Most of the accounting settings often match the authentication settings, depending on whether the RADIUS server is the same for both authentication and accounting.

- **Acct Server IP Address**
- **Acct Server MAC Address**
- **Port:** 1813 is common for the accounting port.
- **Password**



Configure 802.1X port-based network access control for this network.

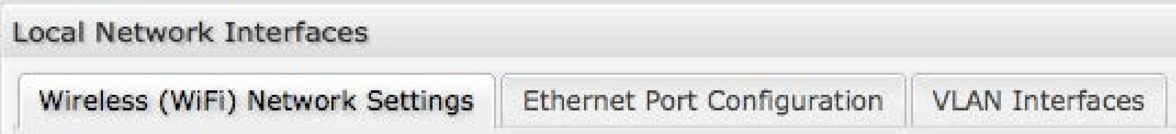
Enable 802.1X: ☑
Reauthentication Period: 3600
Auth Server IP Address: 127 . 0 . 0 . 1
Auth Server MAC Address: 00:00:00:00:00:00
Port: 1812
Password:
Acct Server IP Address: 127 . 0 . 0 . 1
Acct Server MAC Address: 00:00:00:00:00:00
Port: 1813
Password:

6.8.3 Local Network Interfaces

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

Select from the following tabs:

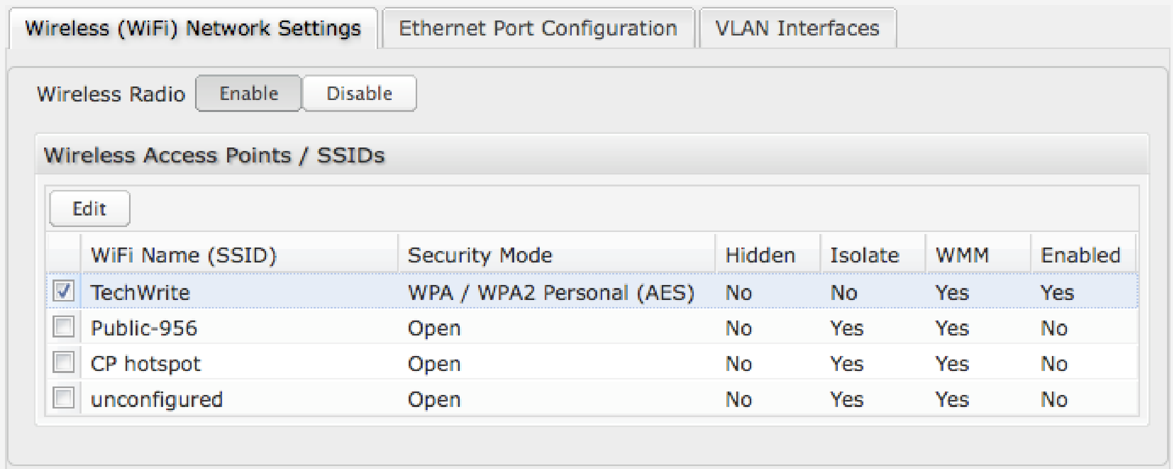
- **Wireless (WiFi) Network Settings**
- **Ethernet Port Configuration**
- **VLAN Interfaces**



<u>Wireless (WiFi) Network Settings</u>

The MBR1400 can broadcast as many as four SSIDs (service set identifiers – the names for WiFi networks). One primary WiFi network is enabled by default, while you may have enabled a second guest network when using the First Time Setup Wizard. You have the ability to change the settings for either of these networks and/or enable two additional networks.

Wireless Radio: Enable/Disable. (Default: Enabled). Leave enabled unless you don't want any WiFi networks broadcast from your router.


Wireless (WiFi) Network Settings
Ethernet Port Configuration
VLAN Interfaces
Wireless Radio
Enable
Disable
Wireless Access Points / SSIDs
Edit

	WiFi Name (SSID)	Security Mode	Hidden	Isolate	WMM	Enabled
☑	TechWrite	WPA / WPA2 Personal (AES)	No	No	Yes	Yes
□	Public-956	Open	No	Yes	Yes	No
□	CP hotspot	Open	No	Yes	Yes	No
□	unconfigured	Open	No	Yes	Yes	No

Select a WiFi network and click **Edit** to change the settings.

Wireless Network Editor

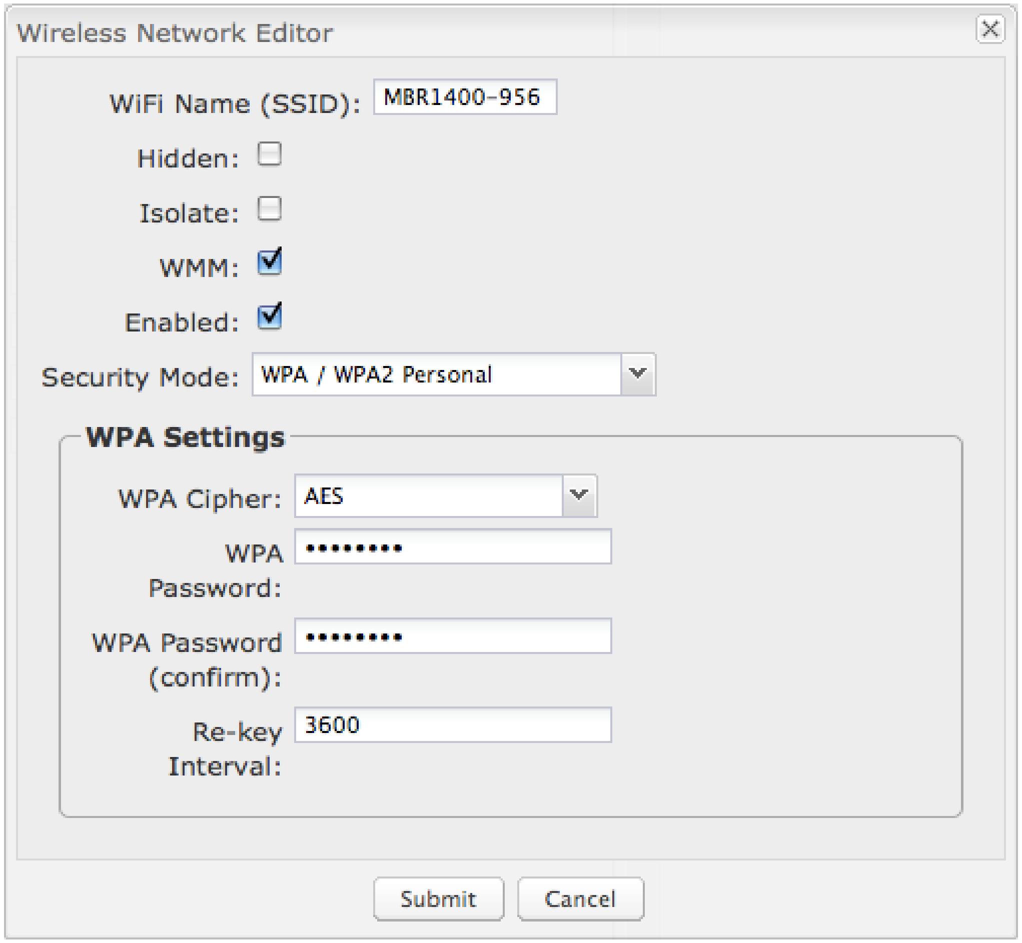
WiFi Name (SSID): When users browse for available wireless networks, this is the name that they will see. This name is referred to as the SSID (service set identifier). For security purposes, Cradlepoint highly recommends that you change this from the pre-configured name.

Hidden: This shows whether the router broadcasts its SSID. It is somewhat harder for hackers to find and attack a router that is not broadcasting its SSID, which adds to the wireless security, but it is also more difficult for friendly users to attach to a WiFi network with a hidden SSID.

Isolate: Select this to isolate all wireless clients so they cannot directly communicate with each other on the wireless network.

WMM: WiFi Multimedia. This is a basic traffic shaping, or QoS (quality of service), system for the network. WMM works behind the scenes to set priorities for different types of traffic on your network. For example, video streams are given higher priority than print jobs, since video streams need consistent throughput.

Enabled: Whether the network is available.



Wireless Network Editor

WiFi Name (SSID): MBR1400-956

Hidden: □

Isolate: □

WMM: ☑

Enabled: ☑

Security Mode: WPA / WPA2 Personal

WPA Settings

WPA Cipher: AES

WPA Password: ••••••••

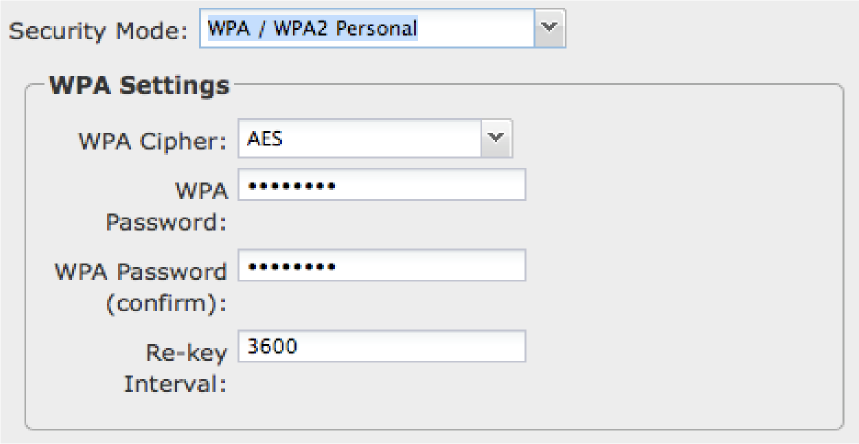
WPA Password (confirm): ••••••••

Re-key Interval: 3600

Security Mode: You have several options for selecting a security mode. The mode you choose depends on the security features your wireless adapters support.

- WPA2 Personal
- WPA / WPA2 Personal
- WPA Personal
- WPA2 Enterprise
- WPA / WPA2 Enterprise
- WPA Enterprise
- WEP Auto
- Open

Select "Open" to create a hotspot: otherwise select the best security that your devices will support (Cradlepoint recommends **WPA2**).



Security Mode: WPA / WPA2 Personal

WPA Settings

WPA Cipher: AES

WPA Password: •••••••••

WPA Password (confirm): •••••••••

Re-key Interval: 3600

Depending on which Security Mode you select, there are different setup options.

- "**Personal**" security modes require passwords.
- "**Enterprise**" security modes are linked to a RADIUS server and require RADIUS authentication: **IP**, **Port**, and **Shared Key** (Secondary IP and NAS ID optional).
- "**WPA2**" (Personal or Enterprise) forces AES as the WPA Cipher.
- "**WPA/WPA2**" and "**WPA**" (Personal or Enterprise) allow AES, TKIP/AES, and TKIP.
- "**WEP Auto**" requires a WEP Key.
- "**Open**" has no password or other security measures.

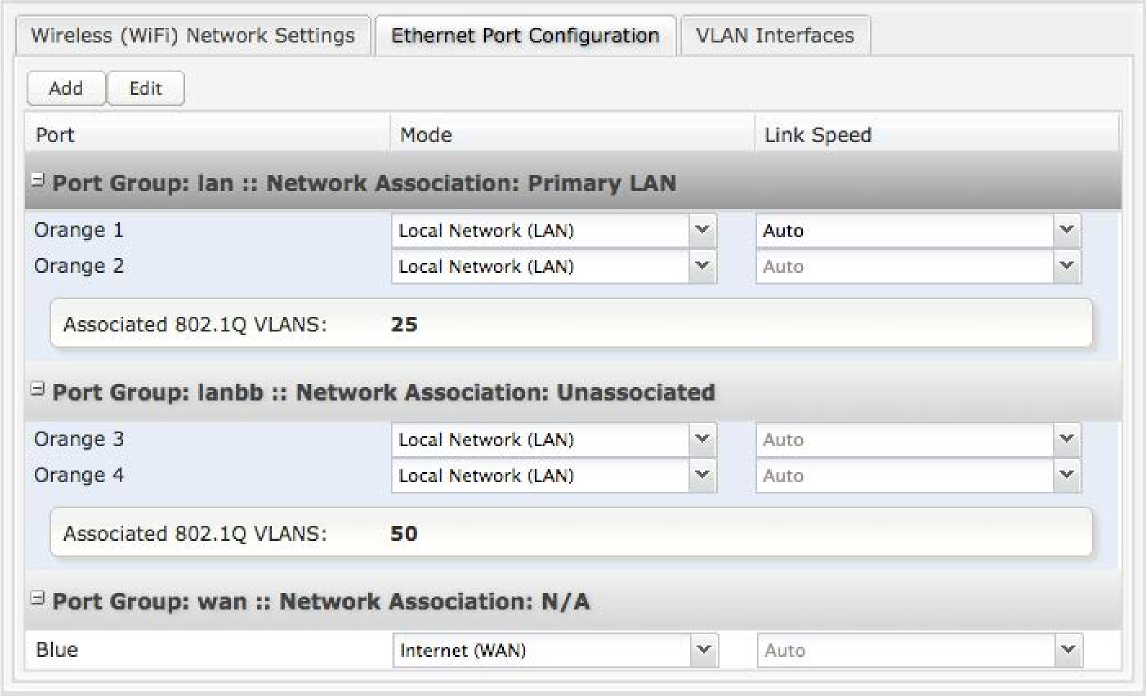
NOTE: If you don't know whether you should choose Personal or Enterprise, assume Personal since you need to know RADIUS authentication for Enterprise.

In order to protect your network from hackers and unauthorized users, Cradlepoint highly recommends **WPA2/AES** for security if your attached devices can support it. WEP and WPA/TKIP are obsolete and have been replaced by WPA/AES. Using those security settings will cause the WiFi to limit to 802.11g modes.

NOTE: If you select one of the security modes and are unable to connect to the router afterwards, you can use the reset buttons to reset the router to its factory default state and try a different security mode instead.

Ethernet Port Configuration

Ethernet Port Configuration provides controls for your router's Ethernet ports. There are five total ports: one blue port and four numbered orange ports. While default settings will be sufficient in most circumstances, you have the ability to control: **Mode** (WAN or LAN) and **Link Speed**. Additional controls for WAN ports are available in **Internet → Ethernet Settings**.



Port	Mode	Link Speed
⊟ **Port Group: lan :: Network Association: Primary LAN**		
Orange 1	Local Network (LAN)	Auto
Orange 2	Local Network (LAN)	Auto
Associated 802.1Q VLANS:	**25**	
⊟ **Port Group: lanbb :: Network Association: Unassociated**		
Orange 3	Local Network (LAN)	Auto
Orange 4	Local Network (LAN)	Auto
Associated 802.1Q VLANS:	**50**	
⊟ **Port Group: wan :: Network Association: N/A**		
Blue	Internet (WAN)	Auto

Mode: WAN or LAN. Default setting is WAN (Wide Area Network) for the blue port and LAN (Local Area Network) for the four orange ports.

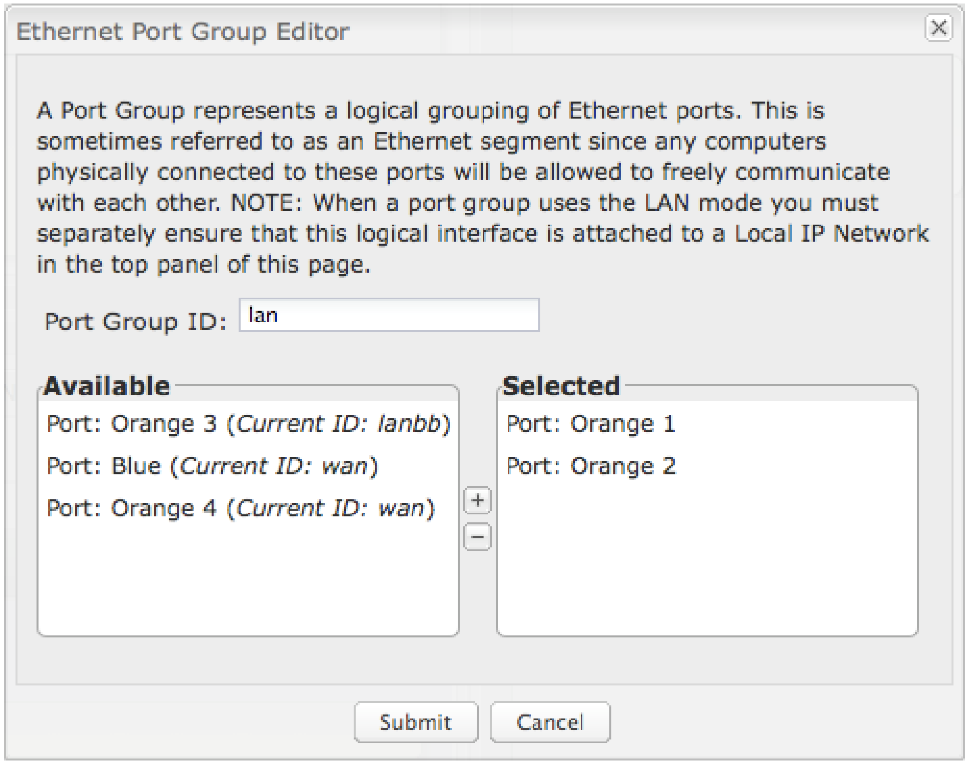
- **Internet (WAN)** is used to connect to another network such as a hotel or office wired network. The WAN connection is used as a possible source of Internet for the MBR1400.
- **Local Network (LAN)** is for connecting a computer or similar device directly to the router with an Ethernet cable.

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

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

Ethernet Port Group Editor

A Port Group represents a logical grouping of Ethernet ports. Any computers physically connected to ports in a group will be allowed to freely communicate with each other. For example, if you leave all four orange ports set as LAN ports, you might group Orange Port 1 and Orange Port 2 together to be part of your primary network, and then group Orange Port 3 and Orange Port 4 together to be part of a guest network.



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

Port Group ID: lan

Available

Port: Orange 3 (*Current ID: lanbb*)

Port: Blue (*Current ID: wan*)

Port: Orange 4 (*Current ID: wan*)

Selected

Port: Orange 1

Port: Orange 2

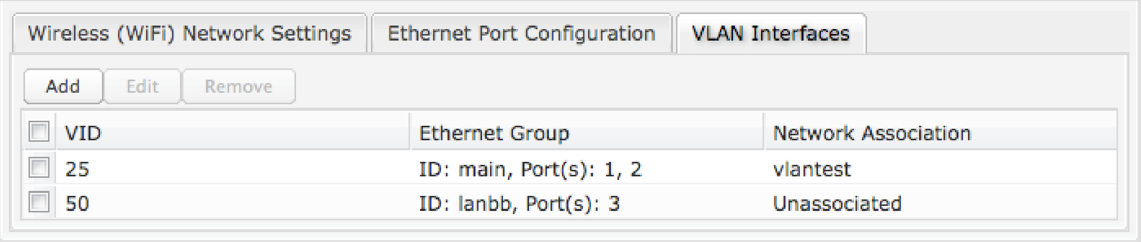
NOTE: When a port group uses the LAN mode you must separately ensure that this logical interface is attached to a **Local IP Network** in the top panel of this page.

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

Select one or more ports to create a port group that you can subsequently attach to a network in the **Local Network Editor**. Double-click on any of the Ethernet ports shown on the left in the **Available** section to move them to the **Selected** section on the right (or highlight a port and click the + button). To deselect an Ethernet port, double-click on an interface in the **Selected** section (or highlight the port and click the – button).

VLAN Interfaces

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

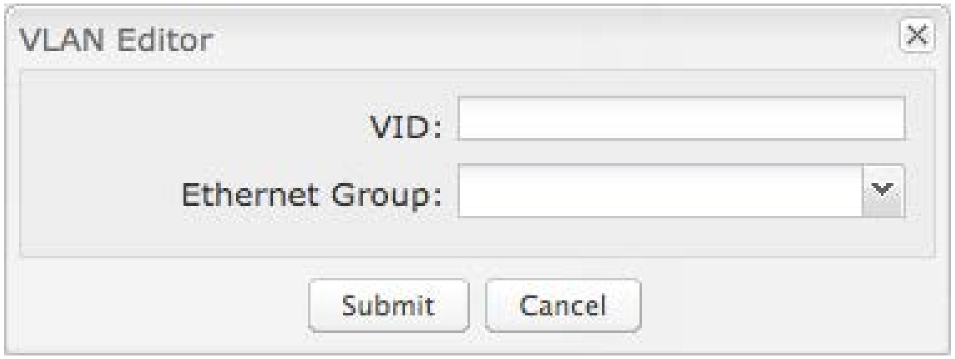


□	VID	Ethernet Group	Network Association
□	25	ID: main, Port(s): 1, 2	vlantest
□	50	ID: lanbb, Port(s): 3	Unassociated

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.

VLAN Editor



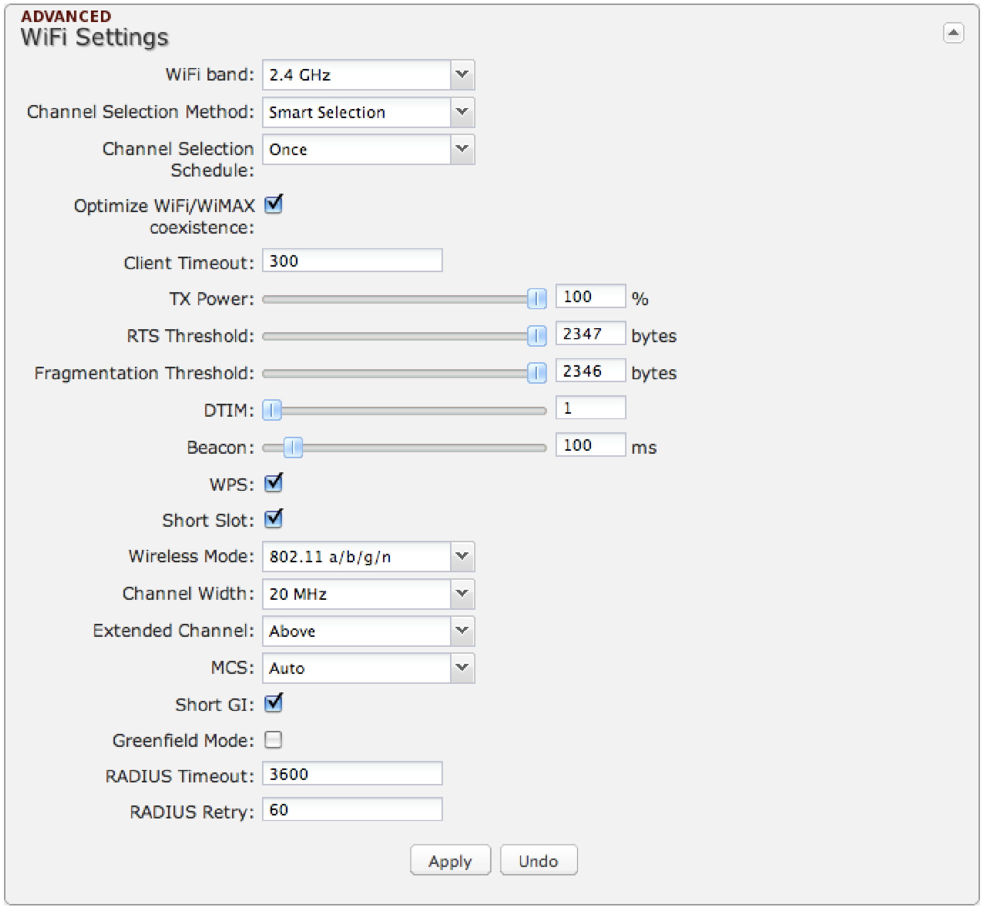
VID: An integer value that is the Virtual LAN ID.

Ethernet Group: Select the LAN port(s) with which you want to associate the VLAN ID from a dropdown list. Your Ethernet group must be created separately under **Ethernet Port Configuration**.

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

6.8.4 WiFi Settings (Advanced)

When you select the **Wireless (WiFi) Networks Settings** tab in the **Local Network Interfaces** section, you have several additional options for configuring your wireless LANs under the **WiFi Settings** heading.



ADVANCED
WiFi Settings

WiFi band: 2.4 GHz
Channel Selection Method: Smart Selection
Channel Selection Schedule: Once
Optimize WiFi/WiMAX coexistence: ☑
Client Timeout: 300
TX Power: 100 %
RTS Threshold: 2347 bytes
Fragmentation Threshold: 2346 bytes
DTIM: 1
Beacon: 100 ms
WPS: ☑
Short Slot: ☑
Wireless Mode: 802.11 a/b/g/n
Channel Width: 20 MHz
Extended Channel: Above
MCS: Auto
Short GI: ☑
Greenfield Mode: □
RADIUS Timeout: 3600
RADIUS Retry: 60

WiFi band: Select the range of frequencies the router will use. The MBR1400 can operate in either the 2.4 GHz or the 5.0 GHz ranges. (Default: 2.4 GHz. The included WiFi antennas are 2.4 GHz. 5 GHz antennas are available as an accessory.)

Channel Selection Method: This controls how a WiFi channel is selected.

- **User Selection.** Manually set the channel.
- **Random Selection.** The router randomly sets the channel.
- **Smart Selection (Default).** Scans to determine the lowest interference WiFi channel.

Channel Selection Schedule: When using the "Smart" channel selection, this controls whether the router will periodically rescan for a better channel and change to it. Select from “Once,” “Daily,” “Weekly,” or “Monthly.” Note that there may be a momentary WiFi disconnection while the channel changes.

Optimize WiFi/WiMAX coexistence: (Shows if **Smart Selection** or **Random Selection** is chosen and the **WiFi Band** is 2.4 GHz.) Setting this will lessen any possible conflict with WiFi in the 2.4 GHz band and an attached WiMAX modem. If a WiMAX modem is attached to the router when the WiFi is enabled, the WiFi channel and transmit power will be set to levels that optimize the performance of the WiMAX modem. If no WiMAX modem is attached, then default channel and power settings will be used even if this is selected.

Channel: (Shows if **User Selection** is selected.) The WiFi channel corresponds to a frequency the router uses to communicate with other devices. For 2.4 GHz, the range is 1 to 11, and 1, 6, and 11 do not overlap each other. If a WiMAX modem is attached, a higher number channel will increase the chance the router's WiFi and modem's WiMAX radios will conflict with each other, which may result in lower throughput. Select a channel from the dropdown list:

- 1 (2412 MHz)
- 2 (2417 MHz)
- 3 (2422 MHz)
- 4 (2427 MHz)
- 5 (2432 MHz)
- 6 (2437 MHz)
- 7 (2442 MHz)
- 8 (2447 MHz)
- 9 (2452 MHz)
- 10 (2457 MHz)
- 11 (2462 MHz)

For 5.0 GHz, the ranges are 36 to 64 and 149 to 165. These channels do not interfere with a WiMAX modem. **If you choose to use 5.0 GHz, you should consider switching antennas. The default WiFi antennas are optimized for the 2.4 GHz range.**

- 36 (5180 MHz)
- 40 (5200 MHz)
- 44 (5220 MHz)
- 48 (5240 MHz)
- 149 (5745 MHz)
- 153 (5765 MHz)
- 157 (5785 MHz)
- 161 (5805 MHz)
- 165 (5825 MHz)

Client Timeout: If the access point is not able to communicate with the client it will disconnect it after this timeout (in seconds).

TX Power: Normally the wireless transmitter operates at 100% power. In some circumstances, however, there might be a need to isolate specific frequencies to a smaller area. By reducing the power of the radio, you can prevent transmissions from reaching beyond your corporate/home office or designated wireless area.

RTS Threshold: When an excessive number of wireless packet collisions are occurring, wireless performance can be improved by using the RTS/CTS (Request to Send/Clear to Send) handshake protocol. The wireless transmitter will begin to send RTS frames (and wait for CTS) when data frame size in bytes is greater than the RTS Threshold. This setting should remain at its default value.

Fragmentation Threshold: Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. This setting should remain at its default value. Setting the Fragmentation value too low may result in poor performance.

DTIM: A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.

Beacon: Beacons are packets sent by a wireless router to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000 milliseconds.

WPS: WiFi Protected Setup is a method for easy and secure establishment of a wireless network. It can be used instead of passwords when connecting clients that support WPS.

Short Slot: Slot Time is the period wireless clients use in determining if the channel is free for transmission. Enabling this value allows clients that can utilize a shorter time to do so. Disabling this option forces all clients to use a longer backoff check and thus may reduce network throughput while reducing the number of transmission collisions.

Wireless Mode: Select the WiFi clients the router will be compatible with. Greater compatibility is a tradeoff with better performance. For greatest compatibility with all WiFi devices, select "802.11 a/b/g/n". For best performance, connect with only other 802.11n-compatible devices and select "802.11 n."

- 802.11 b
- 802.11 b/g
- 802.11 a/b/g/n
- 802.11 b/g/n
- 802.11 n

Channel Width: Selects whether the router uses a single 20 MHz channel to send/receive, or uses two adjacent 20 MHz channels to create a 40 MHz channel. Higher performance is possible with the 40 MHz channel. Selecting Auto is generally best. Enabling WiFi as WAN will force 20 MHz only mode.

Extended Channel: When operating in 40 MHz mode the access point will use an extended channel either below or above the current channel. Optimal selection will depend on the channels of other networks in the area.

MCS: 802.11n uses multiple Modulation Coding Schemes to enable higher throughput in various environments. Since clients can dynamically change rates depending on environment, selecting **Auto** is generally best.

Short GI: Short GI is an optimization for shortening the interval between transmissions. May be incompatible with older clients.

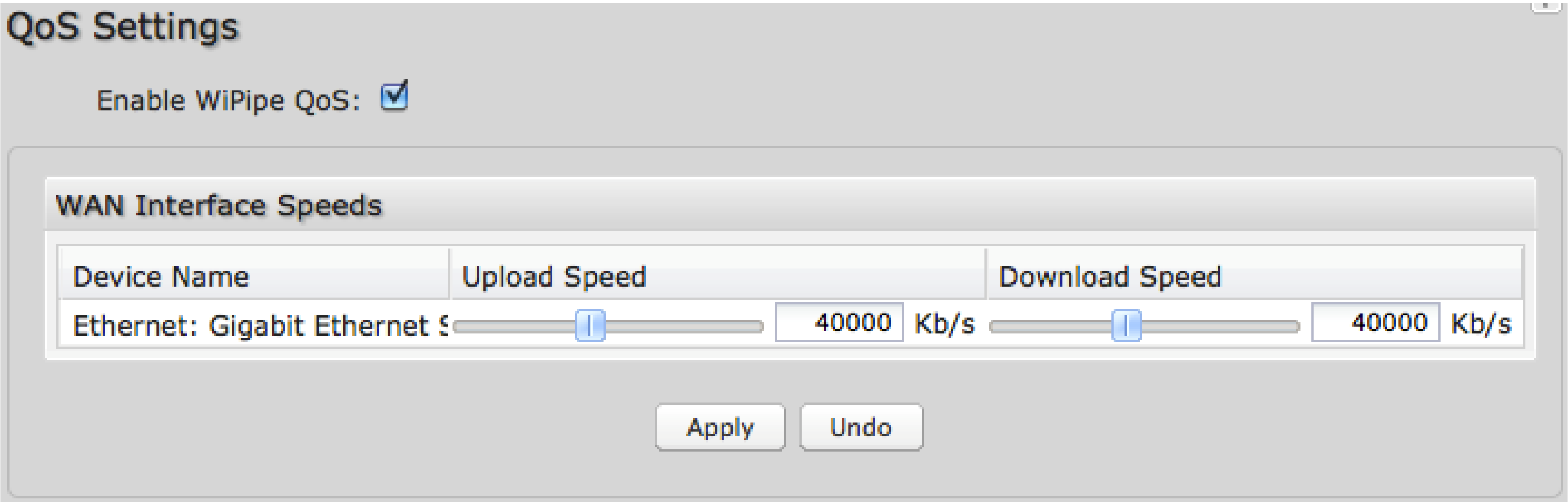
Greenfield Mode: Greenfield mode uses an 802.11n-only preamble to transmit packets that older wireless clients cannot interpret. Use of greenfield mode in a mixed 802.11 environment may result in degraded performance but can improve performance if all devices in the area are 802.11n compatible.

RADIUS Timeout: (Default: 3600 seconds) When using an Enterprise security mode clients will be forced to re-authenticate with the RADIUS server at this interval in seconds. This allows administrators to revoke access so when an attached client’s authentication expires, the client must re-authenticate.

RADIUS Retry: (Default: 60 seconds) When using an Enterprise security mode, if a RADIUS query fails to receive a response from the server it will delay by this interval (in seconds) before attempting another query. This helps protect the network from floods of authentication requests if the RADIUS server is temporarily unreachable.

6.9 WiPipe QoS

When WiPipe QoS (Quality of Service, also known as "Traffic Shaping") is enabled, the router will control the flow of Internet traffic according to the user-defined rules. In other words, Traffic Shaping improves performance by allowing the user to prioritize applications.



QoS Settings

Enable WiPipe QoS: ☑

WAN Interface Speeds

Device Name	Upload Speed	Download Speed
Ethernet: Gigabit Ethernet S	40000 Kb/s	40000 Kb/s

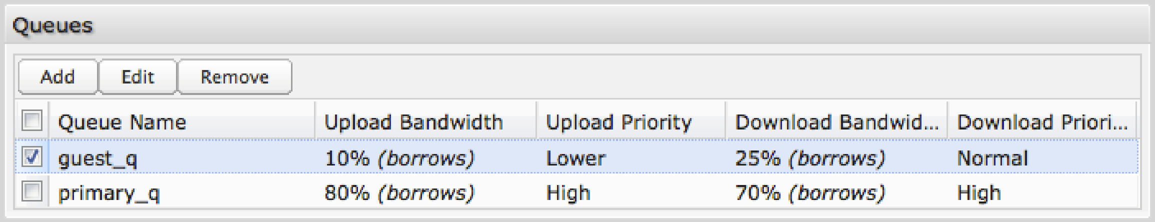
Enable WiPipe QoS: Click on this box to open options for controlling Internet traffic. You can assign maximum Upload Speed and Download Speed values and define your own Traffic Shaping rules.

Upload Speed and **Download Speed:** Setting the **Upload Speed** and **Download Speed** is required to control traffic flow accurately. Adjust the sliding bar to restrict the maximum upload and/or download speed for the Internet source(s) you are using. For example, you might restrict the upload speed to prioritize available bandwidth for download or to reduce overall bandwidth use in order to lower costs. It is recommended that you experiment with different values for your particular Internet connection for best results.

NOTE: Upload speed is the speed at which data can be transferred to your ISP. Download speed is the speed at which data can be transferred to you from your ISP. You can test your connection speeds with a service such as speedtest.net.

6.9.1 Queues

Queues and rules work in conjunction to prioritize bandwidth for the most critical operations. Multiple rules can be associated with one queue. Use rules to associate your more critical operations with queues that have higher bandwidth settings. For example, you might have two queues, one for "critical" and one for "secondary" with critical having most of the bandwidth percentage. Use rules to associate your most important bandwidth needs (POS system, VoIP, etc.) with the critical queue. Restrict the bandwidth available for less important functions with the secondary queue.



□	Queue Name	Upload Bandwidth	Upload Priority	Download Bandwid...	Download Priori...
☑	guest_q	10% *(borrows)*	Lower	25% *(borrows)*	Normal
□	primary_q	80% *(borrows)*	High	70% *(borrows)*	High

Assign percentages of both upload and download bandwidth to each queue. If you assign 80% download bandwidth to the first queue, the next queue will be forced to be 20% or less.

Click **Add** to create a new Traffic Shaping/QoS queue.

Queue Name: Choose a name that is meaningful to you.

<u>Upload Bandwidth</u>

Enable Upload QoS: (Default: Enabled.) Deselect if you want your rule to apply to download traffic only. Leave this selected to include upload restrictions with this queue.

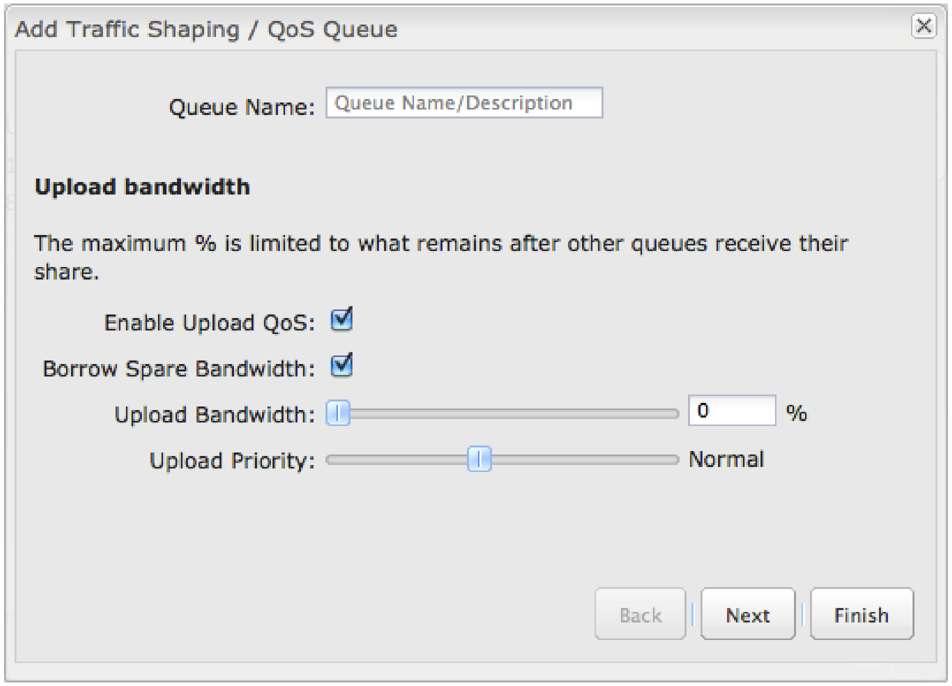
Borrow Spare Bandwidth: (Default: Enabled.) When this is enabled, the interfaces/protocols associated with this rule will borrow unused bandwidth from other rules. Disabling borrowing will restrict the traffic to the specified bandwidth. Higher priority queues will be offered excess bandwidth first.

Upload Bandwidth: This is the percentage of the connected WAN upload bandwidth that will be reserved for the specified traffic. The maximum value is adjusted to the remaining percentage after other rules receive their share.

Upload Priority: The priority value has two different effects on traffic. Higher priority traffic is handled before lower priority traffic, which can lead to shorter response times. Also, when spare bandwidth is available it is offered to higher priority queues first. Move the slider to select from the following options (Default: Normal):

- Lowest
- Lower
- Below Normal
- Normal
- Above Normal
- High
- Higher
- Highest

Click **Next** to continue to the next page.



Add Traffic Shaping / QoS Queue

Queue Name: Queue Name/Description

Upload bandwidth

The maximum % is limited to what remains after other queues receive their share.

Enable Upload QoS: ☑

Borrow Spare Bandwidth: ☑

Upload Bandwidth: 0 %

Upload Priority: Normal

Download Bandwidth

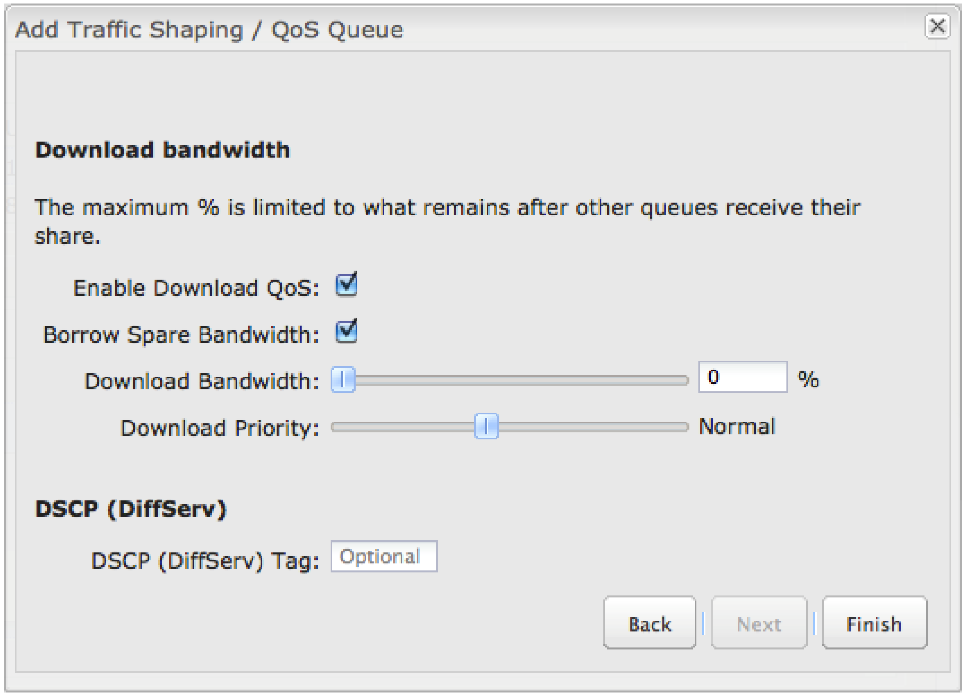
Enable Download QoS: (Default: Enabled.) Deselect if you want your rule to apply to upload traffic only. Leave this selected to include download restrictions with this queue.

