MBR1200

PRODUCT MANUAL

Failsafe Gigabit N Router for Mobile Broadband

with **VPN Support**

for additional information, visit:

knowlegebase.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	May 19, 2010	Initial release for Firmware version 1.6.12	David Rush
1.1	June 7,2010	Minor edits	David Rush

Trademarks

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

`

Table of Contents

`

1 INTRODUCTION

1.1 Package Contents

- CradlePoint MBR1200 Mobile Broadband Router
- AC power adapter (12V, 1.5A) WARNING: using a power adapter other than the one provided may damage the MBR1200 and will void the warranty
- Mounting Hardware
- CAT5 Ethernet Cable
- Quick Start Guide
- Accessory Guide

1.2 System Requirements

- Ethernet-based Cable/DSL modem and/or Broadband Data Modem with Active Subscription (USB, ExpressCard, PC Card), or supported Phone with Active Tethered Data Plan Suggested
- Windows 2000/XP/7, Mac OS X, or Linux Computer with Wi-Fi Adapter (802.11n Recommended)
- Internet Explorer v6.0 or higher, Firefox v2.0 or higher, Safari v1.0 or higher.

1.3 MBR1200 Overview

- Easy Setup and Maintenance
- High Performance Internal 802.11n Antennas
- 10/100/1000 Ethernet WAN and LAN Ports
- Cellular Redundancy Failover to 3G/4G[1]
- Works with USB, PC Card and ExpressCard Modems
- Physical Modem Security Cap Available.

1.3.1 Always Connected

The CradlePoint MBR1200 is a robust 802.11n router with 3G/4G[1] failover capabilities built for home, small business, branch office, temporary and remote enterprise environments seeking to implement continuous, always-on connectivity. With its failover/failback capability, the MBR1200

[1] Data Modem Not Included. This Product Requires an Activated Data Modem or Phone with Data Plan for Full Functionality. See your Cellular/3G/4G Service Provider for Details on Coverage and Data Plan Options.

automatically switches to a secondary connection (either wired or wireless) when your primary service is interrupted. Once your service is restored, the MBR1200 will automatically failback to the primary connection - keeping your business online with minimal interruption to users.

1.3.2 Enterprise Power – Small Business Simple

Powered by WiPipe™ technology, the MBR1200 router includes many features found in expensive, enterprise-class routers at a fraction of the cost. With minimal setup and maintenance, including our pre-installed software, it has “right out of the box” simplicity.

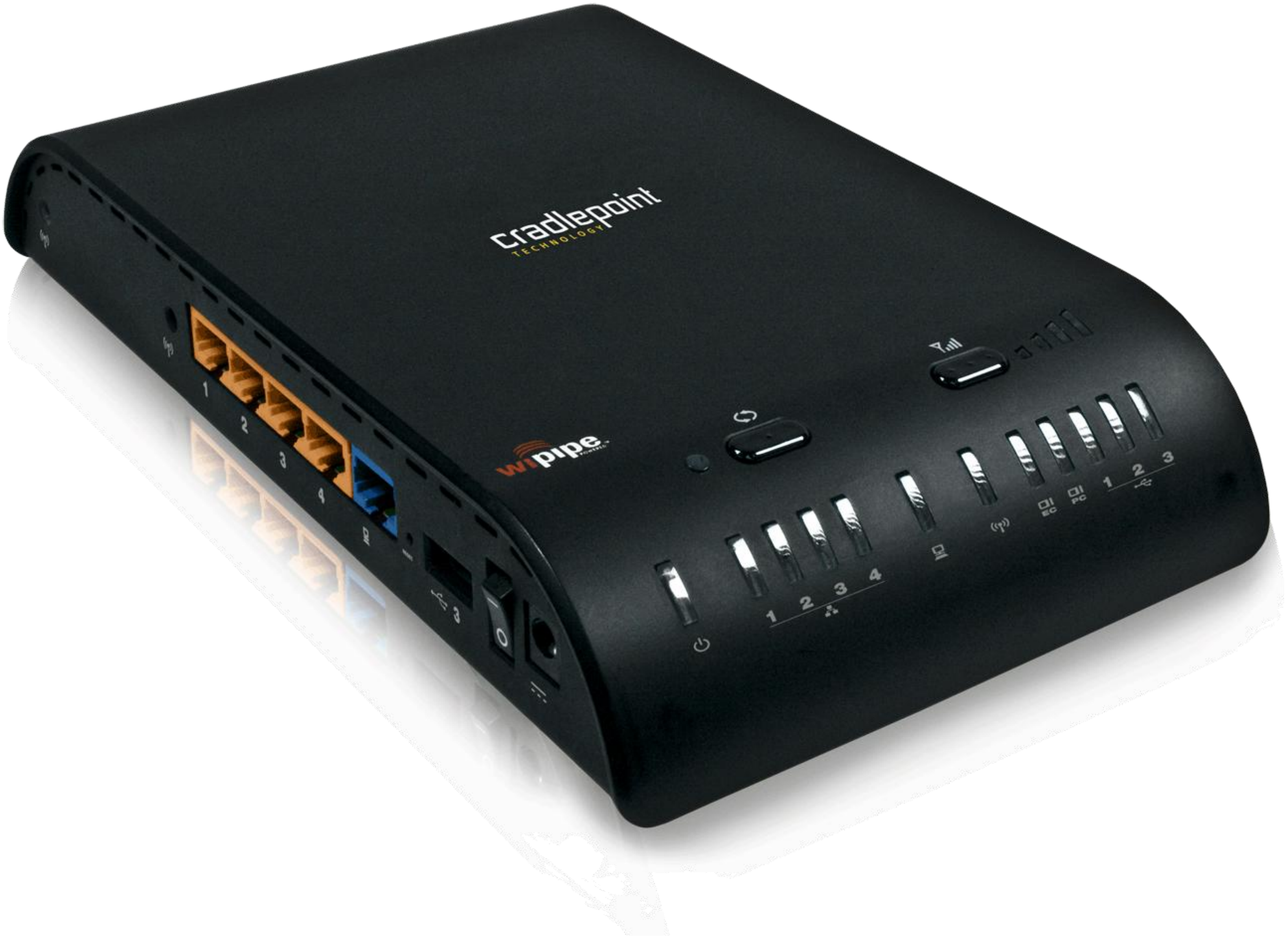
Standard on the MBR1200 are security features such as multiple Wi-Fi encryption modes (WEP and WPA/ WPA2 Personal and Enterprise) and built-in firewall, which prevent unauthorized use of your connection. With no additional software to load, you’ll be up and running in minutes.

1.3.3 VPN: Secure and Reliable

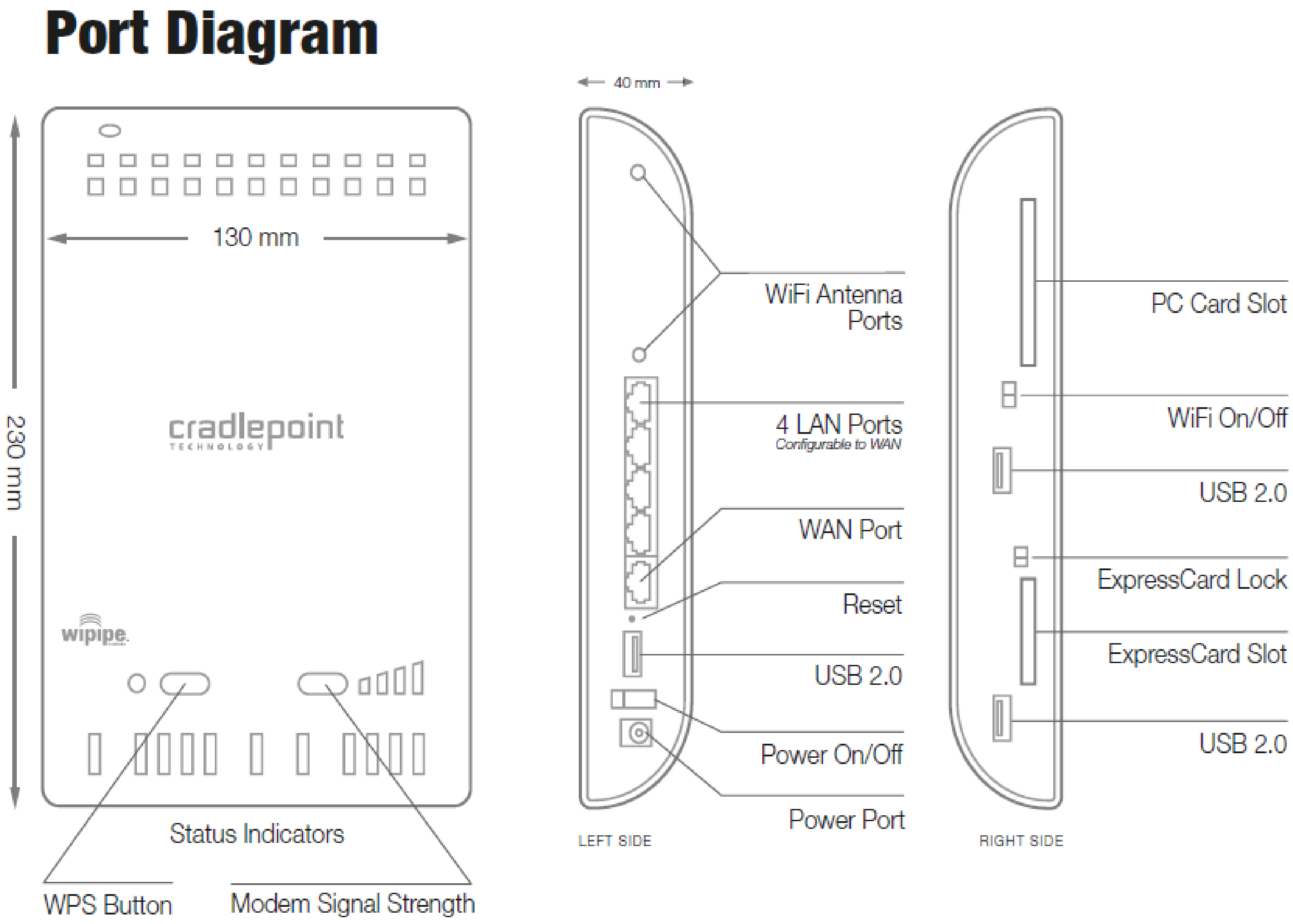
The high-performance MBR1200 has the capability to create, manage, and terminate multiple IPSec VPN sessions. It provides up to five concurrent sessions, supporting transfer and tunnel modes and several Hash and Cipher algorithms. These encryption protocols protect your communications from one private network to another from end-to-end.

[1] Data Modem Not Included. This Product Requires an Activated Data Modem or Phone with Data Plan for Full Functionality. See you Cellular/3G/4G Service Provider for Details on Coverage and Data Plan Options.

2 HARDWARE OVERVIEW



2.1 Ports


Port Diagram
40 mm
130 mm
230 mm
cradlepoint TECHNOLOGY
wipipe
Status Indicators
WPS Button
Modem Signal Strength
WiFi Antenna Ports
4 LAN Ports
Configurable to WAN
WAN Port
Reset
USB 2.0
Power On/Off
Power Port
LEFT SIDE
PC Card Slot
WiFi On/Off
USB 2.0
ExpressCard Lock
ExpressCard Slot
USB 2.0
RIGHT SIDE

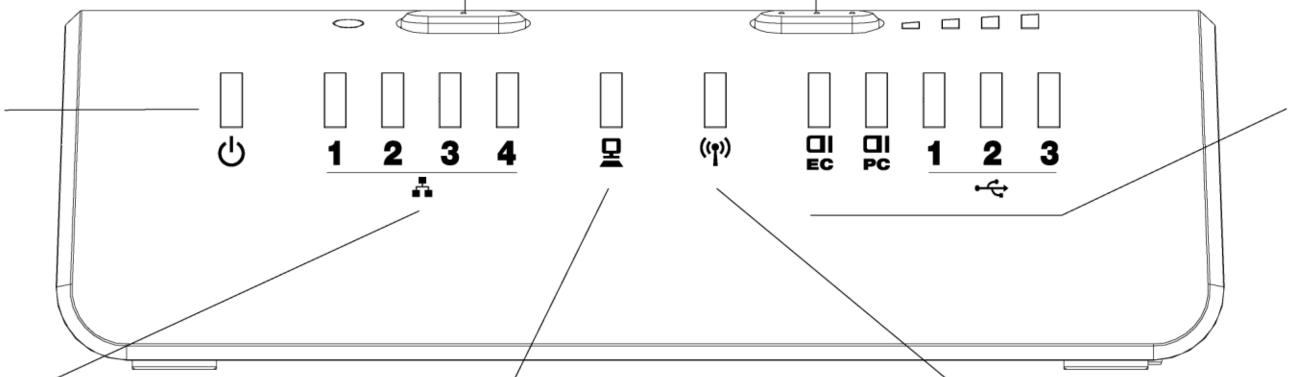
2.2 LEDs

WiFi PROTECTED SETUP STATUS

Blue	WPS is Active and Enabled
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	Unit is On
No Light	Unit is Off

3G/4G MODEM STATUS

Green	Connection Active
Blinking Green	Establishing Connectiion
Amber	Modem Not Active
Blinking Amber	Modem Connection Error
No Light	LAN Cable Disconnected or Link Failed

LAN STATUS (ports 1-4 to connect computers)

Green	LAN Connected
Blinking Green	LAN Activity
No Light	LAN Cable Disconnected or Link Failed

WAN STATUS (to connect cable or dsl modem)

Green	WAN Connected
Blinking Green	WAN Activity
No Light	WAN Cable Disconnected or Link Failed

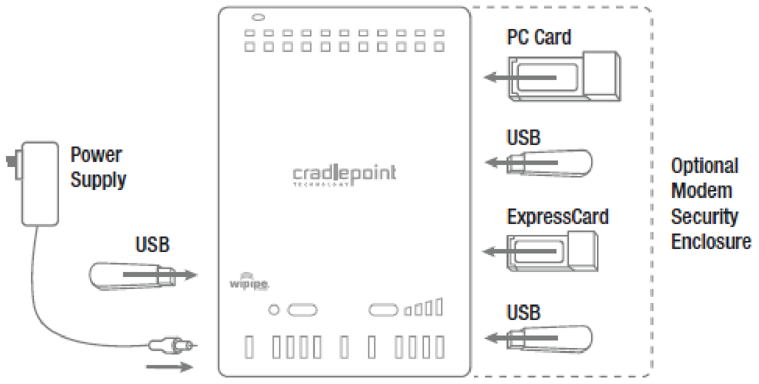
WiFi STATUS

Green	WiFi On and Functioning Normally
Blinking Green	WiFi Activity
Blinking Red	Error with Connection
No Light	WiFi Radio Off

3 QUICK START

3.1 Wireless Setup Using a Mobile Broadband (cellular) Data Modem/s[1]

- Connect the Power Supply
- Insert your ExpressCard, PC Card, or USB modem/s.
- Establish a wireless internet connection as shown below.



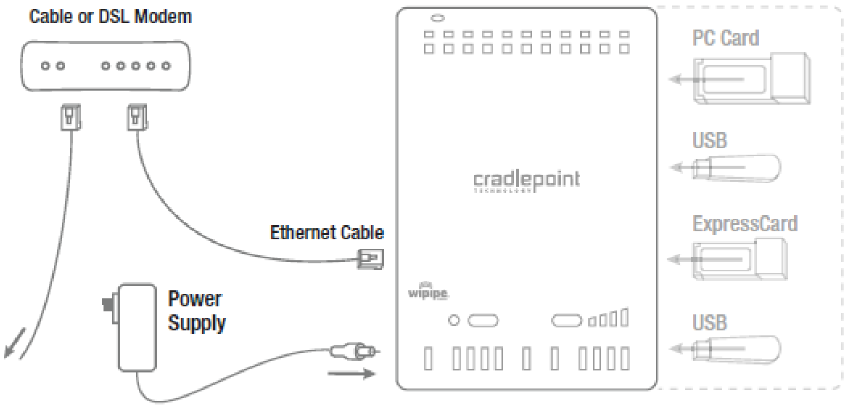
3.2 Wired Connection Using Cable/DSL Internet Service

- Connect the Power Supply
- Insert one end of your Ethernet cable to the WAN port.
- Insert the other end of the Ethernet cable into your Cable or DSL modem. It may take a minute or two for the MBR1200 to initialize.
- Open your web browser.

You can now access the Internet.

For Failover/Failback Functionality, you must have an Active Data Modem attached to the MBR1200.

CradlePoint recommends that Wi-Fi security be setup at this point. See **<u>Setting Up Wireless Network Security</u>**



For Failover/Failback Functionality, you must have an Active Data Modem attached to the MBR1200.

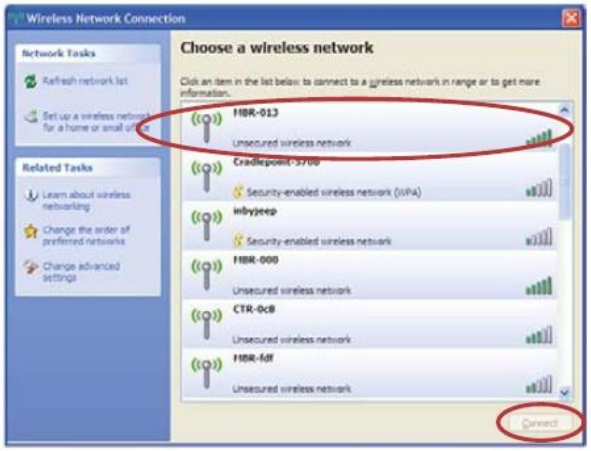
[1] Data Modem Not Included. This Product Requires an Activated Data Modem or Phone with Data Plan for Full Functionality. See you Cellular/3G/4G Service Provider for Details on Coverage and Data Plan Options

3.3 Establishing a Wireless Internet Connection

3.3.1 Wireless Network Connection

On a Wi-Fi-enabled computer or device, open the View Wireless Networks window and click on the MBR1200. Next, click on the **Connect** button in the bottom right corner of the window.

If more than one MBR1200 wireless router is visible, you can find the correct unit by checking for its SSID. Your wireless router uses the SSID of MBR1200-xxx, where "xxx" is the last 3 digits of the router's MAC address. The MAC address can be found on the MBR1200 product box or the bottom of the MBR1200 unit. Once you have completed your wireless connection to the MBR1200 router, you should set up security on your wireless network by following the procedures identified in the next step (recommended). You can connect directly onto the Internet without security (not recommended) by skipping the next step.


Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

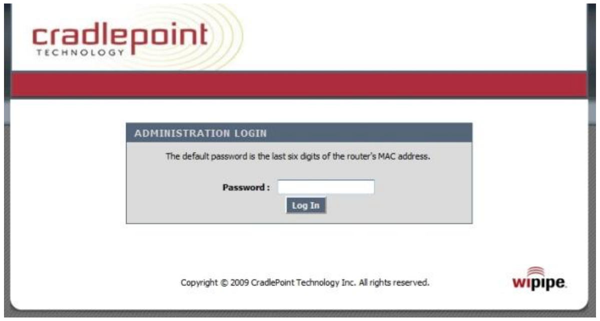
MBR-013 Unsecured wireless network
Cradlepoint-3700 Security-enabled wireless network (WPA)
inbyjeep Security-enabled wireless network
MBR-000 Unsecured wireless network
CTR-0c8 Unsecured wireless network
MBR-fdf Unsecured wireless network

3.3.2 Setting Up Wireless Network Security

Wi-Fi Security is highly recommended by CradlePoint. **Wi-Fi Security is separate from the User Login Page**. Setting "Wi-Fi Security" on your router prevents users from connecting their computers to your router unless they have you wireless security password.

Follow The Steps Below to Set the Wi-Fi Security:

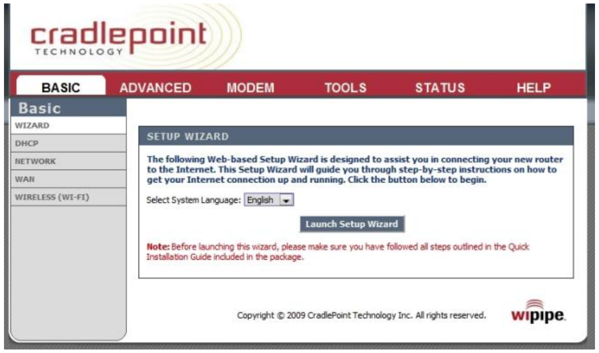
- Access your router **Administration Login** screen by opening a web browser window and typing the IP address **http://192.168.0.1** into the address bar.
- Enter your **Default Administrative Password**. This password is **the last 6 digits of the MBR1200's MAC address** found on the side panel of the MBR1200 product box or the bottom of the MBR1200.
- After you enter the password, click the **Log In** button.
- After you are logged in, click on the **BASIC** menu tab at the top of the setup window. Next, click the **Launch Setup Wizard** button in the middle of the screen.
- Follow the instructions in the Setup Wizard (Outlined in section 4.2 of this document: Wizard) to complete the setup **(Basic → Wizard)**.
- After security setup has been completed, continue to the next Step to use your new Security- Enabled Internet Connection.



The default password is the last six digits of the router's MAC address.

Password :

Copyright © 2009 CradlePoint Technology Inc. All rights reserved.



The following Web-based Setup Wizard is designed to assist you in connecting your new router to the Internet. This Setup Wizard will guide you through step-by-step instructions on how to get your Internet connection up and running. Click the button below to begin.

Select System Language: English

Note: Before launching this wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

Copyright © 2009 CradlePoint Technology Inc. All rights reserved.

3.3.3 Connect to the Internet

Using any device with a supported browser, open a browser window.

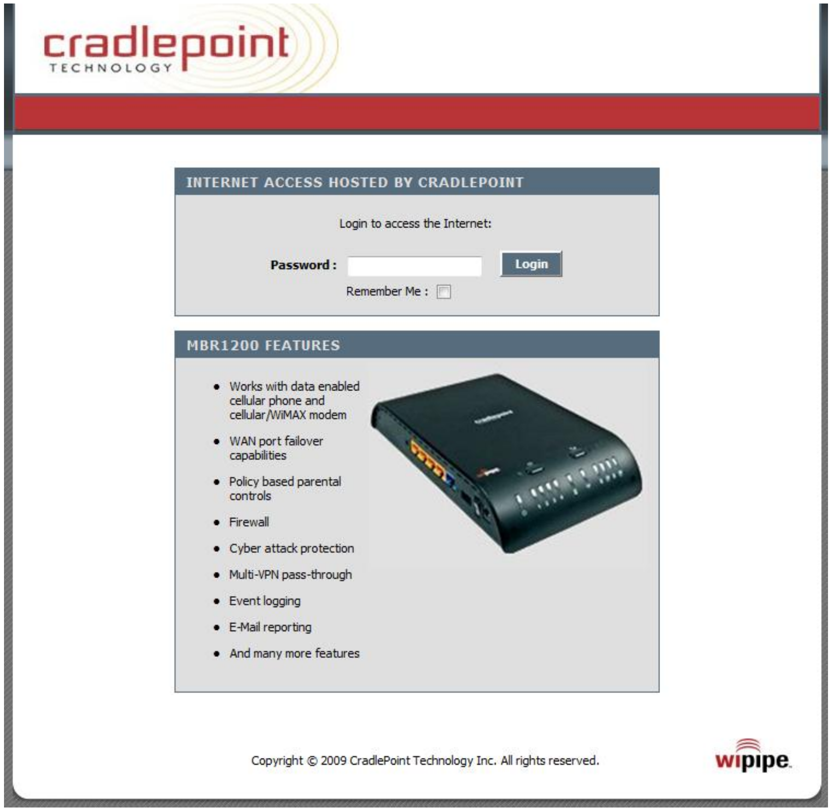
A default CradlePoint page will appear asking for a password.

Use the password you assigned in the **Basic Wizard Setup**. If you did not change the password, or have not yet setup your wireless network security, use the default password. The default password is the last six digits of the MBR1200's MAC address. The MAC address can be found on the MBR1200 product box or the bottom of the MBR1200.

Enter the password and click the **Login** button.

After login, you will be able to click on a **Remember Me** button so that so that the next time user device connects to the MBR1200, no password is needed.

Remember: This password is necessary to protect against unauthorized access to your system.



INTERNET ACCESS HOSTED BY CRADLEPOINT

Login to access the Internet:

Password :

Remember Me : □

MBR1200 FEATURES

- Works with data enabled cellular phone and cellular/WiMAX modem
- WAN port failover capabilities
- Policy based parental controls
- Firewall
- Cyber attack protection
- Multi-VPN pass-through
- Event logging
- E-Mail reporting
- And many more features

Copyright © 2009 CradlePoint Technology Inc. All rights reserved.

3.4 Common Problems

This section contains a list of some of the most common issues faced by users of the MBR1200.

Please visit CradlePoint Knowledgebase at http://knowledgebase.cradlepoint.com/ for more help and answers to your other questions.

3.4.1 Your USB Modem or Phone Does Not Work With the Router

- If your USB data modem or phone is not working with the router, check the list of supported devices to ensure you are using a supported device and carrier. The device you're 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.
  CradlePoint's supported device list changes regularly. We update our supported device list after a device is certified and approved. If the device you have is NOT on the list, that means we do not support it at this time.
  The SUPPORTED DEVICE list can be found at: **cradlepoint.com/support/MBR1200**

- 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 MBR1200. Simply insert your USB data modem into your PC and using the software provided by your cellular carrier, access the Internet. 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 4G modem you need to set the WiMAX Realm. This can be done at the administrative page (login to IP address http://192.168.0.1**)** and go to **Modem → Settings**. Under Modem Specific Settings use the **WiMAX Realm Select** to select your carrier. Make sure you Save Settings.

- Some wireless carriers provide multiple Access Point Names that a modem can connect to. If you wish to specify an APN, this can be done at the administrative page (login to IP address http://192.168.0.1**)** and go to **Modem → Settings.** Enter the APN and **Save Settings**. Some examples of APN are **isp.cingular**, **ecp.tmobile.com** and **vpn.com**. This APN will be set in the first profile position (see **Modem Diagnostics**). The modem must be removed and reinserted for this change to take affect (or the router rebooted). This APN is associated with the modem in the interface referred to in the **Modem Interface** drop down menu, so multiple APNs may be entered.

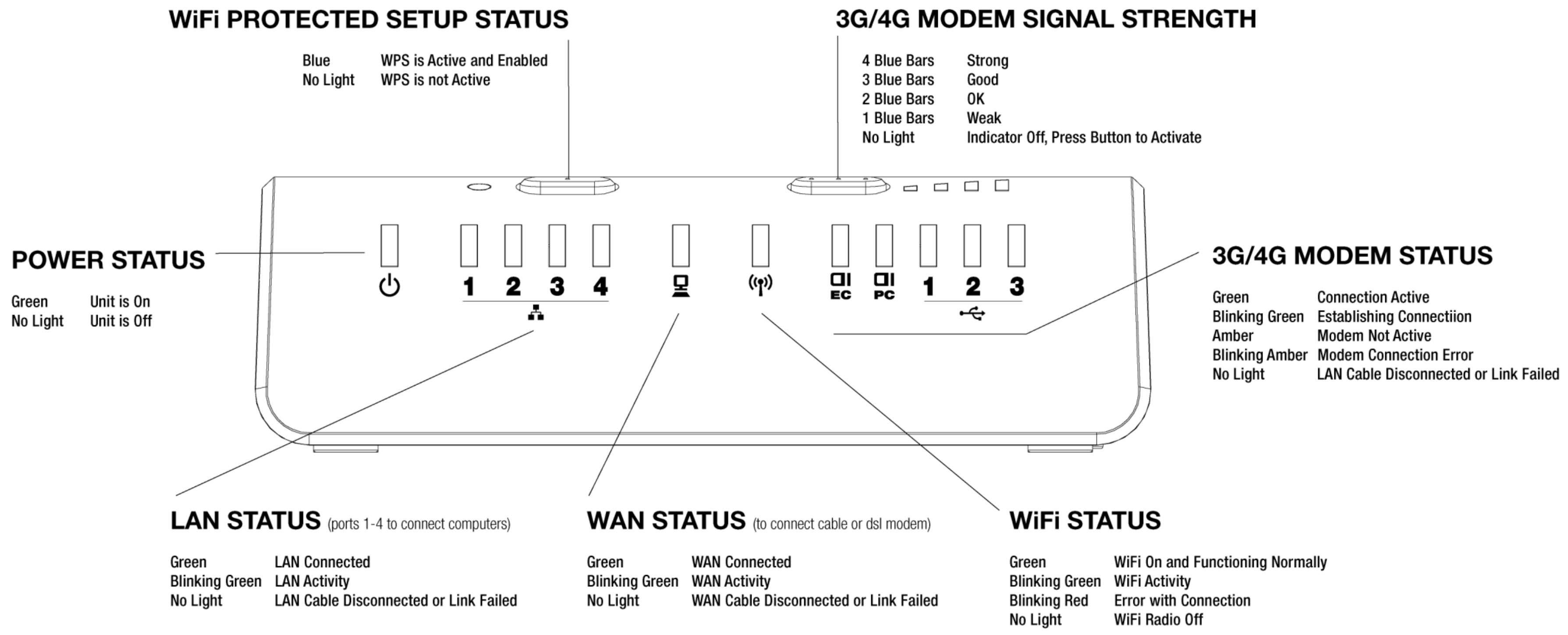
- If the above issues have been resolved and you can connect to the router but not get internet through it using your modem you may need to upgrade the router firmware. Use your computer (you may need to plug your modem directly into your computer if you don't have another way to access the internet) to download the latest firmware for the router (found at: www.cradlepoint.com/support/mbr1200). Then login to the router admin page and manually upload the firmware (directions can be found in this manual in section 7.4.2).