Borrow Spare Bandwidth: (Default: Enabled.) When this is enabled, the interfaces/protocols associated with this rule will borrow unused bandwidth from other rules. Disabling borrowing will restrict the traffic to the specified bandwidth. Higher priority queues will be offered excess bandwidth first.

Download Bandwidth: This is the percentage of the connected WAN upload bandwidth that will be reserved for the specified traffic. The maximum value is adjusted to the remaining percentage after other queues receive their share.

Download Priority: The priority value has two different effects on traffic. Higher priority traffic is handled before lower priority traffic, which can lead to shorter response times. Also, when spare bandwidth is available it is offered to higher priority queues first. Move the slider to select from the following options (Default: Normal):

- Lowest
- Lower
- Below Normal
- Normal
- Above Normal
- High
- Higher
- Highest


Add Traffic Shaping / QoS Queue

Download bandwidth

The maximum % is limited to what remains after other queues receive their share.

Enable Download QoS: ☑

Borrow Spare Bandwidth: ☑

Download Bandwidth: 0 %

Download Priority: Normal

DSCP (DiffServ)

DSCP (DiffServ) Tag: Optional

DSCP (DiffServ) Tag: Differentiated Services Code Point (DSCP) is the successor to TOS (Type of Service). Use this field to 'tag' the traffic by putting the value in the DSCP header of each IP packet that flows through this queue. Use the value of '0' to clear the existing DSCP value in the packet header.

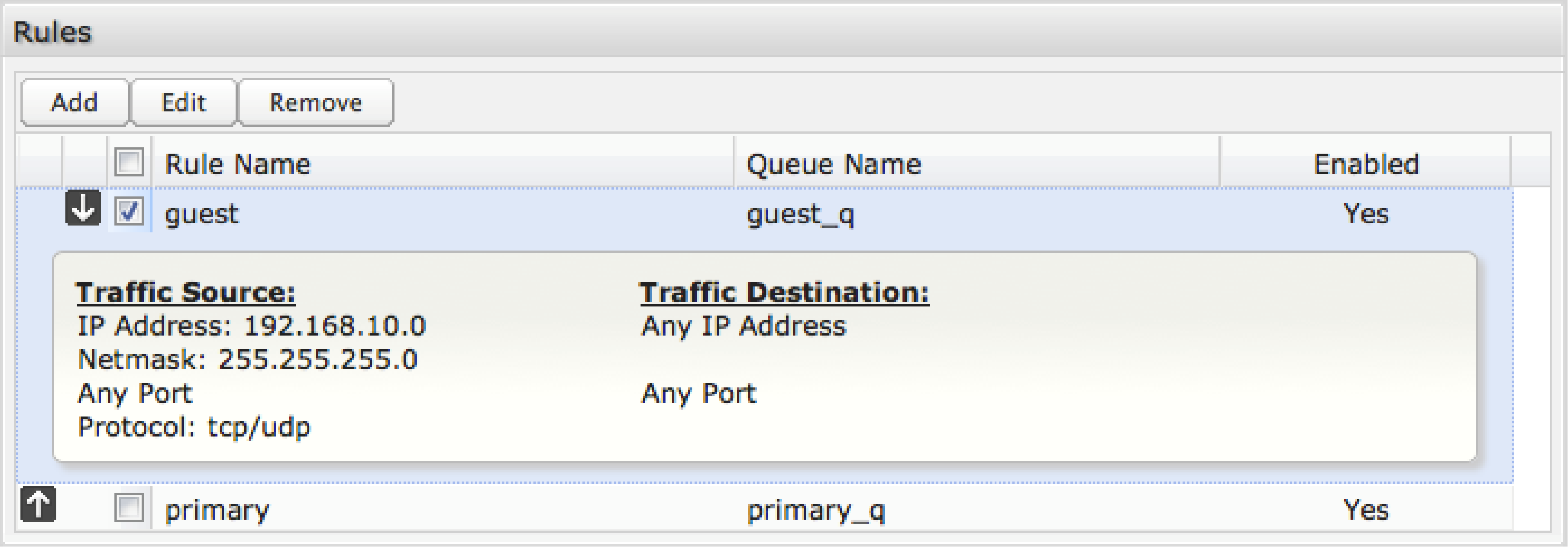
DSCP Tagging is sometimes used so that other networking equipment, upstream or post-NAT, can do traffic shaping based on the DSCP Tags as opposed to IP addresses or ports.

This setting is optional. For more information see the Differentiated services Wikipedia page.

Click **Finish** to save this queue.

6.9.2 Rules

A traffic shaping rule identifies a specific message flow and assigns that flow to one of the queues created above.



	□	Rule Name	Queue Name	Enabled
↓	☑	guest	guest_q	Yes
↑	□	primary	primary_q	Yes

Traffic Source:
IP Address: 192.168.10.0
Netmask: 255.255.255.0
Any Port
Protocol: tcp/udp

Traffic Destination:
Any IP Address

Any Port

Click **Add** to create a new Traffic Shaping rule.

Traffic Shaping / QoS Rule Editor

The first page of the Traffic Shaping / QoS Rule Editor allows you enable/disable the rule, name the rule, specify a protocol for the rule, and select a queue to associate the rule with.

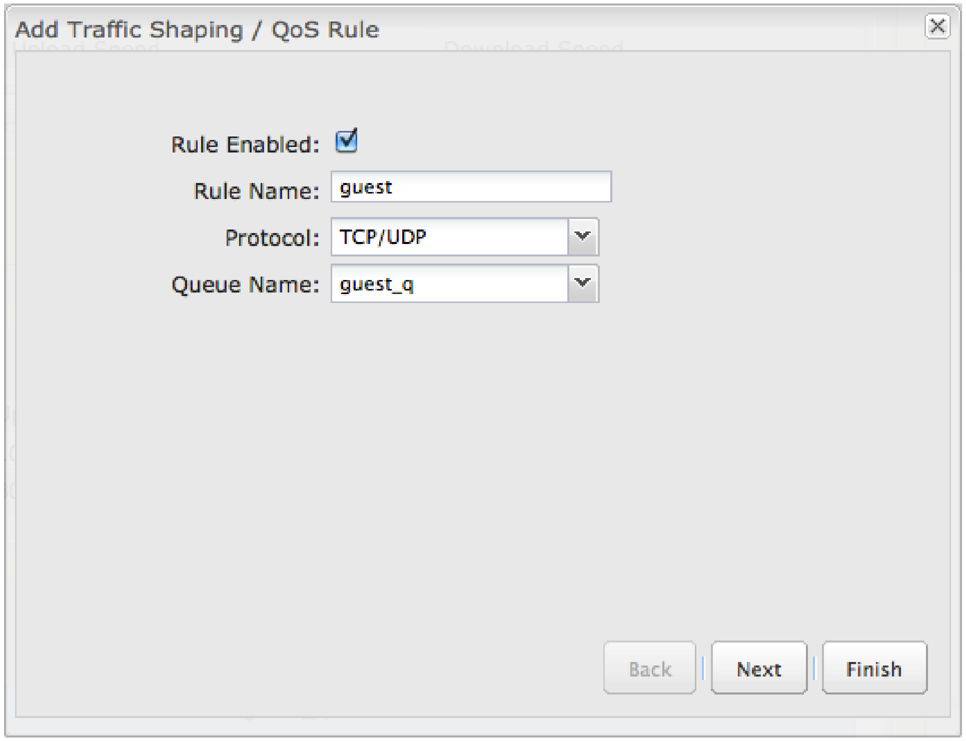
Rule Enabled: (Default: Enabled.) Deselect this to disable this rule. This can be useful for quickly changing configurations. If both upload QoS and download QoS are disabled then the rule will disable automatically.

Rule Name: Create a name for the rule that is meaningful to you.

Protocol. The protocol used by the messages: TCP/UDP, TCP, UDP, or ICMP. Select "Any" if your rule does not control a specific type of message that uses a specific protocol.

Queue Name: Select a queue to associate this rule with.

Click **Next** to continue to the next page.



Add Traffic Shaping / QoS Rule

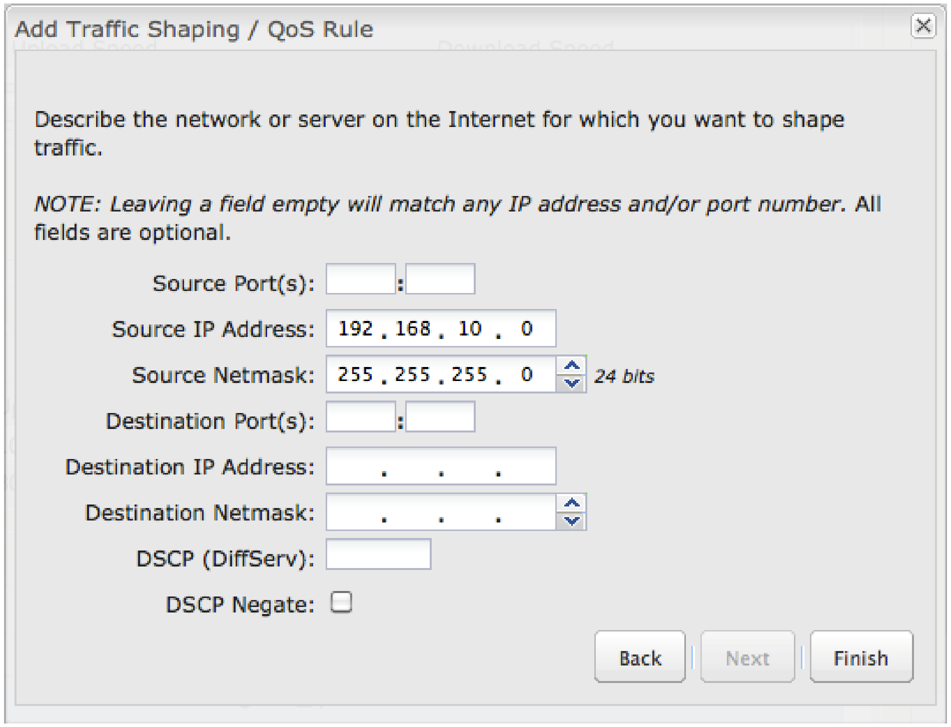
Rule Enabled: ☑

Rule Name: guest

Protocol: TCP/UDP

Queue Name: guest_q

Use ports and/or IP addresses to define the type(s) of traffic attached to this rule. Leaving any field blank will match all values; all fields are optional.



Add Traffic Shaping / QoS Rule

Describe the network or server on the Internet for which you want to shape traffic.

NOTE: Leaving a field empty will match any IP address and/or port number. All fields are optional.

Source Port(s): :

Source IP Address: 192 . 168 . 10 . 0

Source Netmask: 255 . 255 . 255 . 0 *24 bits*

Destination Port(s): :

Destination IP Address: . . .

Destination Netmask: . . .

DSCP (DiffServ):

DSCP Negate: □

Source Port(s) and/or **Destination Port(s):** Enter a port number between 1 and 65535. To enter a single port number, input the number into the left box. To enter a range of ports, fill in both boxes separated by the colon. For example "80:90" would represent all ports between 80 and 90 including 80 and 90 themselves.

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

DSCP (DiffServ): Differentiated Services Code Point (DSCP) 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.

This setting is optional. For more information see the Differentiated services Wikipedia page.

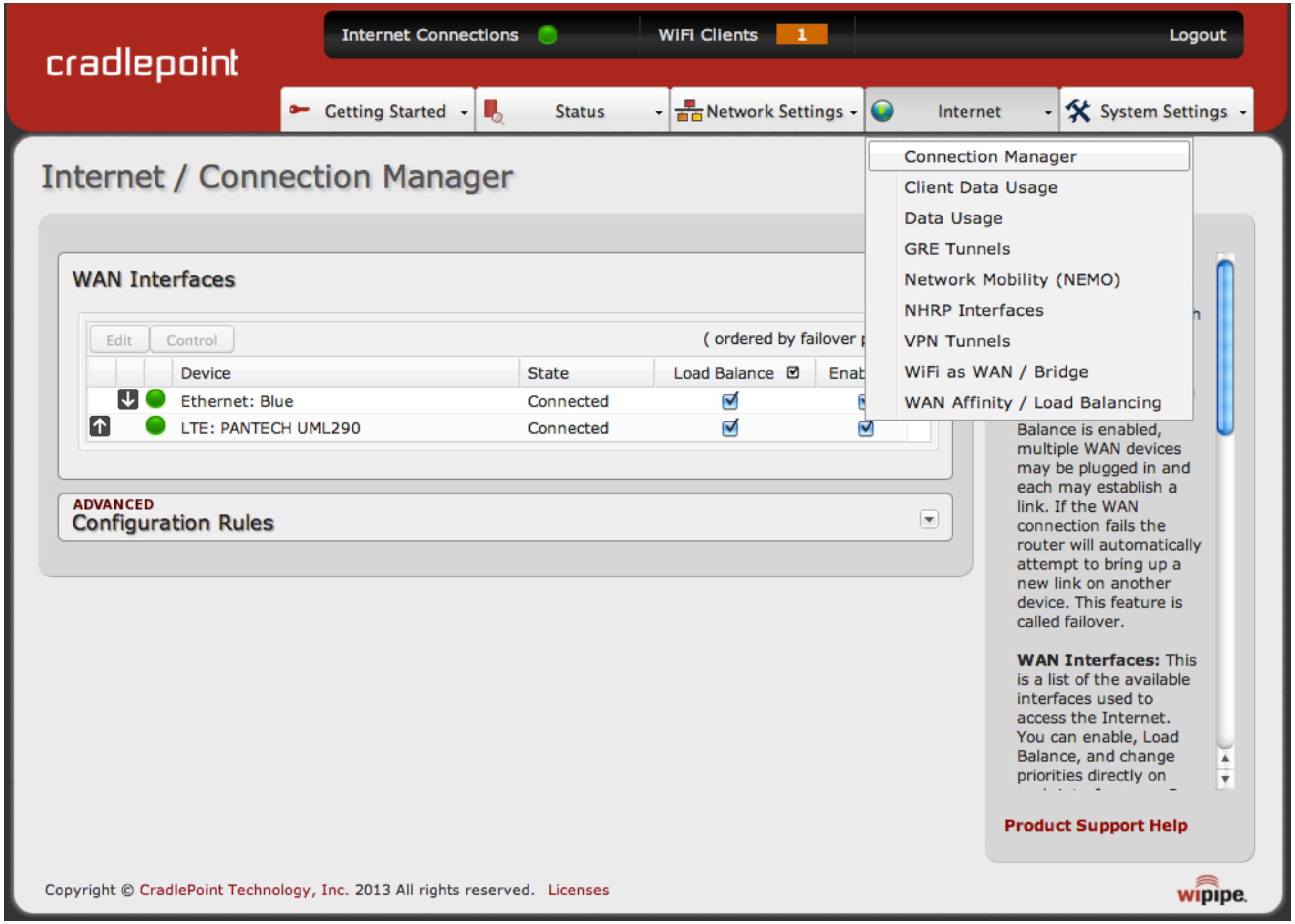
DSCP Negate: When checked this rule will match on any packet that does not match the DSCP field.

Click **Finish** to save this rule.

7 INTERNET

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

- Connection Manager
- CP Connect
- Client Data Usage
- Data Usage
- GRE Tunnels
- L2TP Tunnels
- Network Mobility (NEMO)
- NHRP Interfaces
- OpenVPN Tunnels
- VPN Tunnels
- WiFi as WAN / Bridge
- WAN Affinity / Load Balancing



Internet / Connection Manager

WAN Interfaces

(ordered by failover p

		Device	State	Load Balance ☑	Enab
↓	●	Ethernet: Blue	Connected	☑	☑
↑	●	LTE: PANTECH UML290	Connected	☑	☑

ADVANCED
Configuration Rules

Balance is enabled, multiple WAN devices may be plugged in and each may establish a link. If the WAN connection fails the router will automatically attempt to bring up a new link on another device. This feature is called failover.

WAN Interfaces: This is a list of the available interfaces used to access the Internet. You can enable, Load Balance, and change priorities directly on

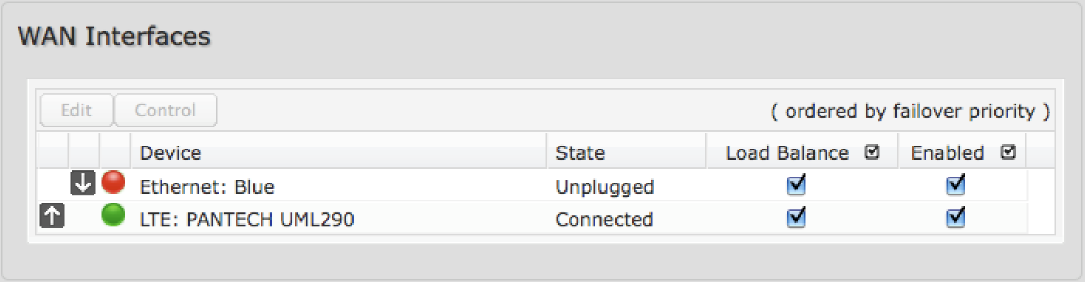
Copyright © CradlePoint Technology, Inc. 2013 All rights reserved.

7.1 Connection Manager

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

7.1.1 WAN Interfaces

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



WAN Interfaces

		Device	State	Load Balance ☑	Enabled ☑
↓	●	Ethernet: Blue	Unplugged	☑	☑
↑	●	LTE: PANTECH UML290	Connected	☑	☑

In the example shown, Ethernet is set as the primary Internet source, while a USB modem is attached for failover. The Ethernet is “Unplugged” while the modem is “Connected.”

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

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

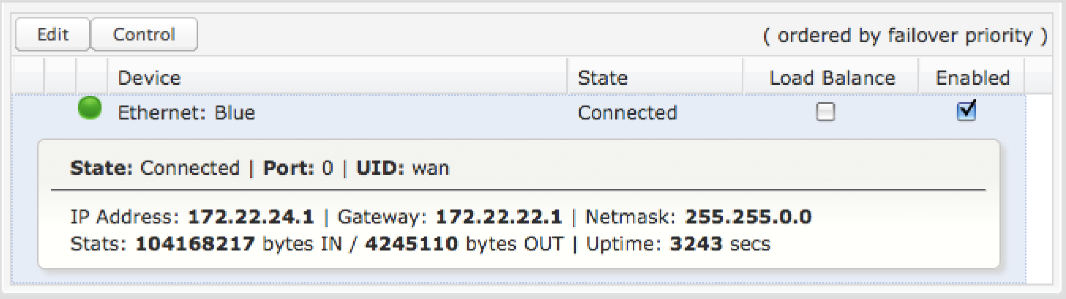
Click on the small box at the top of the list to select/deselect all devices for either **Load Balance** or **Enabled**.

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

7.1.2 Device Configuration

Clicking on a device reveals the following information:

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



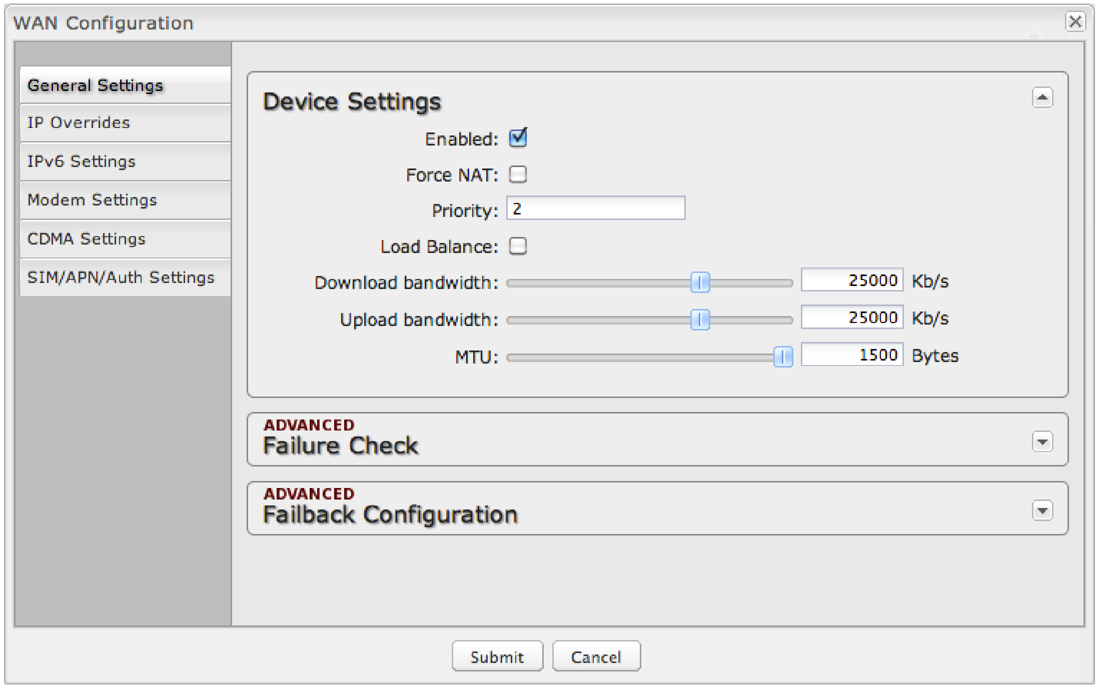
Device	State	Load Balance	Enabled
● Ethernet: Blue	Connected	☐	☑

State: Connected | **Port:** 0 | **UID:** wan

IP Address: **172.22.24.1** | Gateway: **172.22.22.1** | Netmask: **255.255.0.0**
Stats: **104168217** bytes IN / **4245110** bytes OUT | Uptime: **3243** secs

Click “Edit” to view configuration options for the selected device. For USB or ExpressCard modems, click “Control” to view options to activate or update the device.

7.1.3 General Settings



Device Settings

Enabled: ☑

Force NAT: □

Priority: 2

Load Balance: □

Download bandwidth: 25000 Kb/s

Upload bandwidth: 25000 Kb/s

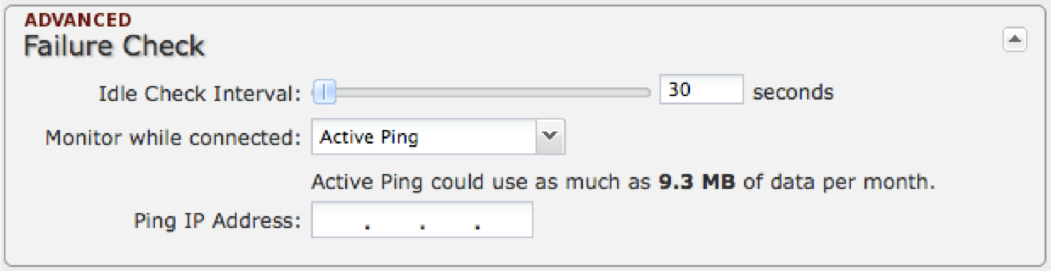
MTU: 1500 Bytes

ADVANCED Failure Check

ADVANCED Failback Configuration

- **Enabled:** Select/deselect to enable/disable.
- **Force NAT:** Normally NAT is part of the Routing Mode setting which is selected on the LAN side in **Network Settings → WiFi / Local Networks**. Select this option to force NAT whenever this WAN device is being used.
- **Priority:** This number controls failover and failback order. The lower the number, the higher the priority and the more use the device will get. This number will change when you move devices around with the priority arrows in the WAN Interfaces list.
- **Load Balance:** Select to allow this device to be available for the Load Balance pool.
- **Download bandwidth:** Defines the default download bandwidth for use in Load Balance or QoS (quality of service, or traffic shaping) algorithms. (Range: 128 Kb/s to 1 Gb/s.)
- **Upload bandwidth:** Defines the default upload bandwidth for use in Load Balance and QoS (quality of service, or traffic shaping) algorithms. (Range: 128 Kb/s to 1 Gb/s.)
- **MTU:** Maximum transmission unit. This is the size of the largest protocol data unit that the device can pass. (Range: 46 to 1500 Bytes.)
- **Hostname** (This only shows for certain devices.)

Failure Check (Advanced)


ADVANCED
Failure Check

Idle Check Interval: 30 seconds

Monitor while connected: Active Ping

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

Ping IP Address: . . .

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

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

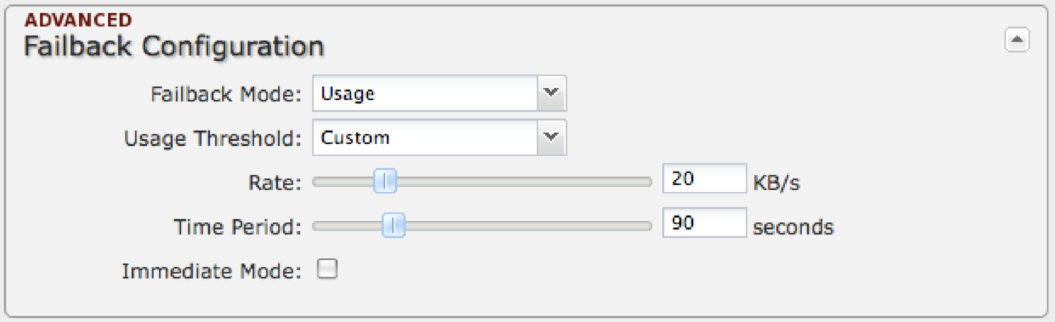
Monitor while connected: (Default: Off) Select from the following dropdown options:

- **Passive DNS (modem only):** The router will take no action until data is detected that is destined for the WAN. When this data is detected, the data will be sent and the router will check for received data for 2 seconds. If no data is received the router behaves as described below under **Active DNS**.
- **Active DNS (modem only):** A DNS request will be sent to the DNS servers. If no data is received, the DNS request will be retried 4 times at 5-second intervals. (The first 2 requests will be directed at the Primary DNS server and the second 2 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 4 times at 5-second intervals. If still no data is received, the device will be disconnected and failover will occur. When “Active Ping” is selected, the next line gives an estimate of data usage in this form: “Active Ping could use as much as **9.3 MB** of data per month.” This amount depends on the Idle Check Interval.
- **Off:** Once the link is established the router takes no action to verify that it is still up.

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

For example, you might ping Google Public DNS at 8.8.8.8 or Level 3 Communications at 4.2.2.2.

Failback Configuration (Advanced)



ADVANCED
Failback Configuration

Failback Mode: Usage
Usage Threshold: Custom
Rate: 20 KB/s
Time Period: 90 seconds
Immediate Mode: □

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

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

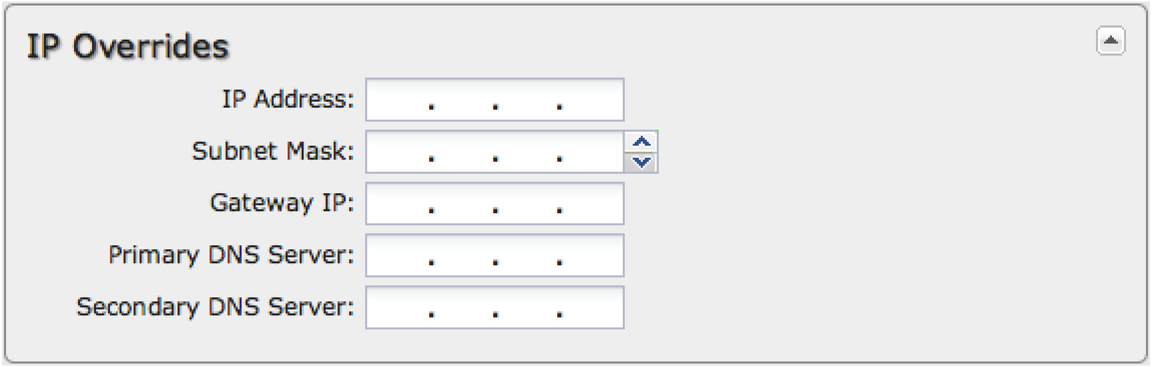
Disabled: Deactivate failback mode.

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.

7.1.4 IP Overrides

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

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


IP Overrides

IP Address: . . .

Subnet Mask: . . .

Gateway IP: . . .

Primary DNS Server: . . .

Secondary DNS Server: . . .

7.1.5 IPv6 Settings

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

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

- RADIUS/TACACS+ accounting for wireless clients and admin/CLI login
- IP Passthrough (not needed with IPv6)
- NAT (not needed with IPv6)
- Bounce pages
- UPnP
- Network Mobility
- DHCP Relay
- VRRP, GRE, GRE over IPSec, OSPF, NHRP
- Syslog
- SNMP over the WAN (LAN works)

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

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

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

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

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

DNS Servers

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

Delegated Networks

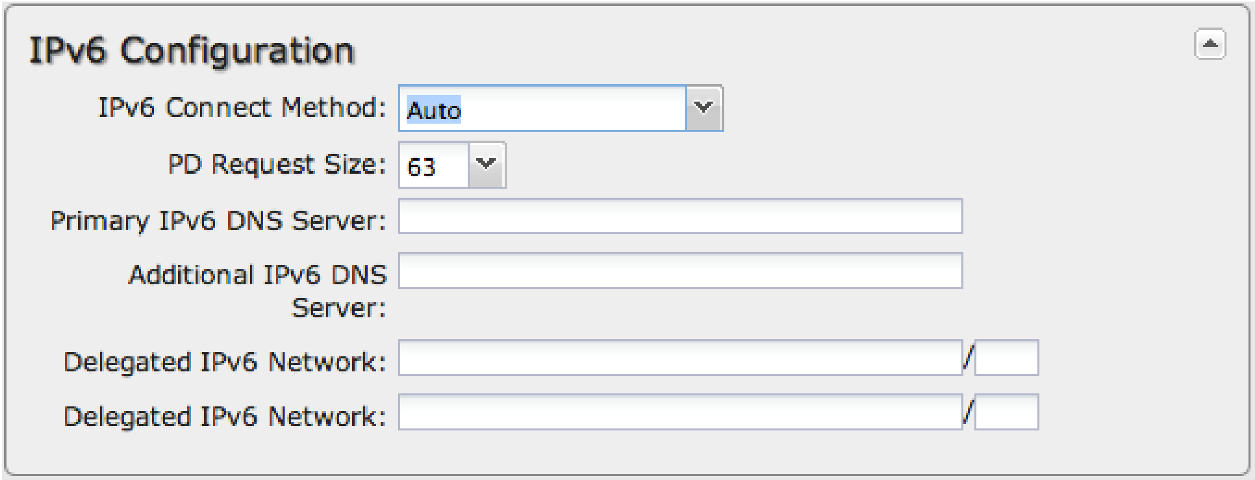
A delegated network is an IPv6 network that is inherently provided by or closely tied to a WAN IP configuration. The IPv6 model is for each device to have end-to-end IP connectivity without relying on any translation mechanism. In order to achieve this, each client device on the LAN network needs to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

Auto

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

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

Example Configuration:



IPv6 Configuration

IPv6 Connect Method: Auto

PD Request Size: 63

Primary IPv6 DNS Server:

Additional IPv6 DNS Server:

Delegated IPv6 Network: /

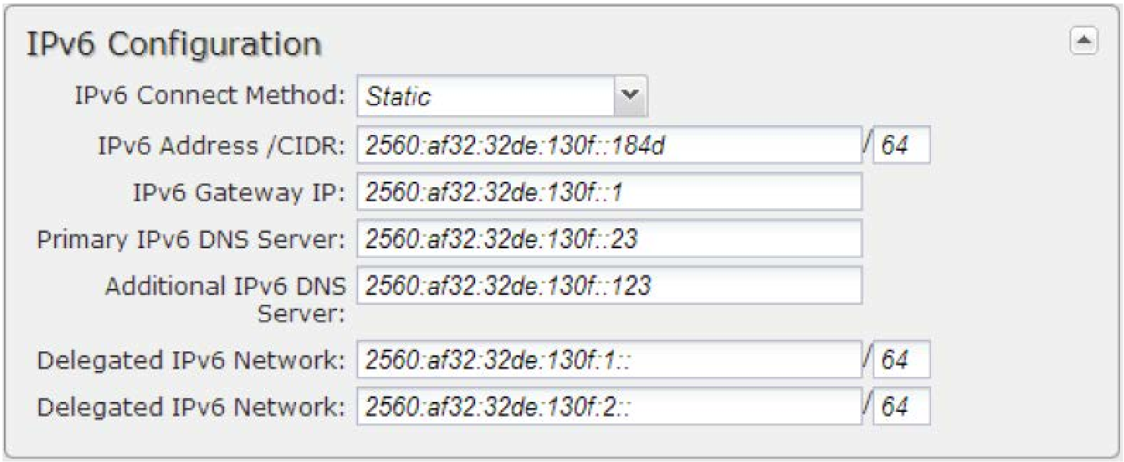
Delegated IPv6 Network: /

Static

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

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

Example Configuration:



IPv6 Configuration

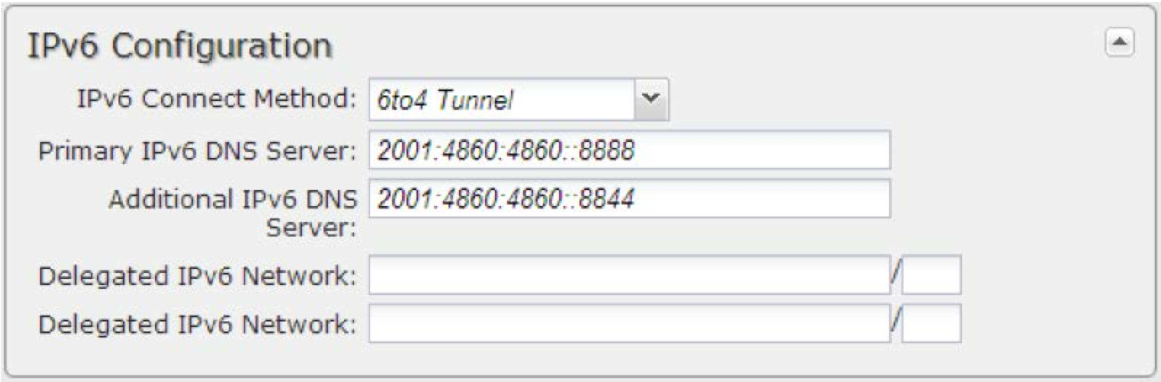
IPv6 Connect Method:	Static	
IPv6 Address /CIDR:	2560:af32:32de:130f::184d	64
IPv6 Gateway IP:	2560:af32:32de:130f::1	
Primary IPv6 DNS Server:	2560:af32:32de:130f::23	
Additional IPv6 DNS Server:	2560:af32:32de:130f::123	
Delegated IPv6 Network:	2560:af32:32de:130f:1::	64
Delegated IPv6 Network:	2560:af32:32de:130f:2::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

6to4 Tunnel

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

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

Example Configuration:



IPv6 Configuration

IPv6 Connect Method: 6to4 Tunnel

Primary IPv6 DNS Server: 2001:4860:4860::8888

Additional IPv6 DNS Server: 2001:4860:4860::8844

Delegated IPv6 Network: /

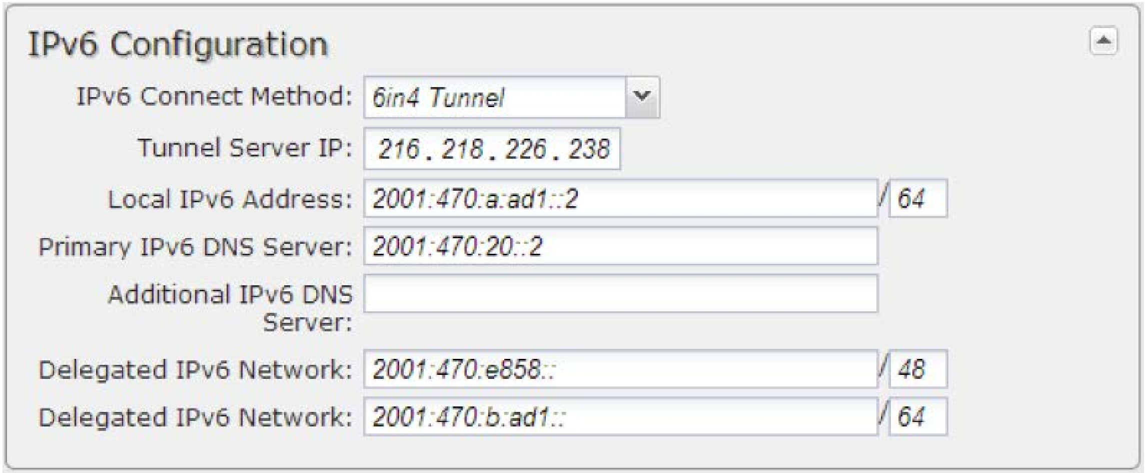
Delegated IPv6 Network: /

6in4 Tunnel

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

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

Example Configuration:



IPv6 Configuration

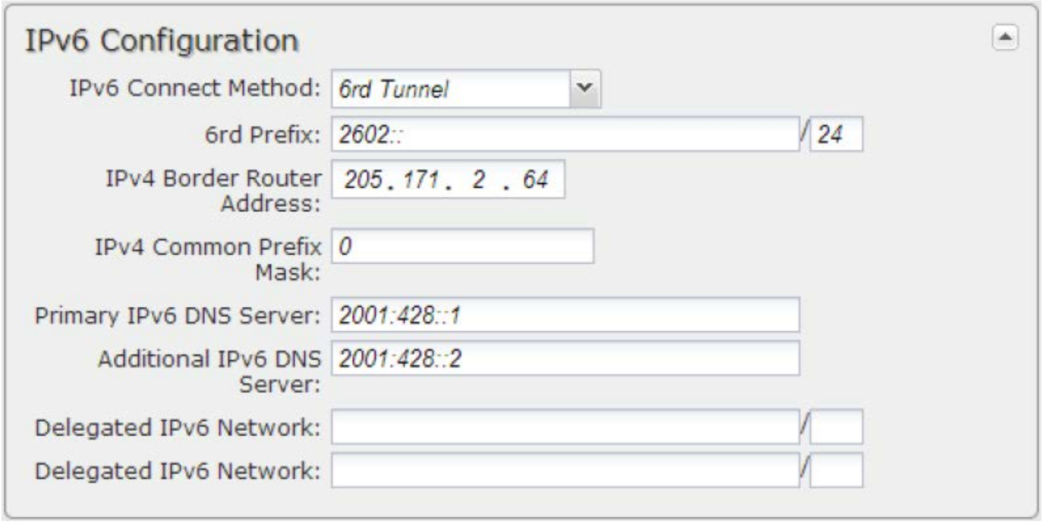
IPv6 Connect Method:	6in4 Tunnel
Tunnel Server IP:	216 . 218 . 226 . 238
Local IPv6 Address:	2001:470:a:ad1::2 / 64
Primary IPv6 DNS Server:	2001:470:20::2
Additional IPv6 DNS Server:	
Delegated IPv6 Network:	2001:470:e858:: / 48
Delegated IPv6 Network:	2001:470:b:ad1:: / 64

6rd Tunnel

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

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

Example Configuration:



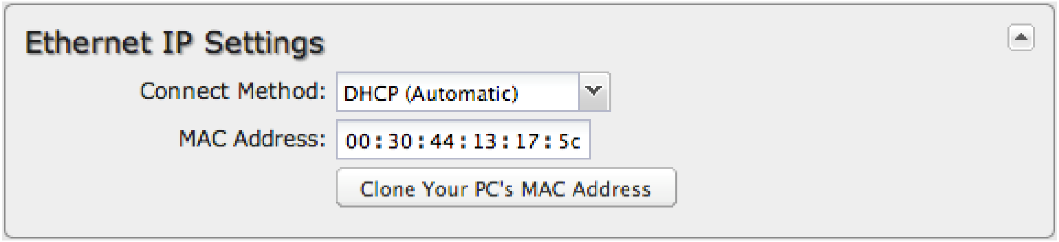
IPv6 Configuration

IPv6 Connect Method:	6rd Tunnel
6rd Prefix:	2602:: / 24
IPv4 Border Router Address:	205 . 171 . 2 . 64
IPv4 Common Prefix Mask:	0
Primary IPv6 DNS Server:	2001:428::1
Additional IPv6 DNS Server:	2001:428::2
Delegated IPv6 Network:	/
Delegated IPv6 Network:	/

7.1.6 Ethernet Settings

While default settings for each WAN Ethernet port will be sufficient in most circumstances, you have the ability to control:

- **Connect Method:** DHCP (Automatic), Static (Manual), or PPPoE (Point-to-Point Protocol over Ethernet).
- **MAC Address:** You have the ability to change the MAC address, but typically this is unnecessary. You can match this address with your device's address by clicking: "**Clone Your PC's MAC Address**".



Ethernet IP Settings

Connect Method: DHCP (Automatic)

MAC Address: 00:30:44:13:17:5c

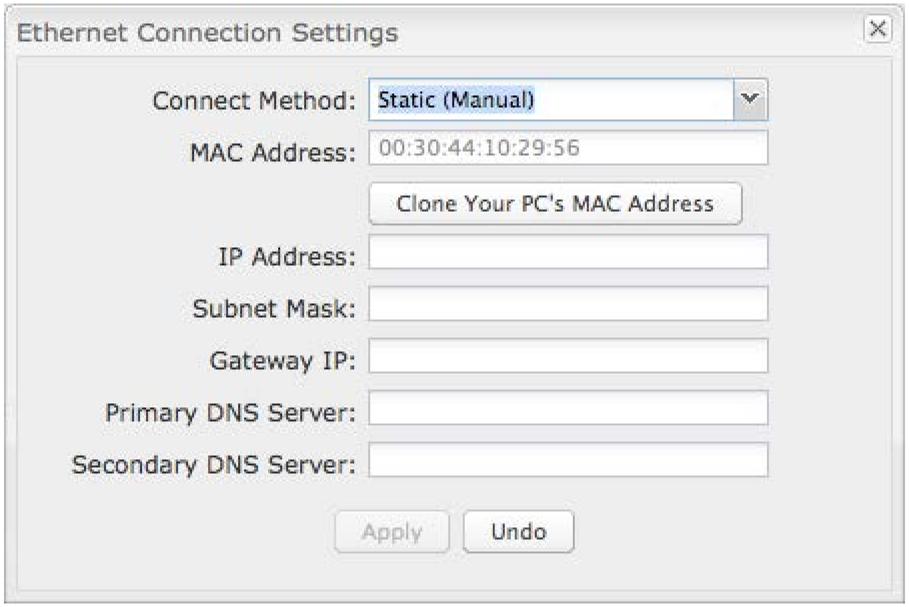
Connect Method
Select the connection type that you need for this WAN connection. You may need to check with your ISP or system administrator for this information.

- **DHCP** (Dynamic Host Configuration Protocol) is the most common configuration. Your router's Ethernet ports are automatically configured for DHCP connection. DHCP automatically assigns dynamic IP addresses to devices in your networks. This is preferable in most circumstances.
- **Static** allows you to input a specific IP address for your WAN connection; this should be provided by the ISP if supported.
- **PPPoE** should be configured with the username, password and other settings provided by your ISP.

If you want to use a Static (Manual) or PPPoE connection, you will need to fill out additional information.

Static (Manual):

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



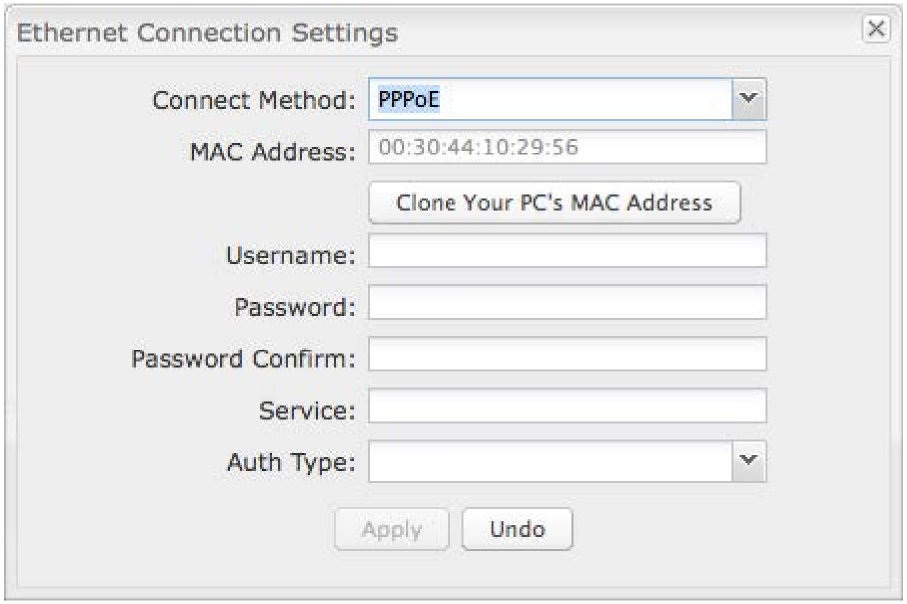
Ethernet Connection Settings

Connect Method: Static (Manual)

MAC Address: 00:30:44:10:29:56

PPPoE:

- Username
- Password
- Password Confirm
- Service
- Auth Type: None, PAP, CHAP



Ethernet Connection Settings

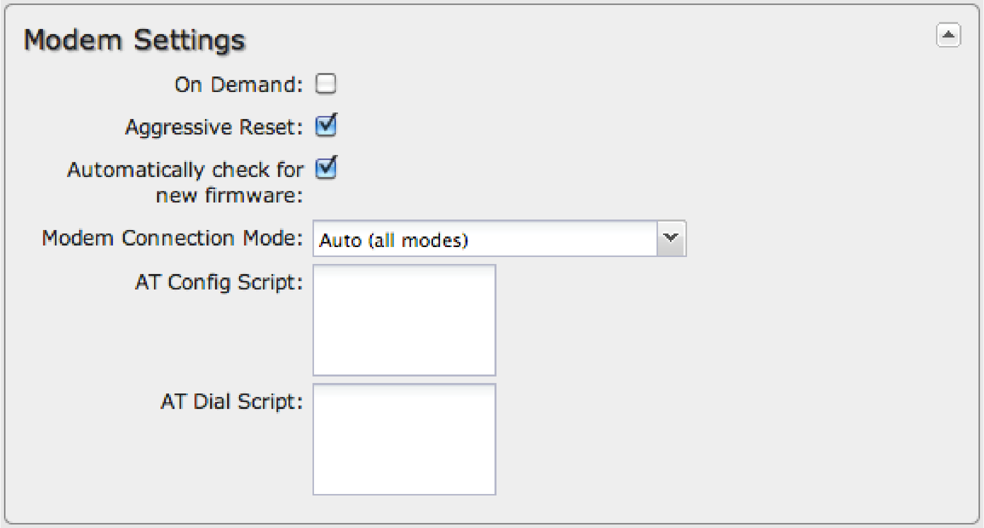
Connect Method: PPPoE

MAC Address: 00:30:44:10:29:56

7.1.7 Modem Settings

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

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



Modem Settings

On Demand: □

Aggressive Reset: ☑

Automatically check for new firmware: ☑

Modem Connection Mode: Auto (all modes)

AT Config Script:

AT Dial Script:

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

Network-Initiated Alerts: This field controls whether the Sprint network can disconnect the modem to apply updates, such as for PRL, modem firmware, or configuration events. These activities do not change any router settings, but the modem connection may be unavailable for periods of time while these updates occur. The modem may also require a reset after a modem firmware update is complete.

- **Disabled:** The request to update will be refused.
- **When Disconnected:** The request to update will only be performed when the modem is either in a disconnected state or dormant state. If the modem is not in one of these states when the request is received, then the router will remember the request and perform the update when the modem becomes disconnected/dormant.
- **On Schedule:** The request to update will only be performed at the specified scheduled time, no matter what the state of the modem is.

Network-Initiated Schedule: When you select “**On Schedule**” for **Network-Initiated Alerts**, you also select a time from this dropdown list. Modem updates will take place at this scheduled time.

Automatically check for new firmware: (Default: selected) The modem will automatically check for firmware updates by default.

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

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

See the following tables for a breakdown of the technologies used with various Cradlepoint ARC models when any **Modem Connection Mode** is selected.

CDMA Technology

	Auto	**Auto 3G**	**Force 4G**	**Force 3G** (module auto selects)			**Force 2G**
		(<= 3G)	LTE	1xEVDOAe (EHRPD)	1xEVDO-A (HRPD) (3G)	1xEVDO-0 (HRPD) (3G)	1xRTT (2.5G)
ARC MBR1400LE (Sierra Wireless MC7750)	✔	✔	✔	✔	✔	✔	✔

GSM Technology

	Auto	**Auto 3G**	**Force 4G**	**Force 3G** (module auto selects)		**Force 2G** (module auto selects)	
		(<= 3G)	LTE	HSPA+ (4G/3.5G)	HSPA (3G)	EDGE (2.75G)	GPRS (2.5G)
ARC MBR1400LP (Sierra Wireless MC7700)	✔	✔	✔	✔	✔	✔	✔
ARC MBR1400LP2 (Sierra Wireless MC7710)	✔	✔	✔	✔	✔	✔	✔

AT Config Script: Enter the AT commands to be used for carrier specific modem configuration settings. Each command must be entered on a separate line. The command and associated response will be logged, so you should check the system log to make sure there were no errors.

NOTE: AT Config Script should not be used unless told to do so by your modem's cellular provider or by a support technician.

AT Dial Script: This is included for legacy devices *only*. Most users will not use this option. Go to **SIM/APN/Auth Settings** instead if you need to select a specific Access Point Name.

If you do need this option for older devices, enter the AT commands to be used in establishing a network connection. Each command must be entered on a separate line. All command responses must include “OK” except the final command response, which must include “CONNECT”.

Example:

```
AT
ATDT*99***2#
```

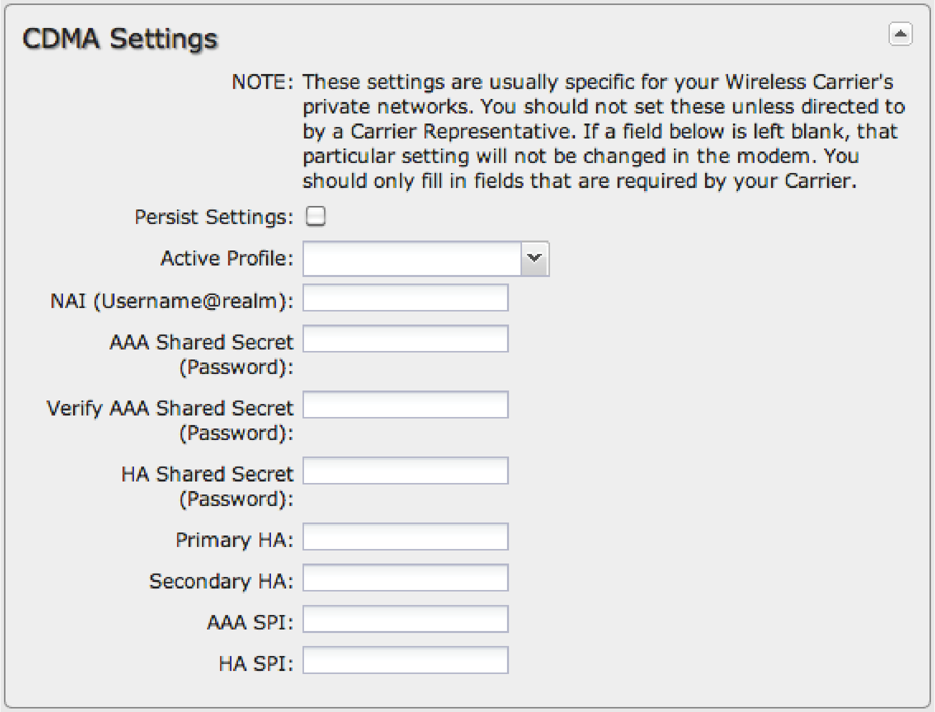
7.1.8 CDMA Settings

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

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

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

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



CDMA Settings

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

Persist Settings: □

Active Profile:

NAI (Username@realm):

AAA Shared Secret (Password):

Verify AAA Shared Secret (Password):

HA Shared Secret (Password):

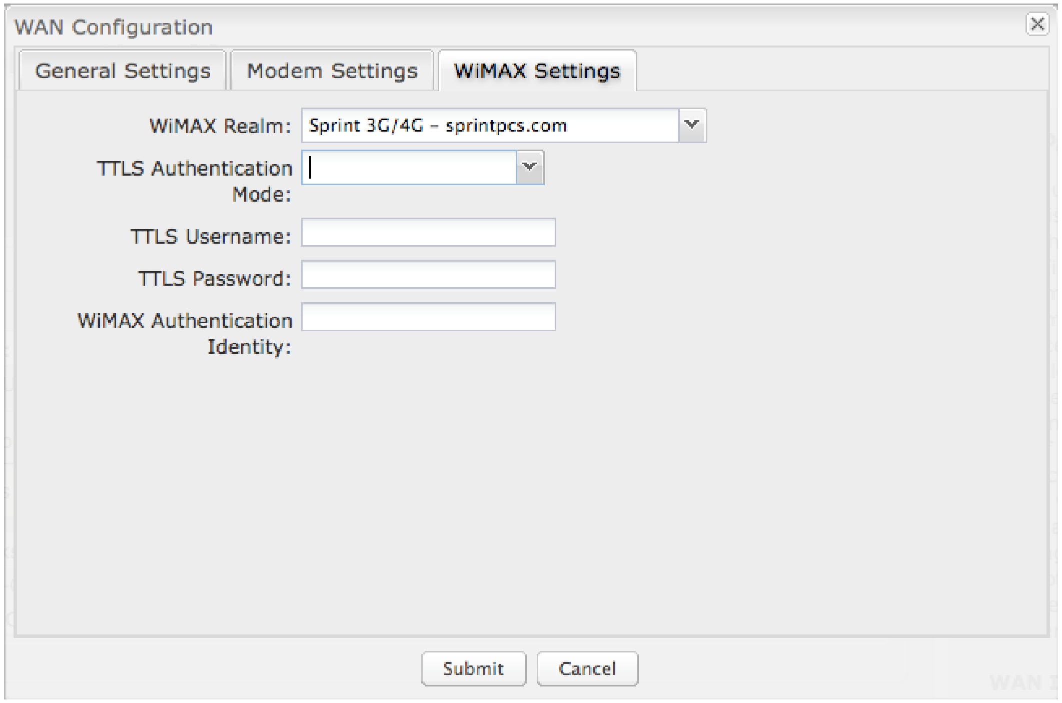
Primary HA:

Secondary HA:

AAA SPI:

HA SPI:

7.1.9 WiMAX Settings



WAN Configuration

WiMAX Realm: Sprint 3G/4G – sprintpcs.com

TTLS Authentication Mode:

TTLS Username:

TTLS Password:

WiMAX Authentication Identity:

WiMAX Realm: Select from the following dropdown options:

- Clear – clearwire-wmx.net
- Rover – rover-wmx.net
- Sprint 3G/4G – sprintpcs.com
- Xohm –xohm.com
- BridgeMAXX – bridgeMAXX.com
- Time Warner Cable – mobile.rr.com
- Comcast – mob.comcast.net

TTLS Authentication Mode: TTLS inner authentication protocol. Select from the following dropdown options:

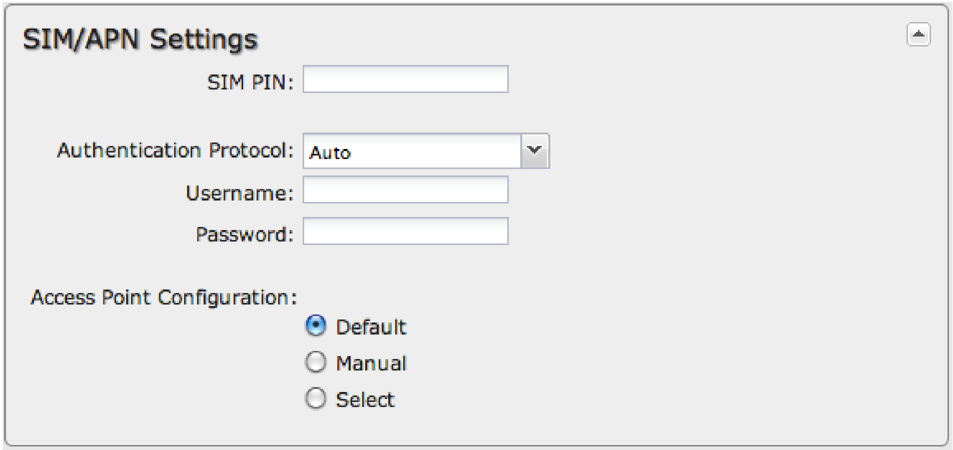
- **MSCHAPv2/MD5** (Microsoft Challenge Handshake Authentication Protocol version2/Message-Digest Algorithm 5)
- **PAP** (Password Authentication Protocol)
- **CHAP** (Challenge Handshake Authentication Protocol)

TTLS Username: Username for TTLS authentication.

TTLS Password: Password for TTLS authentication.

WiMAX Authentication Identity: User ID on the network. Leave this blank unless your provider tells you otherwise.

7.1.10 SIM/APN/Auth Settings



SIM/APN Settings

SIM PIN:

Authentication Protocol: Auto

Username:

Password:

Access Point Configuration:

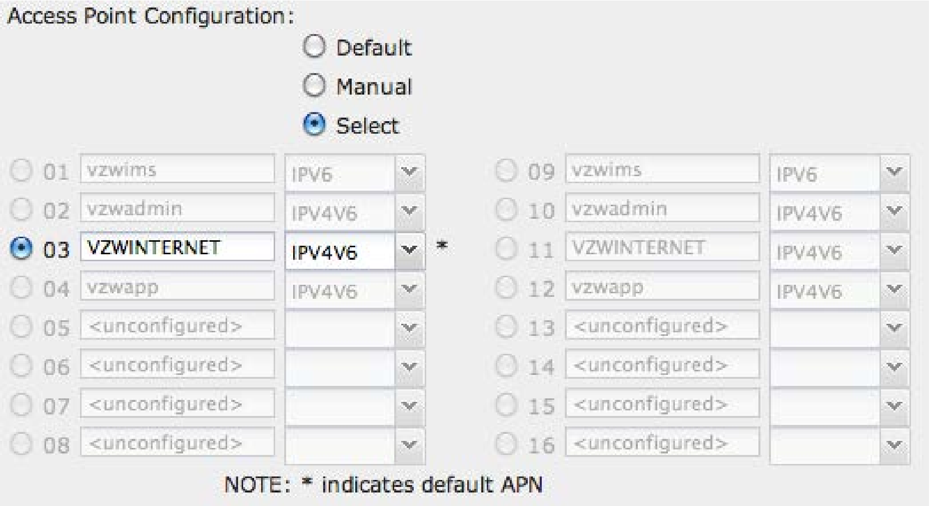
● Default
○ Manual
○ Select

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

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

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

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



Access Point Configuration:

○ Default
○ Manual
● Select

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

NOTE: * indicates default APN

7.1.11 Update/Activate a Modem

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

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

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

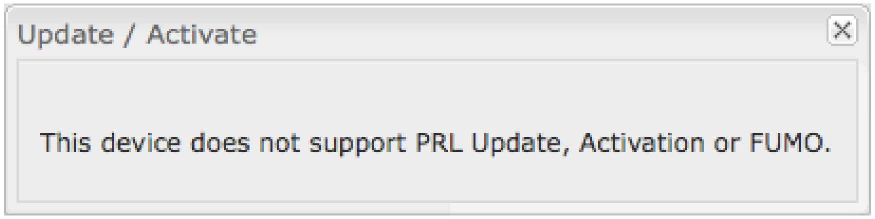
The modem supports Update/Activate methods: A message will display showing options for each supported method:

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

Click the appropriate icon to start the process.

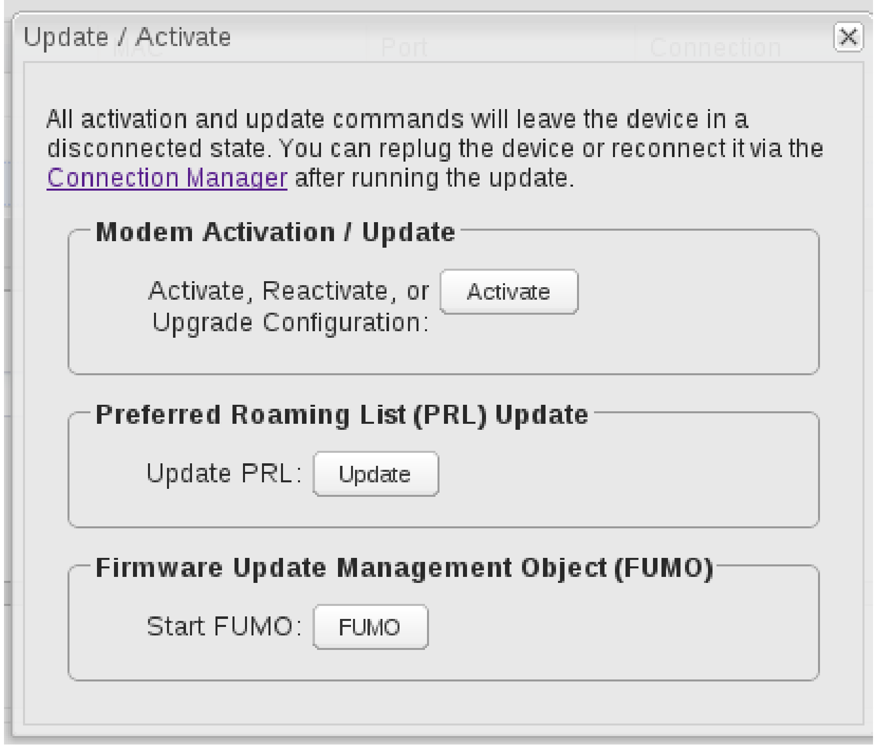
If the modem is connected when you start an operation the router will automatically disconnect it. The router may start another modem as a failover measure. When the operation is done the modem will go back to an idle state, at which point the router may restart it depending on failover and failback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

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



Update / Activate

This device does not support PRL Update, Activation or FUMO.



Update / Activate

All activation and update commands will leave the device in a disconnected state. You can replug the device or reconnect it via the Connection Manager after running the update.

Modem Activation / Update

Activate, Reactivate, or Upgrade Configuration:

Preferred Roaming List (PRL) Update

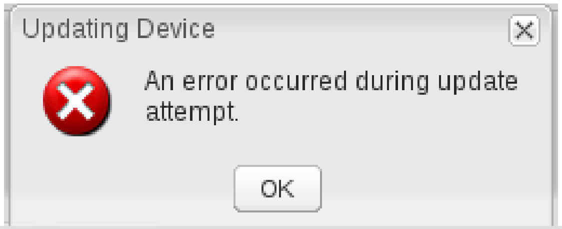
Update PRL:

Firmware Update Management Object (FUMO)

Start FUMO:

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

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



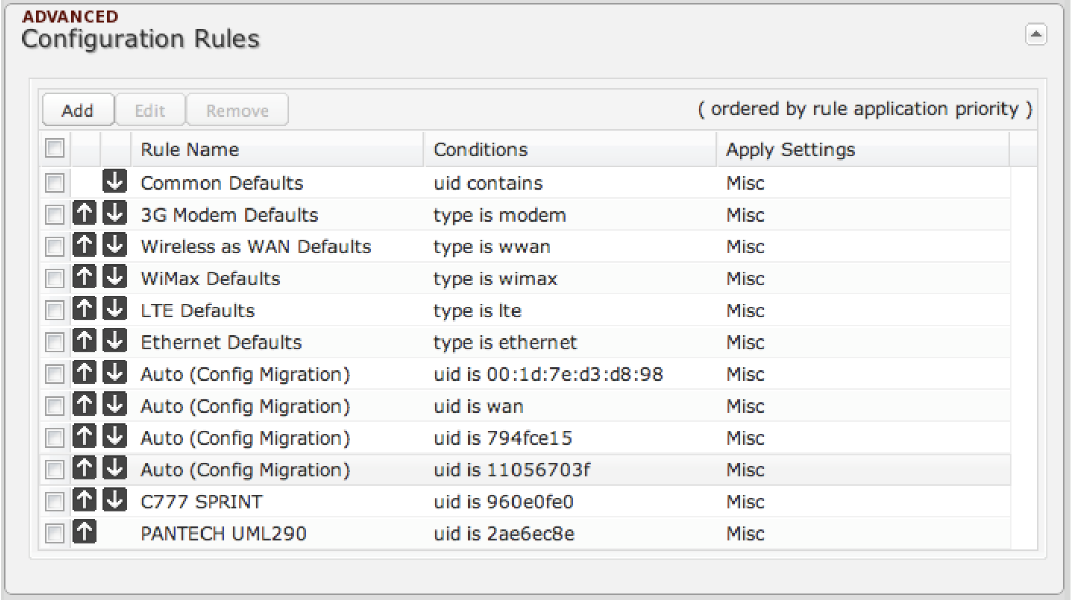
Updating Device

An error occurred during update attempt.

7.1.12 Configuration Rules (Advanced)

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

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



ADVANCED

Configuration Rules

(ordered by rule application priority)

□		Rule Name	Conditions	Apply Settings
□	↓	Common Defaults	uid contains	Misc
□	↑ ↓	3G Modem Defaults	type is modem	Misc
□	↑ ↓	Wireless as WAN Defaults	type is wwan	Misc
□	↑ ↓	WiMax Defaults	type is wimax	Misc
□	↑ ↓	LTE Defaults	type is lte	Misc
□	↑ ↓	Ethernet Defaults	type is ethernet	Misc
□	↑ ↓	Auto (Config Migration)	uid is 00:1d:7e:d3:d8:98	Misc
□	↑ ↓	Auto (Config Migration)	uid is wan	Misc
□	↑ ↓	Auto (Config Migration)	uid is 794fce15	Misc
□	↑ ↓	Auto (Config Migration)	uid is 11056703f	Misc
□	↑ ↓	C777 SPRINT	uid is 960e0fe0	Misc
□	↑	PANTECH UML290	uid is 2ae6ec8e	Misc

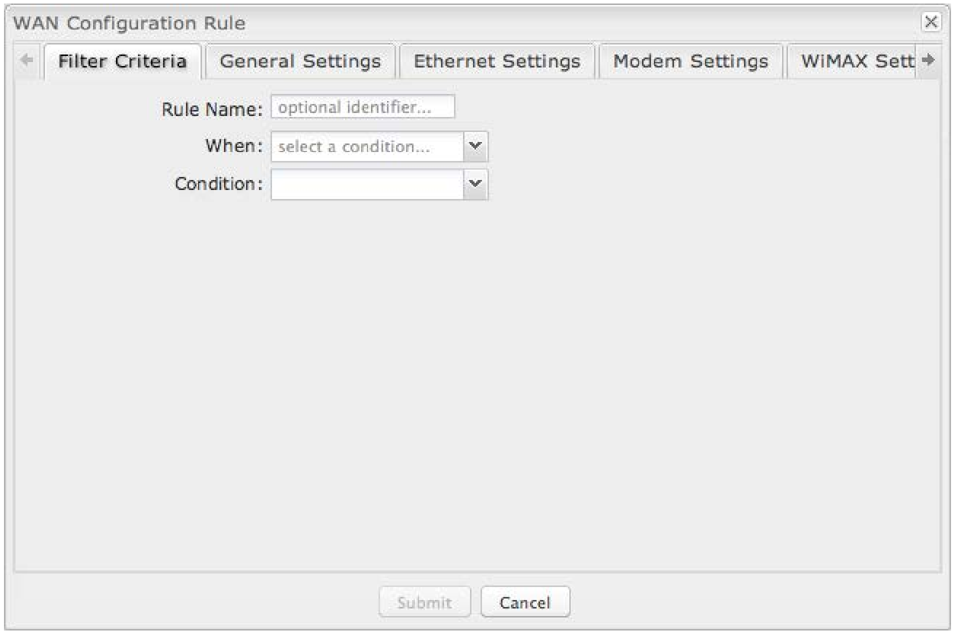
Select any of these rules and click "Edit" to change the settings for a rule. To create a new rule, click "Add."

WAN Configuration Rule

This section allows you to create simple or complex rules that affect how individual Internet sources or classes of sources (perhaps all WiMAX modems or all modems from Sierra Wireless) behave in the router.

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

- **Filter Criteria**
- **General Settings**
- **Ethernet Settings**
- **Modem Settings**
- **WiMAX Settings**
- **CDMA Settings**
- **SIM/APN Settings**



Rule Name: optional identifier...

When: select a condition...

Condition:

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

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

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

- **Port** (USB Port 1, 2, 3; ExpressPort 1, 2): Select by the port that you are plugging the modem into.
- **Manufacturer:** Select by the manufacturer, such as Sierra Wireless.
- **Model**: Set your rule according to the specific model of modem.
- **Type** (Ethernet, LTE, Modem, WiMAX, Wireless as WAN, HSPA): Select by type of Internet source.
- **Serial Number**: Select 3G or LTE modem by Serial Number.
- **MAC Address**: Select WiMAX modem by MAC Address.
- **Unique ID**: Select by ID. This is generated by the router and displayed when the device is connected to the router.

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

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

The condition will be of the following form:
“___(When)___ is/is not ___(value)___”

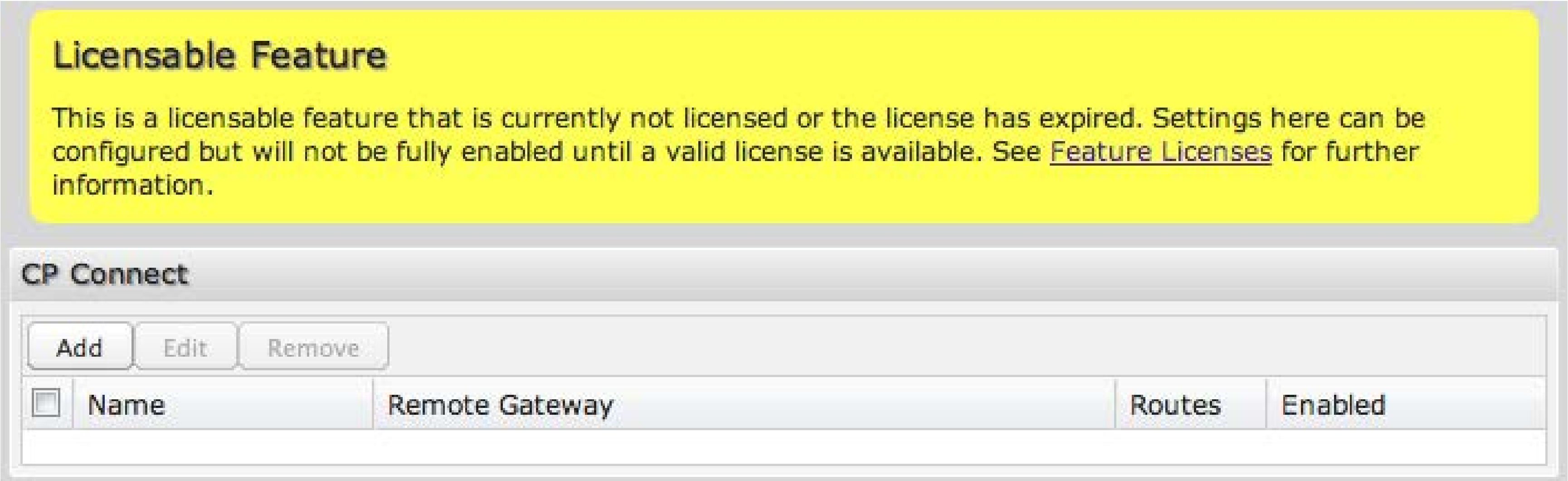
For example:
“Type is not WiMAX”
“Port is USB Port 1”

Once you have established the condition for your configuration rule, choose from the other tabs to set the desired configuration. All of the tabs have the same configuration options shown above in the WAN Configuration section (i.e., the options for Configuration Rules are the same as they are for individual devices).

7.2 CP Connect

CP Connect is a licensable feature used to create a connection to a private network. CP Connect is currently in beta.

CP Connect tunnels can be used to create a connection to a private network.



Licensable Feature

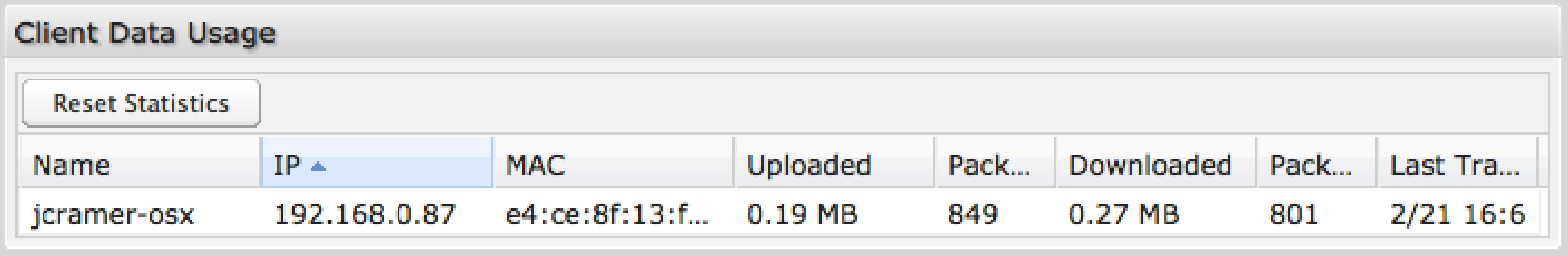
This is a licensable feature that is currently not licensed or the license has expired. Settings here can be configured but will not be fully enabled until a valid license is available. See Feature Licenses for further information.

CP Connect

□	Name	Remote Gateway	Routes	Enabled

7.3 Client Data Usage

Client Data Usage displays upload and download traffic for each LAN client. Click **Enable Client Data Usage Monitoring Service** to begin tracking this information. This data is not retained between router reboots.



Name	IP ▲	MAC	Uploaded	Pack...	Downloaded	Pack...	Last Tra...
jcramer-osx	192.168.0.87	e4:ce:8f:13:f...	0.19 MB	849	0.27 MB	801	2/21 16:6

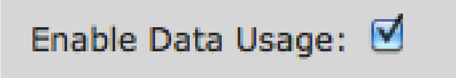
For each client this shows: Name, IP address, MAC address, amount of data (MB) and number of packets uploaded, amount of data and number of packets downloaded, and when traffic was last sent or received for that client ("**Last Traffic**").

The names that are shown are received during a DHCP exchange. If a client disconnects and reconnects with a new IP address there will be an additional entry in this list.

Pressing **Reset Statistics** will restart all counters at 0.

7.4 Data Usage

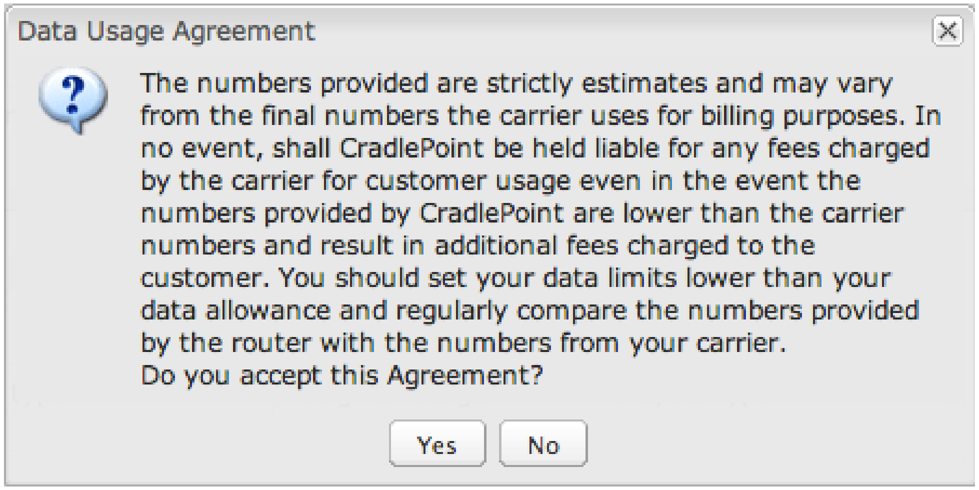
Data Usage Management & Alerts allows you to create and manage rules that help control the data usage of a modem. If you have a limited data plan or a price increase on your plan after a certain amount of usage, a **Data Usage Rule** can help you track these amounts. You can set a rule to shut down use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


Enable Data Usage: ☑

Enable Data Usage: (Default: Disabled.)

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

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

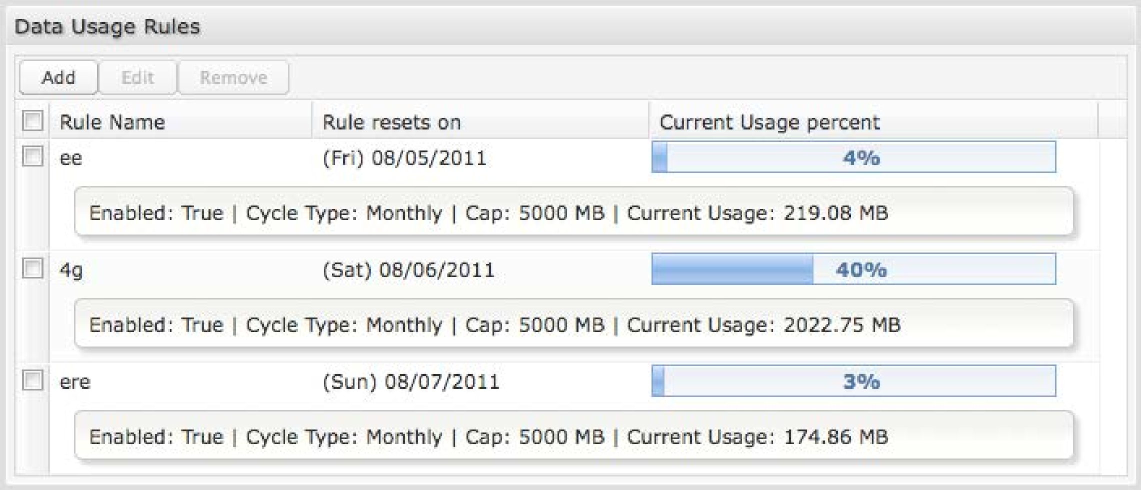

Data Usage Agreement

The numbers provided are strictly estimates and may vary from the final numbers the carrier uses for billing purposes. In no event, shall CradlePoint be held liable for any fees charged by the carrier for customer usage even in the event the numbers provided by CradlePoint are lower than the carrier numbers and result in additional fees charged to the customer. You should set your data limits lower than your data allowance and regularly compare the numbers provided by the router with the numbers from your carrier.
Do you accept this Agreement?