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

3.4.2 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 USB Data Modem LEDs are not illuminated, your modem is not connected and online. You may need to update firmware. Refer to "Your USB Modem or Phone Does Not Work With The Router."



WiFi PROTECTED SETUP STATUS

Blue	WPS is Active and Enabled
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	Unit is On
No Light	Unit is Off

3G/4G MODEM STATUS

Green	Connection Active
Blinking Green	Establishing Connectiion
Amber	Modem Not Active
Blinking Amber	Modem Connection Error
No Light	LAN Cable Disconnected or Link Failed

LAN STATUS (ports 1-4 to connect computers)

Green	LAN Connected
Blinking Green	LAN Activity
No Light	LAN Cable Disconnected or Link Failed

WAN STATUS (to connect cable or dsl modem)

Green	WAN Connected
Blinking Green	WAN Activity
No Light	WAN Cable Disconnected or Link Failed

WiFi STATUS

Green	WiFi On and Functioning Normally
Blinking Green	WiFi Activity
Blinking Red	Error with Connection
No Light	WiFi Radio Off

If you are still not online after updating, call CradlePoint Technical Support for further assistance.

3.4.3 My Wi-Fi-enabled Devices Can't Get Past the Login Page

Some electronic devices may experience problems handling the Internet Access User Login setting. Devices that commonly have trouble are, but not limited to:

- iPod Touch
- iPhone
- Wireless VoIP Phones
- Wireless Printers
- Most Wi-Fi-enabled Video Game Systems
- Most Wi-Fi-enabled Devices that are not PCs or Macs

To Allow These Devices Access, follow the instructions below to disable the user login.

- Access your router administration page by opening your browser and typing **http://192.168.0.1** in the address bar.
- Go to the **TOOLS** tab on the top navigation, then the **USER LOGIN** menu on the left panel.
- Uncheck the **REQUIRE USER LOGIN** check box.
- Scroll to the top of the page and click **SAVE THE SETTINGS**, which will save and reboot the router with your new configuration.

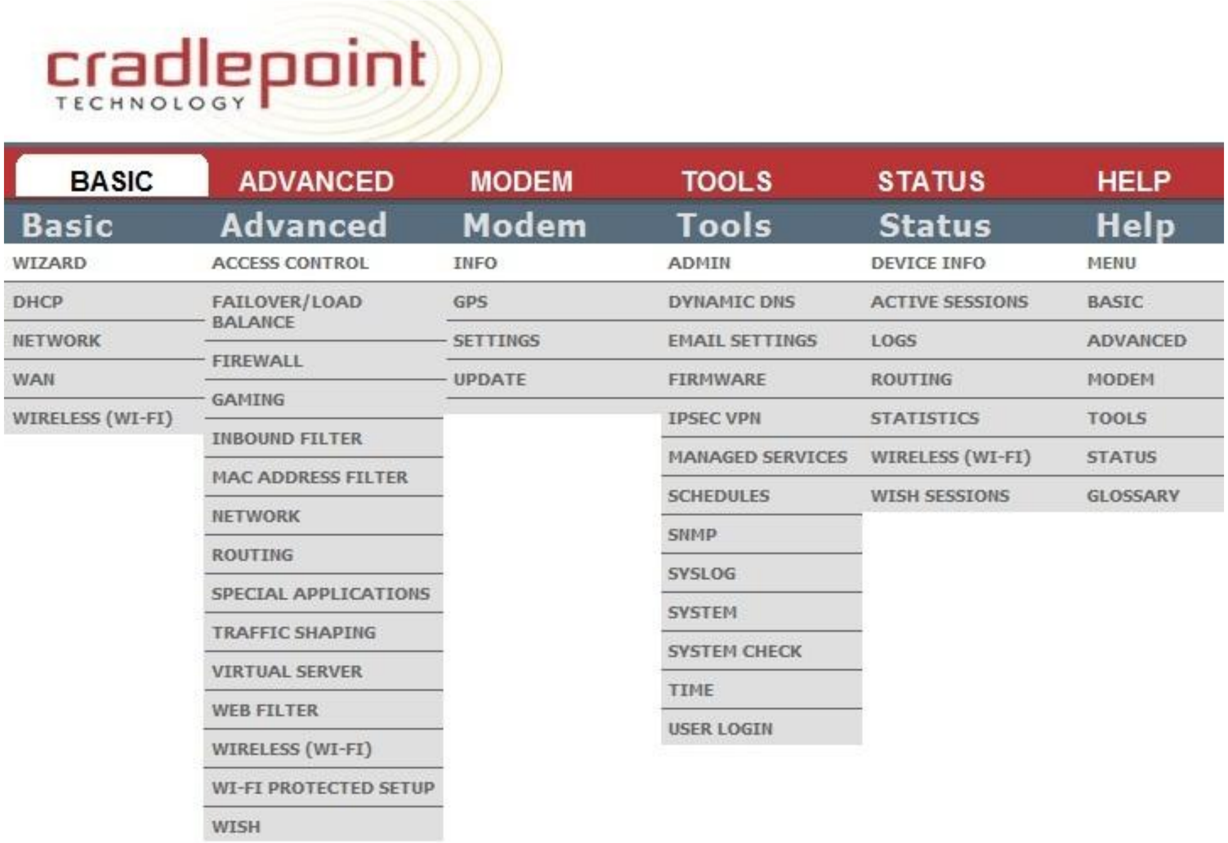
NOTE: Because the User Login page adds security and access control to others connected to your router, you may need to enable additional security features such as WEP, WPA, or MAC Address Filtering (if you are not already doing so) when turning off the User Login Page. See the “Setting Wi-Fi Security on your CradlePoint Router” section of this guide for details.

4 ADMINISTRATIVE TABS AND SUB-MENUS

The MBR1200 has a Web interface that provides a set of tabs and sub-menus for configuration and administration of all features. The interface is organized with 6 tabs at the top of the screen.

- Basic
- Advanced
- Modem
- Tools
- Status
- Help

Within each of the 6 tabs, there are sub-menus along the left side of the web page that you use to navigate to the specific function/task you wish to manage.

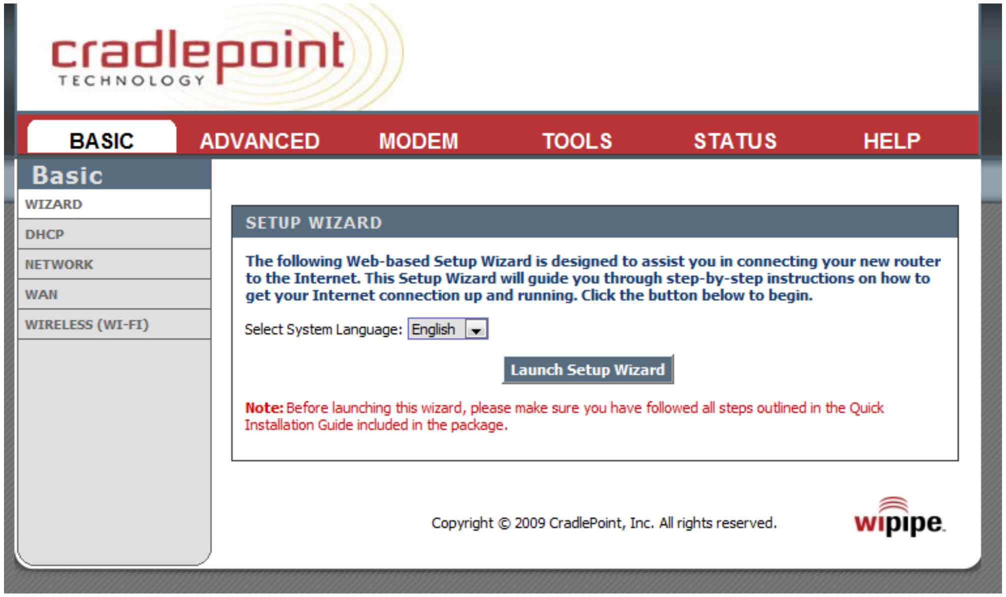


BASIC	ADVANCED	MODEM	TOOLS	STATUS	HELP
Basic	Advanced	Modem	Tools	Status	Help
WIZARD	ACCESS CONTROL	INFO	ADMIN	DEVICE INFO	MENU
DHCP	FAILOVER/LOAD BALANCE	GPS	DYNAMIC DNS	ACTIVE SESSIONS	BASIC
NETWORK	FIREWALL	SETTINGS	EMAIL SETTINGS	LOGS	ADVANCED
WAN	GAMING	UPDATE	FIRMWARE	ROUTING	MODEM
WIRELESS (WI-FI)	INBOUND FILTER		IPSEC VPN	STATISTICS	TOOLS
	MAC ADDRESS FILTER		MANAGED SERVICES	WIRELESS (WI-FI)	STATUS
	NETWORK		SCHEDULES	WISH SESSIONS	GLOSSARY
	ROUTING		SNMP		
	SPECIAL APPLICATIONS		SYSLOG		
	TRAFFIC SHAPING		SYSTEM		
	VIRTUAL SERVER		SYSTEM CHECK		
	WEB FILTER		TIME		
	WIRELESS (WI-FI)		USER LOGIN		
	WI-FI PROTECTED SETUP				
	WISH				

4.1 Basic Tab

The Basic tab provides access to the 5 sub-menus for administering the following function/tasks:

- WIZARD
- DHCP
- NETWORK
- WAN
- WIRELESS (WI-FI)



SETUP WIZARD

The following Web-based Setup Wizard is designed to assist you in connecting your new router to the Internet. This Setup Wizard will guide you through step-by-step instructions on how to get your Internet connection up and running. Click the button below to begin.

Select System Language: English

Note: Before launching this wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

Copyright © 2009 CradlePoint, Inc. All rights reserved.

4.2 Wizard (Setup Wizard)

Use the Setup Wizard to execute the minimum recommended first steps to set up the product. (NOTE: Before launching the Configuration Wizard, you must have followed all the steps outlined in the Quick Start Guide included in the product package)

4.2.1 Launch Setup Wizard.

Launch Setup Wizard. Click the **Launch Setup Wizard** button to start the wizard.

4.2.2 Welcome to the Setup Wizard.

Next/Cancel. Click **Next** to start the Setup Wizard

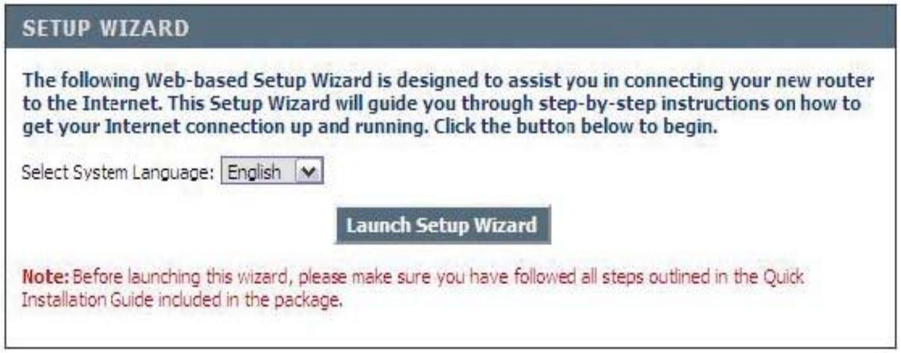
4.2.3 Set your password and time zone.

Password. Enter a password for administrative access. Verify. Re-enter the password. Time Zone. Click on the drop down menu and select the appropriate time zone.

Verify. Re-enter the password

Time Zone. Click on the drop down menu and select the appropriate time zone.

(continued)

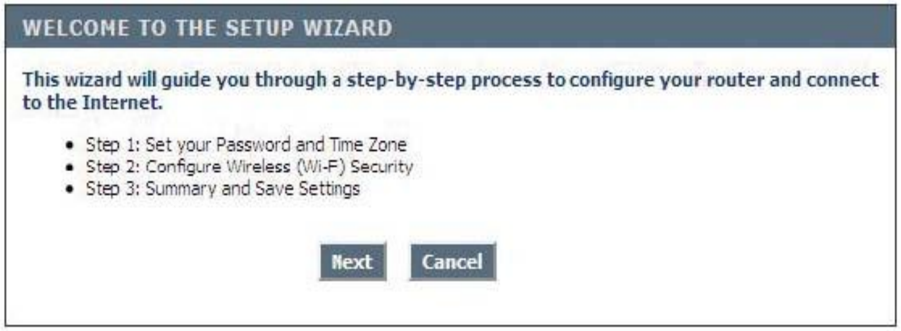


SETUP WIZARD

The following Web-based Setup Wizard is designed to assist you in connecting your new router to the Internet. This Setup Wizard will guide you through step-by-step instructions on how to get your Internet connection up and running. Click the button below to begin.

Select System Language: English

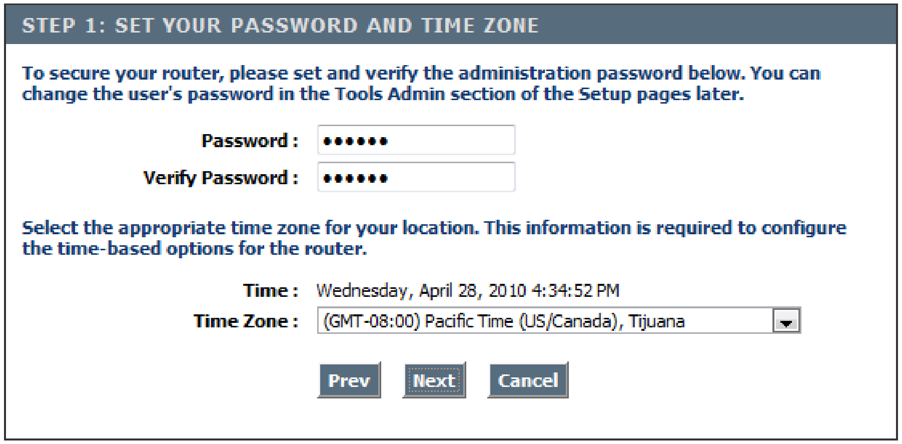
Note: Before launching this wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.



WELCOME TO THE SETUP WIZARD

This wizard will guide you through a step-by-step process to configure your router and connect to the Internet.

- Step 1: Set your Password and Time Zone
- Step 2: Configure Wireless (Wi-F) Security
- Step 3: Summary and Save Settings



STEP 1: SET YOUR PASSWORD AND TIME ZONE

To secure your router, please set and verify the administration password below. You can change the user's password in the Tools Admin section of the Setup pages later.

Password : ••••••

Verify Password : ••••••

Select the appropriate time zone for your location. This information is required to configure the time-based options for the router.

Time : Wednesday, April 28, 2010 4:34:52 PM

Time Zone : (GMT-08:00) Pacific Time (US/Canada), Tijuana

4.2.4 Configure Wireless Security

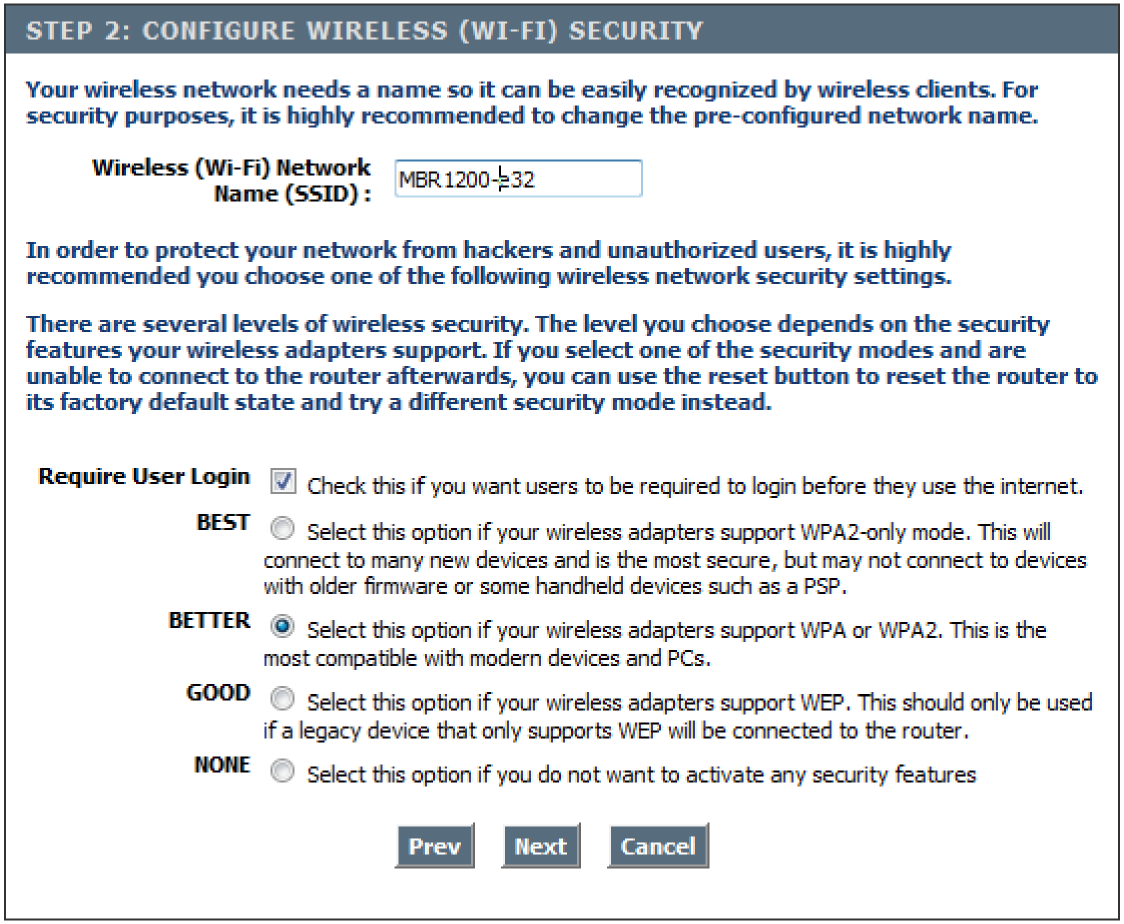
Wireless (Wi-Fi) Network Name (SSID). Enter a name for the wireless network. For security purposes, it is highly recommended that you change the pre-configured network name. NOTE: Be sure to write down the new SSID and keep it in a safe place.

Require User Login. With the box checked, users will be required to login before they can access the internet. With the box unchecked, users will NOT be required to login before they can access the internet.

WPS, Best, Better, Good, None. Choose one of four levels of security, or none.

NOTE: The wireless adapters installed on the wireless clients accessing the MBR1200 must be able to support the security level you choose.

(continued)



STEP 2: CONFIGURE WIRELESS (WI-FI) SECURITY

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name.

Wireless (Wi-Fi) Network Name (SSID) : MBR1200-e32

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

There are several levels of wireless security. The level you choose depends on the security features your wireless adapters support. If you select one of the security modes and are unable to connect to the router afterwards, you can use the reset button to reset the router to its factory default state and try a different security mode instead.

Require User Login ☑ Check this if you want users to be required to login before they use the internet.

BEST ○ Select this option if your wireless adapters support WPA2-only mode. This will connect to many new devices and is the most secure, but may not connect to devices with older firmware or some handheld devices such as a PSP.

BETTER ● Select this option if your wireless adapters support WPA or WPA2. This is the most compatible with modern devices and PCs.

GOOD ○ Select this option if your wireless adapters support WEP. This should only be used if a legacy device that only supports WEP will be connected to the router.

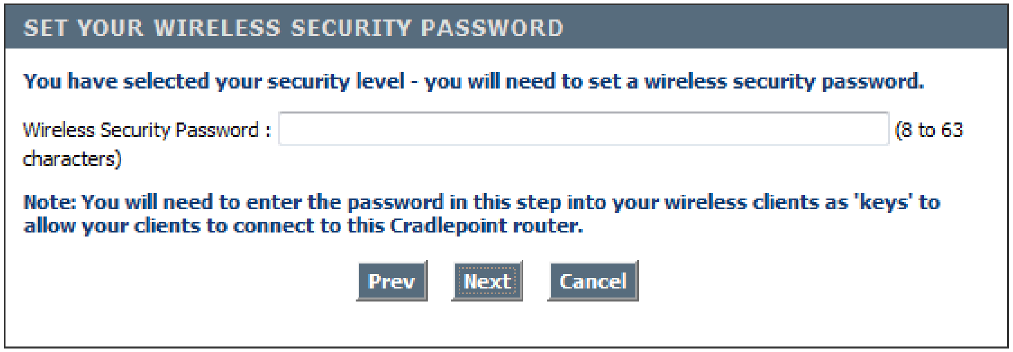
NONE ○ Select this option if you do not want to activate any security features

4.2.5 Set Your Wireless Security Password.

Wireless Security Password. If you have selected one of the four security levels, you will be prompted to enter a **Wireless Security Password**. This is the password that wireless clients will use to access the MBR1200 wireless network.

NOTE: Be sure to write down the password and keep it in a safe place.

If you chose **None** for security, you will not see the **Set Your Wireless Security Password** screen and will be directed to the **Setup Complete** screen.



SET YOUR WIRELESS SECURITY PASSWORD

You have selected your security level - you will need to set a wireless security password.

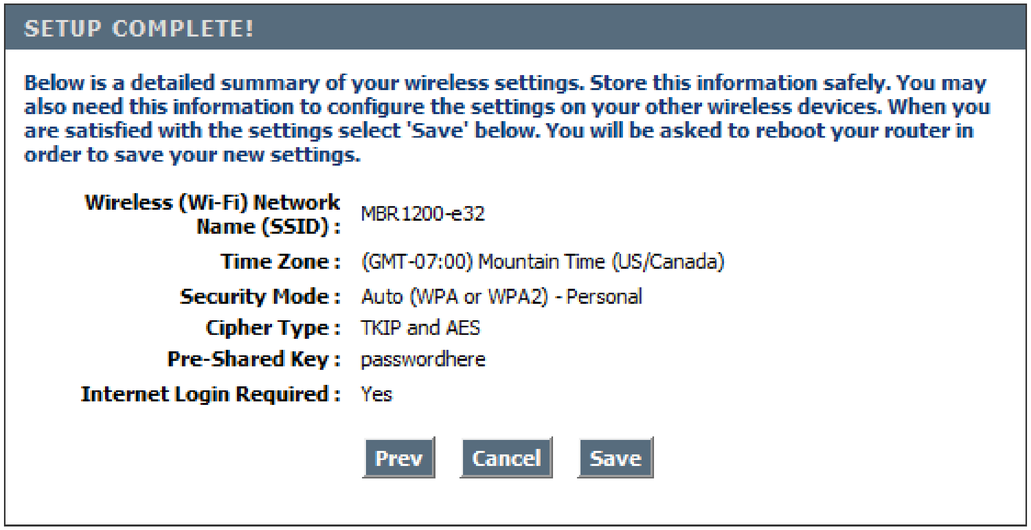
Wireless Security Password : (8 to 63 characters)

Note: You will need to enter the password in this step into your wireless clients as 'keys' to allow your clients to connect to this Cradlepoint router.

4.2.6 Setup Complete.

This screen summarizes the wireless settings you have chosen. NOTE: Make sure you write down this information and keep it in a safe place. You will need some of this information to configure wireless clients and other settings on the MBR1200.

Click **Save**. This will restart the router and enable the settings you have selected.



SETUP COMPLETE!

Below is a detailed summary of your wireless settings. Store this information safely. You may also need this information to configure the settings on your other wireless devices. When you are satisfied with the settings select 'Save' below. You will be asked to reboot your router in order to save your new settings.

Wireless (Wi-Fi) Network Name (SSID) :	MBR1200-e32
Time Zone :	(GMT-07:00) Mountain Time (US/Canada)
Security Mode :	Auto (WPA or WPA2) - Personal
Cipher Type :	TKIP and AES
Pre-Shared Key :	passwordhere
Internet Login Required :	Yes

4.3 DHCP (DHCP Settings)

DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN).

Use the DHCP sub-menu to configure the built-in DHCP Server to assign IP addresses to the computers and other devices on the local area network.

4.3.1 DHCP Server Settings

Enable DHCP Server. (Default: Enabled). Once your MBR1200 router is properly configured and this option is enabled, the DHCP Server will manage the IP addresses and other network configuration information for computers and other devices connected to your Local Area Network. There is no need for you to do this yourself.

The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to "DHCP" or "Obtain an IP address automatically".

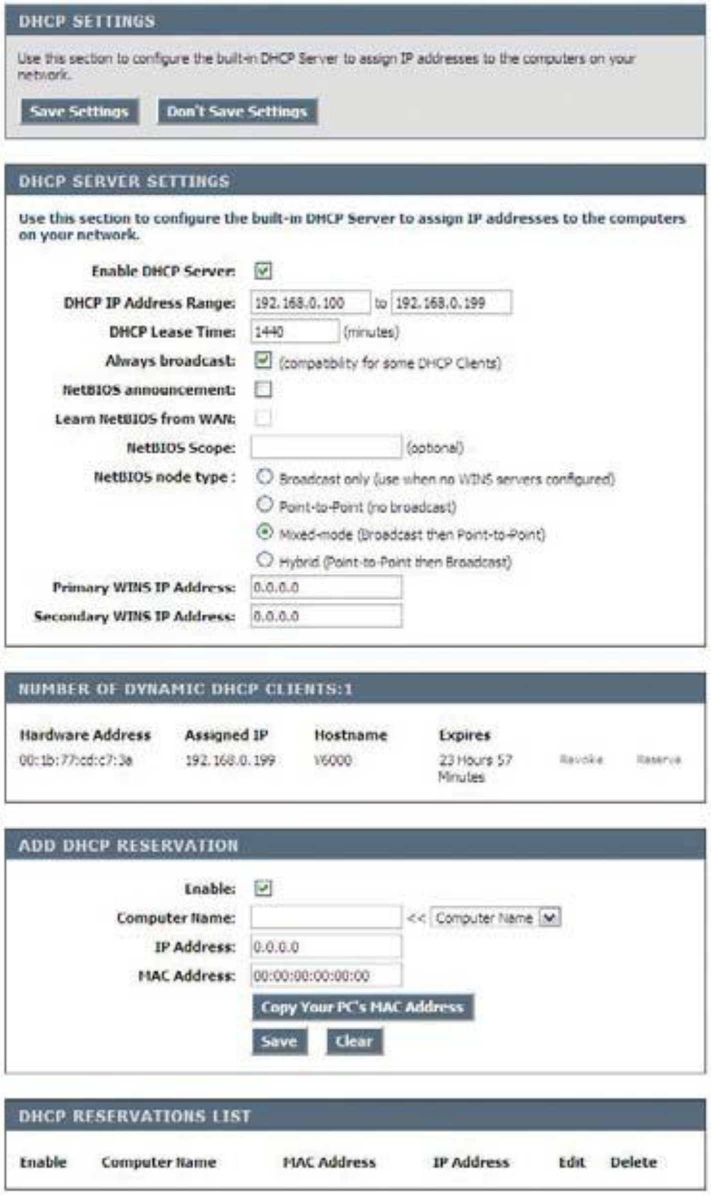
When you set **Enable DHCP Server**, the following options are displayed.

DHCP IP Address Range. (Default: 192.168.0.100-192.168.0.199). This option defines the range of addresses available for the MBR1200 to assign to an internal network. If there are any devices using static IP addresses, you must be sure the addresses do not fall within the range defined here. A Static IP address is one that is entered in manually on the device.

Example: The MBR1200 uses an IP address of 192.168.0.1. 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 above.

DHCP Lease Time. (Default: 1440 minutes [24 hours]). The amount of time a computer may have an IP address before it is required to renew the lease. The initial lease designates the amount of time before the lease expires. If the lease expires and the address is no longer needed, then another tenant may use the address. Units are in minutes, however a value of zero (0) means the lease never expires.