7.4.1 Data Usage Rules

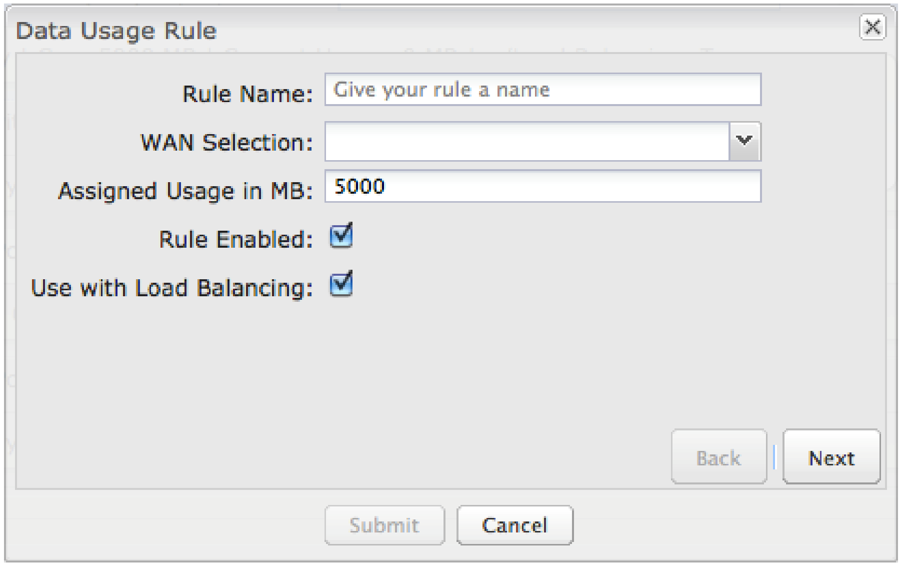
The Date Usage Rule display shows basic information for each rule you have created (including rules created with a template). The following information is displayed:

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



□	Rule Name	Rule resets on	Current Usage percent
□	ee	(Fri) 08/05/2011	4%
	Enabled: True | Cycle Type: Monthly | Cap: 5000 MB | Current Usage: 219.08 MB		
□	4g	(Sat) 08/06/2011	40%
	Enabled: True | Cycle Type: Monthly | Cap: 5000 MB | Current Usage: 2022.75 MB		
□	ere	(Sun) 08/07/2011	3%
	Enabled: True | Cycle Type: Monthly | Cap: 5000 MB | Current Usage: 174.86 MB		

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



Rule Name: Give your rule a name

WAN Selection:

Assigned Usage in MB: 5000

Rule Enabled: ☑

Use with Load Balancing: ☑

<u>Data Usage Rule – page 1</u>

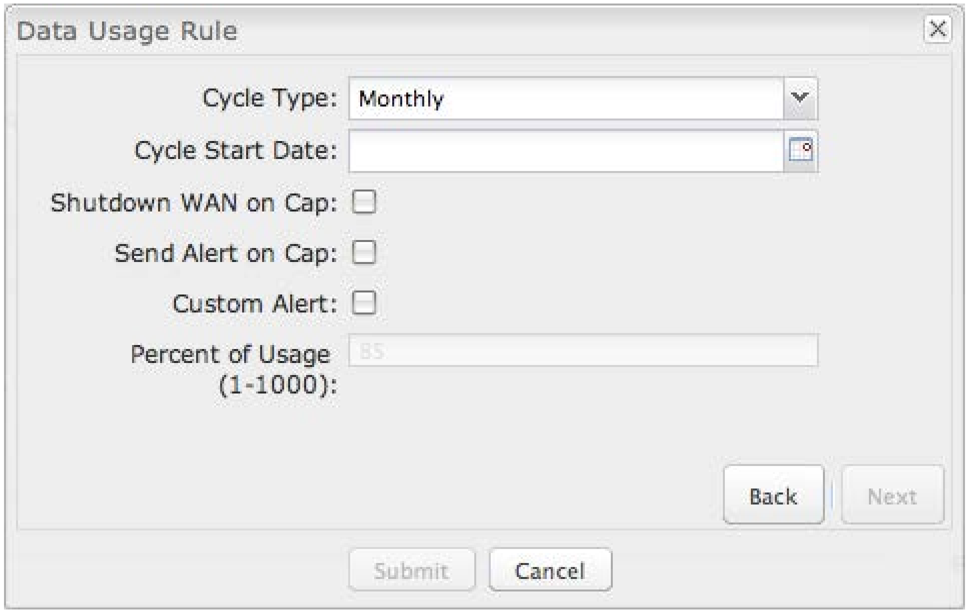
Rule Name: Give your rule a name for later recognition.

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

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

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

Use with Load Balancing: When checked, the Load Balancing feature is *allowed* to use the thresholds and metrics of this rule when making balance decisions. This causes Load Balancing to spread the data usage between interfaces according to the assigned usage rather than bandwidth. This is a best effort to keep all interfaces with these rules at a similar percentage utilization of data (e.g. 10%, 50%, 90%) as the cycle progresses, rather than quickly using 100% of a fast 1GB capped interface while using only a fraction of a slow 10GB capped interface, thus leaving the rest of the cycle with only the slow interface. The **Data Usage algorithm** on the Load Balancing page must be selected or this checkbox has no effect.

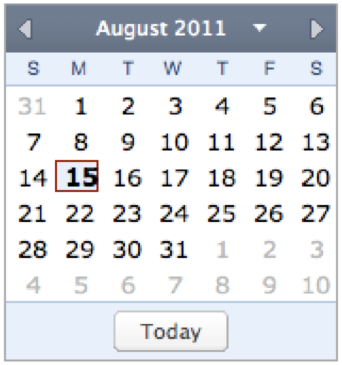


Cycle Type: Monthly
Cycle Start Date:
Shutdown WAN on Cap: □
Send Alert on Cap: □
Custom Alert: □
Percent of Usage (1-1000): 85

Data Usage Rule – page 2

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

- Daily
- Weekly
- Monthly



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

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

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

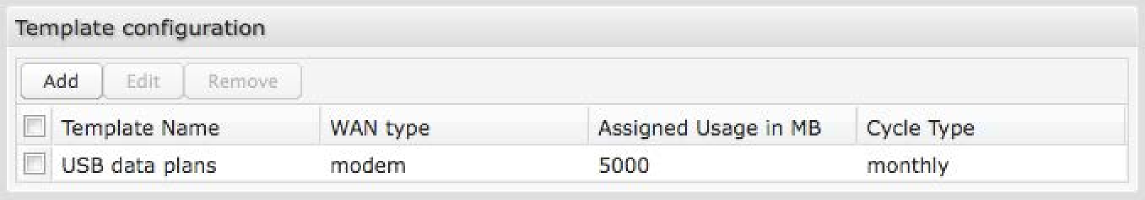
Send Alert on Cap: An email alert will be generated and sent when the assigned usage is reached.
WARNING: The SMTP mail server must be configured in System Settings → Device Alerts.

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

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

7.4.2 Template Configuration

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



Template configuration

	Template Name	WAN type	Assigned Usage in MB	Cycle Type
□	USB data plans	modem	5000	monthly

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

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

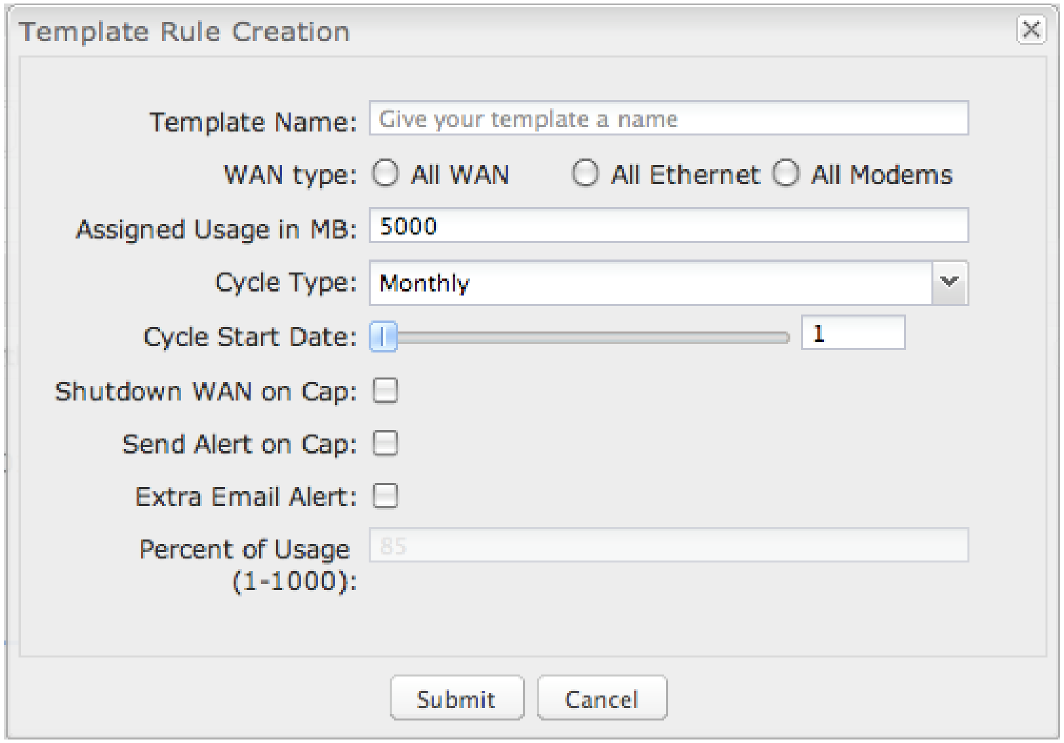
Create a **Template Name** that you can recognize.

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

- All WAN
- All Ethernet
- All Modems

Select one of these types.

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



Template Rule Creation

Template Name: Give your template a name

WAN type: ○ All WAN ○ All Ethernet ○ All Modems

Assigned Usage in MB: 5000

Cycle Type: Monthly

Cycle Start Date: 1

Shutdown WAN on Cap: □

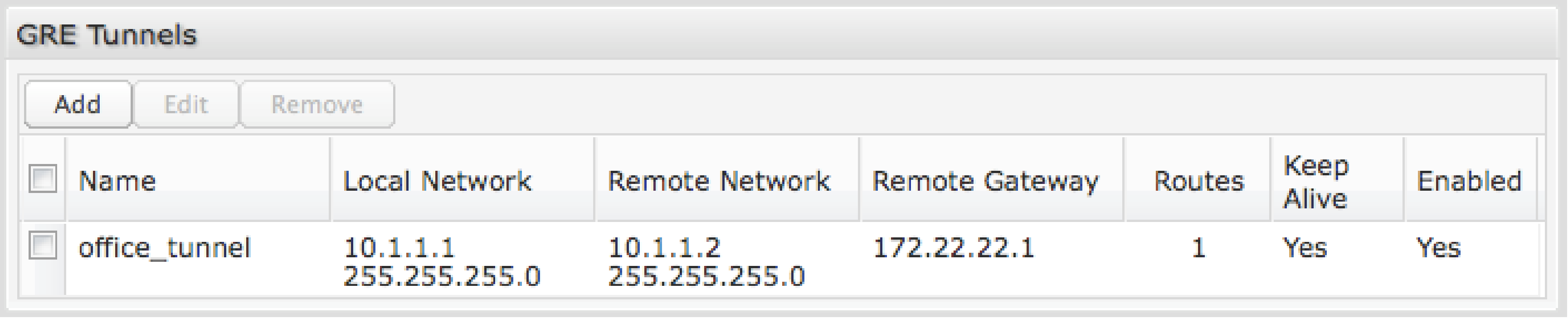
Send Alert on Cap: □

Extra Email Alert: □

Percent of Usage (1-1000): 85

7.5 GRE Tunnels

Generic Routing Encapsulation (GRE) tunnels can be used to create a connection between two private networks. The MBR1400 is enabled for either GRE or VPN tunnels. GRE tunnels are simpler to configure and more flexible for different kinds of packet exchanges, but VPN tunnels are much more secure.



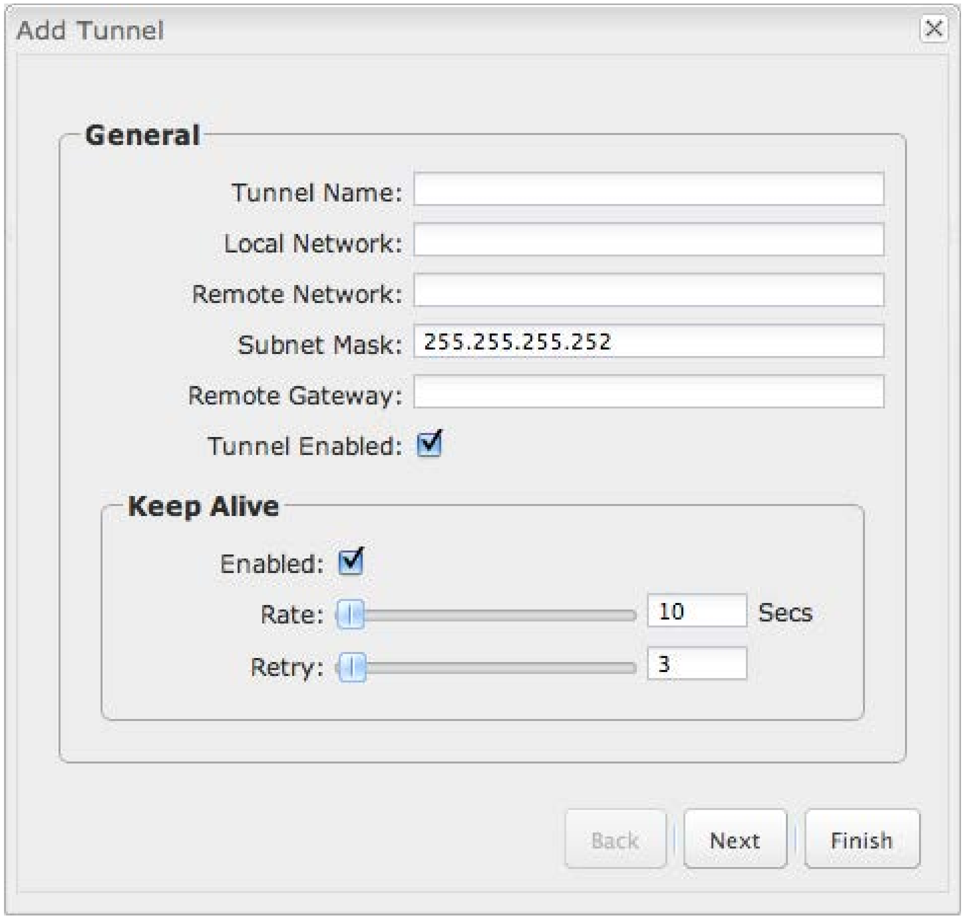
□	Name	Local Network	Remote Network	Remote Gateway	Routes	Keep Alive	Enabled
□	office_tunnel	10.1.1.1 255.255.255.0	10.1.1.2 255.255.255.0	172.22.22.1	1	Yes	Yes

In order to set up a tunnel you must know the following:

- **Local Network** and **Remote Network** addresses for the "**Glue Network**," the network that is created by the administrator that serves as the "glue" between the networks of the tunnel. Each address must be a different IP address from the same private network, and these addresses together form the endpoints of the tunnel.
- **Remote Gateway**, the public facing WAN IP address that the local gateway is going to connect to.
- Optionally, you might also want to enable the tunnel **Keep Alive** feature to monitor the status of a tunnel and more accurately determine if the tunnel is alive or not.

Click **Add** to configure a new GRE tunnel.

Page 1: General


Add Tunnel

General

Tunnel Name:

Local Network:

Remote Network:

Subnet Mask: 255.255.255.252

Remote Gateway:

Tunnel Enabled: ☑

Keep Alive

Enabled: ☑

Rate: 10 Secs

Retry: 3

Tunnel Name: Give the tunnel a name that uniquely identifies it.

Tunnel Key: Enables an ID key for a GRE tunnel, which can be used as an identifier for mGRE (Multipoint GRE).

Local Network: This is the local side of the "**Glue Network**," a network created by the administrator to form the tunnel. The user creates the IP address inputted here. It must be different from the IP addresses of the networks it is gluing together.

Choose any private IP address from the following three ranges that doesn't match either network:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Remote Network: This is the remote side of the "**Glue Network**." Again, the user must create an IP address that is distinct from the IP addresses of the networks that are being glued together.

The Remote Network and Local Network values will be flipped when inputted for the other side of the tunnel configuration.

Subnet Mask: This is the subnet mask for the Glue Network. The Local and Remote Network addresses must fit with this mask. 255.255.255.0 is a logical choice for most users.

Remote Gateway: This is the public facing, WAN-side IP address of the network that the local gateway is going to connect to.

Tunnel Enabled: Select to activate the tunnel.

Keep Alive: This feature monitors the status of a tunnel. This will more accurately determine if the tunnel is alive or not. Choose the length of time in seconds of the **Rate** for each check (Default: 10 seconds. Range: 2 – 3600 seconds) and the number of **Retry** attempts (Default: 3. Range: 1 – 255).

Page 2: Routes

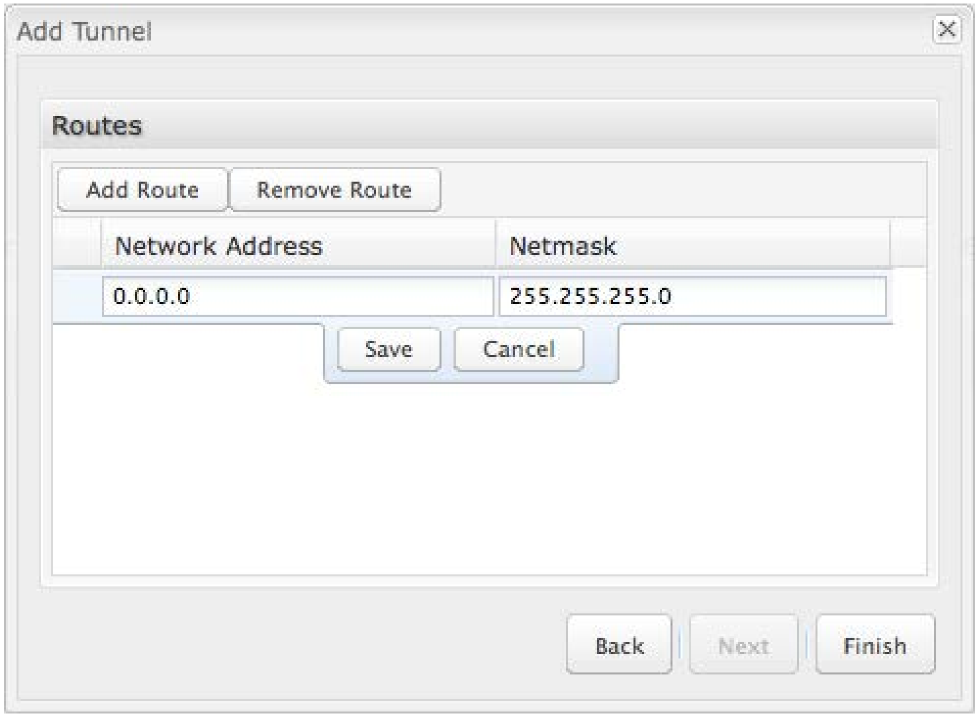
Adding routes allows you to configure what types of network traffic from the local host or hosts will be allowed through the tunnel.

Click **Add Route** to configure a new route. You will need to input the following information, defined by the remote network:

- **Network Address**
- **Netmask:** (Default: 255.255.255.0)

You can set the tunnel to connect to a range of IP addresses or to a single IP address. For example, you could input **192.168.0.0** and **255.255.255.0** to connect your tunnel to all the addresses of the remote network in the **192.168.0.x** range. Alternatively, you could select a single address by inputting that address along with a Netmask of **255.255.255.255**.

Click **Save** to record each new route.



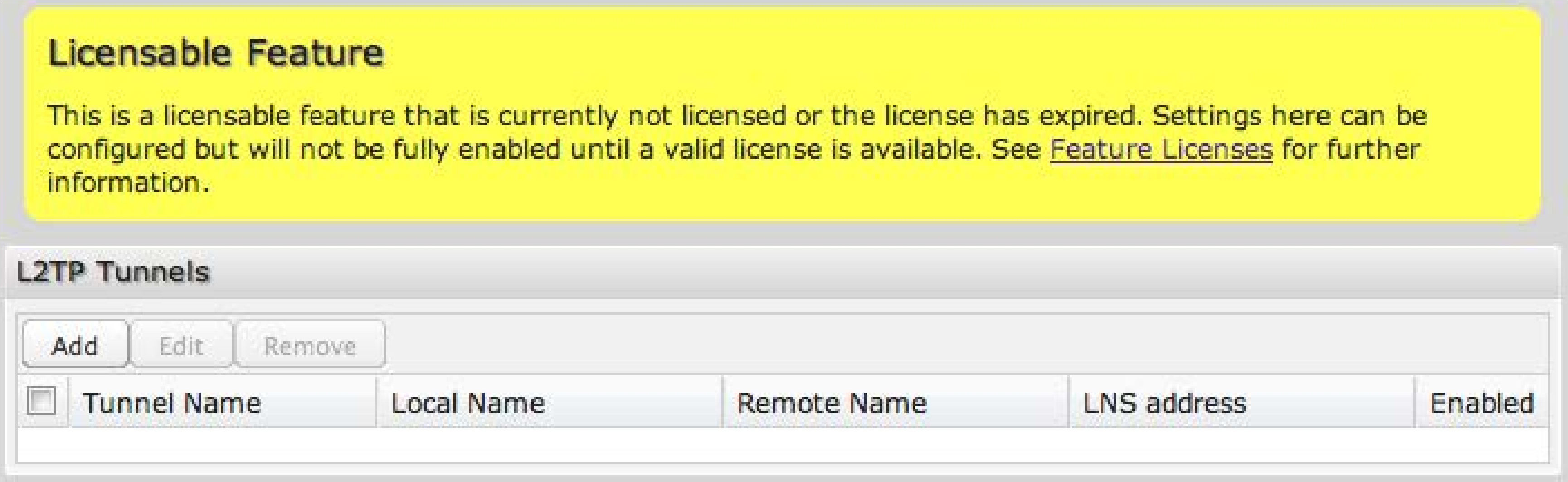
Network Address	Netmask
0.0.0.0	255.255.255.0

When you have finished adding routes, click **Finish** to save your GRE tunnel configuration.

7.6 L2TP Tunnels

NOTE: L2TP requires a feature license and hardware version 2.0. Go to System **Settings → Feature Licenses** to enable this feature.

Layer 2 Tunneling Protocol (L2TP) tunnels can be used to create a connection between two private networks.



Licensable Feature

This is a licensable feature that is currently not licensed or the license has expired. Settings here can be configured but will not be fully enabled until a valid license is available. See Feature Licenses for further information.

L2TP Tunnels

□	Tunnel Name	Local Name	Remote Name	LNS address	Enabled

Once you have a valid feature license, click **Add** to create a new L2TP tunnel.

7.6.1 General

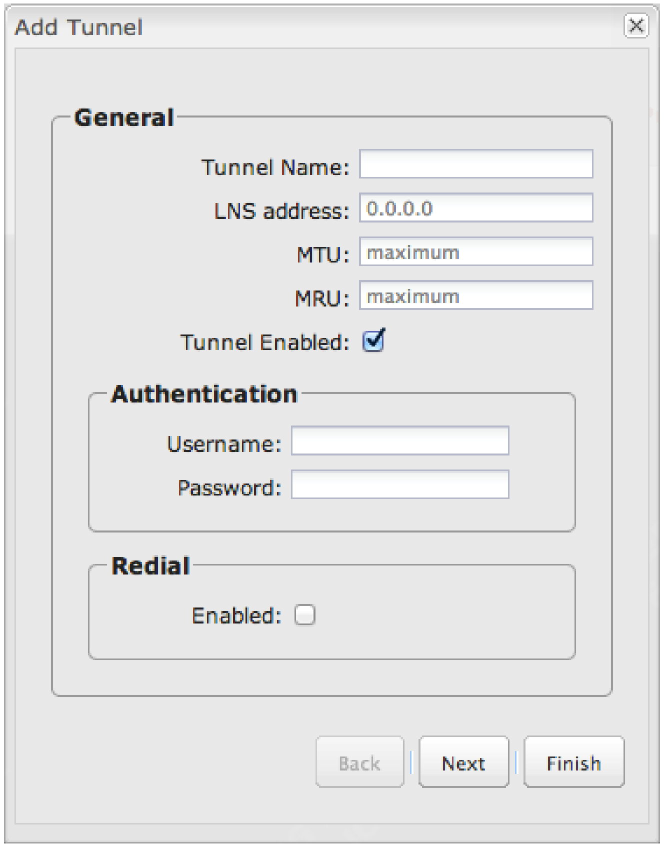
- **Tunnel Name** – Enter a name to uniquely identify this tunnel.
- **LNS address** – Enter the IP Address of the LNS (tunnel server) peer.
- **MTU** – Set the maximum transmission unit (MTU) of the L2TP tunnel.
- **MRU** – Set the maximum receive unit (MRU) to request from the tunnel peer.
- **Tunnel Enabled** – Click to enable/disable this tunnel. Default: Enabled.

Authentication – More authentication options and overrides are available in the next section.

- **Username** – Username for user-specific authorization. Leave blank to disable.
- **Password** – Shared secret (or password) used to authenticate the associated Local and Remote names.

Redial

- **Enabled** – Reconnect if disconnected.



Add Tunnel

General

Tunnel Name:

LNS address: 0.0.0.0

MTU: maximum

MRU: maximum

Tunnel Enabled: ☑

Authentication

Username:

Password:

Redial

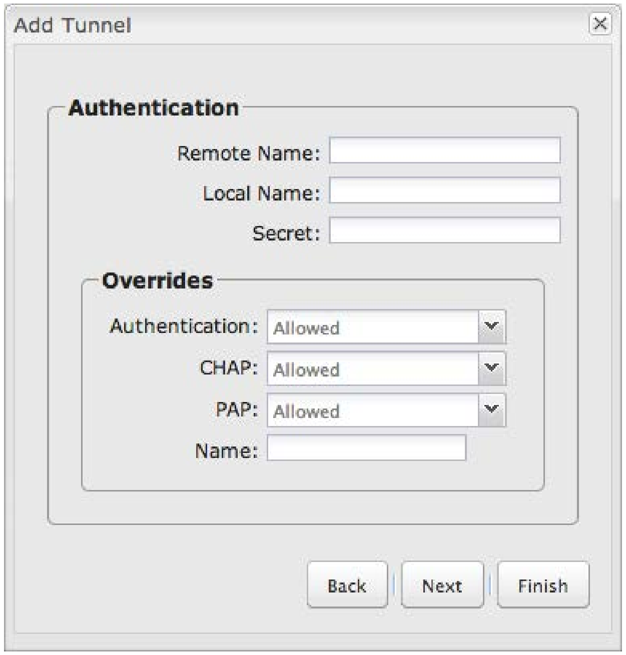
Enabled: □

7.6.2 Authentication

- **Remote Name** – Authorization name specified by and to the remote system as its identity, sometimes a username or hostname. Leave blank to match any.
- **Local Name** – Authorization name specified by and to the remote system as the local system identity; sometimes a username or hostname. Leave blank to match any.
- **Secret** – Shared secret (or password) used to authenticate the associated Local and Remote names.

<ins>**Overrides**</ins> – Override Authentication methods/parameters. With methods set to Allow the two ends of the tunnel can negotiate a common scheme. Some times this negotiation fails, or the implementation on one end is incompatible with the other. To solve those authentication issues, enable the overrides as needed.

- **Authentication** – Username for user-specific authorization. Leave blank to disable.
- **CHAP** – Choose from Allowed, Refused, or Required.
- **PAP** – Choose from Allowed, Refused, or Required.
- **Name** – Override names used to authenticate the router. Leave empty to use the default.



Authentication: Allowed

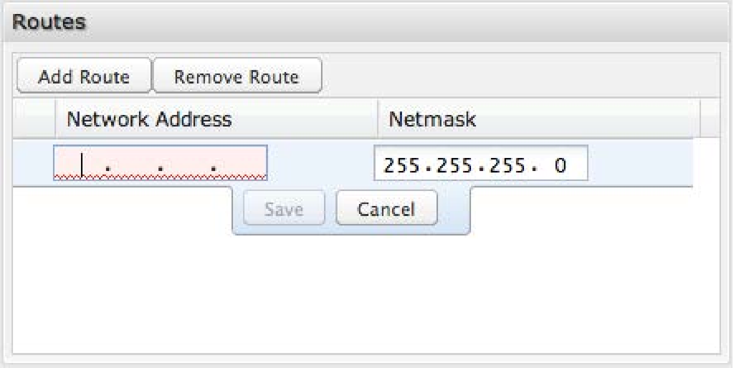
CHAP: Allowed

PAP: Allowed

7.6.3 Routes

Typically specific routes are unnecessary, but they can be added in this section if needed. You can add or remove routes to be used to funnel packets through the tunnel.

- **Network Address** – This is the network address that is the destination of the route. This should be set to the network address at the remote side of the tunnel.
- **Netmask** – This is the corresponding subnet mask of the network being defined.

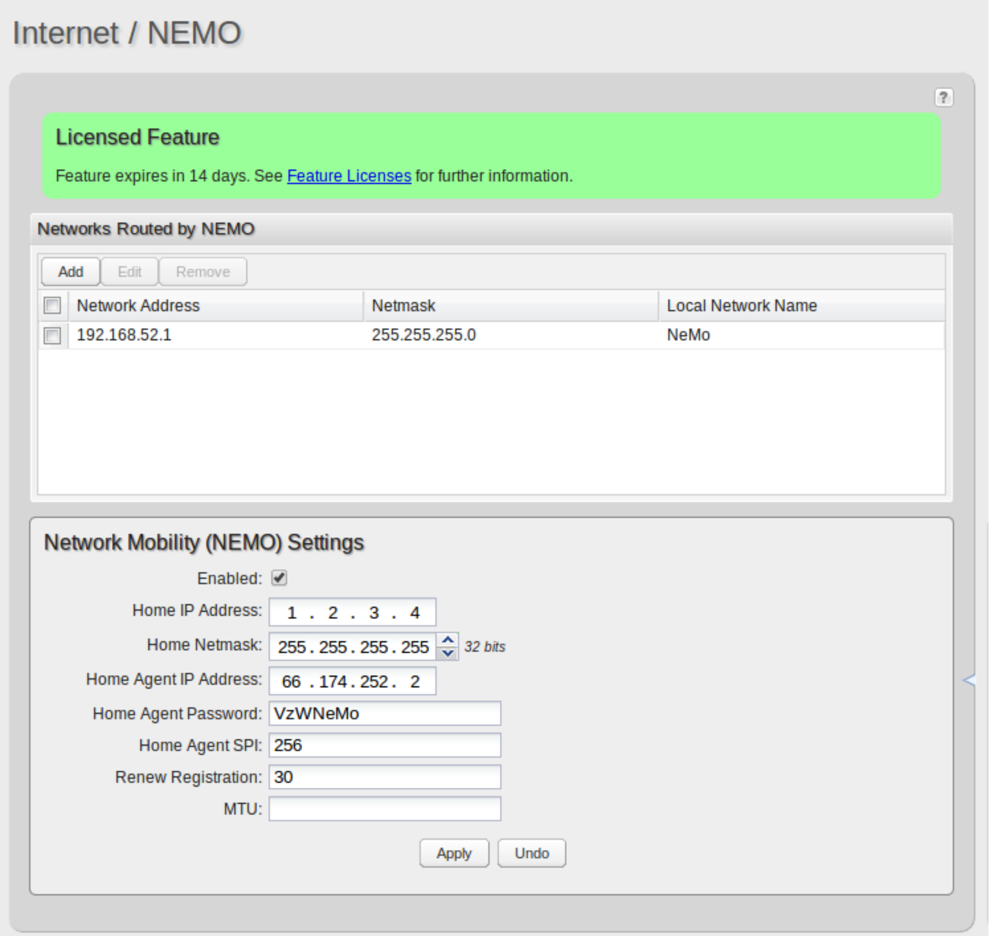


Netmask: 255.255.255. 0

7.7 Network Mobility (NEMO)

NOTE: NEMO requires a feature license and hardware version 2.0. Go to System **Settings → Feature Licenses** to enable this feature.

Network Mobility (NEMO) is an Internet standards track protocol defined in RFC 5177. The protocol allows session continuity for every node in a mobile network as the network moves.


Internet / NEMO

Licensed Feature

Feature expires in 14 days. See Feature Licenses for further information.

Networks Routed by NEMO

□	Network Address	Netmask	Local Network Name
□	192.168.52.1	255.255.255.0	NeMo

Network Mobility (NEMO) Settings

Enabled: ☑
Home IP Address: 1 . 2 . 3 . 4
Home Netmask: 255 . 255 . 255 . 255 *32 bits*
Home Agent IP Address: 66 . 174 . 252 . 2
Home Agent Password: VzWNeMo
Home Agent SPI: 256
Renew Registration: 30
MTU:

This is a licensable feature. Without a valid license, settings can be configured, but will not be implemented. See **System Settings → Feature Licenses** for more information.

NEMO requires a service provider, e.g. Verizon Wireless Private Network with DMNR (Dynamic Mobile Network Routing). Your NEMO service provider will define many of the settings for your NEMO configuration.

Once you have a NEMO service provider and a valid feature license, add networks to the **Networks Routed by NEMO** section by first clicking **Add**. In the popup window, input:

- Network Address
- Netmask

The Network Address and Netmask, or subnet mask, together define a range of IP addresses that comprise the local network you want associated with the NEMO settings.

7.7.1 Network Mobility (NEMO) Settings

Home IP Address and **Home Netmask** – These may be provided by your NEMO service provider. The IP address is a placeholder, "dummy" address; any IP address can be used (1.2.3.4 is common).

Home Agent IP Address, **Home Agent Password**, and **Home Agent SPI** – Your home agent will be defined by your NEMO service provider.

Renew Registration – The NEMO network regularly re-registers with the home agent (e.g., every 30 seconds). Specify the number of seconds between each check-in.

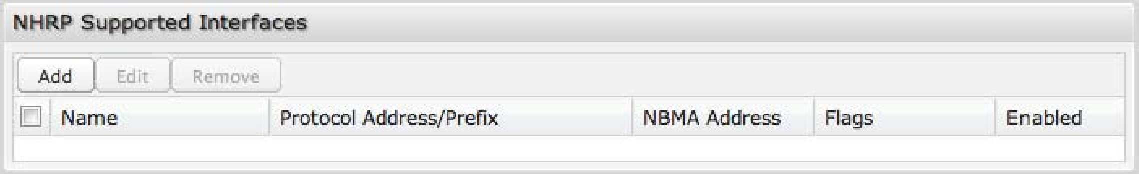
MTU – Override the MTU (maximum transmission unit) of the NEMO tunnel. The TCP MSS (maximum segment size) is automatically derived from the MTU. Leave blank to rely on Path MTU Discovery.

7.8 NHRP Configuration

NOTE: NHRP Configuration requires a feature license and hardware version 2.0. Go to System **Settings → Feature Licenses** to enable this feature.

Next Hop Resolution Protocol is a protocol used to discover addresses of clients on Non-Broadcast Multiple Access (NBMA) networks. It is used to create next-generation VPN technologies that allow shortcutting between spokes. With NHRP, systems attached to an NBMA network dynamically learn the NBMA address of the other systems that are part of that network, allowing these systems to directly communicate without requiring an intermediate hop.

The NHRP Supported Interfaces table displays the following fields for each configured NHRP interface.

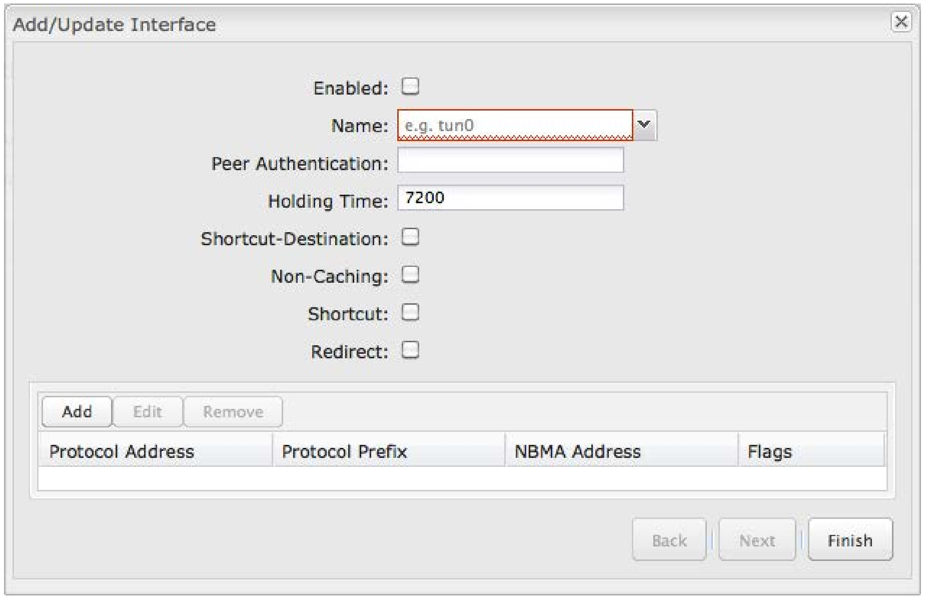


□	Name	Protocol Address/Prefix	NBMA Address	Flags	Enabled

- **Name**: Name of the GRE tunnel that NHRP will use.
- **Protocol Address/Prefix**: GRE tunnel endpoint mapping that NHRP associates with the NBMA server.
- **NBMA Address**: NBMA server address the protocol address/prefix is associated with.
- **Flags**:
  - **SD**: Shortcut-Destination
  - **N**: Non-Caching
  - **S**: Shortcut
  - **R**: Redirect

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

- **Enabled**: Enable or disable the interface.
- **Name**: Give the interface a unique name that matches the mGRE (multipoint GRE) tunnel. Select from configured GRE tunnels or input manually.
- **Peer Authentication**: Embeds the secret plaintext password to outgoing NHRP packets. Incoming NHRP packets on this interface are discarded unless this password is present. Max length: 8 characters.
- **Holding Time**: Specifies the holding time for NHRP registration requests and resolution replies.
- **Shortcut-Destination**: Reply with authoritative answers on NHRP resolution requests destined to addresses in this interface (instead of forwarding the packets).
- **Non-Caching**: Disables caching of peer information from forwarded NHRP resolution reply packets.
- **Shortcut**: Enable creation of shortcut routes.
- **Redirect**: Enable sending of proprietary enterprise-style NHRP traffic indication packets.



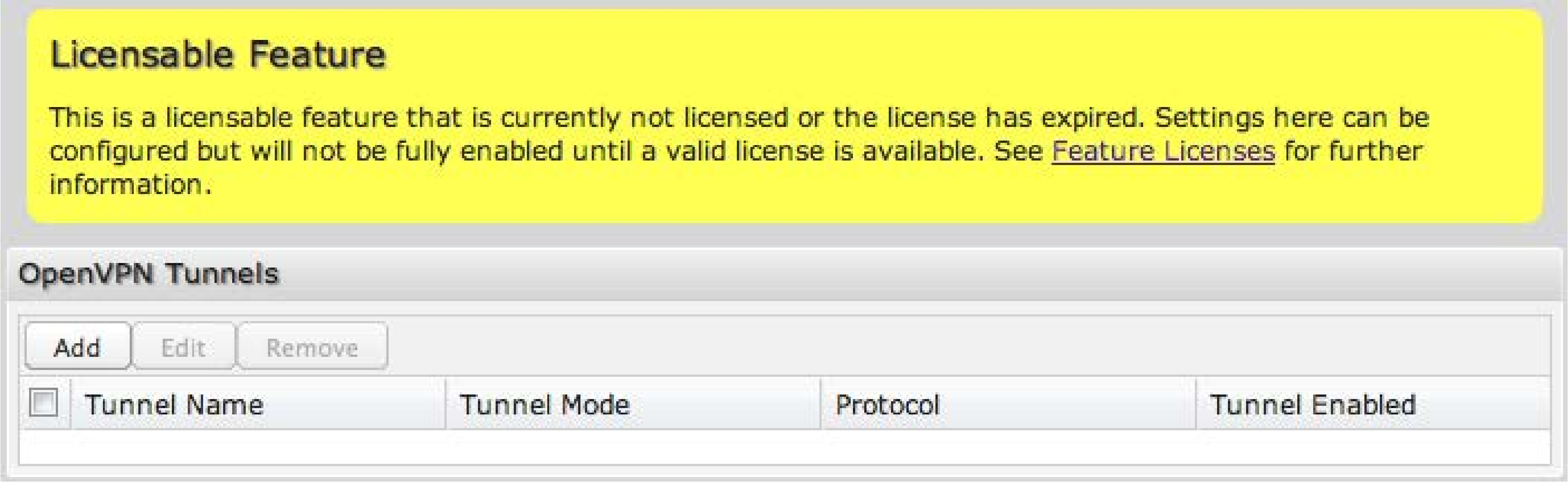
Add/Update Interface

Enabled: □
Name: e.g. tun0
Peer Authentication:
Holding Time: 7200
Shortcut-Destination: □
Non-Caching: □
Shortcut: □
Redirect: □

Protocol Address	Protocol Prefix	NBMA Address	Flags

7.9 OpenVPN Tunnels

NOTE: Using OpenVPN Tunnels requires a feature license and hardware version 2.0. Go to System **Settings → Feature Licenses** to enable this feature.