Always Broadcast. If all the computers on the LAN successfully obtain their IP addresses from the router’s DHCP server, this option can remain disabled. However, if



Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

Enable DHCP Server: ☑

DHCP IP Address Range: 192.168.0.100 to 192.168.0.199

DHCP Lease Time: 1440 (minutes)

Always broadcast: ☑ (compatibility for some DHCP Clients)

NetBIOS announcement: □

Learn NetBIOS from WAN: □

NetBIOS Scope: (optional)

NetBIOS node type :
○ Broadcast only (use when no WINS servers configured)
○ Point-to-Point (no broadcast)
● Mixed-mode (Broadcast then Point-to-Point)
○ Hybrid (Point-to-Point then Broadcast)

Primary WINS IP Address: 0.0.0.0

Secondary WINS IP Address: 0.0.0.0

Hardware Address	Assigned IP	Hostname	Expires
00:1b:77:cd:c7:3a	192.168.0.199	V6000	23 Hours 57 Minutes

Enable: ☑

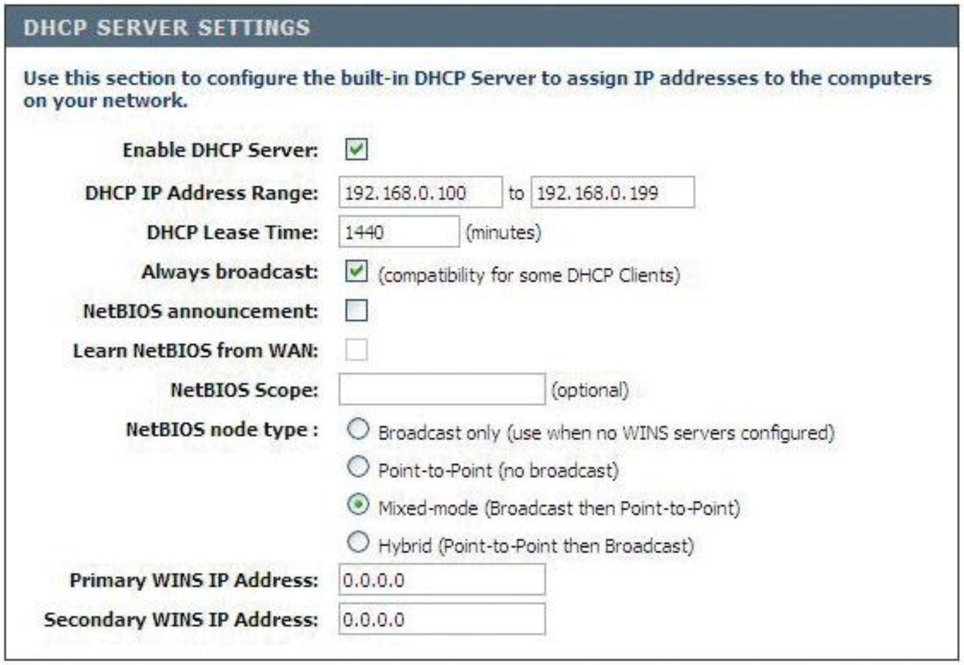
Computer Name: << Computer Name

IP Address: 0.0.0.0

MAC Address: 00:00:00:00:00:00

Enable	Computer Name	MAC Address	IP Address	Edit	Delete

one of the computers on the LAN fails to obtain an IP address, it may have an old DHCP client that incorrectly turns off the broadcast flag of DHCP packets. Enabling **Always Broadcast** will cause the router to always broadcast its responses to all clients, thereby working around the problem (at the cost of increased broadcast traffic on the LAN).



DHCP SERVER SETTINGS

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

Enable DHCP Server:	☑
DHCP IP Address Range:	192.168.0.100 to 192.168.0.199
DHCP Lease Time:	1440 (minutes)
Always broadcast:	☑ (compatibility for some DHCP Clients)
NetBIOS announcement:	□
Learn NetBIOS from WAN:	□
NetBIOS Scope:	(optional)
NetBIOS node type :	○ Broadcast only (use when no WINS servers configured) ○ Point-to-Point (no broadcast) ● Mixed-mode (Broadcast then Point-to-Point) ○ Hybrid (Point-to-Point then Broadcast)
Primary WINS IP Address:	0.0.0.0
Secondary WINS IP Address:	0.0.0.0

NetBIOS Announcement. Check this box to allow the DHCP Server to offer NetBIOS configuration settings to the LAN hosts. NetBIOS allows LAN hosts to discover all other computers within the network, e.g. within "Network Neighborhood."

Learn BIOS from WAN. If NetBIOS advertisement is switched on, WINS information will be learned from the WAN side, if available. Turn this setting off to configure manually.

NetBIOS Scope. This is an advanced setting and is normally left blank. This allows the configuration of a NetBIOS "domain" name under which network hosts operate. This setting has no effect if the **Learn NetBIOS information from WAN** is activated.

NetBIOS Node Type. Indicates how network hosts are to perform NetBIOS name registration and discovery. This setting has no effect if the **Learn**

NetBIOS information from WAN is activated.

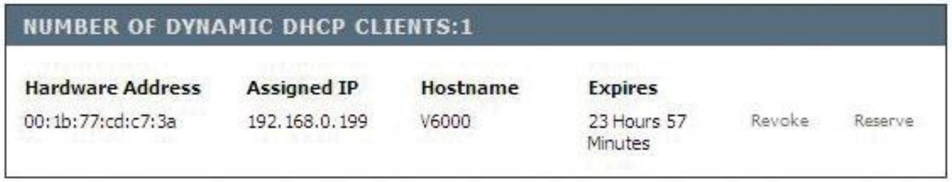
- **Broadcast only.** This setting is useful where there are no WINS servers available, however, it is preferred you try **Mixed-Mode** operation first.
- **Point-to-Point** Mode. This setting indicates to use WINS servers ONLY. This setting is useful to force all NetBIOS operation to the configured WINS servers. You must have configured at least the primary WINS server IP to point to a working WINS server.
- **Mixed-Mode** (default). First broadcast operation is performed to register hosts and discover other hosts, if broadcast operation fails, WINS servers are tried, if any. This mode favors broadcast operation which may be preferred if WINS servers are reachable by a slow network link and the majority of network services such as servers and printers are local to the LAN.
- **Hybrid-State.** First WINS servers are tried, if any, followed by local network broadcast. This is generally the preferred mode if you have configured WINS servers.

Primary WINS IP Address. Configure the IP address of the preferred WINS server. WINS Servers store information regarding network hosts, allowing hosts to 'register' themselves as well as discover other available hosts, e.g. for use in "Network Neighborhood." This setting has no effect if the **Learn NetBIOS information from WAN** is activated.

Secondary WINS IP Address. Configure the IP address of the backup WINS server, if any. This setting has no effect if the **Learn NetBIOS information from WAN** is activated.

4.3.2 Number of Dynamic DHCP Clients.

This section displays what devices are currently leasing IP addresses. The DHCP Client table displays the number of clients that are receiving an IP address from the router, the computer name, MAC address, and IP address assigned to each computer. You can use the **Revoke IP address** option to take away a leased IP address from a client. This feature is useful for freeing up addresses when the client table is full or nearly full.

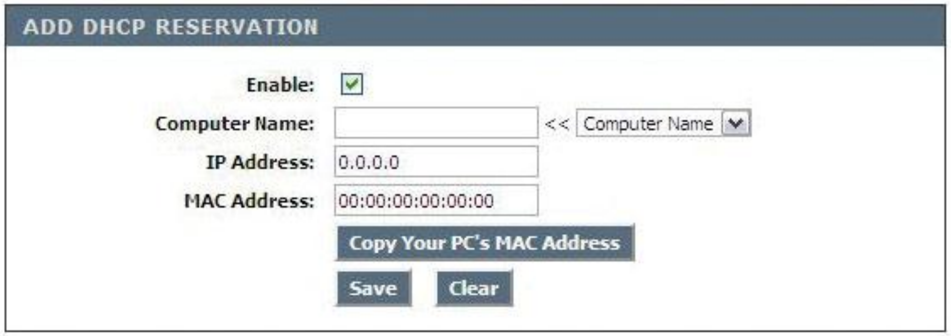


NUMBER OF DYNAMIC DHCP CLIENTS:1

Hardware Address	Assigned IP	Hostname	Expires		
00:1b:77:cd:c7:3a	192.168.0.199	V6000	23 Hours 57 Minutes	Revoke	Reserve

4.3.3 Add DHCP Reservation

Clients configured as DHCP can receive the same IP address all the time using this feature. This is almost the same as if a device has a static IP address except that it must still actually request an IP address from the MBR1200. The MBR1200 will provide the device the same IP address all the time. Servers on the network should either use a static IP address or this option.



ADD DHCP RESERVATION

Enable: ☑

Computer Name: << Computer Name

IP Address: 0.0.0.0

MAC Address: 00:00:00:00:00:00

Enable. Specifies whether the entry will be active or inactive.

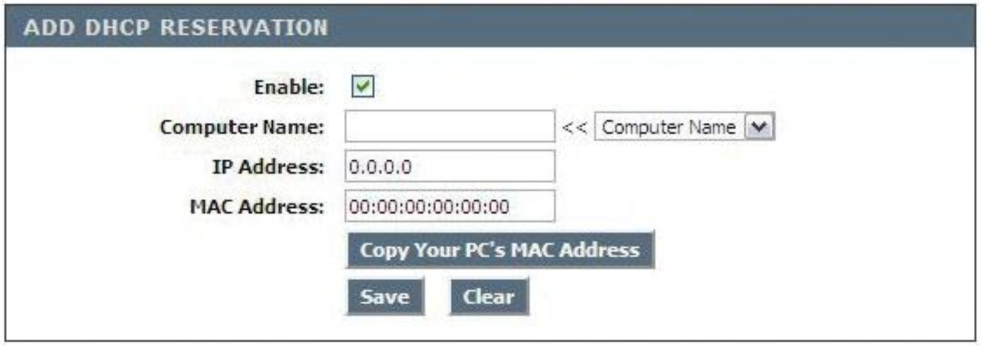
Computer Name. You can assign a name for each computer that is given a reserved IP address. This may help you keep track of which computers are assigned this way. Example: **Game Server**.

IP Address. The LAN address that you want to reserve.

MAC Address. To input the MAC address of your system, enter it manually or connect to the router's Web-Management interface from the system and click the **Copy Your PC's MAC Address** button.

A MAC address is usually located on a sticker on the bottom of a network device. The MAC address is comprised of twelve digits. Each pair of hexadecimal digits are usually separated by dashes or colons such as 00-0D-88-11-22-33 or 00:0D:88:11:22:33. If your network device is a computer and the network card is already located inside the computer, you can connect to the router from the computer and click the **Copy Your PC's MAC Address** button to enter the MAC address.

(continued)



ADD DHCP RESERVATION

Enable: ☑

Computer Name: << Computer Name

IP Address: 0.0.0.0

MAC Address: 00:00:00:00:00:00

As an alternative, you can locate a MAC address in a specific operating system by following the steps below:

- Windows 98/Windows Me. Go to the computer's **Start** menu, select **Run**, type in **winipcfg**, and hit **Enter**. A popup window will be displayed. Select the appropriate adapter from the pull-down menu and you will see the Adapter Address. This is the MAC address of the device.
- Windows 2000/Windows XP/Windows 7. Go to the computer's Start menu, select **Programs**, select **Accessories**, and select **Command Prompt**. At the command prompt, type in **ipconfig /all** and hit **Enter**. The physical address displayed for the adapter connecting to the router is the MAC address.
- Mac OS X. Go to the computer's Apple Menu, select **System Preferences**, select **Network**, and select the **Ethernet Adapter** connecting to the router. Select the **Ethernet** button and the **Ethernet ID** will be listed. This is the same as the MAC.

Save/Update. Record the changes you have made.

Clear. Re-initialize this area of the screen, discarding any changes you have made.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

Example: A DHCP reservation is used for making sure the router always gives a computer or device the same IP address. Let's say you have a Wi-Fi printer that you want to access via the Internet. You can connect to the CradlePoint Router from the Wi-Fi printer designated in this section.

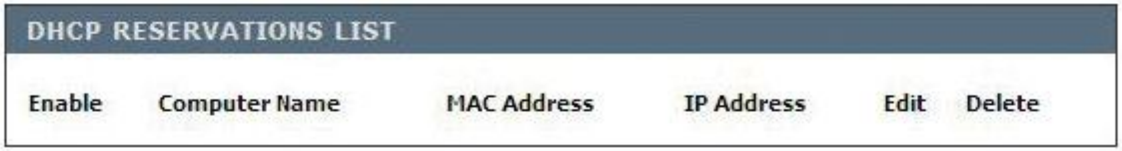
1. Enter a designated IP address somewhere between the **Starting IP** and **Ending IP** addresses.
2. Click the **Copy Your PC's MAC Address** button and the MBR1200 will detect the MAC address of the device and enter it automatically.
3. The printer name can be entered in for reference but is not required.
4. Click the **Save Settings** button at the top of the page.

The IP address will now only be assigned to the designated Wi-Fi printer and it will always receive the same IP address as long as it uses the same wireless adapter.

Default: No static DHCP clients.

NOTE: If you replace the wireless adapter in a computer that is using Static DHCP, you will need to click the Copy the PC's MAC Address button again because every wireless adapter has a unique MAC address. The same goes for any network device. If you replace a network device such as a print server, you will need to input the MAC address of the new print server into the Static DHCP configuration.

4.3.4 DHCP Reservation List



DHCP RESERVATIONS LIST

Enable	Computer Name	MAC Address	IP Address	Edit	Delete

The section shows the current DHCP Reservation List. Certain required routes are predefined and cannot be changed. Routes that you add can be changed by clicking the **Edit** icon or can be deleted by clicking the **Delete** icon. When you click the **Edit** icon, the item is highlighted, and the **DHCP Reservation List** section is activated for editing. Click the **Enable** check box at the left to directly activate or de-activate the entry.

After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted **to Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with all configuration settings, click the **Reboot the Device** button.

Default: empty list.

4.4 Network

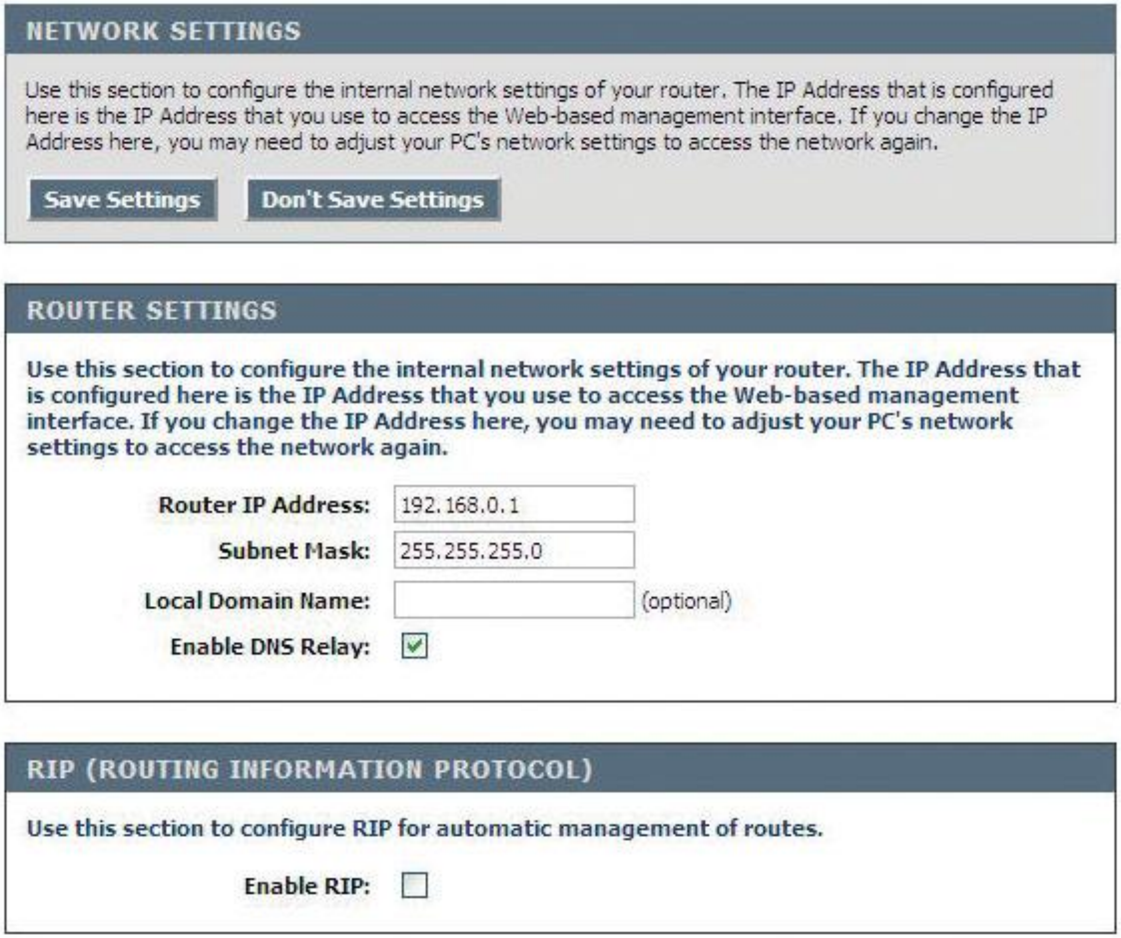
Use the Basic Network sub-menu to establish the local IP address for the router. These are the settings of the LAN (Local Area Network) interface for the router. The router's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this sub-menu. The IP address is also used to access this Web-based management Interface. It is recommended that you use the default settings if you do not have an existing network.

4.4.1 Router Settings.

Router IP Address. The IP address of your router on the local area network. Your local area network settings are based on the address assigned here. For example, **192.168.0.1**

Subnet Mask. The subnet mask of your router on the local area network.

Local Domain Name. This entry is optional. Enter a domain name for the local network. LAN computers will assume this domain name when they get an address from the router's built in DHCP server. So, for example, if you enter **mynetwork.net** here, and you have a LAN side laptop with a name of **chris**, that laptop will be known as **chris.mynetwork.net**. NOTE: the entered domain name can be overridden by the one obtained from the router's upstream DHCP server.



NETWORK SETTINGS

Use this section to configure the internal network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

ROUTER SETTINGS

Use this section to configure the internal network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
Local Domain Name:	(optional)
Enable DNS Relay:	☑

RIP (ROUTING INFORMATION PROTOCOL)

Use this section to configure RIP for automatic management of routes.

Enable RIP: □

Enable DNS Relay. When **DNS Relay** is enabled, the router plays the role of a DNS server. DNS requests sent to the router are forwarded to the ISP's DNS server. This provides a constant DNS address that LAN computers can use, even when the router obtains a different DNS server address from the ISP upon re-establishing the WAN connection. You should disable DNS relay if you implement a LAN-side DNS server as a virtual server.

(continued)

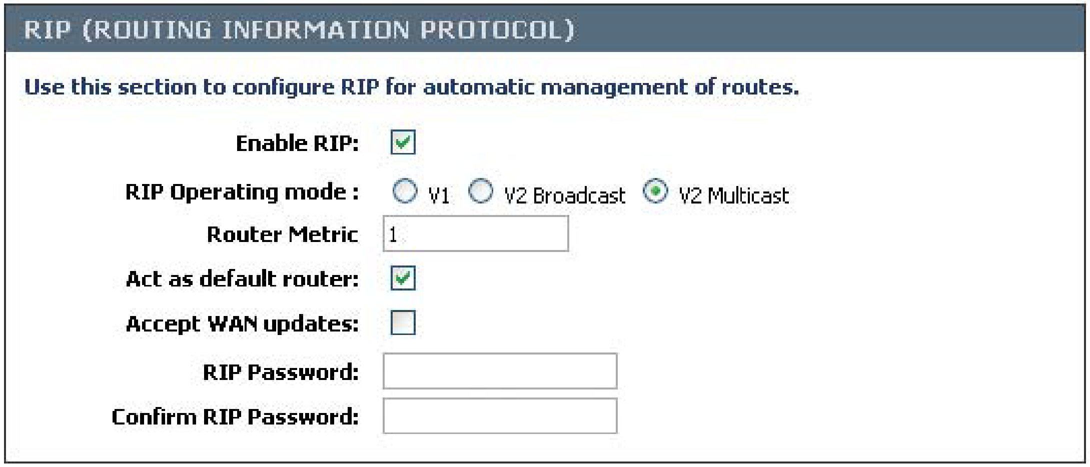
4.4.2 RIP (Router Information Protocol).

RIP is used to broadcast routing information among routers.

Enable RIP. Enable RIP if required by the ISP, if the LAN has multiple routers, or if the LAN has auto-IP devices. NOTE: When you select the **Enable RIP** check box, these additional features appear:

RIP Operating Mode. The MBR1200 router supports both version 2 and version 1 of the RIP specification.

- V1. Use if none of the routers supports Version 2.
- V2 Broadcast. Use if some routers are capable of Version 2, but some are only capable of Version 1.
- V2 Multicast. Use if this is the only router on the LAN or if all the routers support Version 2.



RIP (ROUTING INFORMATION PROTOCOL)

Use this section to configure RIP for automatic management of routes.

Enable RIP:	☑
RIP Operating mode :	○ V1 ○ V2 Broadcast ● V2 Multicast
Router Metric	1
Act as default router:	☑
Accept WAN updates:	□
RIP Password:	
Confirm RIP Password:	

Router Metric. The additional cost of routing a packet through this router. The normal value for a simple network is 1. This metric is added to routes learned from other routers; it is not added to static or system routes.

Act as Default Router. Make this router the preferred destination for packets that are not otherwise destined.

Accept WAN Updates. For security, disable this option unless required by the ISP.

RIP Password. RIP Version 2 supports the use of a password to limit access to routers through the RIP protocol. If the ISP or other LAN router requires a RIP password, enter the password here.

4.5 WAN Configuration

Use the WAN Configuration sub-menu to configure the network settings for the Wired and Cellular Modem WAN.

4.5.1 Cellular Modem PPP Authentication (optional).

Enter your Cellular Service Provider information in these three fields only if directed by your Cellular Service Provider.

Modem Interface. Modem interface is the physical port the modem is connected to. Select the appropriate port to change its settings.

Username. If required by your ISP, enter the username provided to you by your ISP. If not required by your ISP, leave this field blank.

Password. If required by your ISP, enter the password provided to you by your ISP. If not required by your ISP, leave this field blank.

Verify Password. Re-enter the password.

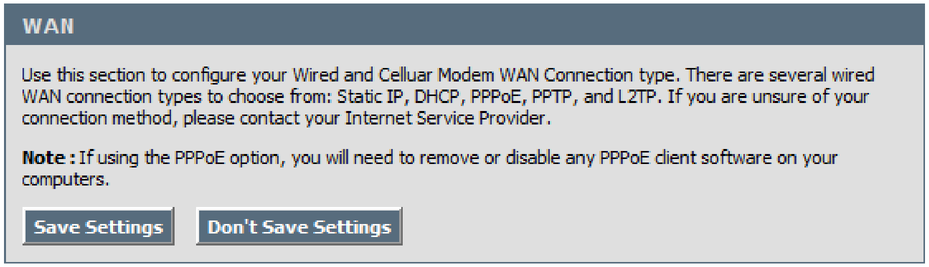
4.5.2 Wired WAN Connection Type.

There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP. If you are unsure of your connection method, please contact your Internet Service Provider. Note: If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers is removed or disabled.

Internet Service Provider. The MBR1200 will automatically determine your ISP. If it is not able to detect your ISP, choose your ISP from the drop down menu. If your ISP is not listed, choose **Not Listed or Don't Know**.

Internet Connection. If you select **Not Listed or Don't Know** option, use the **Internet Connection** drop down menu to identify the type of **Internet Connection** you have.

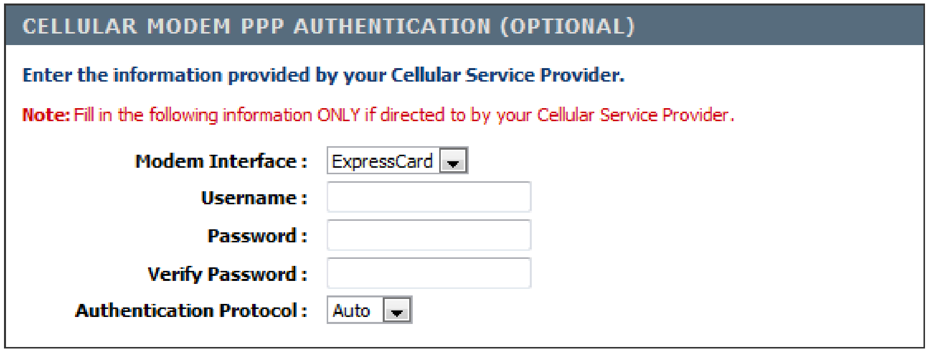
(continued)



WAN

Use this section to configure your Wired and Celluar Modem WAN Connection type. There are several wired WAN connection types to choose from: Static IP, DHCP, PPPoE, PPTP, and L2TP. If you are unsure of your connection method, please contact your Internet Service Provider.

Note : If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.



CELLULAR MODEM PPP AUTHENTICATION (OPTIONAL)

Enter the information provided by your Cellular Service Provider.

Note: Fill in the following information ONLY if directed to by your Cellular Service Provider.

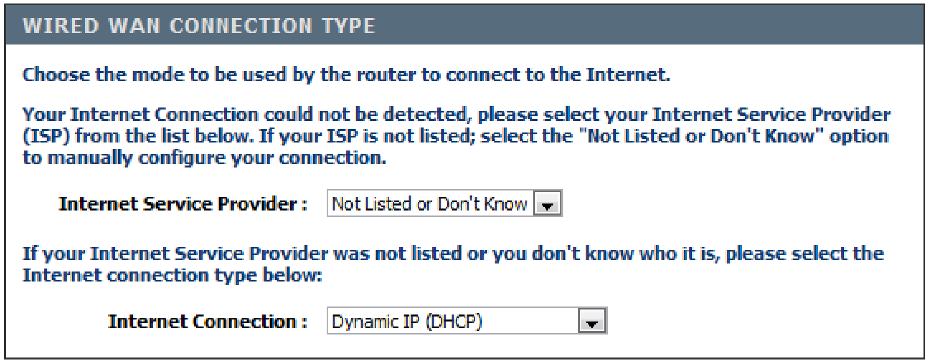
Modem Interface : ExpressCard

Username :

Password :

Verify Password :

Authentication Protocol : Auto



WIRED WAN CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

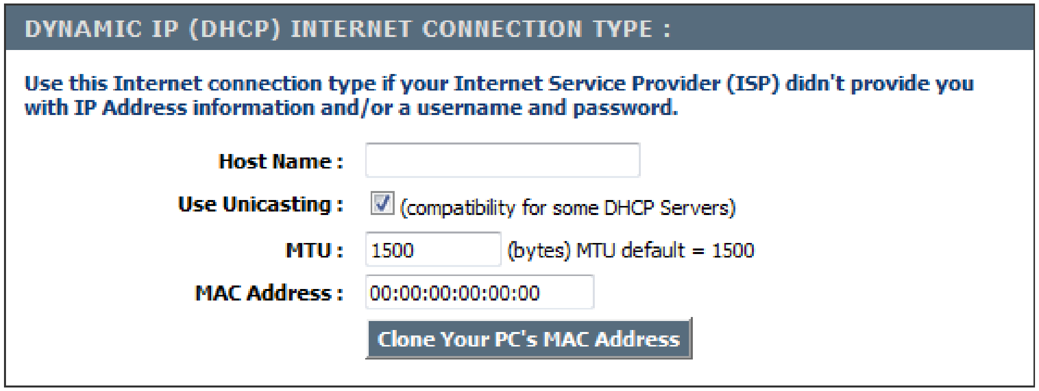
Your Internet Connection could not be detected, please select your Internet Service Provider (ISP) from the list below. If your ISP is not listed; select the "Not Listed or Don't Know" option to manually configure your connection.

Internet Service Provider : Not Listed or Don't Know

If your Internet Service Provider was not listed or you don't know who it is, please select the Internet connection type below:

Internet Connection : Dynamic IP (DHCP)

4.5.3 Dynamic (DHCP) Internet Connection Type.



DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE :

Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password.

Host Name :

Use Unicasting : ☑ (compatibility for some DHCP Servers)

MTU : 1500 (bytes) MTU default = 1500

MAC Address : 00:00:00:00:00:00

You will not need to complete this section unless your ISP requires you to.