Licensable Feature

This is a licensable feature that is currently not licensed or the license has expired. Settings here can be configured but will not be fully enabled until a valid license is available. See Feature Licenses for further information.

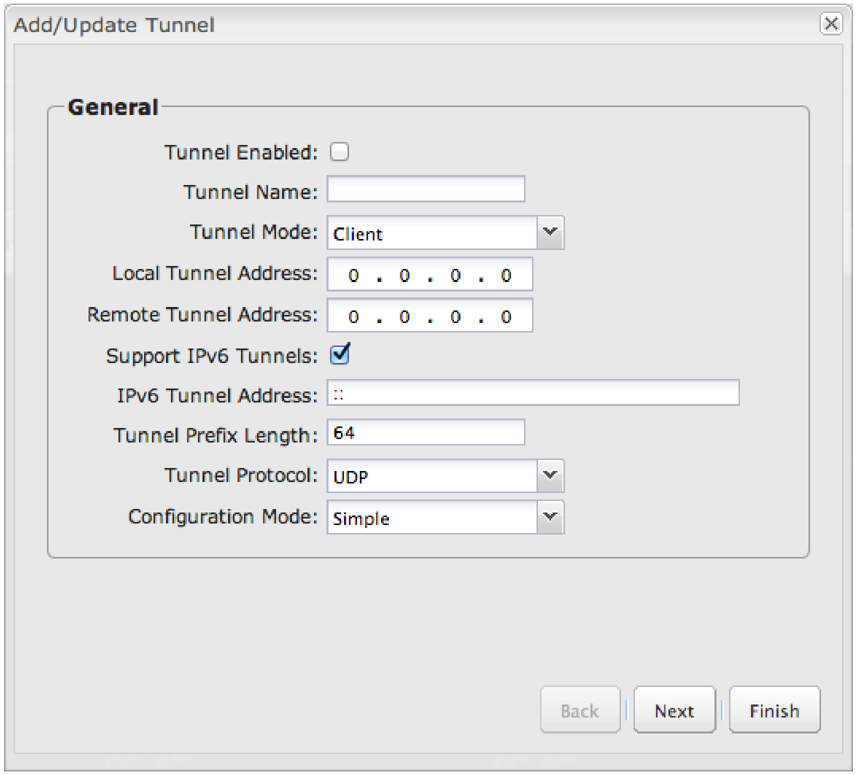
OpenVPN Tunnels

□	Tunnel Name	Tunnel Mode	Protocol	Tunnel Enabled

Once you have a valid feature license, click **Add** to create a new OpenVPN tunnel.

7.9.1 General

- **Tunnel Enabled** – Click to enable/disable this tunnel.
- **Tunnel Name** – Enter a name to uniquely identify this tunnel.
- **Tunnel Mode** – Select which mode this tunnel endpoint is required to be. Choose from the following:
  - Client
  - Server
- **Local Tunnel Address** – Enter the IP Address of the LNS (tunnel server) peer.
- **Remote Tunnel Address** – Enter the IP Address of the LNS (tunnel server) peer.
- **Support IPv6 Tunnels** – Allow IPv6 traffic to be forwarded over this tunnel. If you select this option, also input an **IPv6 Tunnel Address** and **Tunnel Prefix Length** for IPv6
- **Tunnel Protocol** – Choose UDP or TCP.
- **Configuration Mode** – Simple configuration requires the least amount of configuration for the tunnel, while advanced allows for a more detailed setup.
- **Ping** – (Displays if the **Configuration Mode** is **Advanced**) If no packets have been sent in the amount of time entered, a ping is sent to the remote endpoint.
- **Ping Restart** – (Displays if the **Configuration Mode** is **Advanced**) If no pings have been received in the amount of time entered, OpenVPN restarts the tunnel.



Add/Update Tunnel

General

Tunnel Enabled: □

Tunnel Name:

Tunnel Mode: Client

Local Tunnel Address: 0 . 0 . 0 . 0

Remote Tunnel Address: 0 . 0 . 0 . 0

Support IPv6 Tunnels: ☑

IPv6 Tunnel Address: ::

Tunnel Prefix Length: 64

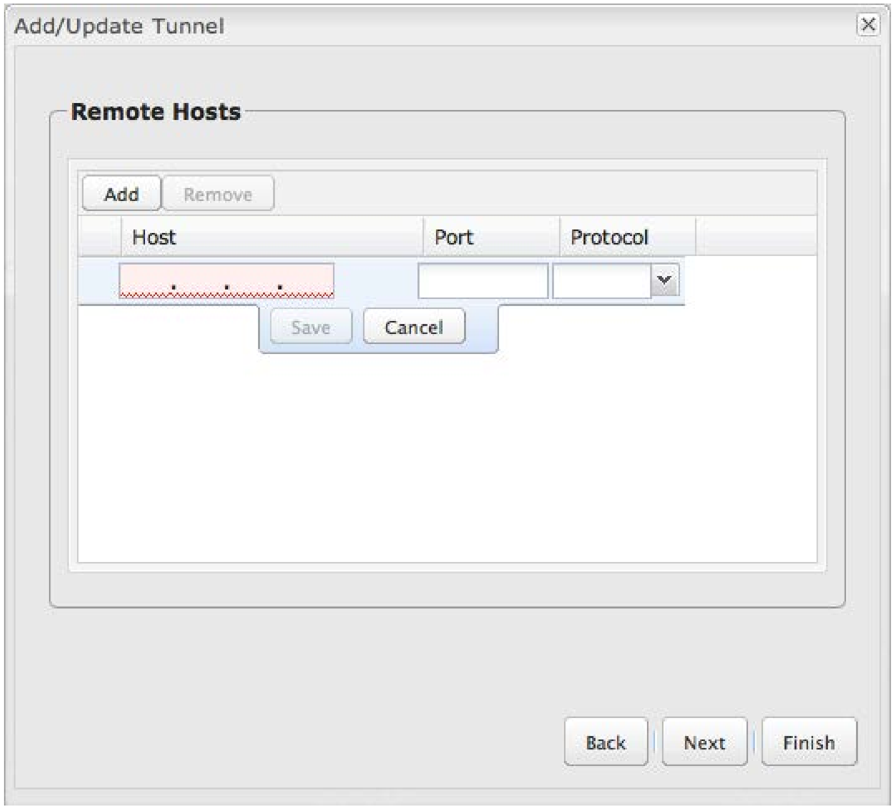
Tunnel Protocol: UDP

Configuration Mode: Simple

7.9.2 Remote Hosts

Create a list of remote server connections to connect to. OpenVPN will try to connect to each host in the list. If a disconnect occurs from a given server, the next server will be tried in a round-robin fashion.

- **Host** – IP address of the remote server.
- **Port** – Specify the port if desired.
- **Protocol** – Select UDP or TCP.



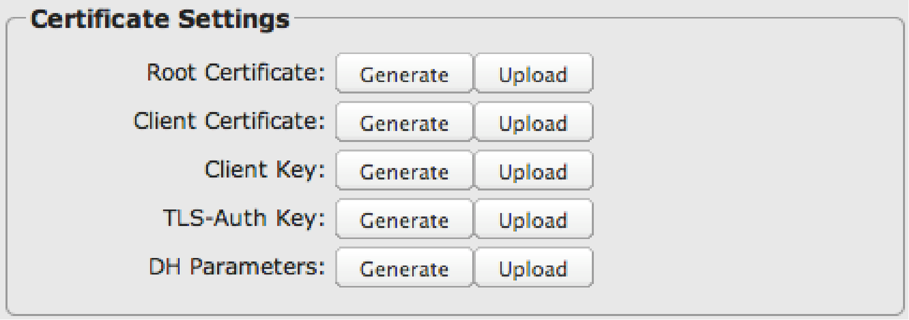
7.9.3 Certificate Settings

Generate or upload certificates for OpenVPN.

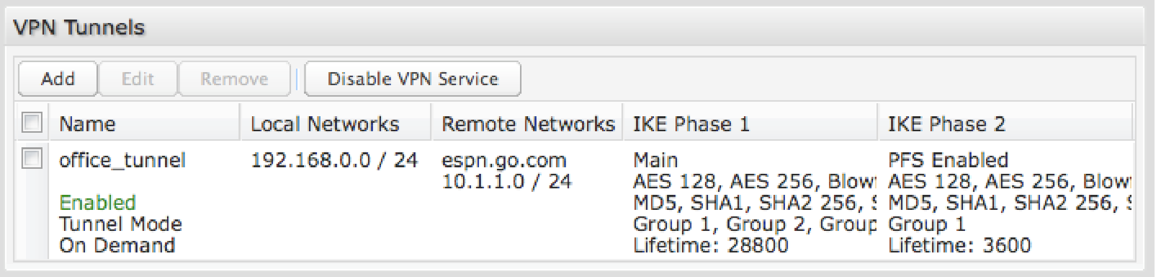
If the **Configuration Mode** is set to **Simple**, you have the option to set the **TLS-Auth Key**.

If the **Configuration Mode** is set to **Advanced**, set any of the following:

- **Root Certificate**
- **Client Certificate**
- **Client Key**
- **TLS-Auth Key**
- **DH Parameters**



7.10 VPN Tunnels



☐	Name	Local Networks	Remote Networks	IKE Phase 1	IKE Phase 2
☐	office_tunnel Enabled Tunnel Mode On Demand	192.168.0.0 / 24	espn.go.com 10.1.1.0 / 24	Main AES 128, AES 256, Blow MD5, SHA1, SHA2 256, S Group 1, Group 2, Group Lifetime: 28800	PFS Enabled AES 128, AES 256, Blow MD5, SHA1, SHA2 256, S Group 1 Lifetime: 3600

VPN (virtual private network) tunnels are used to establish a secure connection to a remote network over a public network. For example, VPN tunnels can be used across the Internet by an individual to connect to an office network while traveling or by two office networks to function as one network. The two networks set up a secure connection across the (normally) unsecure Internet by assigning VPN encryption protocols.

The MBR1400 uses IPsec (Internet Protocol security) to authenticate and encrypt packets exchanged across the tunnel. To set up a VPN tunnel with the MBR1400 on one end, there must be another device (usually a router) that also supports IPsec on the other end.

IKE (Internet Key Exchange) is the security protocol in IPsec. IKE has two phases, Phase 1 and Phase 2. The MBR1400 has several different security protocol options for each phase, but the default selections will be sufficient for most users.

The VPN tunnel status page allows you to view the state of the VPN tunnels. If a tunnel fails to connect to the remote site, check the System Logs for more information. You may double click on a cell to directly edit that information.

Click **Add** to configure a new VPN tunnel.

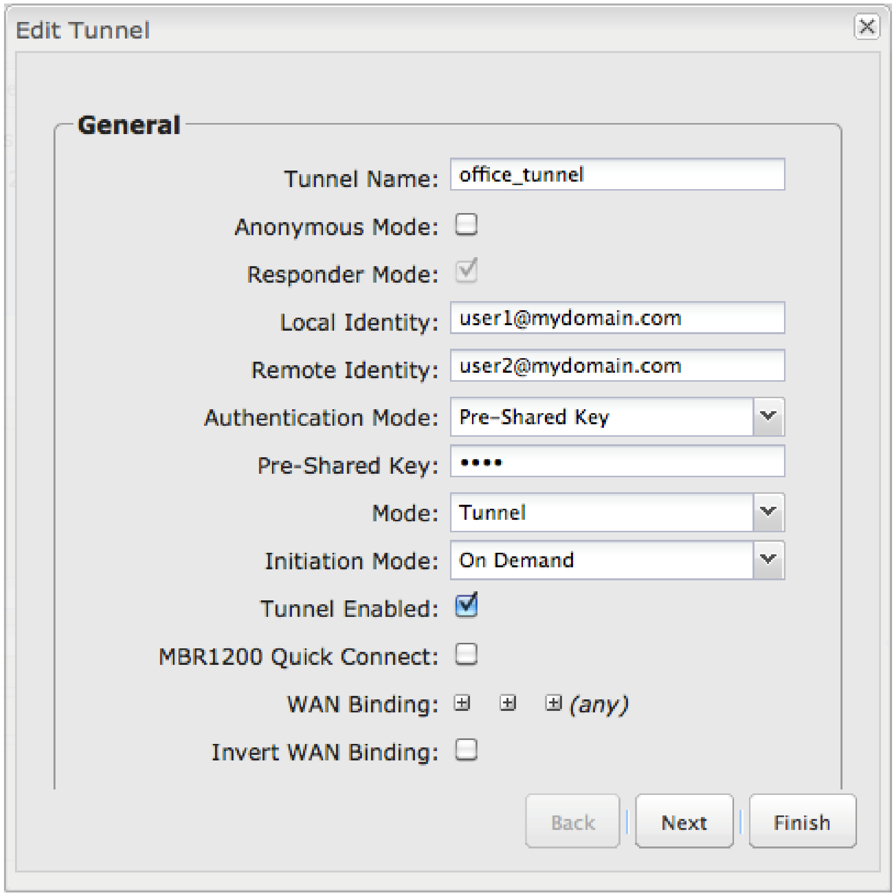
7.10.1 Page 1: General

<u>Tunnel Name</u>: Give the tunnel a name that uniquely identifies it.

<u>Anonymous Mode</u>: Select to allow remote connections from any IP address.

<u>Responder Mode</u>: When enabled, the router will not initiate negotiation with peers, otherwise start negotiations as soon as possible.

<u>Local Identity</u>: Specifies the identifier sent to the remote host during phase 1 negotiation. If left blank it will default to the IP address of the WAN connection. Currently we only support identifiers in the form of an **IP address**, a **user-fully qualified domain name** (user@mydomain.com) or just a **fully qualified domain name** (www.mydomain.com). If the remote side of the tunnel is configured to expect an identifier, then both ***must match*** in order for the negotiation to succeed. If **NAT-T** is being used, a single word (instead of an address) can be used if a DynDNS connection is not being used.



Edit Tunnel

General

Tunnel Name: office_tunnel

Anonymous Mode: □

Responder Mode: ☑

Local Identity: user1@mydomain.com

Remote Identity: user2@mydomain.com

Authentication Mode: Pre-Shared Key

Pre-Shared Key: ••••

Mode: Tunnel

Initiation Mode: On Demand

Tunnel Enabled: ☑

MBR1200 Quick Connect: □

WAN Binding: ⊞ ⊞ ⊞ *(any)*

Invert WAN Binding: □

<u>Remote Identity</u>: Specifies the identifier we expect to receive from the remote host during phase 1 negotiation. If no identifier is defined then no verification of the remote peer's identification will be done. Currently we only support identifiers in the form of an **IP address**, a **user-fully qualified domain name** (user@mydomain.com) or just a **fully qualified domain name** (www.mydomain.com). If left blank we will default to the IP address of the WAN connection. If **NAT-T** is being used, a single word (instead of an address) can be used if a DynDNS connection is not being used.

<u>Authentication Mode</u>: Select from **Pre-Shared Key** and **Certificate**. **Pre-Shared Key** is used when there is a single key common to both ends of the VPN. **Certificate** requires the creation of a set of certificates and a private key that can be uploaded to the router. Enable Certificate Support in the Global VPN Settings to upload a single set of certificates for the router to use.

Pre-shared Key: Create a password or key. The routers on both sides of the tunnel must use this same key.

Mode: **Tunnel** or **Transport**. **Tunnel Mode** is used for protecting traffic between different networks, when traffic must pass through an intermediate, untrusted network. **Transport Mode** is used for end-to-end communications (for example, for communications between a client and a server).

Initiation Mode: "**Always On"** or "**On Demand**." "**Always On**" is used if you want the tunnel to initiate the tunnel connection whenever the WAN becomes available. Select **On Demand** if you want the tunnel to initiate a connection if and only if there is data traffic bound for the remote side of the tunnel.

Tunnel Enabled: Enabled or Disabled.

MBR1200 Quick Connect: VPN tunnels in the MBR1400 have more choices than they do in the MBR1200, so it is more complex to configure. Check this box to simplify setup by streamlining your options.

WAN Binding: WAN Binding is an advanced optional parameter used to configure a VPN tunnel to ONLY operate when the specified WAN device(s) are available and connected. An example use case is a router with both a primary and backup WAN connection and the VPN tunnel should only be used when the system has failed over to the backup connection. This use case makes the most sense when the primary and backup connections are mutually exclusive, i.e., not connected at the same time.

Select each of the following to create a condition for your WAN Binding setup. **When:**

- **Port** (USB Port 1, 2, 3; ExpressPort 1, 2): Select by the port that you are plugging the modem into.
- **Manufacturer:** Select by the manufacturer, such as Sierra Wireless.
- **Model**: Set your rule according to the specific model of modem.
- **Type** (Ethernet, LTE, Modem, WiMAX, Wireless as WAN, HSPA): Select by type of Internet source.
- **Serial Number**: Select 3G or LTE modem by Serial Number.
- **MAC Address**: Select WiMAX modem by MAC Address.
- **Unique ID**: Select by ID. This is generated by the router and displayed when the device is connected to the router.

Condition: Select "is," "is not," "starts with," "contains," or "ends with" to create your condition's statement.

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

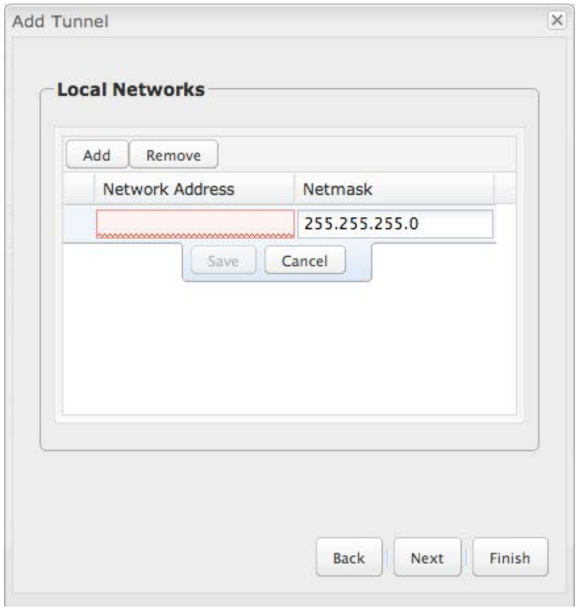
The condition will be of the following form:
“___(When)___ is/is not ___(value)___”

For example:
“Type is not WiMAX”
“Port is USB Port 1”

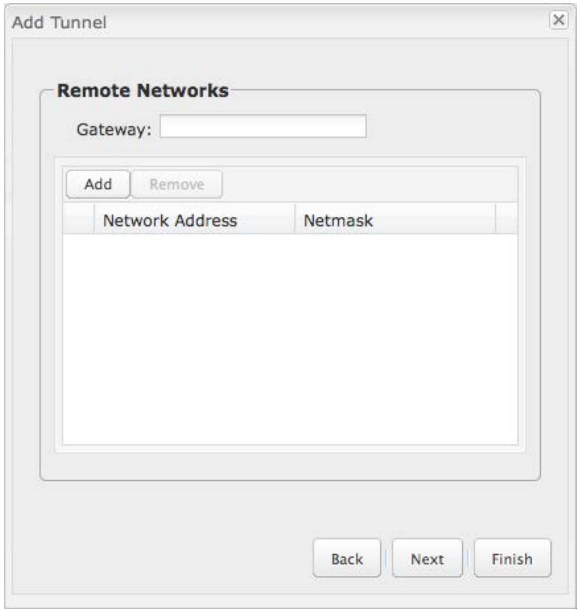
If you intend to have multiple WAN devices connected simultaneously, with either Load Balancing or more likely WAN Affinity, then you may consider using the **Invert WAN Binding** option which will invert the expression to only establish the VPN tunnel when the specified WAN Binding devices are NOT connected.

Invert WAN Binding: Advanced option that inverts the meaning of WAN Binding to only establish this tunnel when the specified WAN Binding device(s) are NOT connected. This is typically useful when the VPN tunnel is being used as a hot-spare on a router with multiple active WAN connections and the VPN tunnel is only needed in the absence or unavailability of a particular WAN device (for example, an MPLS-based WAN device).

7.10.2 Page 2-3: Local and Remote Networks



Netmask: 255.255.255.0



Local Network: The **Network Address** and the **Netmask** define what local devices have access to or can be accessed from the VPN tunnel. The MBR1400 will automatically fill in the values for your network, but you can change the values to limit the tunnel to only some of the devices in your network.

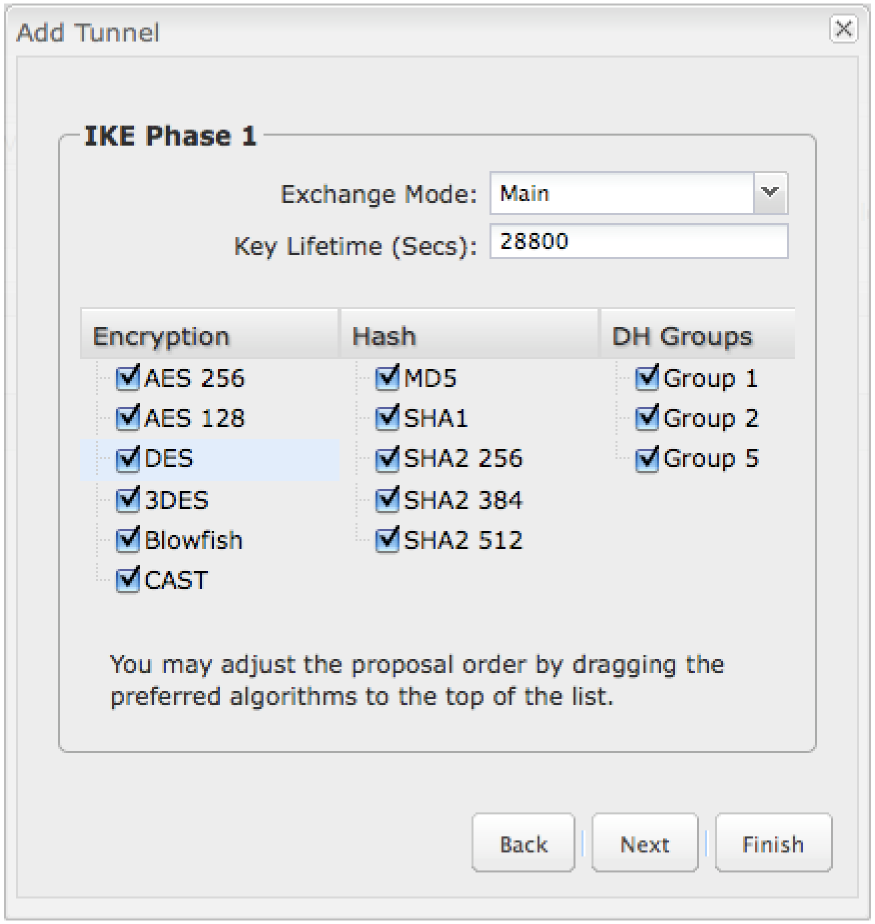
NOTE**:** The local network IP address ***must*** be different from the remote network IP address.

Remote Network: Enter the remote **Gateway**'s IP address or fully qualified domain name (my.domain.com). It is recommended you use a dynamic DNS host name instead of the static IP address. By using the dynamic DNS host name updates of the remote WAN IP are compensated for while connecting to a VPN tunnel.

Enter the **Network** IP address with the **Subnet Mask** to define the remote network subnet that the local devices will have access to.

NOTE**:** The remote network IP address ***must*** be different from the local network IP address.

7.10.3 Page 3: IKE Phase 1



Add Tunnel

IKE Phase 1

Exchange Mode: Main

Key Lifetime (Secs): 28800

Encryption	Hash	DH Groups
☑ AES 256	☑ MD5	☑ Group 1
☑ AES 128	☑ SHA1	☑ Group 2
☑ DES	☑ SHA2 256	☑ Group 5
☑ 3DES	☑ SHA2 384	
☑ Blowfish	☑ SHA2 512	
☑ CAST		

You may adjust the proposal order by dragging the preferred algorithms to the top of the list.

IKE security has two phases, Phase 1 and Phase 2. You have the ability to distinctly configure each phase, but the default settings will be sufficient for most users.

To set up a tunnel with a remote site, you need to match your tunnel's IKE negotiation parameters with the remote site. By selecting several encryption, hash, and DH group options, you improve your chances for a successful tunnel negotiation. For greatest compatibility, select all options; for greatest security, select only the most secure options that your devices support.

Exchange Mode: The IKE protocol has 2 modes of negotiating phase 1 - **Main** (also called Identity Protection) and **Aggressive**.

- In **Main** mode, IKE separates the key information from the identities, allowing for the identities of peers to be secure at the expense of extra packet exchanges.
- In **Aggressive** mode, IKE tries to combine as much information into fewer packets while maintaining security. Aggressive mode is slightly faster but less secure.

Because it has better security, **Main** mode is recommended for most users.

Key Lifetime: The lifetime of the generated keys of Phase 1 of the IPsec negotiation from IKE. After the time has expired, IKE will renegotiate a new set of Phase 1 keys.

Encryption, Hash, and DH Groups: Each IKE exchange uses one encryption algorithm, one hash function, and one DH group to make a secure exchange.

- **Encryption:** Used to encrypt messages sent and received by IPsec.

- AES 128
- AES 256
- blowfish
- Cast128
- DES
- 3DES

- **Hash:** Used to compare, authenticate, and validate that data across the VPN arrives in its intended form and to derive keys used by IPsec.
  - MD5
  - SHA1
  - SHA2 256
  - SHA2 384
  - SHA2 512

- **DH Groups:** The DH (Diffie-Hellman) Group is a property of IKE and is used to determine the length of prime numbers associated with key generation. The strength of the key generated is partially determined by the strength of the DH Group. Group 5, for instance, has greater strength than Group 2.
  - DH group 1: 768-bit key.
  - DH group 2: 1024-bit key.
  - DH group 5: 1536-bit key.

  In Phase 1, only one DH group can be selected while using **Aggressive** exchange mode.

By default, all the algorithms (encryption, hash, and DH groups) supported by the MBR1400 are checked, which means they are *allowed* for any given exchange. Deselect these options to limit which algorithms will be accepted. Be sure to check that the router (or similar device) at the other end of the tunnel has matching algorithms.

The algorithms are listed in order by priority. You can reorder this priority list by clicking and dragging algorithms up or down. Any selected algorithm may be used for IKE exchange, but the algorithms on the top of the list are more likely to be used more often.

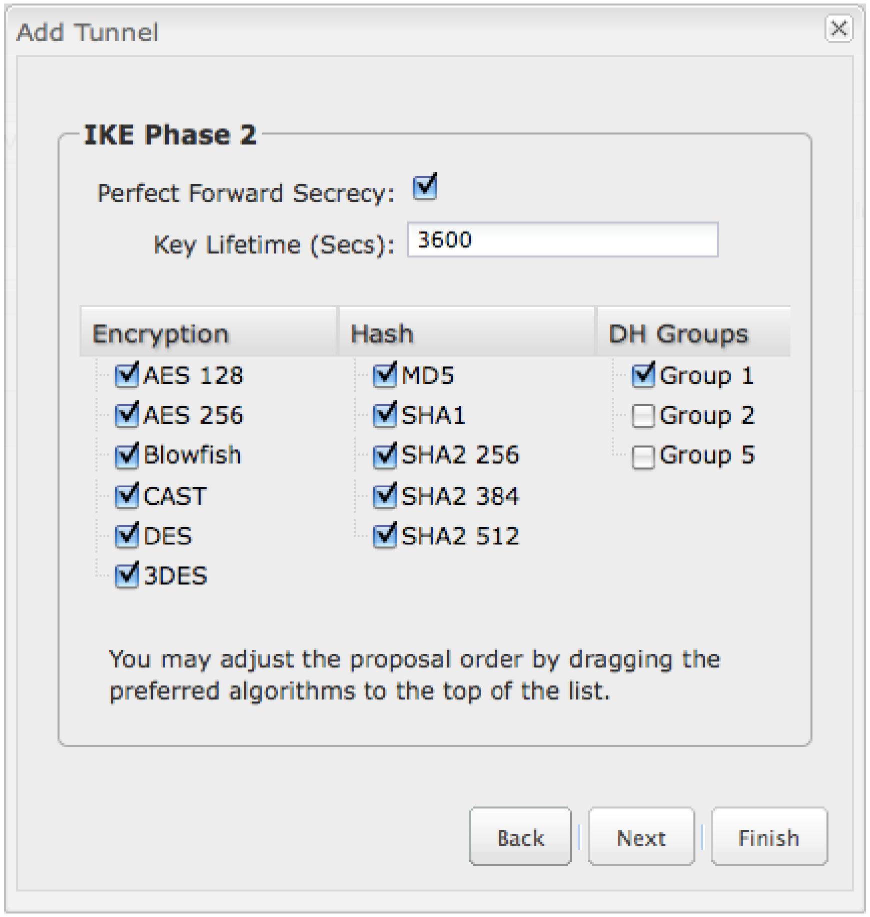
7.10.4 Page 4: IKE Phase 2

Perfect Forward Secrecy (PFS): Enabling this feature will require IKE to generate a new set of keys in Phase 2 rather than using the same key generated in Phase 1.

Additionally, the new keys generated in Phase 2 (with this option enabled) are exchanged in an encrypted session. Enabling this feature affords the policy greater security.

Key Lifetime: The lifetime of the generated keys of Phase 2 of the IPsec negotiation from IKE. After the time has expired, IKE will renegotiate a new set of Phase 2 keys.

Phase 2 has the same selection of **Encryption**, **Hash**, and **DH Groups** as Phase 1, but you are restricted to only one DH Group. Phase 2 and Phase 1 selections do not have to match.



IKE Phase 2

Perfect Forward Secrecy: ☑

Key Lifetime (Secs): 3600

Encryption	Hash	DH Groups
☑ AES 128	☑ MD5	☑ Group 1
☑ AES 256	☑ SHA1	□ Group 2
☑ Blowfish	☑ SHA2 256	□ Group 5
☑ CAST	☑ SHA2 384	
☑ DES	☑ SHA2 512	
☑ 3DES		

You may adjust the proposal order by dragging the preferred algorithms to the top of the list.

7.10.5 Page 5: Dead Peer Detection

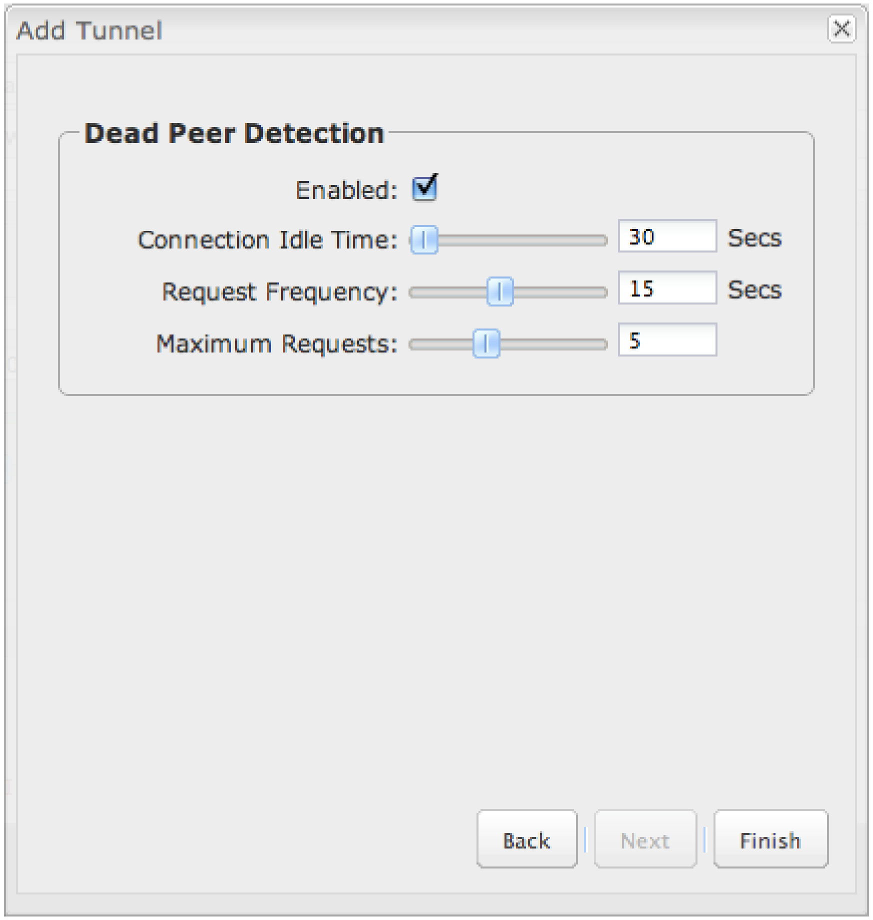
Dead Peer Detection (DPD) defines how the router will detect when one end of the IPsec session loses connection while a policy is in use.

Connection Idle Time allows you to configure how long the router will allow an IPsec session to be idle before beginning to send Dead Peer Detection (DPD) packets to the peer machine.

Request Frequency allows you to adjust the delay between these DPD packets to send as quickly as every 2 seconds up to 30 seconds apart.

Additionally, you can specify how many **Maximum Requests** to send at the selected time interval before the tunnel is considered dead.

You must click **Finish** to save your VPN tunnel.



Dead Peer Detection

Enabled: ☑

Connection Idle Time: 30 Secs

Request Frequency: 15 Secs

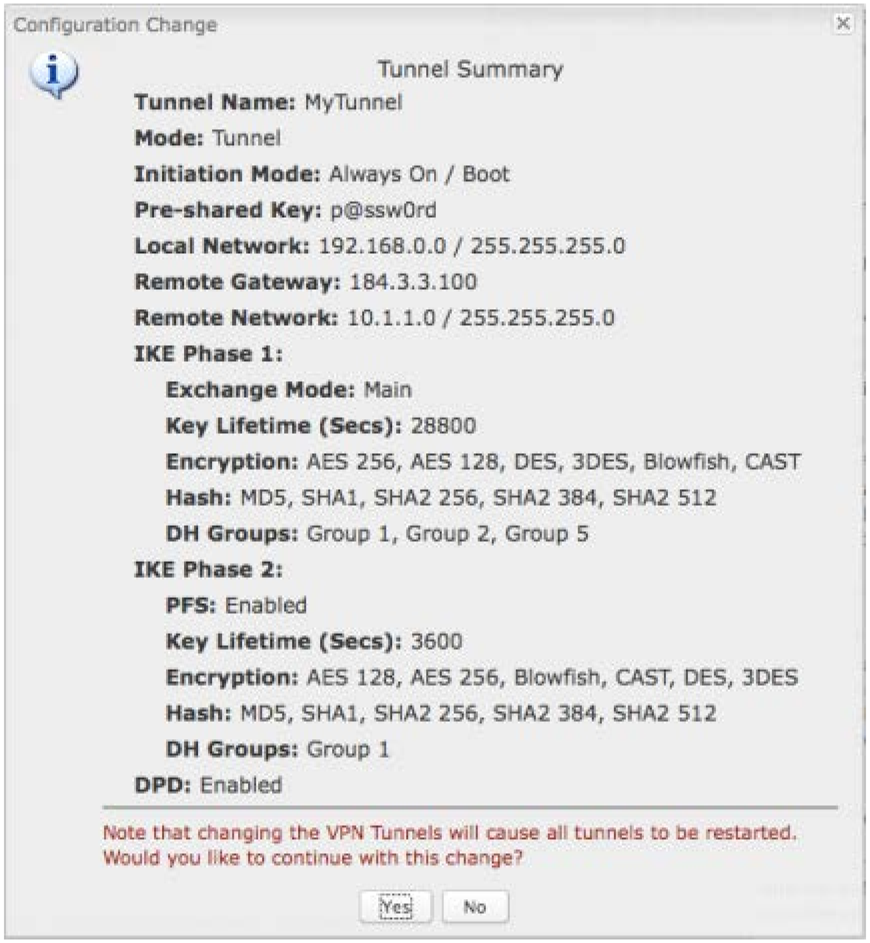
Maximum Requests: 5

7.10.6 Page 6: Tunnel Summary

The final page of the tunnel configuration interface is a summary of the tunnel specifications. This is especially helpful for matching this information with the router (or similar device) at the other end of the tunnel.

- Tunnel Name
- Mode
- Initiation Mode
- Pre-shared Key
- Local Network
- Remote Gateway
- Remote Network
- IKE Phase 1:
  - Exchange Mode
  - Key Lifetime (Secs)
  - Encryption
  - Hash
  - DH Groups
- IKE Phase 2:
  - PFS
  - Key Lifetime (Secs)
  - Encryption
  - Hash
  - DH Groups
- DPD

Click **Yes** at the bottom of the Tunnel Summary page to save your configuration changes. This will cause active tunnels to restart.



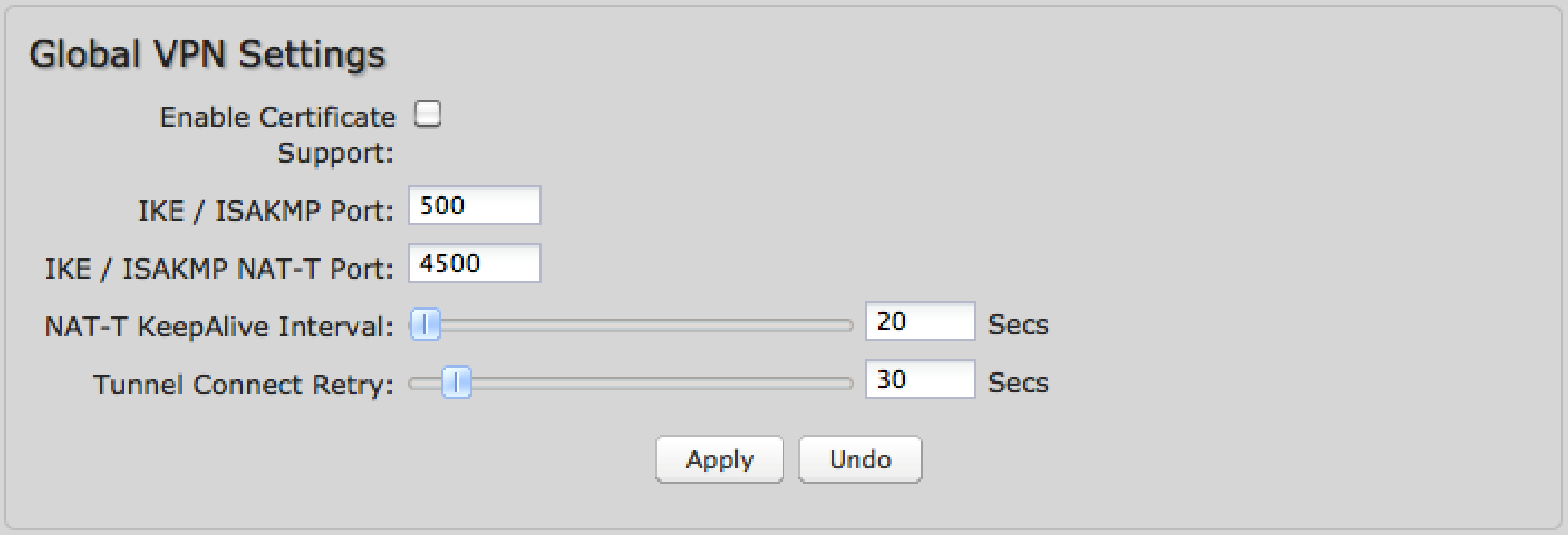
Tunnel Summary

Tunnel Name: MyTunnel
Mode: Tunnel
Initiation Mode: Always On / Boot
Pre-shared Key: p@ssw0rd
Local Network: 192.168.0.0 / 255.255.255.0
Remote Gateway: 184.3.3.100
Remote Network: 10.1.1.0 / 255.255.255.0
IKE Phase 1:
Exchange Mode: Main
Key Lifetime (Secs): 28800
Encryption: AES 256, AES 128, DES, 3DES, Blowfish, CAST
Hash: MD5, SHA1, SHA2 256, SHA2 384, SHA2 512
DH Groups: Group 1, Group 2, Group 5
IKE Phase 2:
PFS: Enabled
Key Lifetime (Secs): 3600
Encryption: AES 128, AES 256, Blowfish, CAST, DES, 3DES
Hash: MD5, SHA1, SHA2 256, SHA2 384, SHA2 512
DH Groups: Group 1
DPD: Enabled

Note that changing the VPN Tunnels will cause all tunnels to be restarted. Would you like to continue with this change?