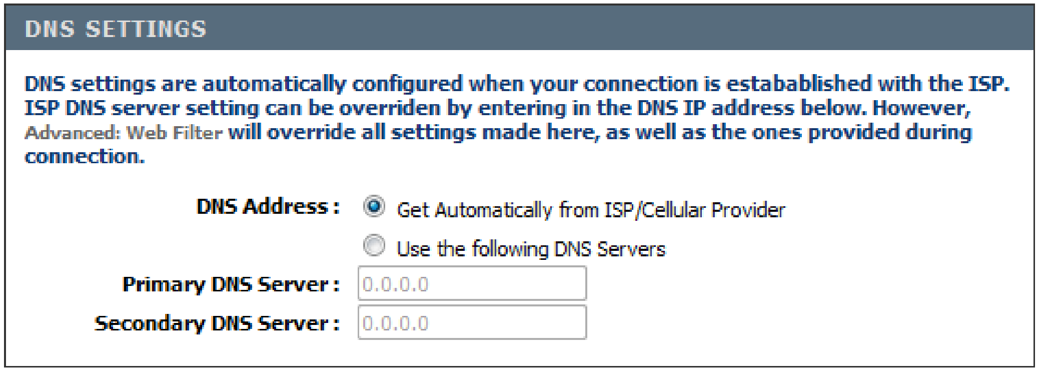
Host Name. Enter the host name provided to you by your ISP.

Use Unicasting. Select the check box if advised to so by your ISP.

MTU. Enter the MTU provided to you by your ISP (default: 1500).

MAC Address. To input the MAC address of your system, enter it manually or connect to the MBR1200's Web-Management interface from the system and click the **Clone Your PC's MAC Address** button.

4.5.4 DNS Settings



DNS SETTINGS

DNS settings are automatically configured when your connection is estabablished with the ISP. ISP DNS server setting can be overriden by entering in the DNS IP address below. However, Advanced: Web Filter will override all settings made here, as well as the ones provided during connection.

DNS Address : ● Get Automatically from ISP/Cellular Provider

○ Use the following DNS Servers

Primary DNS Server : 0.0.0.0

Secondary DNS Server : 0.0.0.0

Use the WAN Configuration sub-menu to configure the network settings for the Wired and Cellular Modem WAN (the first connected cellular handset or modem).

DNS Address. Select the **Get Automatically from ISP/Cellular Provider** radio button to acquire a DNS Address automatically from our ISP/Cellular Provider or select the **Use the Following DNS Servers** radio button to specify DNS Servers. NOTE: You would specify DNS Servers if you want Wi-Fi clients to access DNS servers that you use for customized addressing or if you have a local DNS server on your network.

Primary DNS Server. If you choose to use specify your DNS Servers, then enter the IP address of the server you want as your Primary DNS Server in this field.

Secondary DNS Server. If you choose to use specify your DNS Servers, then enter the IP address of the server you want as your Secondary DNS Server in this field.

4.6 Wireless (WI-FI)

Use the Wireless (Wi-Fi) sub-menu configure the wireless settings for the MBR1200. NOTE: changes made in this section may also need to be duplicated on wireless clients that you want to connect to your wireless network. Add Wireless Devices with WPS (WI-FI Protected Setup) Wizard

Add Wireless Device with WPS. This Wizard helps you add wireless devices to the wireless network using the Wi-Fi Protected Setup protocol.

The wizard will prompt you to enter the PIN for the device, or ask you to press the **Configuration** button on the device. If the device supports Wi-Fi Protected Setup and has a configuration button, you can add it to the network by pressing the **Configuration** button on the device and then the **WPS** button on the router within 60 seconds. The **WPS** status LED on the router will flash three times if the device has been successfully added to the network.

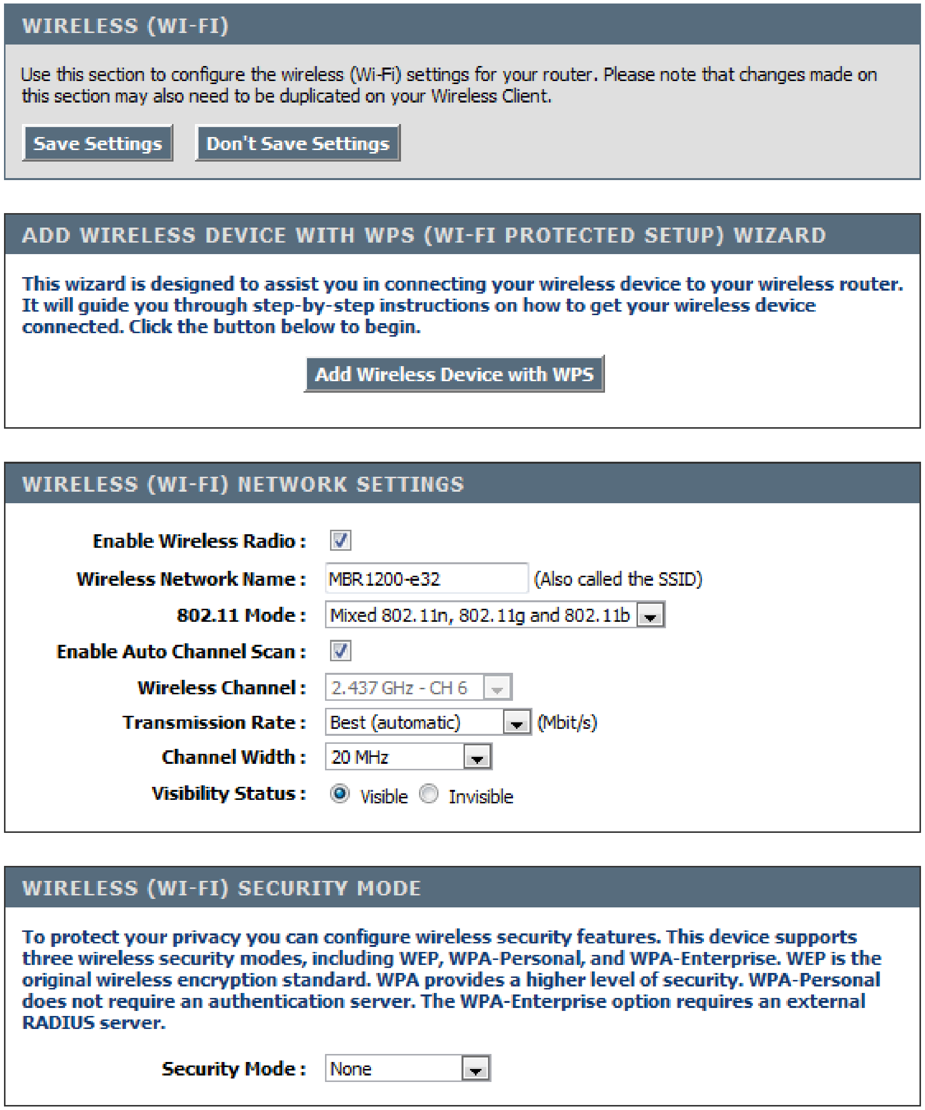
There are several ways to add a wireless device to your network. Access to the wireless network is controlled by a "registrar." A registrar only allows devices onto the wireless network if you have entered the PIN, or pressed a **Wi-Fi Protected Setup** button on the device. The router acts as a registrar for the network, although other devices may act as a registrar as well.

4.6.1 Wireless (WI-FI) Network Settings

Enable Wireless Radio. *(*Default: Enabled). When checked, wireless connectivity is enabled.

Wireless Network Name. (Default: visible). The SSID name for the router. Default: "MBR1200-xxx" where "xxx" is the last three digits of the MBR1200's MAC address. The MAC address can be found on the product label of the MBR1200.

(continued)



WIRELESS (WI-FI)

Use this section to configure the wireless (Wi-Fi) settings for your router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD

This wizard is designed to assist you in connecting your wireless device to your wireless router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

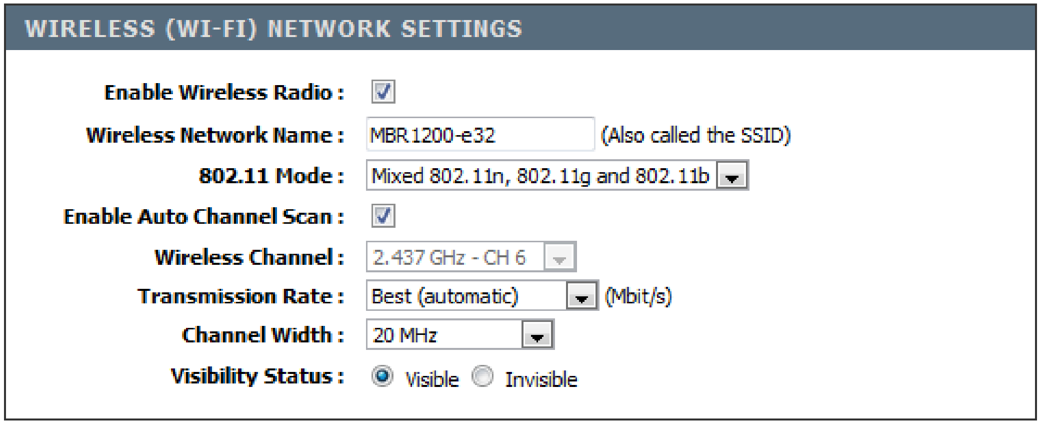
WIRELESS (WI-FI) NETWORK SETTINGS

Enable Wireless Radio :	☑
Wireless Network Name :	MBR1200-e32 (Also called the SSID)
802.11 Mode :	Mixed 802.11n, 802.11g and 802.11b
Enable Auto Channel Scan :	☑
Wireless Channel :	2.437 GHz - CH 6
Transmission Rate :	Best (automatic) (Mbit/s)
Channel Width :	20 MHz
Visibility Status :	● Visible ○ Invisible

WIRELESS (WI-FI) SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : None



WIRELESS (WI-FI) NETWORK SETTINGS

Enable Wireless Radio :	☑
Wireless Network Name :	MBR1200-e32 (Also called the SSID)
802.11 Mode :	Mixed 802.11n, 802.11g and 802.11b
Enable Auto Channel Scan :	☑
Wireless Channel :	2.437 GHz - CH 6
Transmission Rate :	Best (automatic) (Mbit/s)
Channel Width :	20 MHz
Visibility Status :	● Visible ○ Invisible

802.11 Mode. (Default [Mixed 802.11 b/g/n]). Select Wi-Fi operating mode (802.11b/g/n, 802.11b/g, 802.11n, 802.11b, 802.11g).

Enable Auto Channel Scan. When the power is first turned on, the MBR1200 will check the available wireless bands for the least-used channel.

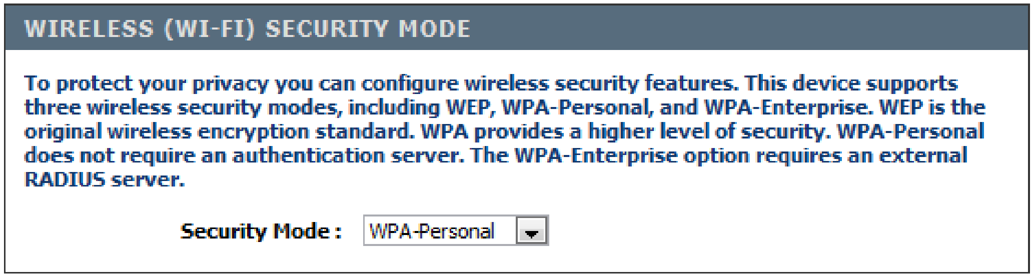
Wireless Channel. (Default: randomly selected among channels appropriate for 802.11 setting). Channel to transmit and receive. Channels 1 through 11 are available for 802.11 b/g/n in the U.S. Check if you employ channel planning in your building.

Transmission Rate. (Default: Best). By default the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary. Channel rates are doubled for MCS when **Channel Width** is set to 40 MHz.

Channel Width. The **Auto 20/40 MHz** option is usually best. The other options are available for special circumstances.

Visibility Status. Whether or not the SSID will be visible on the LAN. The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

4.6.2 Wireless (WI-FI) Security Mode



WIRELESS (WI-FI) SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WPA-Personal

Unless one of these encryption modes is selected, wireless transmissions to and from your wireless network can be easily intercepted and interpreted by unauthorized users.

Security Mode. (Default:WPA-Personal). The MBR1200 supports three wireless security modes including: **WEP**, **WPA-Personal**, and **WPA-Enterprise**. WEP is the original wireless encryption standard, and is not considered as secure as WPA. WEP should only be used if encryption is needed, but WPA encryption is not supported by your client devices.

WPA provides a higher level of security, and is the recommended security setting for most users. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server for authentication.

(continued)

4.6.3 WEP

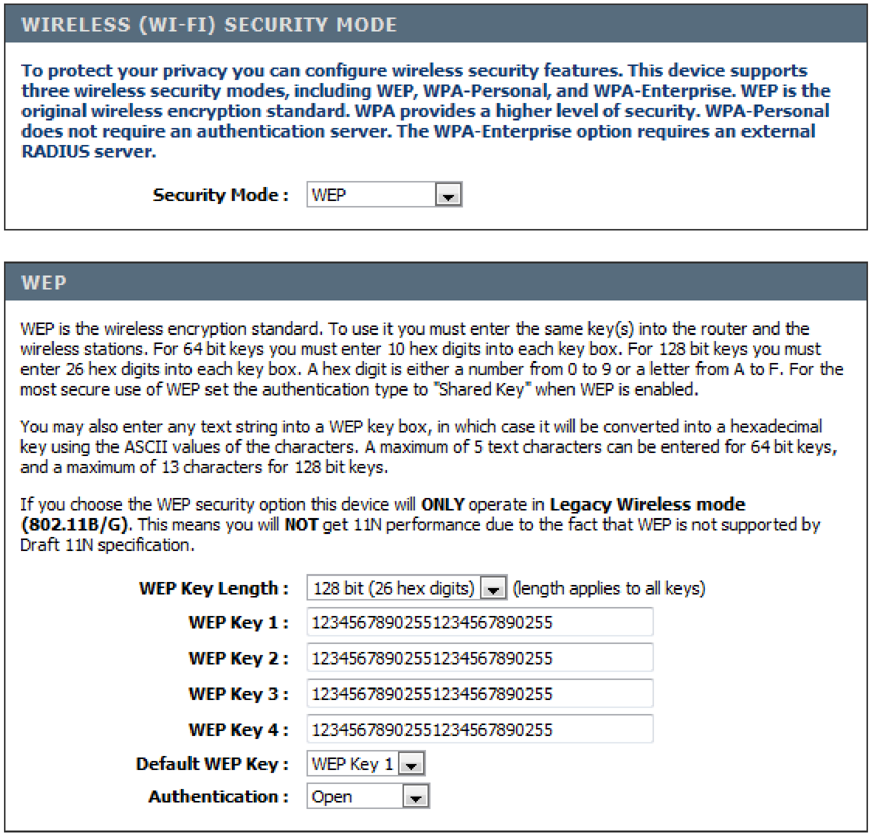
A method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key.