7.10.7 Global VPN Settings

These settings apply to all configured VPN tunnels.



Global VPN Settings

Enable Certificate Support: □

IKE / ISAKMP Port: 500

IKE / ISAKMP NAT-T Port: 4500

NAT-T KeepAlive Interval: 20 Secs

Tunnel Connect Retry: 30 Secs

Enable Certificate Support: Enabling Certificate Support will allow you to load a certificate for VPN to the router. Click the “Upload Certificate” button that appears to browse for a certificate on a local device. Disabling certificate support will no longer use any previously loaded certificate but will not delete it from the router. Only one certificate at a time is supported.

IKE / ISAKMP Port: Internet Key Exchange / Internet Security Association and Key Management Protocol port. Default: 500. This is a standard VPN port that usually does not need to be changed.

IKE / ISAKMP NAT-T Port: Internet Key Exchange / Internet Security Association and Key Management Protocol network address translation traversal port. Default: 4500. This is a standard VPN NAT-T port that usually does not need to be changed.

NAT-T KeepAlive Interval: Default: 20 seconds. Range: 0-3600 seconds. 20 seconds will be sufficient in almost all cases.

Tunnel Connect Retry: Default: 30 seconds. Range: 10-255 seconds. 30 seconds will be sufficient in almost all cases.

7.10.8 VPN with NAT-T

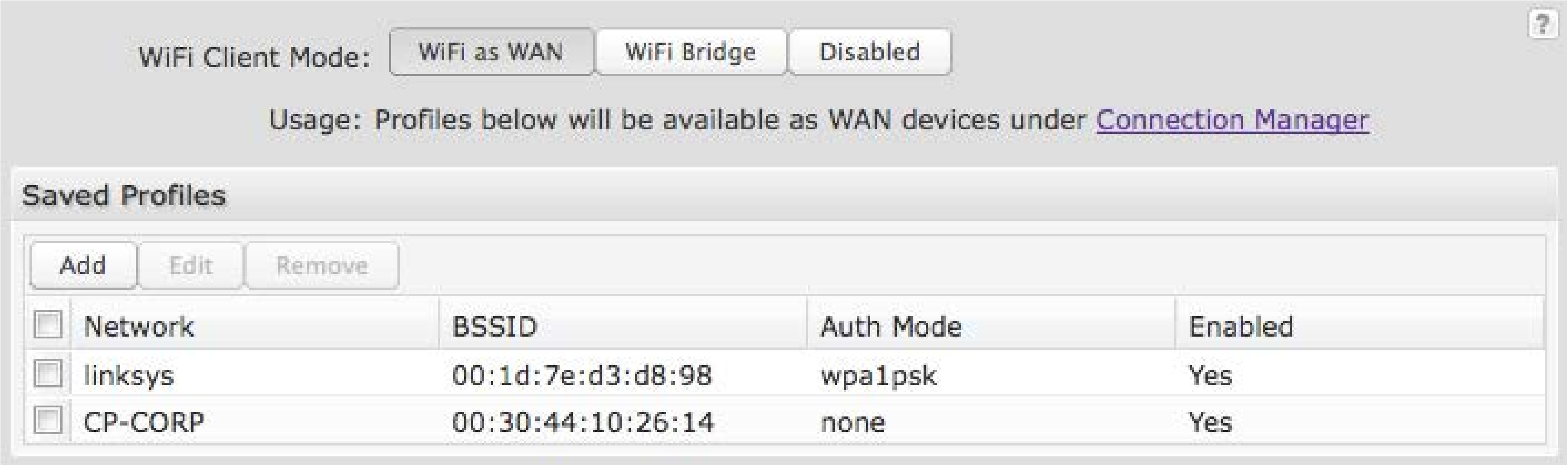
If one side of a planned VPN tunnel is behind a NAT (network address translation) firewall, the setup of your tunnel requires the following specifications:

1. Each side of the tunnel must use both a **Local Identity** and a **Remote Identity**. These must match the identities on the other side: The Local Identity must match the Remote Identity on the other side of the tunnel, and vice versa. In this case, these identities can each be a simple word.
2. The **Tunnel Name** for the side of the tunnel that is not behind the NAT firewall must be "anonymous".
3. The VPN tunnel must be initiated from the side that is behind the NAT firewall.

7.11 WiFi as WAN / Bridge

WiFi as WAN uses an outside WiFi network as its Internet source and then rebroadcasts its own local network. For example, the MBR1400 can create a private LAN using the public WiFi from a hotel as its WAN. **WiFi Bridge** functions similarly, but it rebroadcasts the original network – the router passes on the same settings and addresses already set up by the original NAT. **The WiFi as WAN and WiFi Bridge features cannot both be used at the same time.**

When either **WiFi as WAN** or **WiFi Bridge** is enabled, the MBR1400 will find other WiFi networks that you can select and connect to. Unless a selected WiFi source is on an unprotected network, you will need to know its password or key.



Usage: Profiles below will be available as WAN devices under Connection Manager

Saved Profiles

☐	Network	BSSID	Auth Mode	Enabled
☐	linksys	00:1d:7e:d3:d8:98	wpa1psk	Yes
☐	CP-CORP	00:30:44:10:26:14	none	Yes

All Cradlepoint routers and some other routers use the same default IP address for the primary network, 192.168.0.1. If you attempt to set up WiFi as WAN and there is an “IP conflict,” you need to change the IP address. The router is attempting to use the same IP address for both WAN and LAN, which is impossible. Go to **Network Settings → WiFi / Local Networks**. Select the network and click **Edit**. You can change the IP address under **IP Settings**. For example, you might change 192.168.**0**.1 to 192.168.**1**.1.

NOTE: Connecting to a corporate network with enterprise authentication requires a feature license and hardware version 2.0. Go to System **Settings → Feature Licenses** to enable this feature.

7.11.1 WiFi Bridge

When in **WiFi Bridge** mode with a configured profile, a WiFi Bridge device will be added to the local network interfaces, providing a way to bridge two LANs over a WiFi connection. For example, two separate Cradlepoint routers linked through WiFi Bridge mode allows you to have one WiFi-connected network in two separated sections of a large office building. This eliminates the need for extensive Ethernet cords to link the two routers, while allowing the full functionality of having one network.

A router that is using Bridge mode passes network information through from the partner access point, so typically DHCP and NAT should be disabled. The router will connect to the remote WiFi access point and enable the bridging of two LAN networks together over WiFi.

Under **Network Settings → WiFi / Local Networks**, choose the Local IP Network you want to attach this LAN interface to. Edit that Network, and under the "Interfaces" tab you will be able to see your WiFi Bridge profiles as "Available" interfaces.

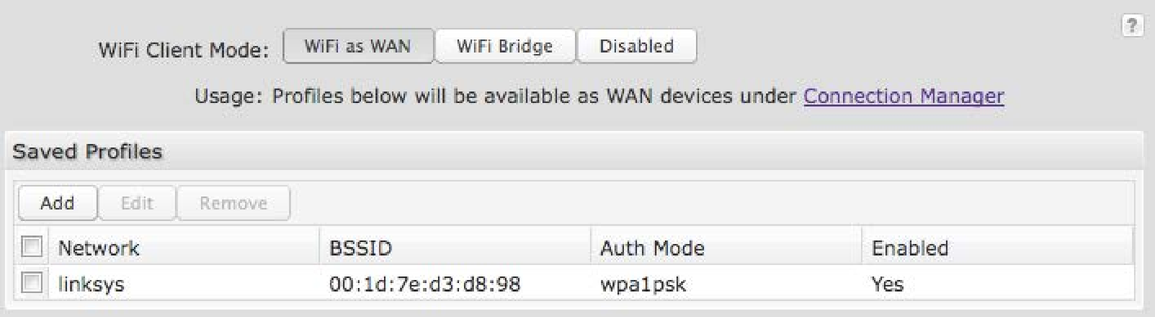
NOTE: The LAN IP address of this router and the attached WiFi access point cannot be the same address.

To set up WiFi Bridge, follow these steps:

1) In **Internet → WiFi as WAN / Bridge** under **WiFi Client Mode**, click on “WiFi Bridge” to enable this mode.
2) Your bridge network must be enabled under **Saved Profiles**. Either import the desired network from **Site Survey** or click **Add** to configure it.
3) Once WiFi Bridge is enabled and a bridge network is configured in **Saved Profiles**, go to **Network Settings → WiFi / Local Networks** and select a network from the Local IP Networks list. Click on **Edit** to open the **Local Network Editor** and find the **Interfaces** tab. Your configured bridge network should be listed in the “Available” section. Add this interface to your chosen network.
4) You need to turn off the DHCP Server. If you click **Submit** after attaching the WiFi bridge interface, a window will pop up asking you if you want to turn off the DHCP Server. You can also do this manually: click on the **DHCP Server** tab while still under **Network Settings → WiFi / Local Networks** in the **Local Network Editor**. Deselect “DCHP Server” to disable it.
5) Optional: Also under **Network Settings → WiFi / Local Networks** in the **Local Network Editor**, click on the **IP Settings** tab. Change the **Routing Mode** to “Disabled.” Changing the routing mode may improve security. You may also need to change the IP address to prevent IP conflict. Click **Submit** to save your configuration.

7.11.2 Saved Profiles

This is a list of WiFi networks that have already been configured as WAN sources (or Bridge profiles). The router will attempt to connect to any of these access points using the password you have configured. If more than one access point is in range, then the router will connect with the highest priority network.



WiFi Client Mode: WiFi as WAN | WiFi Bridge | Disabled

Usage: Profiles below will be available as WAN devices under Connection Manager

Saved Profiles

	Network	BSSID	Auth Mode	Enabled
□	linksys	00:1d:7e:d3:d8:98	wpa1psk	Yes

Network: The name (SSID, or Service Set Identifier) that is broadcast by the access point.

BSSID: The numeric ID of the network (Basic Service Set Identifier). This parameter is required when trying to connect to a hidden network using WiFi as WAN. It is optional when connecting to a visible network. If it is set in a profile, both the SSID and BSSID must match to connect to an access point. If the BSSID is not set in a profile, then the router will connect to any access point that matches the given SSID.

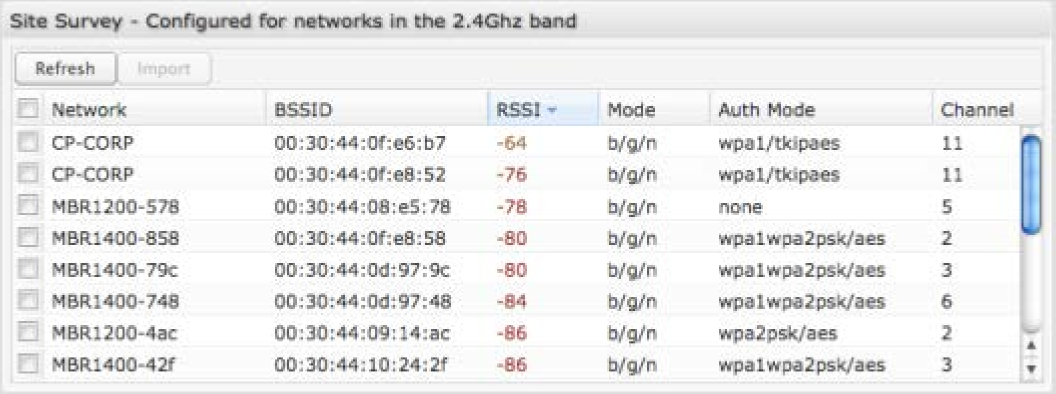
Auth Mode: The type of encryption that is used by the network.

- None
- WEP Auto
- WEP Open
- WEP Shared
- WPA1 Personal
- WPA2 Personal
- WPA1 & WPA2 Personal

7.11.3 Site Survey

This is a list of WiFi networks that the router can currently find, along with information about the network such as its mode and channel. If you click on a network in the **Site Survey**, you can import it as a saved profile. You can sort the list based on any of the fields by clicking on the field name.

Click “Refresh” if a WiFi network to which you want to connect is invisible. **Site Survey** only operates on the band—2.4 GHz or 5.0 GHz—that is currently configured in the WiFi advanced settings. In order to connect to networks in a different band, first switch the WiFi settings to that band (**Network Settings → WiFi / Local Networks** in **Advanced Mode**).



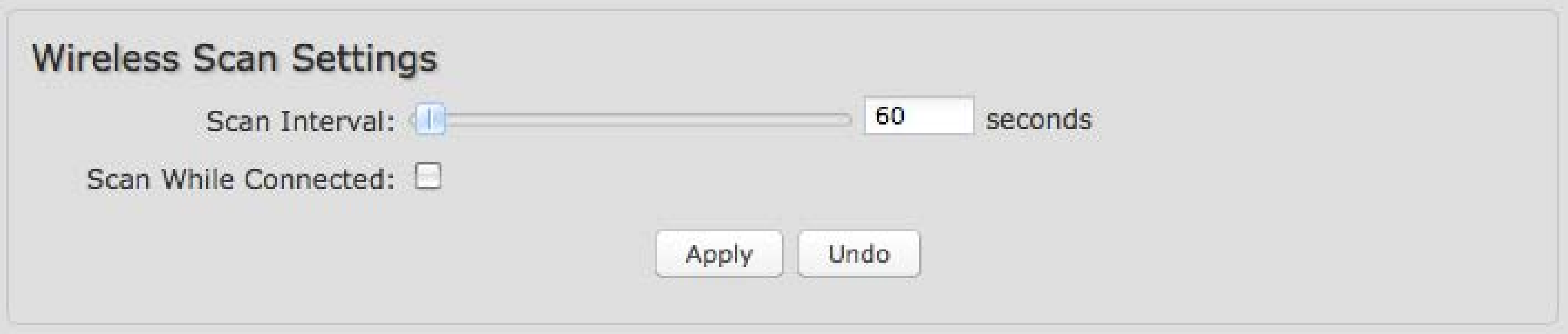
Site Survey - Configured for networks in the 2.4Ghz band

□	Network	BSSID	RSSI ▾	Mode	Auth Mode	Channel
□	CP-CORP	00:30:44:0f:e6:b7	-64	b/g/n	wpa1/tkipaes	11
□	CP-CORP	00:30:44:0f:e8:52	-76	b/g/n	wpa1/tkipaes	11
□	MBR1200-578	00:30:44:08:e5:78	-78	b/g/n	none	5
□	MBR1400-858	00:30:44:0f:e8:58	-80	b/g/n	wpa1wpa2psk/aes	2
□	MBR1400-79c	00:30:44:0d:97:9c	-80	b/g/n	wpa1wpa2psk/aes	3
□	MBR1400-748	00:30:44:0d:97:48	-84	b/g/n	wpa1wpa2psk/aes	6
□	MBR1200-4ac	00:30:44:09:14:ac	-86	b/g/n	wpa2psk/aes	2
□	MBR1400-42f	00:30:44:10:24:2f	-86	b/g/n	wpa1wpa2psk/aes	3

You have the option to manually add network profiles, but it is usually much easier to import them from **Site Survey**. Either click on **Add** under “**Saved Profiles**” or select a WiFi network in “**Site Survey**” and click **Import**.

If you import a network from **Site Survey**, most of the information about the network will already be completed. You need to input the password (if there is one) and then click submit to save the WiFi as WAN profile.

7.11.4 Wireless Scan Settings



Wireless Scan Settings

Scan Interval: 60 seconds

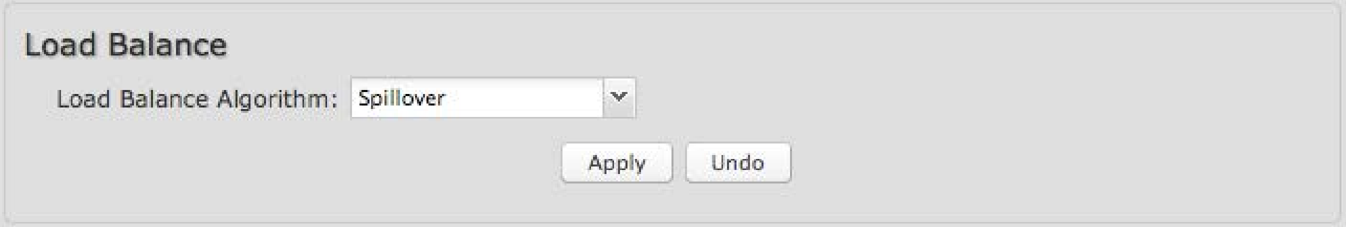
Scan While Connected: □

Scan Interval: How often WiFi as WAN scans the environment for updates. (Default: 60 seconds. Range: 5-3600 seconds.)

Scan While Connected: Continue to scan for WiFi as WAN profile updates when connected. Each time a scan occurs the wireless communication of the router will be temporarily interrupted. Normally this should be disabled.

7.12 WAN Affinity and Load Balancing

Load Balance


Load Balance

Load Balance Algorithm: Spillover

Select the Load Balance Algorithm from the following dropdown options:

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

WAN Affinity

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

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

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

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

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

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

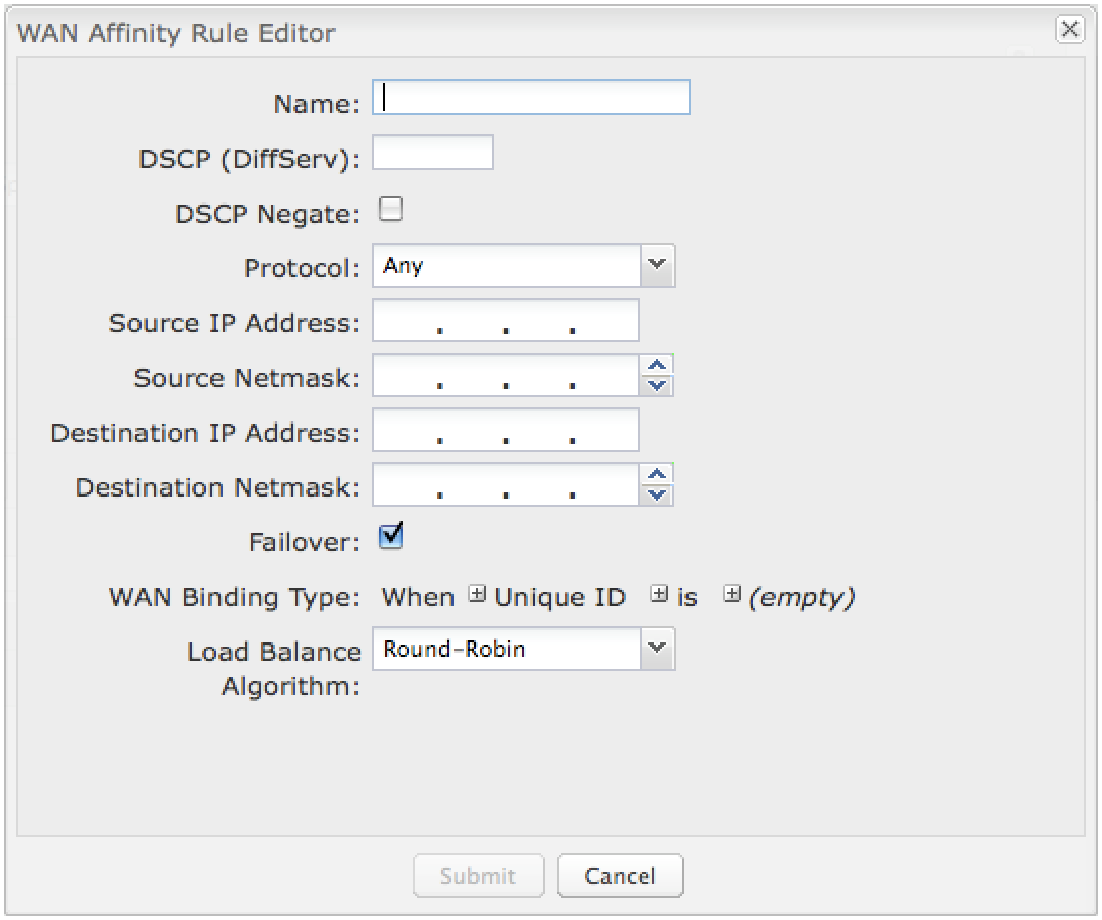
Protocol: Select from the dropdown list to specify the protocol for a particular data use. Otherwise, leave “Any” selected.

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

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

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

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



WAN Affinity Rule Editor

Name:

DSCP (DiffServ):

DSCP Negate: □

Protocol: Any

Source IP Address: . . .

Source Netmask: . . .

Destination IP Address: . . .

Destination Netmask: . . .

Failover: ☑

WAN Binding Type: When ⊞ Unique ID ⊞ is ⊞ *(empty)*

Load Balance Algorithm: Round-Robin

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.

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

- **Port:** Select from the dropdown list of possible WAN ports on the router.
  - WAN Ethernet
  - LAN Ethernet
  - Undefined
- **Manufacturer:** Select from a dropdown list of attached devices.
- **Model:** Select from a dropdown list of attached devices.
- **Type:** Select from the dropdown list of possible WAN types.
  - WiMAX
  - Modem
  - LTE
  - Ethernet
  - Wireless As WAN
- **Serial Number:** Select from a dropdown list of attached devices.
- **MAC Address:** Select from a dropdown list of attached devices.
- **Unique ID:** Select from a dropdown list of attached devices.

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

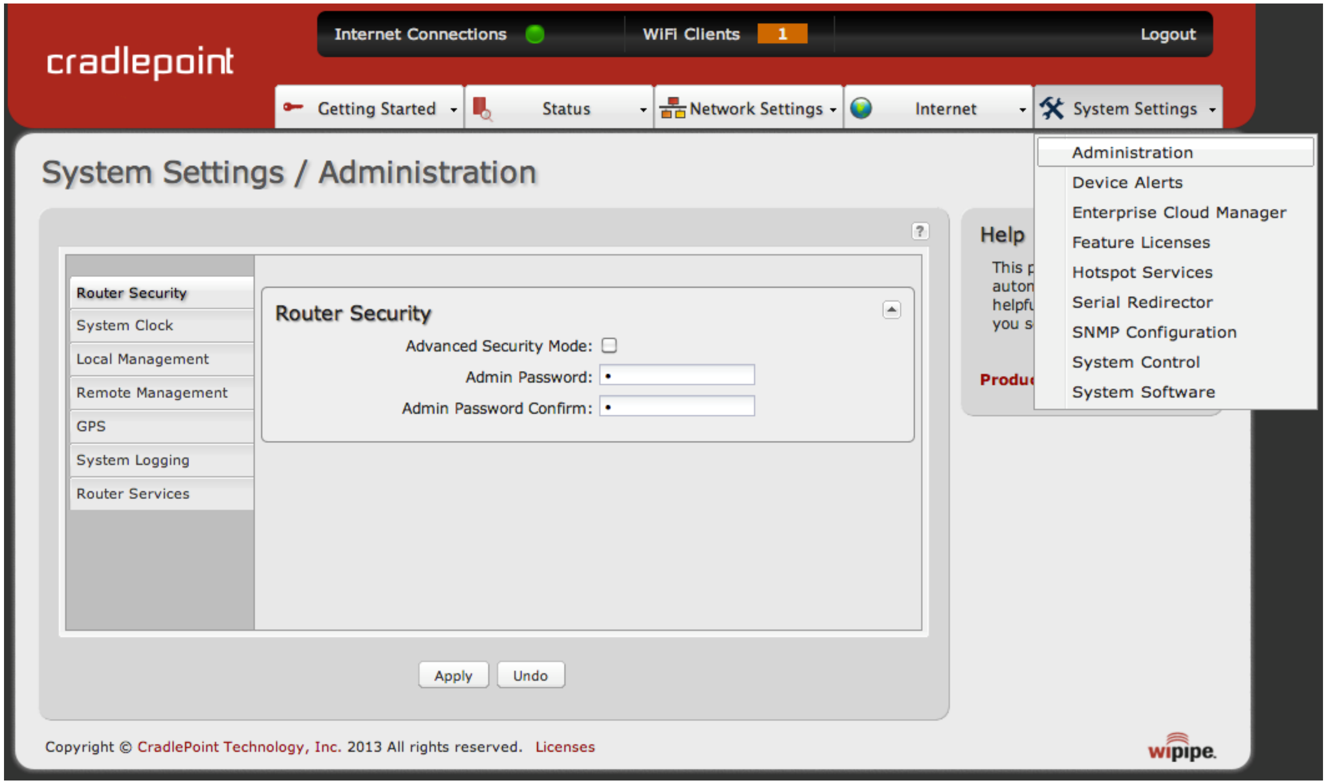
- **Round-Robin:** Evenly distribute each session to the available WAN connections.
- **Rate:** Distribute load based on the current upload and download rates. A WAN device's upload and download bandwidth values can be set in **Internet → Connection Manager**.
- **Spillover:** This was the default algorithm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

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

8 SYSTEM SETTINGS

The System Settings tab has the following submenu items that provide access to tools for broad administrative control of the MBR1400:

- Administration
- Device Alerts
- Enterprise Cloud Manager
- Feature Licenses
- Hotspot Services
- Serial Redirector
- SNMP Configuration
- System Control
- System Software



System Settings / Administration

Router Security

Advanced Security Mode: ☐

Admin Password: •

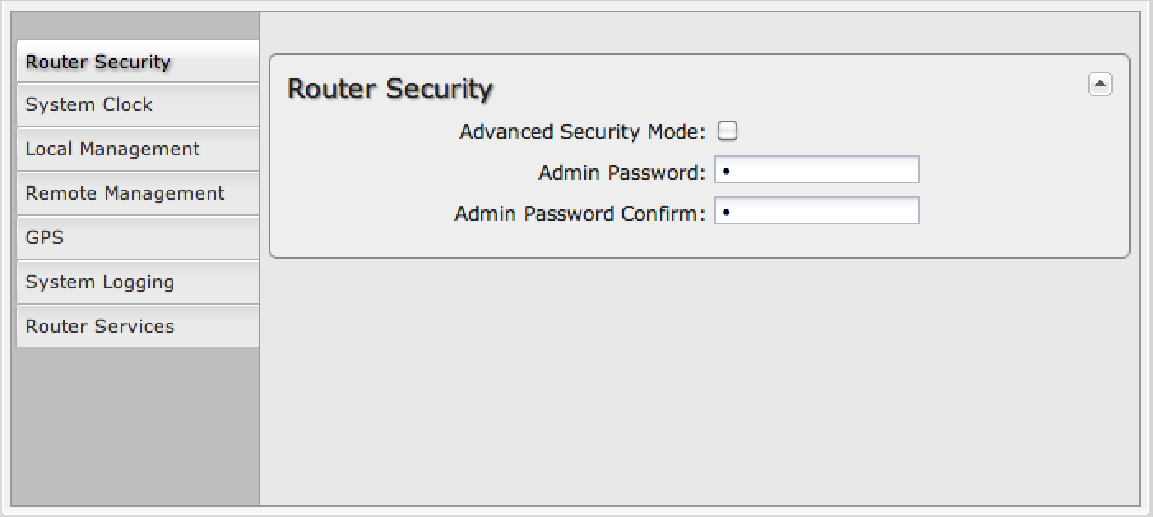
Admin Password Confirm: •

8.1 Administration

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

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

8.1.1 Router Security



Router Security

Advanced Security Mode: □

Admin Password: •

Admin Password Confirm: •

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

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

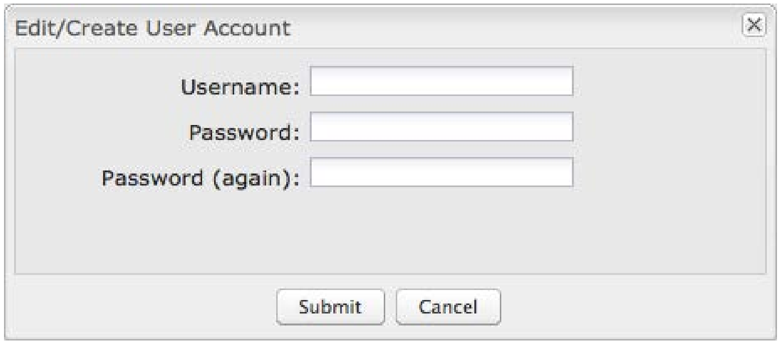
Advanced Security Mode

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

- Local Users
- TACACS+
- RADIUS

Local Users

Create users with administrative privileges by inputting usernames and passwords in the **Advanced User Management** table. The default username is “admin,” but you can edit this name, or delete it once you create other users (you can’t delete the user you are currently signed in as).



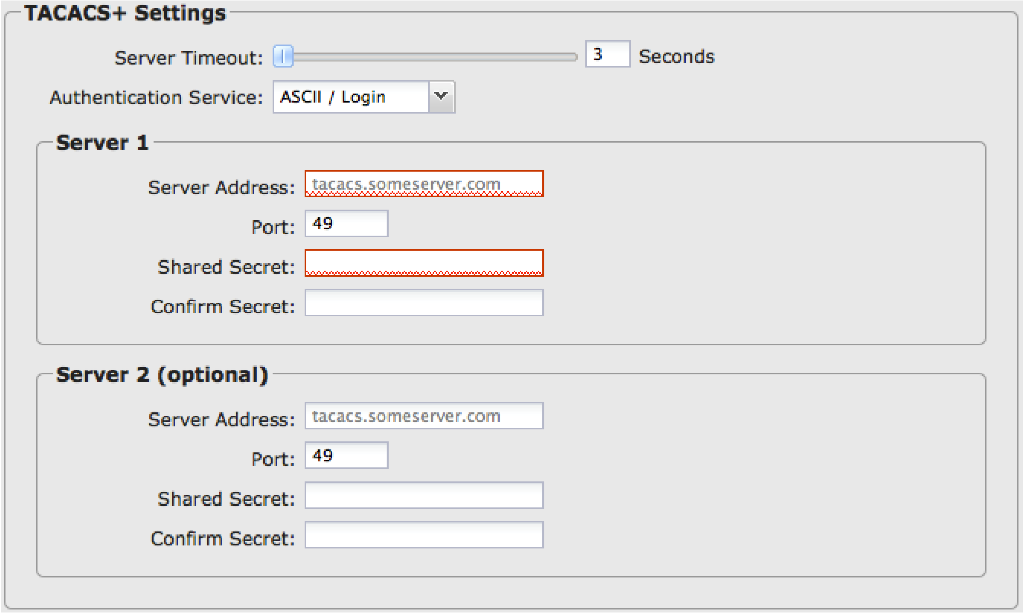
Edit/Create User Account

Username:

Password:

Password (again):

In **TACACS+** and **RADIUS** modes, if the servers cannot be reached, either because the **WAN** is down or a response is not received within the selected **Server Timeout**, the router will automatically fall back to using **Local Users** mode to prevent any potential of being locked out.



TACACS+ Settings

Server Timeout: 3 Seconds

Authentication Service: ASCII / Login

Server 1

Server Address: tacacs.someserver.com

Port: 49

Shared Secret:

Confirm Secret:

Server 2 (optional)

Server Address: tacacs.someserver.com

Port: 49

Shared Secret:

Confirm Secret:

TACACS+

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

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

Authentication Service: Choose from:

- ASCII / Login

- PAP
- CHAP

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

Port: Port 49 is default for TACACS+.

Shared Secret

RADIUS

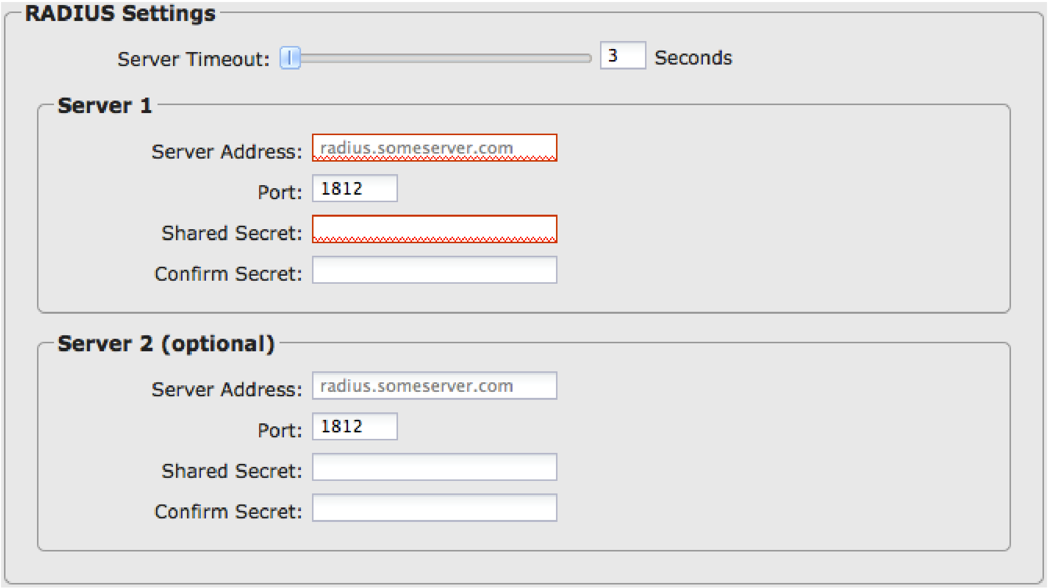
RADIUS stands for “Remote Authentication Dial In User Service”. The router will use a RADIUS server (or two, optionally) to authorize administration.

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

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

Port: Port 1812 is common for RADIUS servers.

Shared Secret



RADIUS Settings

Server Timeout: 3 Seconds

Server 1

Server Address: radius.someserver.com

Port: 1812

Shared Secret:

Confirm Secret:

Server 2 (optional)

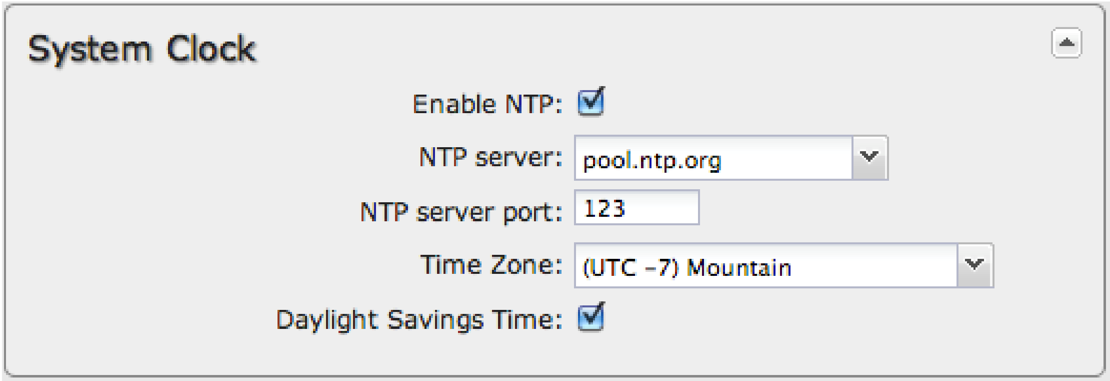
Server Address: radius.someserver.com

Port: 1812

Shared Secret:

Confirm Secret:

8.1.2 System Clock



System Clock

Enable NTP: ☑

NTP server: pool.ntp.org

NTP server port: 123

Time Zone: (UTC -7) Mountain

Daylight Savings Time: ☑

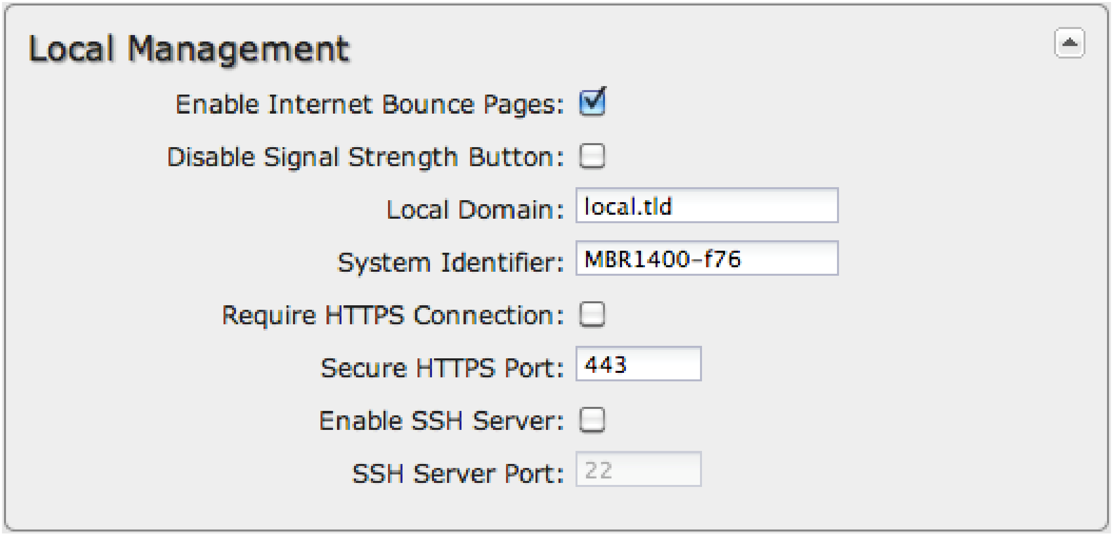
Enabling NTP will tell the router to get its system time from a remote server on the Internet. If you do not enable NTP then the router time will be based on when the router firmware was built, which is guaranteed to be wrong. Whenever the Internet connection is re-established and once a week thereafter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

8.1.3 Local Management



Local Management

Enable Internet Bounce Pages: ☑

Disable Signal Strength Button: □

Local Domain: local.tld

System Identifier: MBR1400-f76

Require HTTPS Connection: □

Secure HTTPS Port: 443

Enable SSH Server: □

SSH Server Port: 22

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.

Disable Signal Strength Button: This disables the Signal Strength button on the physical router.

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

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

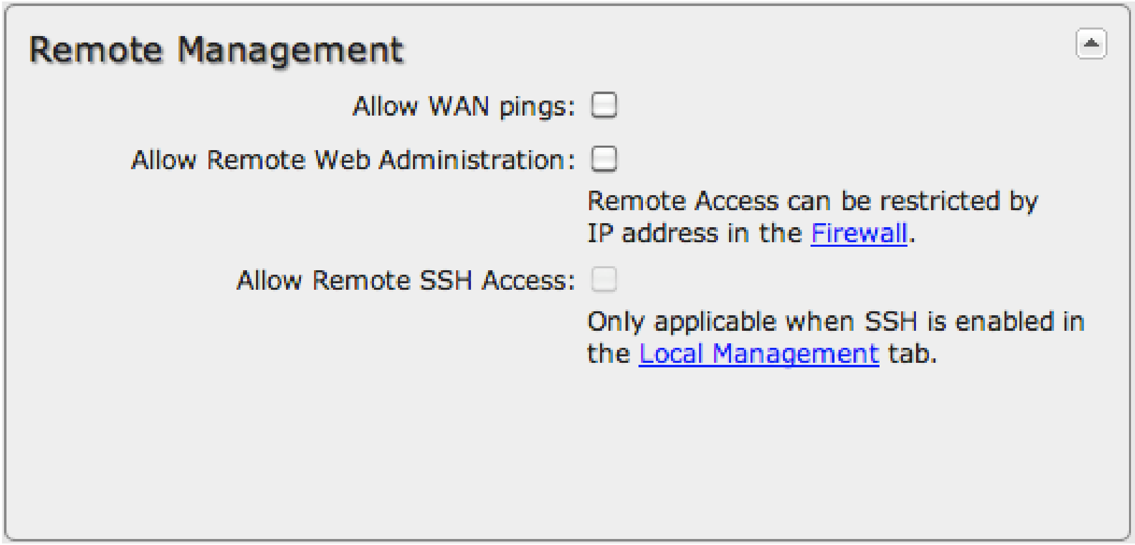
Require HTTPS Connection: Check this box if you want to encrypt all router administration communication.

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.

8.1.4 Remote Management



Remote Management

Allow WAN pings: □

Allow Remote Web Administration: □

Remote Access can be restricted by IP address in the Firewall.

Allow Remote SSH Access: □

Only applicable when SSH is enabled in the Local Management tab.

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

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

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

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

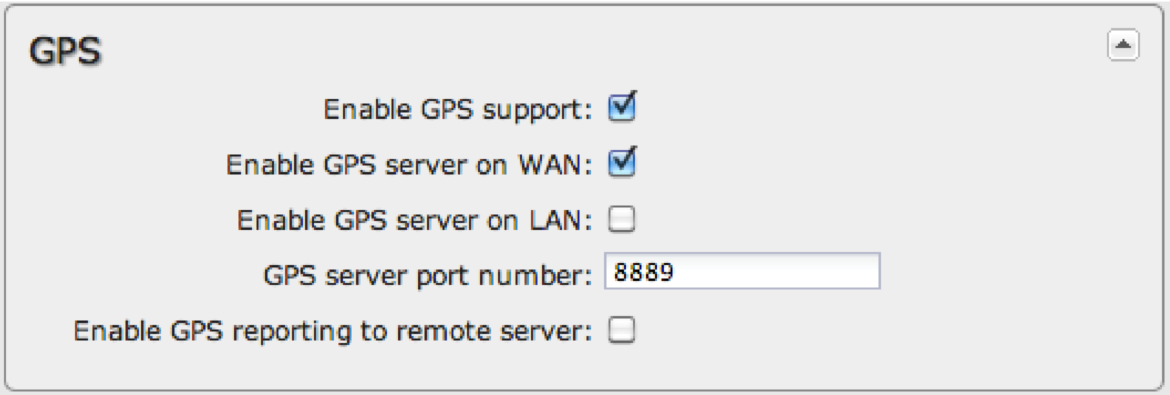
NOTE: You can restrict remote access to only specified IP addresses in **Network Settings → Firewall** under Remote Administration Access Control.

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

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

8.1.5 GPS

If you have an attached device with GPS support (SIM-based models with GPS support require the SIM be inserted), you can enable a graphical view of your router's location which will appear in **Status → GPS**.



GPS

Enable GPS support: ☑

Enable GPS server on WAN: ☑

Enable GPS server on LAN: □

GPS server port number: 8889

Enable GPS reporting to remote server: □

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

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

- **Enable GPS support:** Enables support for querying GPS information from supported modems.
- **Enable GPS server on WAN:** Enables a TCP server on the WAN side of the firewall, which will periodically send GPS NMEA sentences to connected clients.
- **Enable GPS server on LAN:** Enables a TCP server on the LAN side of the firewall, which will periodically send GPS NMEA sentences to connected clients.
  - **GPS server port number**
- **Enable GPS reporting to remote server:** Enables periodic reporting of GPS NMEA sentences to a remote server. The router will buffer NMEA data if errors are encountered or if the Internet connection goes down and send the buffered sentences when the connection is restored.
  - **Remote server hostname or IP**
  - **Remote server port**
  - **Report only over specific time interval:** Restricts the NMEA sentence reporting to a remote server to a specific time interval.

The following GPS spec is copied from http://aprs.gids.nl/nmea/

8.1.6 $GPGGA – Global Positioning System Fix Data

Name	Example Data	Description
Sentence Identifier	$GPGGA	Global Positioning System Fix Data
Time	170834	17:08:34 Z
Latitude	4124.8963, N	41d 24.8963' N or 41d 24' 54" N
Longitude	08151.6838, W	81d 51.6838' W or 81d 51' 41" W
Fix Quality: - 0 = Invalid - 1 = GPS fix - 2 = DGPS fix	1	Data is from a GPS fix
Number of Satellites	05	5 Satellites are in view
Horizontal Dilution of Precision (HDOP)	1.5	Relative accuracy of horizontal position
Altitude	280.2, M	280.2 meters above mean sea level
Height of geoid above WGS84 ellipsoid	-34.0, M	-34.0 meters
Time since last DGPS update	blank	No last update
DGPS reference station id	blank	No station id
Checksum	*75	Used by program to check for transmission errors

Courtesy of Brian McClure, N8PQI.

Global Positioning System Fix Data. Time, position, and fix related data for a GPS receiver.

eg2. $--GGA,hhmmss.ss,llll.ll,a,yyyyy.yy,a,x,xx,x.x,x.x,M,x.x,M,x.x,xxxx

hhmmss.ss = UTC of position
llll.ll = latitude of position
a = N or S
yyyyy.yy = Longitude of position
a = E or W
x = GPS Quality indicator (0=no fix, 1=GPS fix, 2=Dif. GPS fix)
xx = number of satellites in use
x.x = horizontal dilution of precision
x.x = Antenna altitude above mean-sea-level
M = units of antenna altitude, meters
x.x = Geoidal separation
M = units of geoidal separation, meters
x.x = Age of Differential GPS data (seconds)
xxxx = Differential reference station ID

eg3. $GPGGA,hhmmss.ss,llll.ll,a,yyyyy.yy,a,x,xx,x.x,x.x,M,x.x,M,x.x,xxxx*hh

1 = UTC of Position
2 = Latitude
3 = N or S
4 = Longitude
5 = E or W
6 = GPS quality indicator (0=invalid; 1=GPS fix; 2=Diff. GPS fix)
7 = Number of satellites in use [not those in view]
8 = Horizontal dilution of position
9 = Antenna altitude above/below mean sea level (geoid)
10 = Meters (Antenna height unit)

11 = Geoidal separation (Diff. between WGS-84 earth ellipsoid and mean sea level. -=geoid is below WGS-84 ellipsoid)
12 = Meters (Units of geoidal separation)
13 = Age in seconds since last update from diff. reference station
14 = Diff. reference station ID#
15 = Checksum

8.1.7 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 on 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:

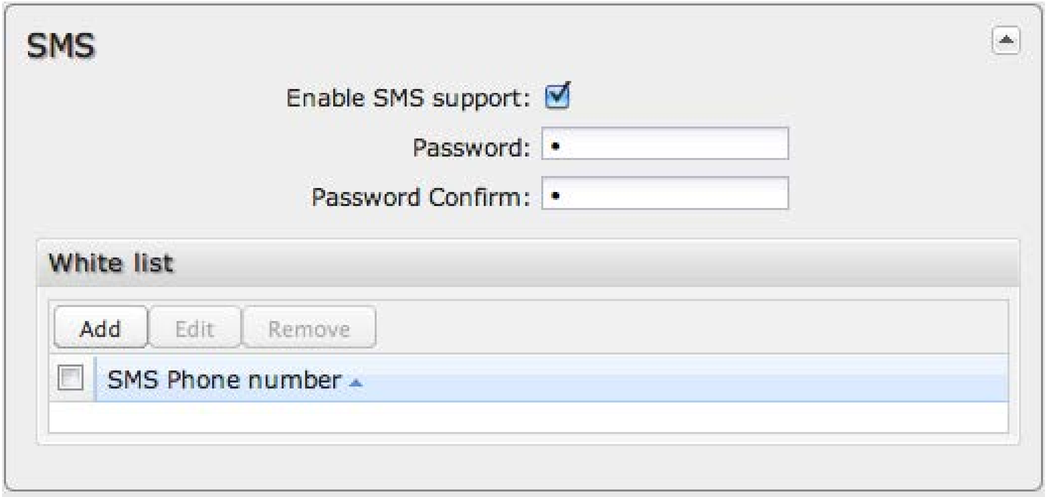
- Messages are limited to 160 characters.
- SMS is not a guaranteed delivery protocol. The carriers do not guarantee that the SMS message will be delivered to the modem or that the modem’s response will be delivered to the sender. This means an administrator might have to send messages multiple times 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 8 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).



SMS

Enable SMS support: ☑

Password: •

Password Confirm: •

White list

□ SMS Phone number

White List

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

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

How to Send an SMS Message

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

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

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

How to Text from a Phone

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

How to Text from an Email

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

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

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

SMS Commands

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

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

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

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

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

Supported Commands:

reboot: Reboot the router (not the modem)

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

restore: Restore the router to factory defaults

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

rstatus: Get router status

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

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

Example of response:

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

mstatus: Get modem status*

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

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

Example of response:

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

mreboot: Reboot the modem*

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

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

- Syntax: <password>,apn,<new APN>,[port,]
- Example: 1234,apn,myapn@apn.com, //set APN of highest priority modem
- Example: 1234,apn,myapn@apn.com,usb1, //set APN for modem in port usb1

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

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

simpin: Set the SIM's PIN*

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

log: Return a portion of the router log

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

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

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

Sample Debug Session

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

Figure out the state of the modems on the router:

1234,rstatus,

Receive the modem’s status and settings:

1234,mstatus,

Set the modem’s APN to the correct setting:

1234,apn,broadband,

Verify the APN was set properly:

1234,mstatus,

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

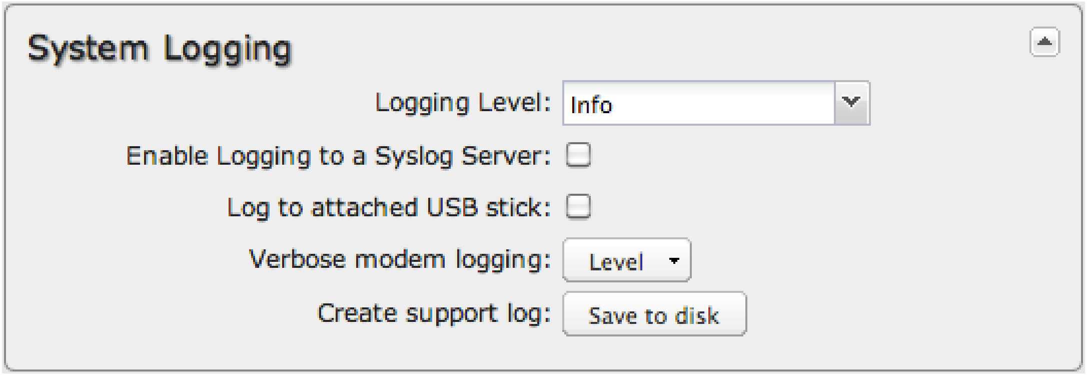
1234,rstatus,

8.1.8 System Logging

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

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

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).



System Logging

Logging Level: Info

Enable Logging to a Syslog Server: □

Log to attached USB stick: □

Verbose modem logging: Level

Create support log: Save to disk

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

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

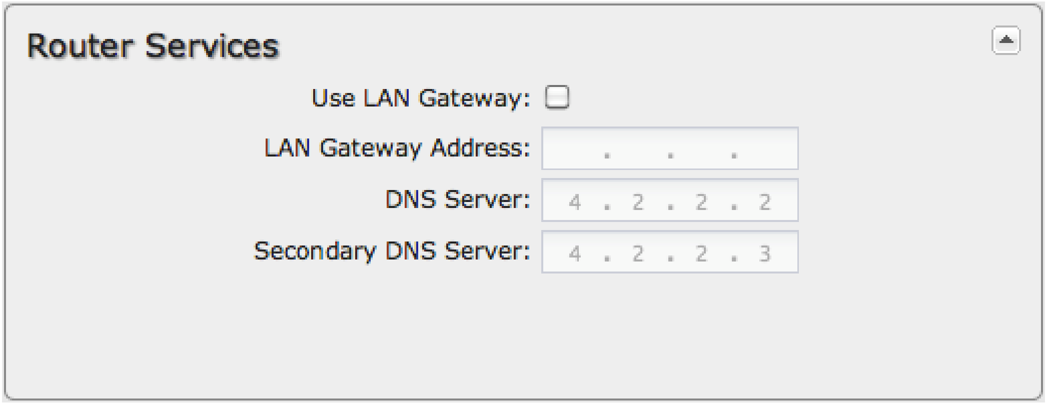
Include UTF8 Byte Order Mark: The log message is sent using UTF-8 encoding. By default the router will attach the Unicode Byte Order Mark (BOM) to the Syslog message in compliance with the Syslog protocol, RFC5424. Some Syslog servers may not fully support RFC5424 and will treat the BOM as ASCII text,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

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

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

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

8.1.9 Router Services



Router Services

Use LAN Gateway: □

LAN Gateway Address: . . .

DNS Server: 4 . 2 . 2 . 2

Secondary DNS Server: 4 . 2 . 2 . 3

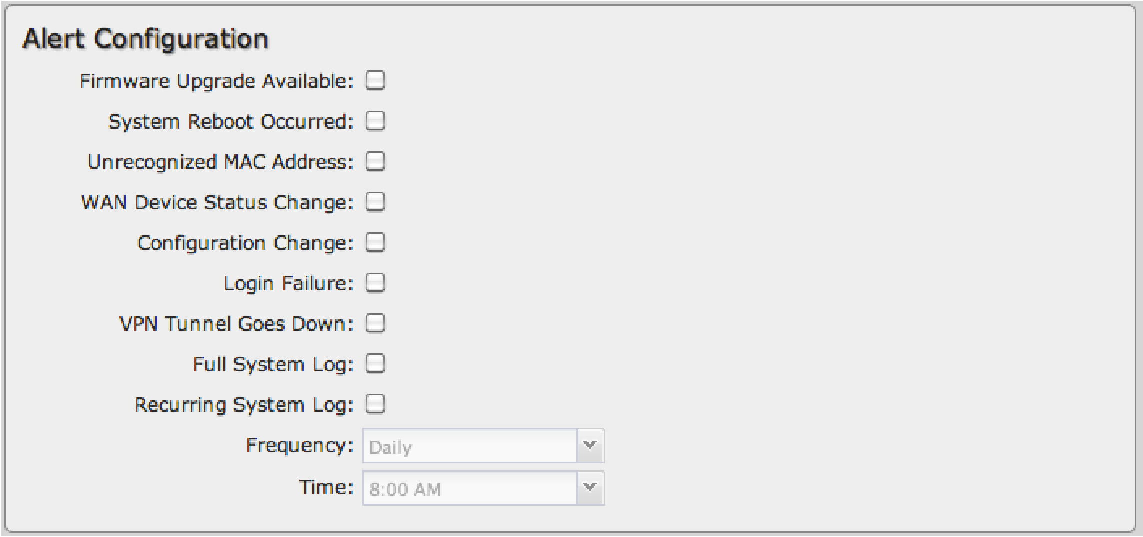
By default, router services (Enterprise Cloud Manager, NTP, etc.) connect to the router via the WAN. In some setups it makes sense to use the LAN instead. For example, if your router is used strictly for 3G/4G failover behind another router, you may not want to use 3G/4G data unnecessarily. Select **Use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

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

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

8.2 Device Alerts

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



Alert Configuration

Firmware Upgrade Available: □
System Reboot Occurred: □
Unrecognized MAC Address: □
WAN Device Status Change: □
Configuration Change: □
Login Failure: □
VPN Tunnel Goes Down: □
Full System Log: □
Recurring System Log: □
Frequency: Daily
Time: 8:00 AM

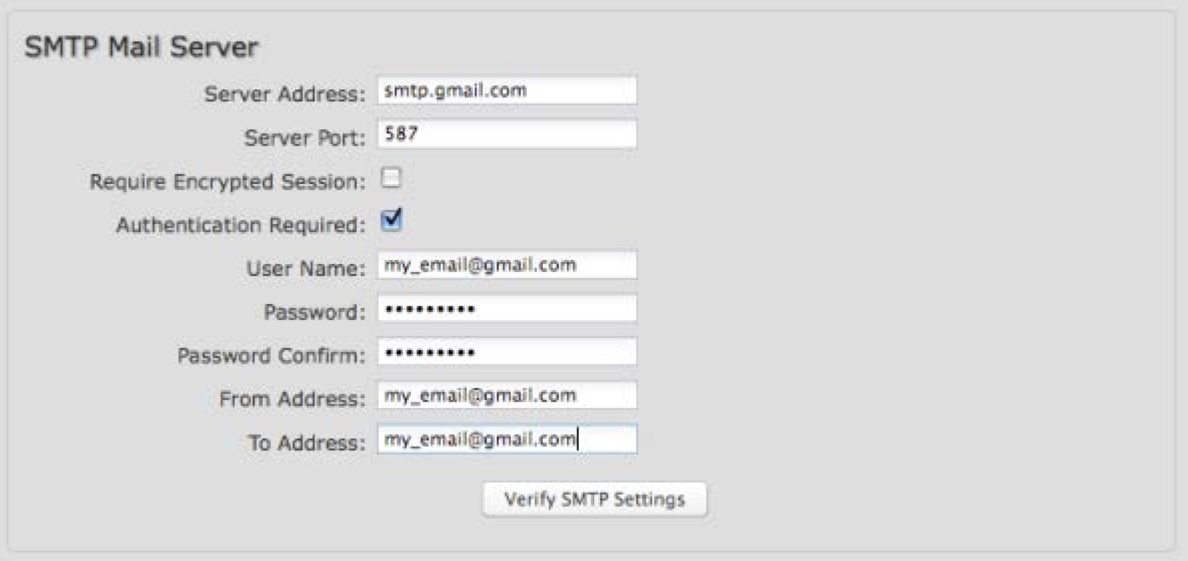
- **Firmware Upgrade Available:** A firmware update is available for this device.
- **System Reboot Occurred:** This router has rebooted. This depends on NTP being enabled and available to report the correct time.
- **Unrecognized MAC Address:** Used with the MAC monitoring lists. An alert is sent when 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 Failure:** A failed login attempt has been detected.
- **VPN Tunnel Goes Down:** Sends an alert when a VPN tunnel goes down.
- **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.

8.2.1 SMTP Mail Server

Since the MBR1400 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 MBR1400 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



SMTP Mail Server

Server Address: smtp.gmail.com

Server Port: 587

Require Encrypted Session: ☐

Authentication Required: ☑

User Name: my_email@gmail.com

Password: ••••••••••

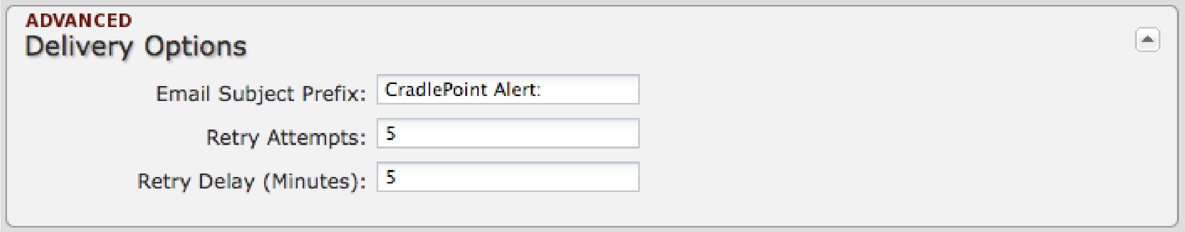
Password Confirm: ••••••••••

From Address: my_email@gmail.com

To Address: my_email@gmail.com

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

Advanced: **Delivery Options**



ADVANCED
Delivery Options

Email Subject Prefix:	CradlePoint Alert:
Retry Attempts:	5
Retry Delay (Minutes):	5

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

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

Retry Delay: The delay between retry attempts.

8.3 Enterprise Cloud Manager

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

Key features include:

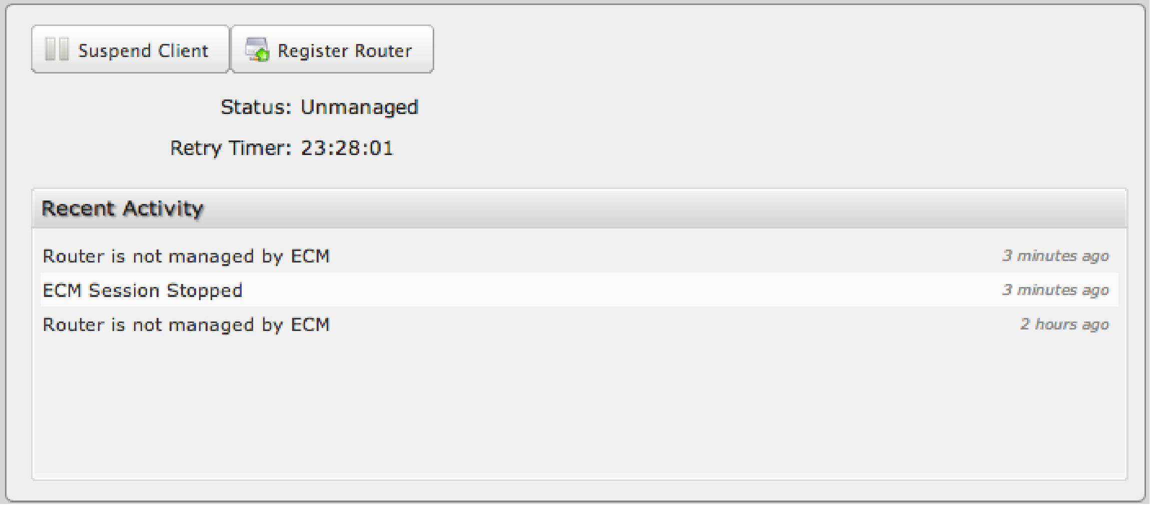
- Group based configuration management
- Health monitoring of router connectivity and data usage
- Remote management and control of routers
- Historical record keeping of device logs and status

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

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

Registering Your Router

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



Status: Unmanaged

Retry Timer: 23:28:01

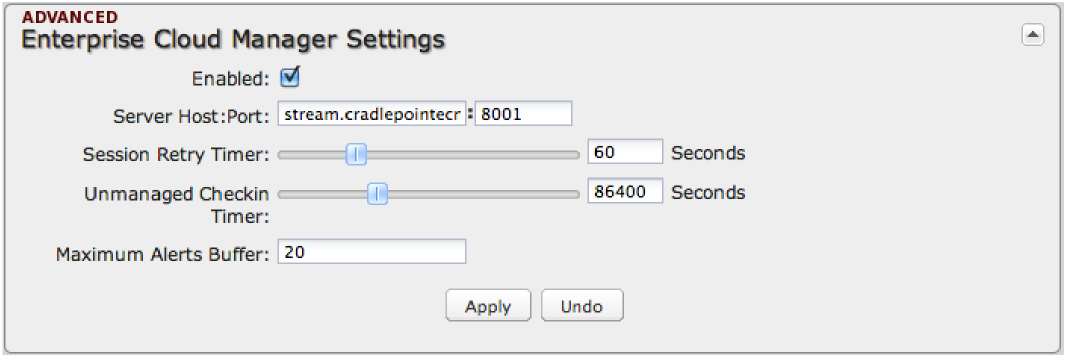
Recent Activity

Router is not managed by ECM	*3 minutes ago*
ECM Session Stopped	*3 minutes ago*
Router is not managed by ECM	*2 hours ago*

Suspending the ECM Client

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

8.3.1 Enterprise Cloud Manager Settings (Advanced)



ADVANCED

Enterprise Cloud Manager Settings

Enabled: ☑

Server Host:Port: stream.cradlepointecr : 8001

Session Retry Timer: 60 Seconds

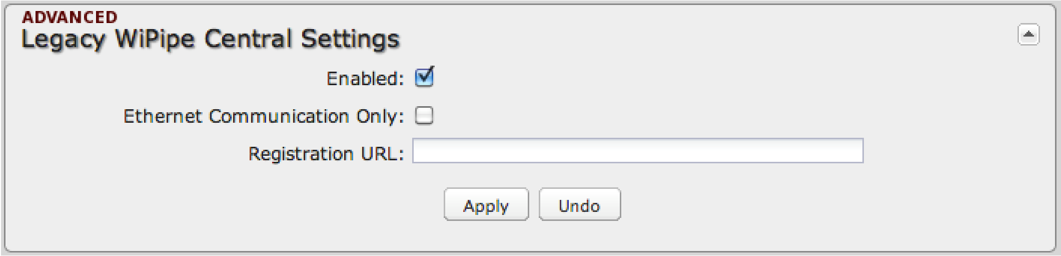
Unmanaged Checkin Timer: 86400 Seconds

Maximum Alerts Buffer: 20

- **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.

8.3.2 Legacy WiPipe Central Settings (Advanced)

WiPipe Central is Cradlepoint's legacy remote management system.



ADVANCED

Legacy WiPipe Central Settings

Enabled: ☑

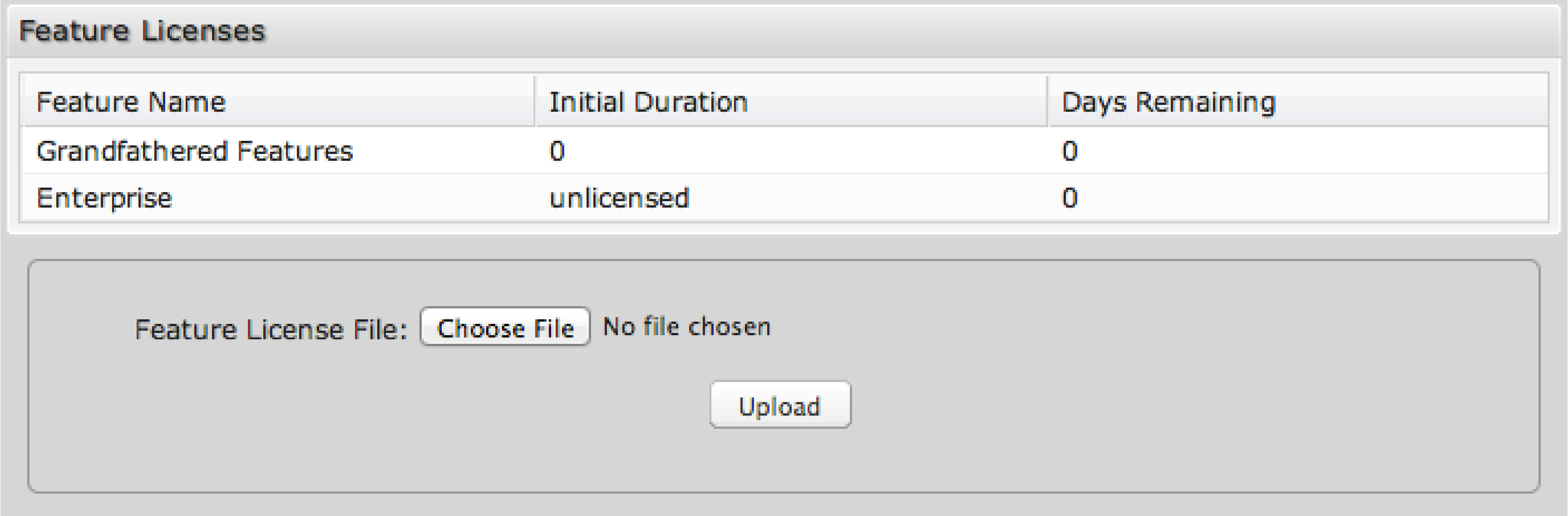
Ethernet Communication Only: □

Registration URL:

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

8.4 Feature Licenses

Some Cradlepoint features may require a license. These features are disabled by default. To obtain a feature license, contact your Cradlepoint sales representative.



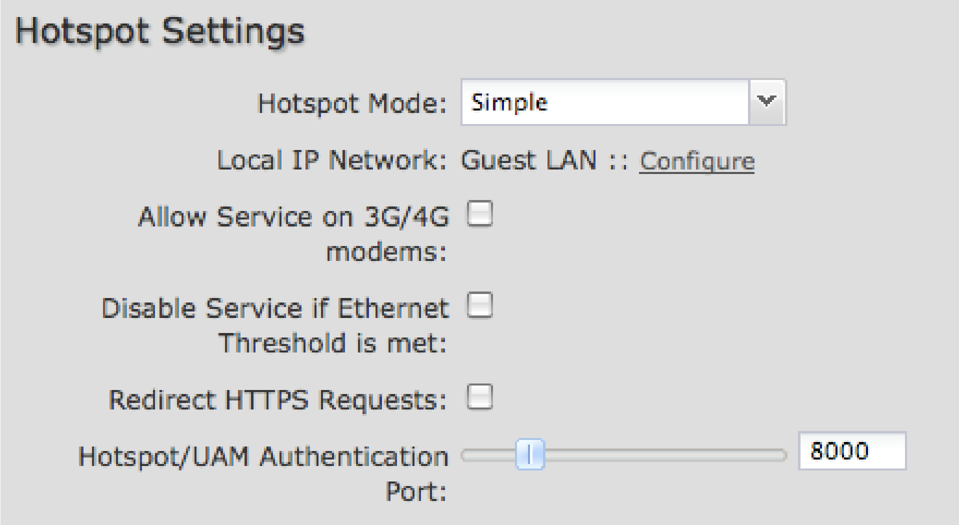
Feature Licenses

Feature Name	Initial Duration	Days Remaining
Grandfathered Features	0	0
Enterprise	unlicensed	0

Feature License File: Choose File No file chosen

Once you have obtained the feature license file, upload the file to enable the feature. A reboot is required after uploading a feature license file.

8.5 Hotspot Services



Hotspot Settings

Hotspot Mode: Simple

Local IP Network: Guest LAN :: Configure

Allow Service on 3G/4G modems: □

Disable Service if Ethernet Threshold is met: □

Redirect HTTPS Requests: □

Hotspot/UAM Authentication Port: 8000

Any of your networks can be enabled as a hotspot. To enable a hotspot, you need to select a network and set it as a hotspot in **Network Settings → WiFi / Local Networks**.

NOTE: Although any network can be a hotspot, the MBR1400 allows only one hotspot.

Hotspot Mode: Choose from the following dropdown options:

- **Simple:** Allows "Terms of Use" page and timeout settings controlled within the router.
- **RADIUS/UAM:** Allows you to set up external authentication servers.

Local IP Network: A single LAN Group—including both WiFi and Ethernet—can be configured as your hotspot. If you do not already have a LAN Group configured as a hotspot, go to the WiFi / Local Networks page (you can click **Configure** to link to this page) and set the **Routing Mode** to "Hotspot" for the LAN Group you want to use.

NOTE: Routing Mode is in the Local Network Editor under the IP Settings tab. Select a network in **Network Settings → WiFi / Local Networks** and click **Edit** to open the Local Network Editor. The IP Settings tab will already be open: the Routing Mode dropdown menu is at the bottom.

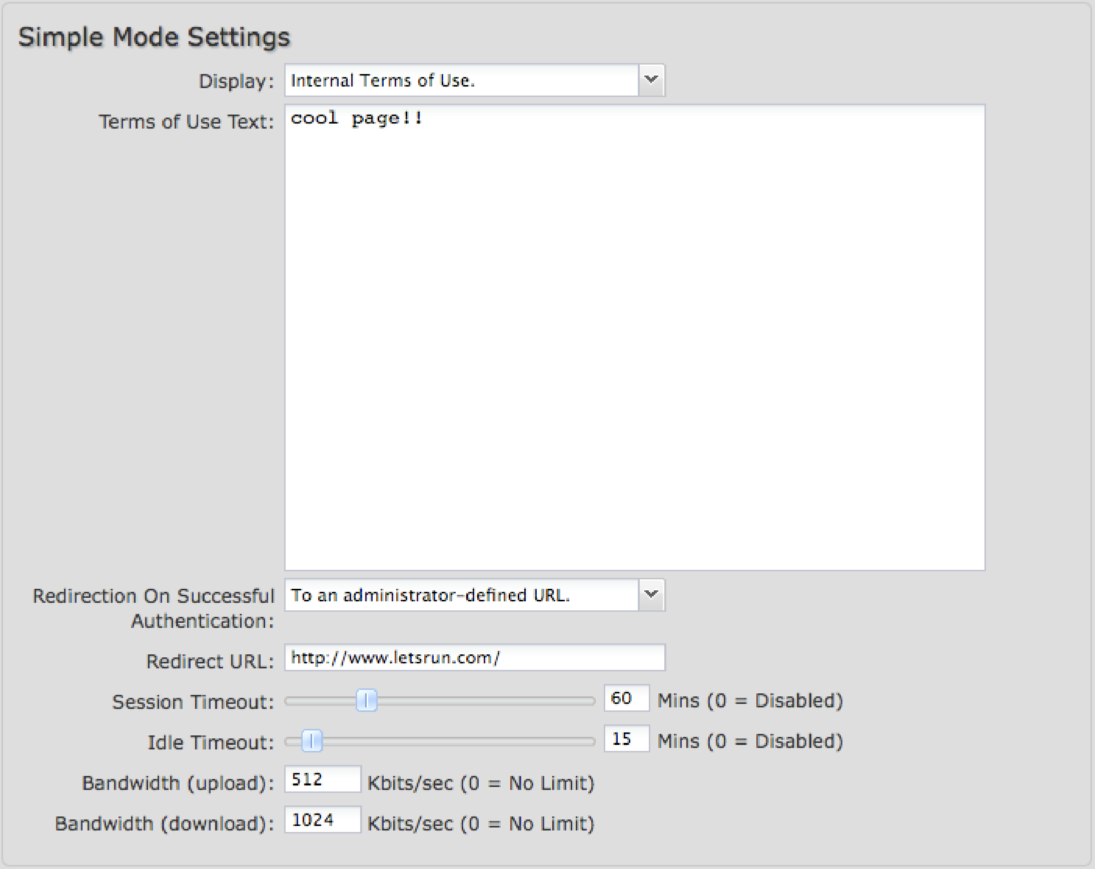
Allow Service on 3G/4G Modems: Allows you to enable or disable hotspot access to the Internet over a modem. This is often used if the router has a main wired link and a secondary modem for failover (typically with a more expensive/limited data plan). Select this option if you want the router to allow data traffic over the modem if the wired connection goes down.

Disable Service if Ethernet Threshold is met: This will block Hotspot use of the WAN when the threshold is met. This can be used if the router is being used as a backup failover connection to another router with a wired connection. If that other router's wired connection goes down and it starts using this router for its primary connection, then disable Hotspot use of the WAN connection. Set the limiting **Rate** (KB/s) and **Time Period** (seconds).

Redirect HTTPS Requests: This allows initial requests to HTTPS websites to be redirected appropriately.

Hotspot/UAM Authentication Port: Default: 8000. Type in a different port number, or use the slider to change the port.

8.5.1 Simple Mode Settings



Simple Mode Settings

Display: Internal Terms of Use.

Terms of Use Text: cool page!!

Redirection On Successful Authentication: To an administrator-defined URL.

Redirect URL: http://www.letsrun.com/

Session Timeout: 60 Mins (0 = Disabled)

Idle Timeout: 15 Mins (0 = Disabled)

Bandwidth (upload): 512 Kbits/sec (0 = No Limit)

Bandwidth (download): 1024 Kbits/sec (0 = No Limit)

Display: This section allows you to choose if a "Terms of Use" page will be given to the user connecting to the hotspot.

- **Internal Terms of Use.** Fill in your own terms of use.
- **External Terms of Use.** Specify a URL that has the Terms of Use page. Users will automatically be directed to this page.
- **No Terms of Use. Redirect Only.**

Redirection on Successful Authentication: Depending on your choice for the “Terms of Use” page, your have further options for where the user will be directed. After the user accepts the terms, you can either let him/her continue to the URL they were trying to reach or you can force the user to go to a specified URL once before continuing on.

- **To the URL the user intended to visit.**
- **To an administrator-defined URL.**

Redirect URL: If you have chosen to send users to an administrator-defined URL, you will need to specify the address.

Session Timeout: (Default: 60 minutes.) The amount of time the user may use the router before being forced to authenticate again.

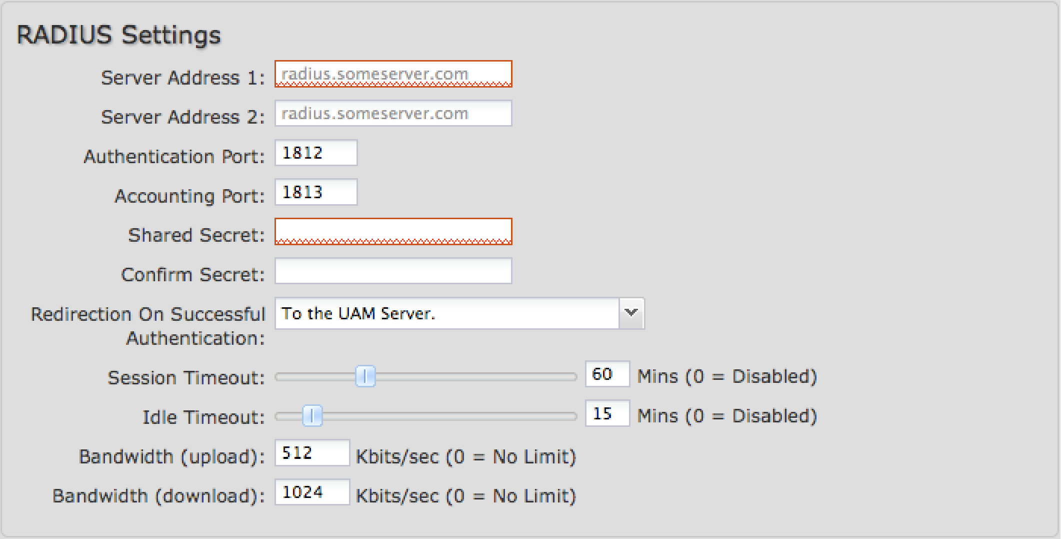
Idle Timeout: (Default: 15 minutes.) If the user is idle for this amount of time, make them re-authenticate.

Bandwidth (upload): (Default: 512 Kbits/sec.) The data rate limit for users uploading data through the hotspot.

Bandwidth (download): (Default: 1024 Kbits/sec.) The data rate limit for users downloading data through the hotspot.

8.5.2 RADIUS/UAM Settings

This section allows you to configure a RADIUS and Universal Access Method server. After the user accepts the terms, you can either let him/her continue to the URL they were trying to reach or you can force the user to go to a specified UAM Server or URL once before continuing on.



RADIUS Settings

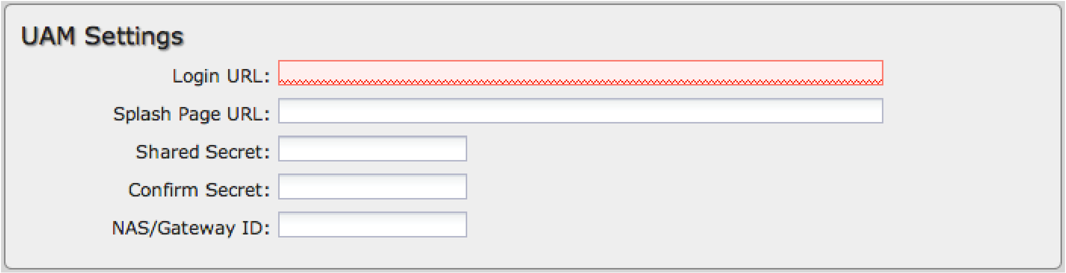
Server Address 1:	radius.someserver.com
Server Address 2:	radius.someserver.com
Authentication Port:	1812
Accounting Port:	1813
Shared Secret:	
Confirm Secret:	
Redirection On Successful Authentication:	To the UAM Server.
Session Timeout:	60 Mins (0 = Disabled)
Idle Timeout:	15 Mins (0 = Disabled)
Bandwidth (upload):	512 Kbits/sec (0 = No Limit)
Bandwidth (download):	1024 Kbits/sec (0 = No Limit)

RADIUS settings:

- **Server Address 1:** Assigned by RADIUS service.
- **Server Address 2:** This is an optional backup server.
- **Authentication Port:** The standard port number, 1812, will usually be sufficient.
- **Accounting Port:** The standard port number, 1813, will usually be sufficient.
- **Shared Secret:** Assigned by RADIUS service.
- **Redirection On Successful Authentication:** Choose from the dropdown list of options for redirection:
  - Redirect to the UAM Server.
  - Redirect to the URL that the user intends to visit.
  - Redirect to the following URL (input the desired URL).
- **Session Timeout:** (Default: 60 minutes.) The amount of time the user may use the router before being forced to authenticate again. This value can be overwritten by the RADIUS server.
- **Idle Timeout:** (Default: 15 minutes.) If the user is idle for this amount of time, make them re-authenticate.
- **Bandwidth (upload):** (Default: 512 Kbits/sec.) The data rate limit for users uploading data through the hotspot.
- **Bandwidth (download):** (Default: 1024 Kbits/sec.) The data rate limit for users downloading data through the hotspot.

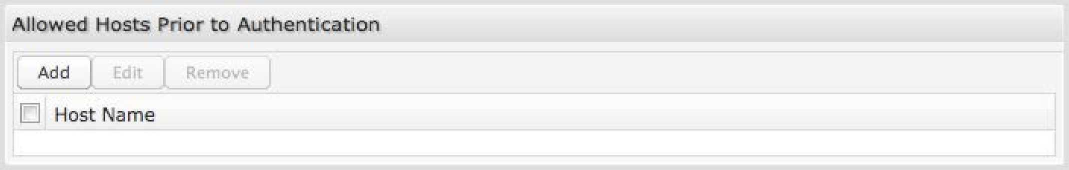
UAM Settings:

- **Login URL:** Assigned by UAM service.
- **Splash Page URL:** Optional URL that can point to an external page that can provide specific information to the user prior to being authenticated. The page **must** provide a link back to the **Login URL** in order for the user to be authenticated. For example - http://***lan ip address:uam port***/prelogin or http://192.168.10.1:8000/prelogin.
- **Shared Secret:** Optional, depending on the UAM service.
- **NAS/Gateway ID:** Assigned by UAM service.



8.5.3 Allowed Hosts Prior to Authentication

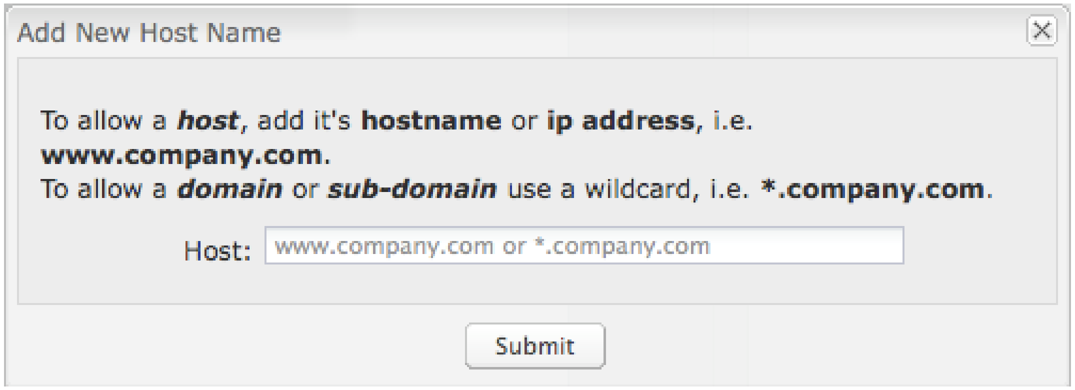
Adding host names to this list will **allow** access from your network to any external domain or website prior to being authenticated. For example, a hotel might allow access to its own website prior to authentication.



Click **Add** to enter new hostnames you wish to allow.

Enter the Host or Domain Name of the website you wish to **allow**, i.e. **www.company.com** or **company.com**. To allow all domain and sub-domain options, use a wildcard, i.e. ***.company.com.**

Click **Submit** to save your additions.



To allow a ***host***, add it's **hostname** or **ip address**, i.e. **www.company.com**.
To allow a ***domain*** or ***sub-domain*** use a wildcard, i.e. ***.company.com**.

Host: www.company.com or *.company.com

8.5.4 Authorized MAC Addresses

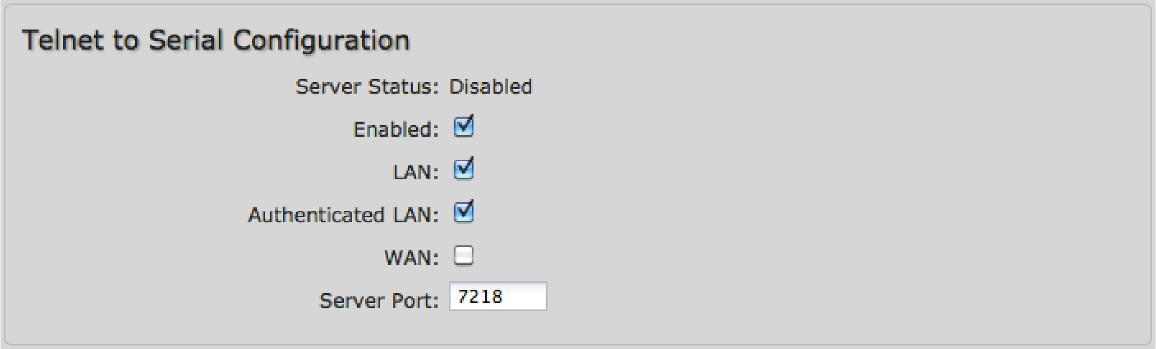
Add the MAC addresses of trusted machines to which you want to give automatic access through the Hotspot portal.

8.6 Serial Redirector

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

8.6.1 Telnet to Serial Configuration

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



Telnet to Serial Configuration

Server Status: Disabled

Enabled: ☑

LAN: ☑

Authenticated LAN: ☑

WAN: □

Server Port: 7218

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)

8.6.2 USB Serial Adapter Configuration

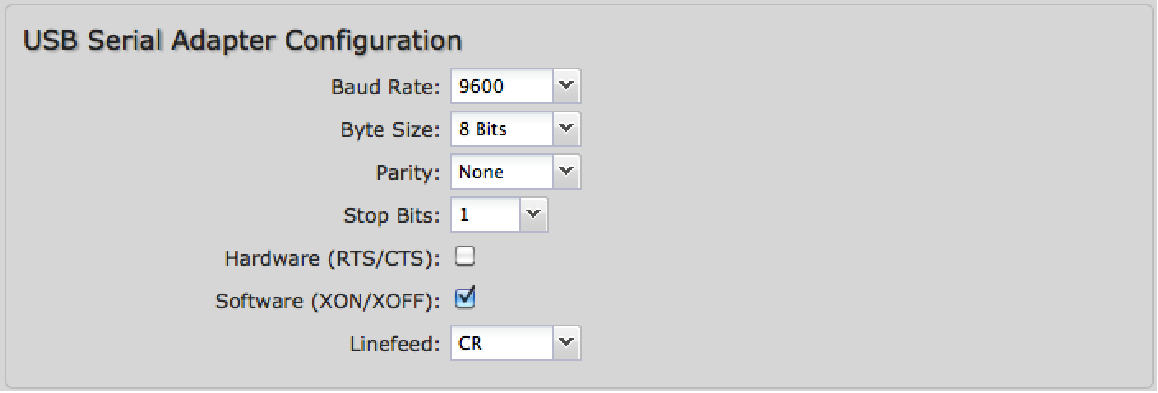
Baud Rate: Select from the dropdown list.

- 50
- 75
- 110
- 134
- 150
- 200
- 300
- 600

- 1200
- 1800
- 2400
- 4800
- 9600
- 19200

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

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



USB Serial Adapter Configuration

Baud Rate: 9600

Byte Size: 8 Bits

Parity: None

Stop Bits: 1

Hardware (RTS/CTS): □

Software (XON/XOFF): ☑

Linefeed: CR

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

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

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

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

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

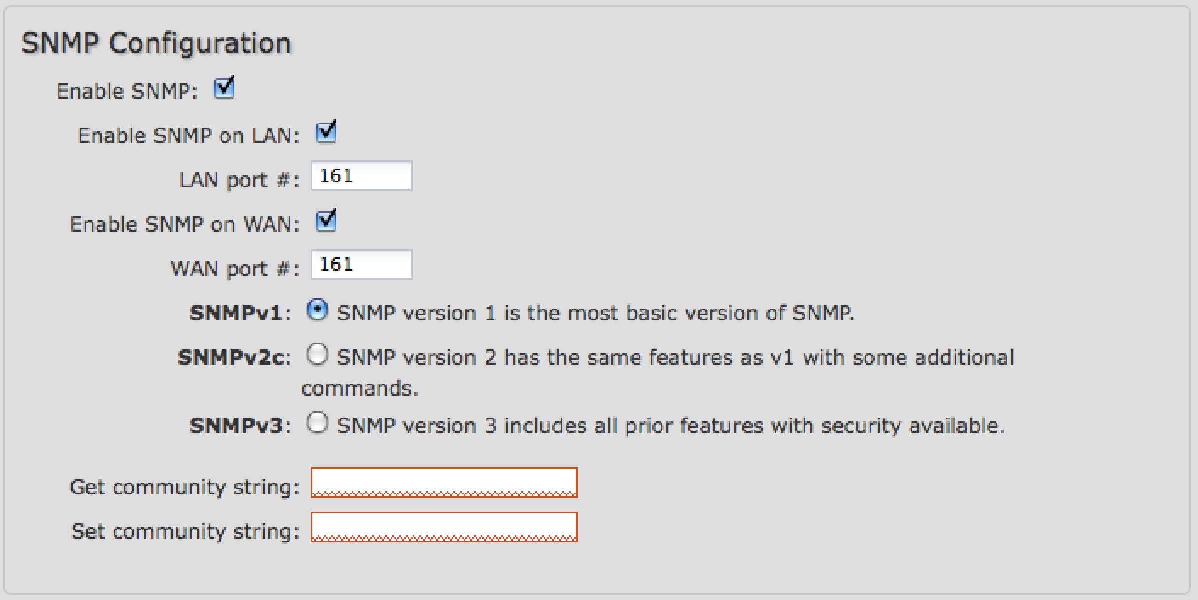
- Ignore
- CR/LF
- CR
- LF

8.7 SNMP Configuration

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

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

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



SNMP Configuration

Enable SNMP: ☑

Enable SNMP on LAN: ☑

LAN port #: 161

Enable SNMP on WAN: ☑

WAN port #: 161

SNMPv1: ● SNMP version 1 is the most basic version of SNMP.

SNMPv2c: ○ SNMP version 2 has the same features as v1 with some additional commands.

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

Get community string:

Set community string:

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

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

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

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

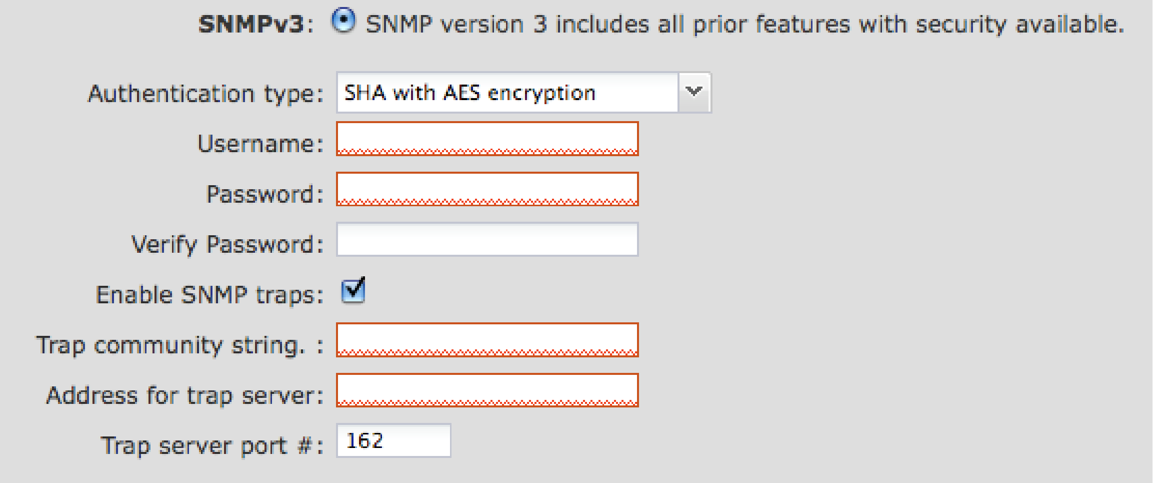
SNMPv2c: SNMP version 2c has the same features as v1 with some additional commands. SNMPv2c will configure the router to use settings and data formatting compatible with SNMP version 2c.

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

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

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

8.7.1 SNMPv3



SNMPv3:	● SNMP version 3 includes all prior features with security available.
Authentication type:	SHA with AES encryption
Username:	
Password:	
Verify Password:	
Enable SNMP traps:	☑
Trap community string. :	
Address for trap server:	
Trap server port #:	162

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 8 characters long.

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

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

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

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

8.7.2 System Information

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

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

System Name: Input the router's hostname.

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

8.8 System Control

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

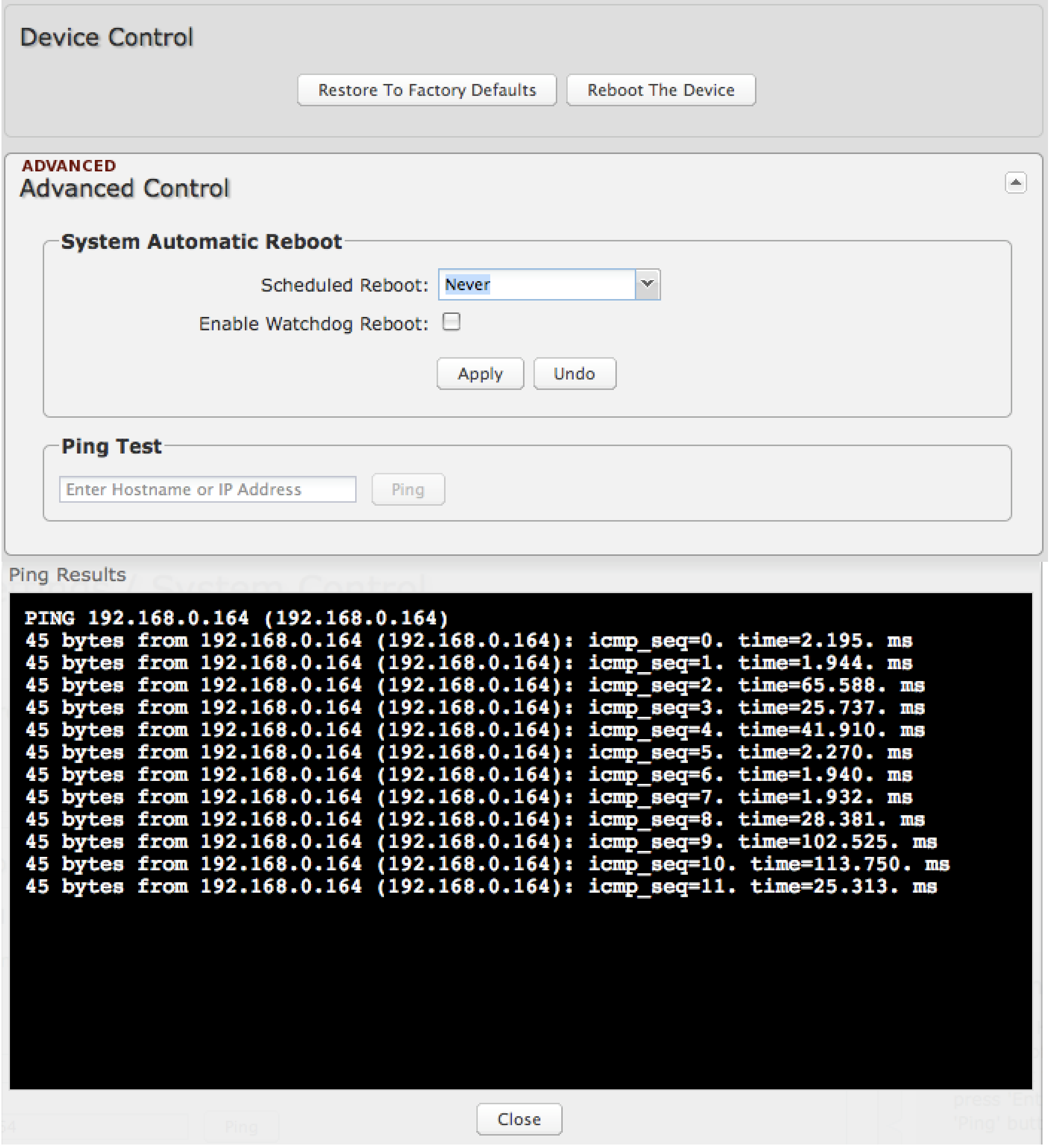
Reboot The Device: This causes the router to restart.

Advanced: System Automatic Reboot and Ping Test

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

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

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



Scheduled Reboot: Never

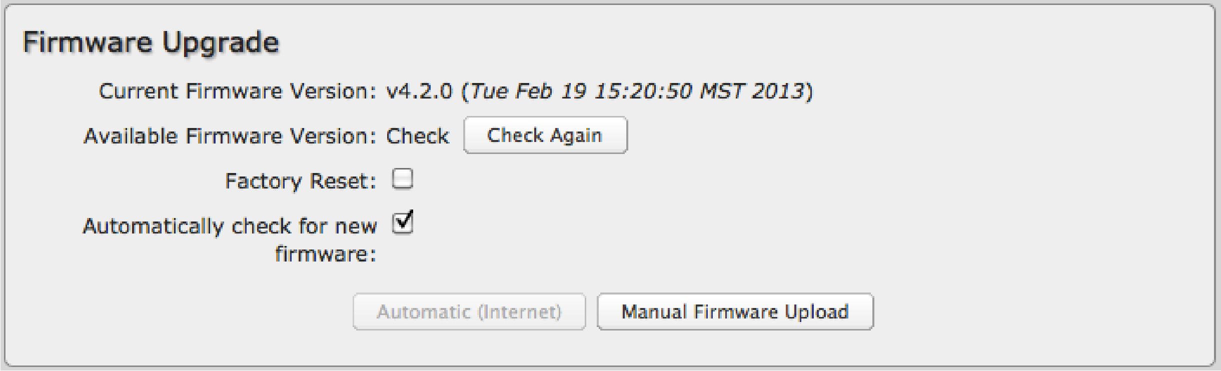
Enable Watchdog Reboot: □

```
PING 192.168.0.164 (192.168.0.164)
45 bytes from 192.168.0.164 (192.168.0.164): icmp_seq=0. time=2.195. ms
45 bytes from 192.168.0.164 (192.168.0.164): icmp_seq=1. time=1.944. ms
45 bytes from 192.168.0.164 (192.168.0.164): icmp_seq=2. time=65.588. ms
45 bytes from 192.168.0.164 (192.168.0.164): icmp_seq=3. time=25.737. ms
45 bytes from 192.168.0.164 (192.168.0.164): icmp_seq=4. time=41.910. ms
45 bytes from 192.168.0.164 (192.168.0.164): icmp_seq=5. time=2.270. ms
45 bytes from 192.168.0.164 (192.168.0.164): icmp_seq=6. time=1.940. ms
45 bytes from 192.168.0.164 (192.168.0.164): icmp_seq=7. time=1.932. ms
45 bytes from 192.168.0.164 (192.168.0.164): icmp_seq=8. time=28.381. ms
45 bytes from 192.168.0.164 (192.168.0.164): icmp_seq=9. time=102.525. ms
45 bytes from 192.168.0.164 (192.168.0.164): icmp_seq=10. time=113.750. ms
45 bytes from 192.168.0.164 (192.168.0.164): icmp_seq=11. time=25.313. ms
```

8.9 System Software

8.9.1 Firmware Upgrade

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



Firmware Upgrade

Current Firmware Version: v4.2.0 (*Tue Feb 19 15:20:50 MST 2013*)

Available Firmware Version: Check

Factory Reset: □

Automatically check for new firmware: ☑

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

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

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

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

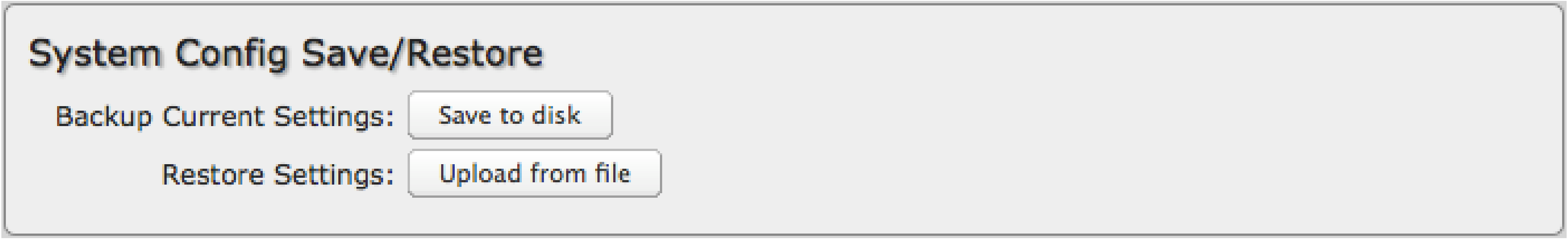
Automatic (Internet): Have the router download the file and perform the upgrade with no user interaction.

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

8.9.2 System Config Save/Restore

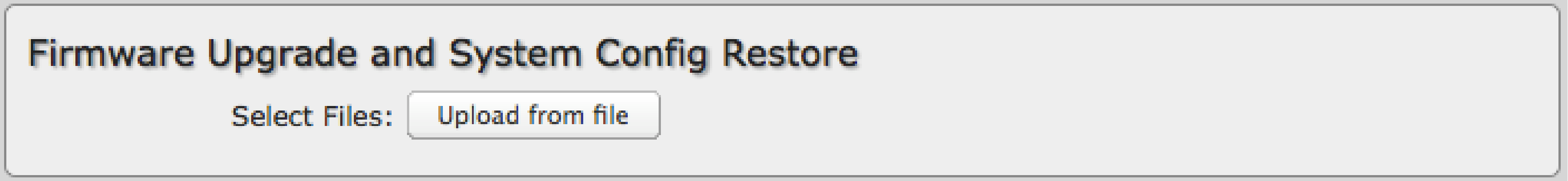
Backup Current Settings: Click on “Save to disk” to save your current settings to a file on a computer.

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



8.9.3 Firmware Upgrade and System Config Restore

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



9 GLOSSARY

802.11

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

Access Control List

ACL. A database of network devices that are allowed to access resources on the network.

Access Point

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

ActiveX

A Microsoft specification for the interaction of software components.

Ad-hoc network

Peer-to-Peer network between wireless clients.

Address Resolution Protocol

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

ADSL

Asymmetric Digital Subscriber Line.

Advanced Encryption Standard

AES. Government encryption standard.

Alphanumeric

Characters A-Z and 0-9.

Antenna

Used to transmit and receive RF signals.

Anti-virus

A security program that can run on a computer or mobile device and protects you by identifying and stopping the spread of malware on your system. Anti-virus cannot detect all malware, so even if it is active, your system might still get infected. Anti-virus can also be used at the organizational level. For example, email servers may have anti-virus integrated with it to scan incoming or outgoing email. Sometimes anti-virus tools are called 'anti-malware', because these products are designed to defend against various types of malicious software.

AppleTalk

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

AppleTalk Address Resolution Protocol

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

Application layer

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

ASCII

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

Attenuation

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

Authentication

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

Automatic Private IP Addressing

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

Backward Compatible

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

Bandwidth

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

Basic Input/Output System

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

Baud

Data transmission speed.

Beacon

A data frame by which one of the stations in a Wi-Fi network periodically broadcasts network control data to other wireless stations.

Bit rate

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

Bit/sec

Bits per second.

BOOTP

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

Bottleneck

A time during processes when something causes the process to slowdown or stop all together.

Broadband

A wide band of frequencies available for transmitting data.

Broadcast

Transmitting data in all directions at once.

Browser

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

Cable modem

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

CardBus

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

CAT 5

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

Client

A program or user that requests data from a server.

Collision

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

Cookie

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

Data

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

Data Encryption Standard

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

Data-Link layer

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

Database

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

DB-25

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

DB-9

A 9-pin connector for RS-232 connections

dBd

Decibels related to dipole antenna.

dBi

Decibels relative to isotropic radiator.

dBm

Decibels relative to one milliwatt.

Decrypt

To unscramble an encrypted message back into plain text.

Default

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

Demilitarized zone

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

DHCP

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

Digital certificate

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

Direct Sequence Spread Spectrum

DSSS: Modulation technique used by 802.11b wireless devices.

DNS

Domain Name System. Translates Domain Names to IP addresses.

Domain name

A name that is associated with an IP address.

Download

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

Drive-by Download

These attacks exploit vulnerabilities in your browser or its plugins and helper applications when you simply surf to an attacker-controlled website. Some computer attackers set up their own evil websites that are designed to automatically attack and exploit anyone that visits the website. Other attackers compromise trusted websites such as ecommerce sites and deploy their exploit software there. Often these attacks occur without the victims realizing that they are under attack.

DSL

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

Duplex

Sending and Receiving data transmissions at the same time.

Dynamic DNS service

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

Dynamic IP address

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

EAP

Extensible Authentication Protocol.

Email

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

Encryption

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

Ethernet

The most widely used technology for Local Area Networks.

Exploit

Code that is designed to take advantage of a vulnerability. An exploit is designed to give an attacker the ability to execute additional malicious programs on the compromised system or to provide unauthorized access to affected data or application.

Fiber optic

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

File server

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

File sharing

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

Firewall

A security program that filters inbound and outbound network connections. In some ways you can think of a firewall as a virtual traffic cop, determining which traffic can go through the firewall. Almost all computers today come with firewall software installed. In addition, firewalls can be implemented as network devices to filter traffic that traverses through them.

Firmware

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

Fragmentation

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

FTP

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

Full-duplex

Sending and Receiving data at the same time.

Gain

The amount an amplifier boosts the wireless signal.

Gateway

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

Gbps

Gigabits per second.

Gigabit Ethernet

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

GUI

Graphical user interface.

H.323

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

Half-duplex

Data cannot be transmitted and received at the same time.

Hashing

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

Hexadecimal

Characters 0-9 and A-F.

Hop

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

Host

Computer on a network.

HTTP

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

HTTPS

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

Hub

A networking device that connects multiple devices together.

ICMP

Internet Control Message Protocol.

IEEE

Institute of Electrical and Electronics Engineers.

IGMP

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

IIS

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

IKE

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

Infrastructure

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

Internet

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

Internet Explorer

A World Wide Web browser created and provided by Microsoft.

Internet Protocol

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

Internet Protocol Security

IPsec provides security at the packet processing layer of network communication.

Internet Service Provider

An ISP provides access to the Internet to individuals or companies.

Intranet

A private network.

Intrusion Detection

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

IP

Internet Protocol.

IP address

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

IPsec

Internet Protocol Security.

IPX

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

ISP

Internet Service Provider.

Java

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

Kbps

Kilobits per second.

Kbyte

Kilobyte.

L2TP

Layer 2 Tunneling Protocol.

LAN

Local Area Network.

Latency

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

LED

Light Emitting Diode.

Legacy

Older devices or technology.

Local Area Network

LAN. A group of computers in a building that usually access files from a server.

LPR/LPD

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

MAC Address

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

Malware

Malware stands for 'malicious software'. It is any type of code or program cyber attackers use to perform malicious actions. Traditionally there have been different types of malware based on their capabilities and means of propagation, as listed below. However, these technical distinctions are no longer relevant as modern malware combines the characteristics from each of these in a single program.

- Virus: A type of malware that spreads by infecting other files, rather than existing in a standalone manner. Viruses often – though not always – spread through human interaction, such as opening an infected file or application.
- Worm: A type of malware that can propagate automatically, typically without requiring any human interaction for it to spread. Worms often spread across networks, though they can also infect systems through other means, such as USB keys. An example of a worm is Conficker, which infected millions of computer systems starting in 2008 and is still active today.
- Trojan: A shortened form of "Trojan Horse", this type of malware appears to have a legitimate or at least benign use, but masks a hidden sinister function. For example, you may download and install a free screensaver which actually works well as a screensaver. But that software could also be malicious, it will infect your computer once you install it.

- Spyware: A type of malware that is designed to spy on the victim's activities, capturing sensitive data such as the person's passwords, online shopping, and screen contents. One popular type of spyware, a keylogger, is optimized for logging the victim's keyboard activity and transmitting the captured information to the remote attacker.

Mbps

Megabits per second.

MDI

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

MDIX

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

MIB

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

Modem

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

MPPE

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

MTU

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

Multicast

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

NAT

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

NetBEUI

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

NetBIOS

Network Basic Input/Output System.

Netmask

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

Network Interface Card

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

Network Layer

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

Network Time Protocol

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

NIC

Network Interface Card.

NTP

Network Time Protocol.

OFDM

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

OSI

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

OSPF

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

Password

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

Patch

A patch is an update to a vulnerable program or system. A common practice to keep your computer and mobile devices secure is installing the vendor’s latest patches in a timely fashion. Some vendors release patches on a monthly or quarterly basis. Therefore, having a computer that is unpatched for even a few weeks could leave it vulnerable.

Personal Area Network

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

Phishing

Phishing is a social engineering technique where cyber attackers attempt to fool you into taking an action in response to an email. Phishing was a term originally used to describe a specific attack scenario. Attackers would send out emails pretending to be a trusted bank or financial institution; their goal was to fool victims into clicking on a link in the email. Once clicked, victims were taken to a website that pretended to be the bank, but was really created and controlled by the attacker. If the victim attempted to log in thinking they were at their bank, their login and password would then be stolen by the attacker. The term has evolved and often means not just attacks designed to steal your password, but emails designed to send you to websites that hack into your browser, or even emails with infected attachments.

Physical layer

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

Ping

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

PoE

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

POP3

Post Office Protocol 3. Used for receiving email.

Port

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

PPP

Point-to-Point Protocol. Used for two computers to communicate with each over a serial interface, like a phone line.

PPPoE

Point-to-Point Protocol over Ethernet. Used to connect multiple computers to a remote server over Ethernet.

PPTP

Point-to-Point Tunneling Protocol. Used for creating VPN tunnels over the Internet between two networks.

Preamble

Used to synchronize communication timing between devices on a network.

QoS

Quality of Service.

RADIUS

Remote Authentication Dial-In User Service. Allows for remote users to dial into a central server and be authenticated in order to access resources on a network.

Reboot

To restart a computer and reload its operating software or firmware from nonvolatile storage.

Rendezvous

Apple’s version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings.

Repeater

Retransmits the signal of an access point in order to extend its coverage.

RIP

Routing Information Protocol. Used to synchronize the routing table of all the routers on a network.

RJ-11

The most commonly used connection method for telephones.

RJ-45

The most commonly used connection method for Ethernet.

RS-232C

The interface for serial communication between computers and other related devices.

RSA

Algorithm used for encryption and authentication.

Server

A computer on a network that provides services and resources to other computers on the network.

Session key

An encryption and decryption key that is generated for every communication session between two computers.

Session layer

The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends.

Simple Mail Transfer Protocol

Used for sending and receiving email.

Simple Network Management Protocol

Governs the management and monitoring of network devices.

SIP

Session Initiation Protocol. A standard protocol for initiating a user session that involves multimedia content, such as voice or chat.

SMTP

Simple Mail Transfer Protocol.

SNMP

Simple Network Management Protocol.

Social Engineering

A psychological attack used by cyber attackers to deceive their victims into taking an action that will place the victim at risk. For example, cyber attackers may trick you into revealing your password or fool you into installing malicious software on your computer. They often do this by pretending to be someone you know or trust, such as a bank, company or even a friend.

SOHO

Small Office/Home Office.

Spam

Unwanted or unsolicited emails, typically sent to numerous recipients with the hope of enticing people to read the embedded advertisements, click on a link or open an attachment. Spam is often used to convince recipients to purchase illegal or questionable products and services, such as pharmaceuticals from fake companies. Spam is also often used to distribute malware to potential victims.

Spear Phishing

Spear phishing describes a type of phishing attack that targets specific victims. But instead of sending out an email to millions of email addresses, cyber attackers send out a very small number of crafted emails to very specific individuals, usually all at the same organization. Because of the targeted nature of this attack, spear phishing attacks are often harder to detect and usually more effective at fooling the victims.

SPI

Stateful Packet Inspection.

SSH

Secure Shell. A command line interface that allows for secure connections to remote computers.

SSID

Service Set Identifier. A name for a wireless network.

Stateful Packet Inspection

A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests are allowed to pass though the firewall.

Subnet mask

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

Syslog

System Logger. A distributed logging interface for collecting in one place the logs from different sources. Originally written for UNIX, it is now available for other operating systems, including Windows.

TCP

Transmission Control Protocol.

TCP Raw

A TCP/IP protocol for transmitting streams of printer data.

TCP/IP

Transmission Control Protocol/Internet Protocol.

TFTP

Trivial File Transfer Protocol. A utility used for transferring files that is simpler to use than FTP but with fewer features.

Throughput

The amount of data that can be transferred in a given time period.

Traceroute

A utility that displays the routes between your computer and a specific destination.

UDP

User Datagram Protocol.

Unicast

Communication between a single sender and receiver.

Update

To install a more recent version of a software or firmware product.

Upgrade

To install a more recent version of a software or firmware product.

Upload

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

UPnP

Universal Plug and Play. A standard that allows network devices to discover each other and configure themselves to be a part of the network.

URL

Uniform Resource Locator. A unique address for files accessible on the Internet.

USB

Universal Serial Bus.

UTP

Unshielded Twisted Pair.

Virtual Private Network

VPN. A secure tunnel over the Internet to connect remote offices or users to their company's network.

VLAN

Virtual LAN.

VoIP

Voice over IP. Sending voice information over the Internet as opposed to the PSTN.

Vulnerability

Any weakness that attackers or their malicious programs may be able to exploit. For example, it can be a bug in a computer program or a misconfigured webserver. An attacker or malware may be able to take advantage of the vulnerability to gain unauthorized access to the affected system. However, vulnerabilities can also be a weakness in people or organizational processes.

Wake on LAN

Allows you to power up a computer through its Network Interface Card.

WAN

Wide Area Network.

WCN

Windows Connect Now. A Microsoft method for configuring and bootstrapping wireless networking hardware (access points) and wireless clients, including PCs and other devices.

WDS

Wireless Distribution System. A system that enables the interconnection of access points wirelessly.

Web browser

A utility that allows you to view content and interact with all of the information on the World Wide Web.

WEP

Wired Equivalent Privacy. Security for wireless networks that is supposed to be comparable to that of a wired network.

Wi-Fi

Wireless Fidelity. Used to describe any of the 802.11 wireless networking specifications.

Wi-Fi Protected Access

An updated version of security for wireless networks that provides authentication as well as encryption.

Wide Area Network

The larger network that your LAN is connected to, which may be the Internet itself, or a regional or corporate network.

Wireless (Wi-Fi) LAN

Connecting to a Local Area Network over one of the 802.11 wireless standards.

WISP

Wireless Internet Service Provider. A company that provides a broadband Internet connection over a wireless connection.

WLAN

Wireless Local Area Network.

WPA

Wi-Fi Protected Access. A Wi-Fi security enhancement that provides improved data encryption, relative to WEP.

xDSL

A generic term for the family of digital subscriber line (DSL) technologies, such as ADSL, HDSL, RADSL, and SDSL.

Yagi antenna

A directional antenna used to concentrate wireless signals on a specific location.

10 APPENDIX

10.1 Product Information and Safety Guide

This important Product Information and Safety Guide contains safety, handling, disposal, regulatory, trademark, copyright, and software licensing information. Read all safety information below and operating instructions before using the MBR1400 device to avoid injury.

SAFETY AND HAZARDS
Under no circumstances should the MBR1400 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 MBR1400 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 MBR1400 device be used in any aircraft, regardless of whether the aircraft is on the ground or in flight. In any aircraft, the MBR1400 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 MBR1400 device be used by the driver or operator of any vehicle. Such use of the device will detract from the driver or operator’s control of that vehicle. In some jurisdictions, use of the MBR1400 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 MBR1400 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 MBR1400 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!

To comply with FCC/IC regulations limiting both maximum RF output power and human exposure to RF radiation, the maximum antenna gain must not exceed 5 dBi in the Cellular band and 4 dBi in the PCS band.

ANTENNA CONSIDERATIONS
Although the antenna model(s) used with these devices meet(s) the Industry Canada Radio Frequency requirements, it is possible that the future customers may swap them for different ones without network providers knowledge and approval. Such customers must be made aware of, and follow, the Radio Frequency requirements applied in the Technical Approval:

- RSS-102 “Radio Frequency Exposure Compliance of Radiocommunication Apparatus (All Frequency Bands)”
- RSS-129 “800 MHz Dual-Mode CDMA Cellular Telephones”
- RSS-132e “Cellular Telephones Employing New Technologies Operating in the Bands 824-849 MHz and 869-894 MHz”
- RSS-133 r1 “2 GHz Personal Communications Services”

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.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

IMPORTANT NOTE

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 minimum distance 20cm between the radiator & your body.

OPEN SOURCE SOFTWARE

This product contains software distributed under one or more of the following open source licenses: GNU General Public License Version 2, NetBSD Foundation License, and PSF License Agreement for Python 3.1.1. For more information on this software, including licensing terms and your rights to access source code, contact Cradlepoint at www.Cradlepoint.com/opensource.

WARRANTY INFORMATION

Limited 1 Year Warranty included featuring 5x12 technical support + access to software updates + hardware repair or replacement. Optional Enterprise Support Agreement available with 24x7 technical support + software updates and upgrades + advanced hardware exchange.

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. Cradlepoint does not warrant that the operation of the device will meet your requirements or be error free. Within thirty (30) days of receipt should the product fail for any reason other than damage due to customer negligence, purchaser may return the product to the point of purchase for a full refund of the purchase price. If the purchaser wishes to upgrade or convert to another Cradlepoint, Inc. product within the thirty (30) day period, purchaser may return the product and apply the full purchase price toward the purchase of another Cradlepoint product. Any other return will be subject to Cradlepoint, Inc.'s existing return policy.

LIMITATION OF CRADLEPOINT LIABILITY

The information contained in this Quick Start Guide is subject to change without notice and does not represent any commitment on the part of Cradlepoint or its affiliates. CRADLEPOINT AND ITS AFFILIATES HEREBY SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL: (A) DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES, INCLUDING WITHOUT LIMITATION FOR LOSS OF PROFITS OR REVENUE OR OF ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE THE MBR1400 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 MBR1400 device, regardless of the number of events, occurrences, or claims giving rise to liability, exceed the price paid by the original purchaser of the MBR1400 device.

PRIVACY

Cradlepoint may collect general data pertaining to the use of Cradlepoint products via the Internet including, by way of example, IP address, device ID, operating system, browser type and version number, etc. To review Cradlepoint's privacy policy, please visit: http://www.Cradlepoint.com/privacy.

OTHER BINDING DOCUMENTS; TRADEMARKS; COPYRIGHT
By activating or using your MBR1400 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. Cradlepoint, the Cradlepoint logo, and MBR1400 are trademarks of Cradlepoint, Inc.

10.2 Specifications

MODEL NAME

MBR1400 Mission-Critical Broadband Router

WAN / INTERNET

3G/4G via five modem ports (3 USB 2.0, 2 ExpressCard); one default Ethernet port (10/100/1000); additional LAN Ethernet ports re-configurable to WAN for redundancy

LAN

Wi-Fi 802.11 a/b/g/n, four default Ethernet ports (10/100/1000); one additional WAN Ethernet port re-configurable to LAN use

ANTENNAS

3 external 2.4 GHz Wi-Fi antennas; 5 GHz antennas available as an accessory

BUTTONS / SWITCHES

Wi-Fi On/Off Switch, WPS Button (Wi-Fi Protected Setup), Modem Signal Strength, Reset, and Power Switch

LED INDICATORS

Power, Ethernet LAN (1-4), Ethernet WAN, 3G/4G WAN, 3G/4G Modem Status (5), WPS (Wi-Fi Protected Setup), Signal Strength

DIMENSIONS

9” x 5.1” x 1.57” (230mm x 130mm x 40mm)

CERTIFICATIONS

FCC, IC, CE, Wi-Fi Alliance

OPERATING TEMPERATURE

0ºC to 40ºC

DETAILS

- 2.412 to 2.484 GHz Wi-Fi frequency band operation
- Compliant with IEEE 802.3 and 3u Standards
- Supports OFDM and CCK modulation
- Supports Cable/DSL modems with Dynamic IP, Static IP, PPPoE, PPTP, or L2TP connection types
- Traffic Control, Port Forwarding, Virtual Server (max 32 servers) and DMZ
- Compatible with HSPA, EVDO, LTE, & WiMAX cellular network devices
- Easy management via HTTP and remote management via HTTP and SNMP
- Create, manage, and terminate up to 20 IPsec VPN sessions
- Supported VPN implementations: Cradlepoint to Cradlepoint, Cradlepoint to Cisco/Linksys Routers, and Cradlepoint to Linux Systems.
- Tunnel (default) and Transfer (a.k.a. Transport) Modes
- Hash algorithms (hardware accelerated) - MD5, SHA128, SHA256, SHA384, SHA512
- Cipher algorithms (hardware accelerated) - AES, 3DES, DES
- Keying – automatic using IKE 1.0 or manual
- Authentication method: pre-shared key

http://www.Cradlepoint.com/