WEP Key Length. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64- bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network.

WEP Key 1, 2, 3 and 4. Four keys can be defined so that you can change keys easily.

Default WEP Key. A default key is selected for use on the network.

Authentication. Open Key authentication involves supplying the correct SSID to connect to the Access Point, with no key authentication performed. Shared Key authentication involves the Access Point sending the client device a challenge text packet that the client must then encrypt with the correct WEP key and return to the Access Point. If the client has the wrong key or no key, authentication fails and client will not connect to the Access Point.



WIRELESS (WI-FI) SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WEP

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**. This means you will **NOT** get 11N performance due to the fact that WEP is not supported by Draft 11N specification.

WEP Key Length : 128 bit (26 hex digits) (length applies to all keys)
WEP Key 1 : 12345678902551234567890255
WEP Key 2 : 12345678902551234567890255
WEP Key 3 : 12345678902551234567890255
WEP Key 4 : 12345678902551234567890255
Default WEP Key : WEP Key 1
Authentication : Open

Example:

- 64-bit hexadecimal keys are exactly 10 characters in length. (**12345678FA** is a valid string of 10 characters for 64-bit encryption.)
- 128-bit hexadecimal keys are exactly 26 characters in length. (**12345678902551234567890255** is a valid string of 26 characters for 128-bit encryption.)
- 64-bit ASCII keys are up to 5 characters in length (**DMODE** is a valid string of 5 characters for 64-bit encryption.)
- 128-bit ASCII keys are up to 13 characters in length (**2002HALOSWIN1** is a valid string of 13 characters for 128-bit encryption.)

NOTE: if you enter fewer characters in the WEP key than required, the remainder of the key is automatically padded with zeros.

4.6.4 WPA (Personal)

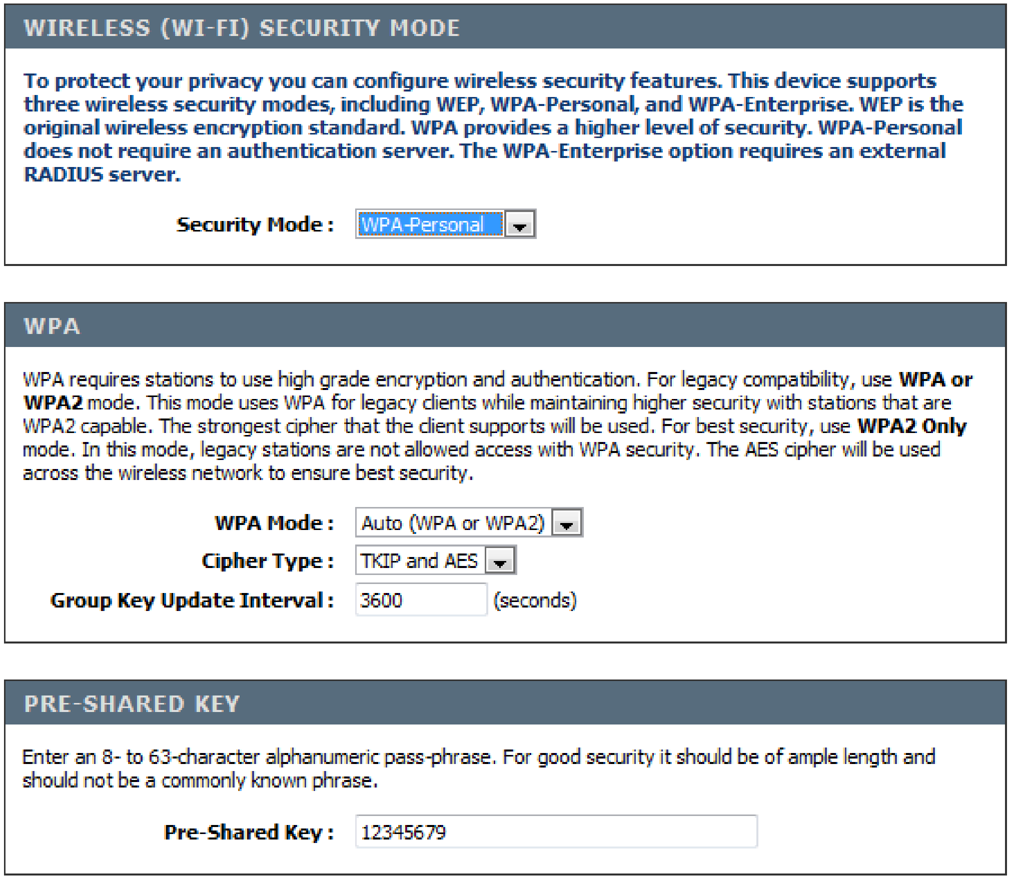
WPA-Personal is one variant of Wi-Fi Protected Access (WPA) – security standards published by the Wi-Fi Alliance. The WPA Mode further refines the variant that the router should employ. The WPA-Personal option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK).

WPA Mode. WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the **WPA2** option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the **WPA2 Only** option, the router associates only with clients that also support WPA2 security.

Cipher Type. The encryption algorithm used to secure the data communication. **TKIP** (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. **AES** (Advanced Encryption Standard) is a very secure block based encryption. With the **TKIP and AES** option, the router negotiates the cipher type with the client, and uses AES when available.

Group Key Update Interval. The amount of time before the group key used for broadcast and multicast data is changed.

Pre-Shared Key. The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.



WIRELESS (WI-FI) SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WPA-Personal

WPA

WPA requires stations to use high grade encryption and authentication. For legacy compatibility, use **WPA or WPA2** mode. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. In this mode, legacy stations are not allowed access with WPA security. The AES cipher will be used across the wireless network to ensure best security.

WPA Mode : Auto (WPA or WPA2)

Cipher Type : TKIP and AES

Group Key Update Interval : 3600 (seconds)

PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key : 12345679

NOTE: Be sure to write down the Pre-Shared Key and keep it in a safe place.

4.6.5 WPA (Enterprise)

The WPA-Enterprise is one variant of Wi-Fi Protected Access (WPA) – security standards published by the Wi-Fi Alliance. The WPA Mode further refines the variant that the router should employ.

The WPA-Enterprise option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this gateway to authenticate users.

WPA Mode. WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the **WPA2** option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the **WPA2 Only** option, the router associates only with clients that also support WPA2 security.

Cipher Type. The encryption algorithm used to secure the data communication. **TKIP** (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. **AES** (Advanced Encryption Standard) is a very secure block based encryption. With the **TKIP and AES** option, the router negotiates the cipher type with the client, and uses AES when available.

Group Key Update Interval. The amount of time before the group key used for broadcast and multicast data is changed.

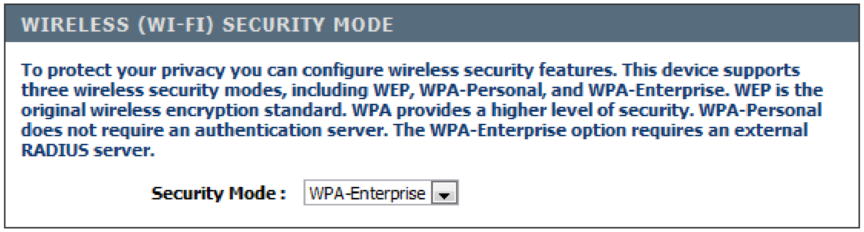
4.6.6 EAD (802.1X)

Authentication Timeout. Amount of time before a client will be required to re-authenticate.

RADIUS Server IP Address. The IP address of the authentication server.

RADIUS Server Port. The port number used to connect to the authentication server.

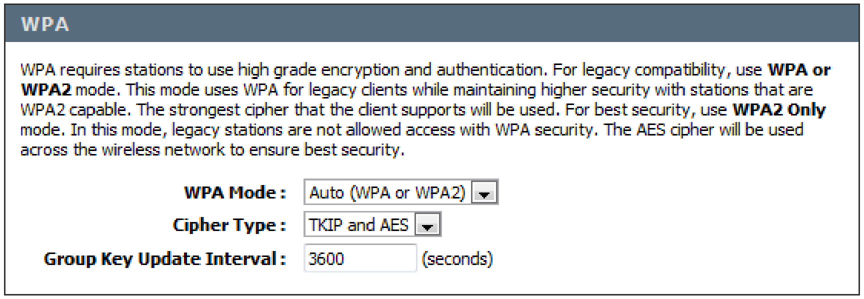
(continued)



WIRELESS (WI-FI) SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WPA-Enterprise



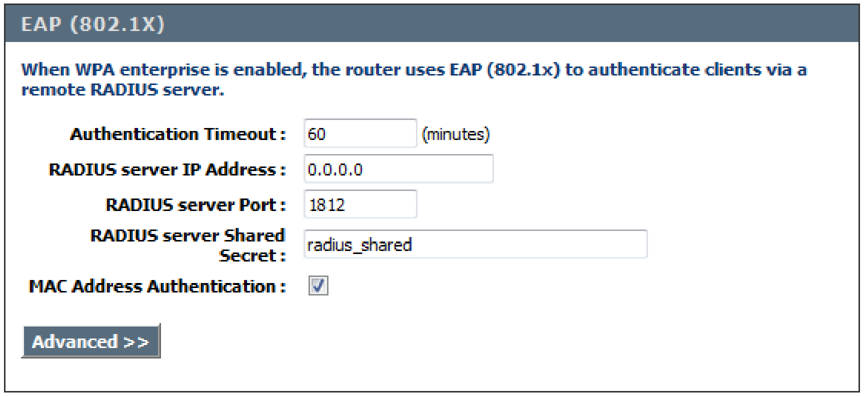
WPA

WPA requires stations to use high grade encryption and authentication. For legacy compatibility, use **WPA or WPA2** mode. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. In this mode, legacy stations are not allowed access with WPA security. The AES cipher will be used across the wireless network to ensure best security.

WPA Mode : Auto (WPA or WPA2)

Cipher Type : TKIP and AES

Group Key Update Interval : 3600 (seconds)



EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

Authentication Timeout : 60 (minutes)

RADIUS server IP Address : 0.0.0.0

RADIUS server Port : 1812

RADIUS server Shared Secret : radius_shared

MAC Address Authentication : ☑

RADIUS Server Shared Secret. A pass-phrase that must match with the authentication server.

MAC Address Authentication. If this check box is selected, the user must connect from the same computer whenever logging into the wireless network.

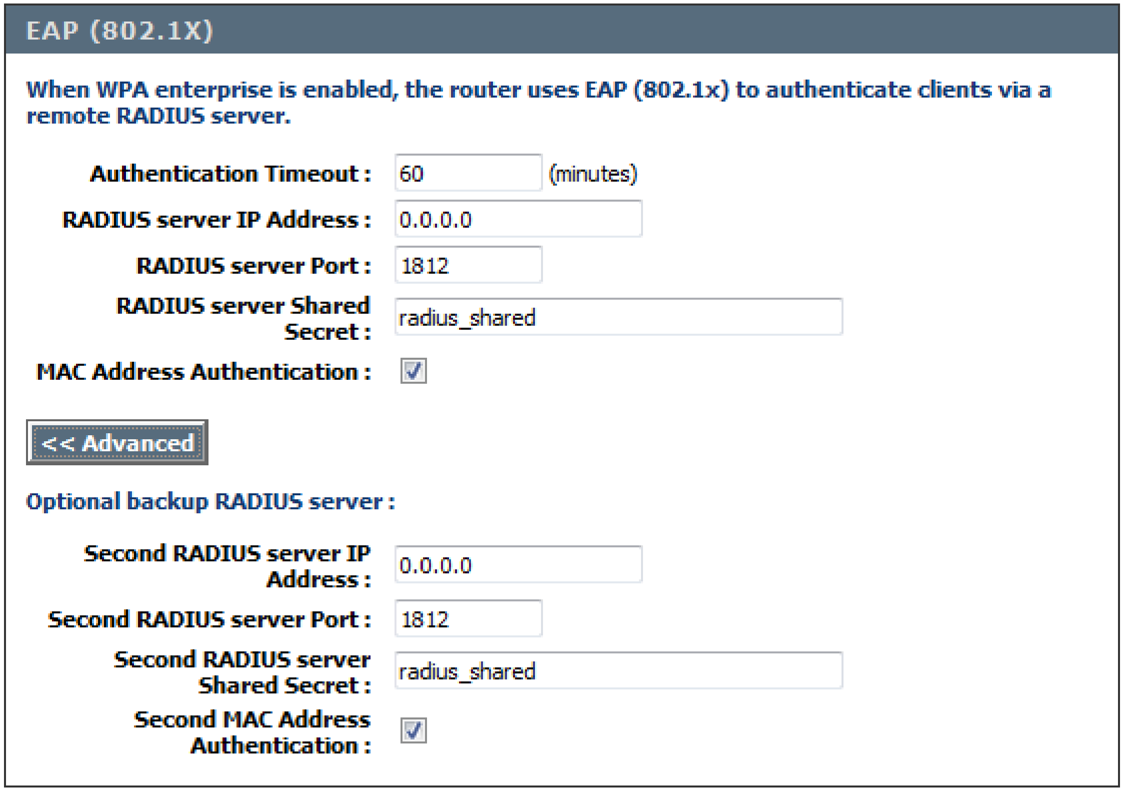
Clicking on the **<<Advanced** button displays additional menu features.

Optional Backup RADIUS Server. This option enables configuration of an optional second RADIUS server. A second RADIUS server can be used as backup for the primary RADIUS server. The second RADIUS server is consulted only when the primary server is not available or not responding.

The fields for **Second RADIUS Server IP Address**, **RADIUS Server Port**, **Second RADIUS server Shared Secret**, and **Second MAC Address Authentication** provide the corresponding parameters for the second RADIUS Server.

Second MAC Address Authentication. If this check box is selected, the user must connect from the same computer whenever logging into the wireless network.

NOTE: Be sure to write down the Radius server Shared Secret and keep it in a safe place.



EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

Authentication Timeout : 60 (minutes)

RADIUS server IP Address : 0.0.0.0

RADIUS server Port : 1812

RADIUS server Shared Secret : radius_shared

MAC Address Authentication : ☑

<< Advanced

Optional backup RADIUS server :

Second RADIUS server IP Address : 0.0.0.0

Second RADIUS server Port : 1812

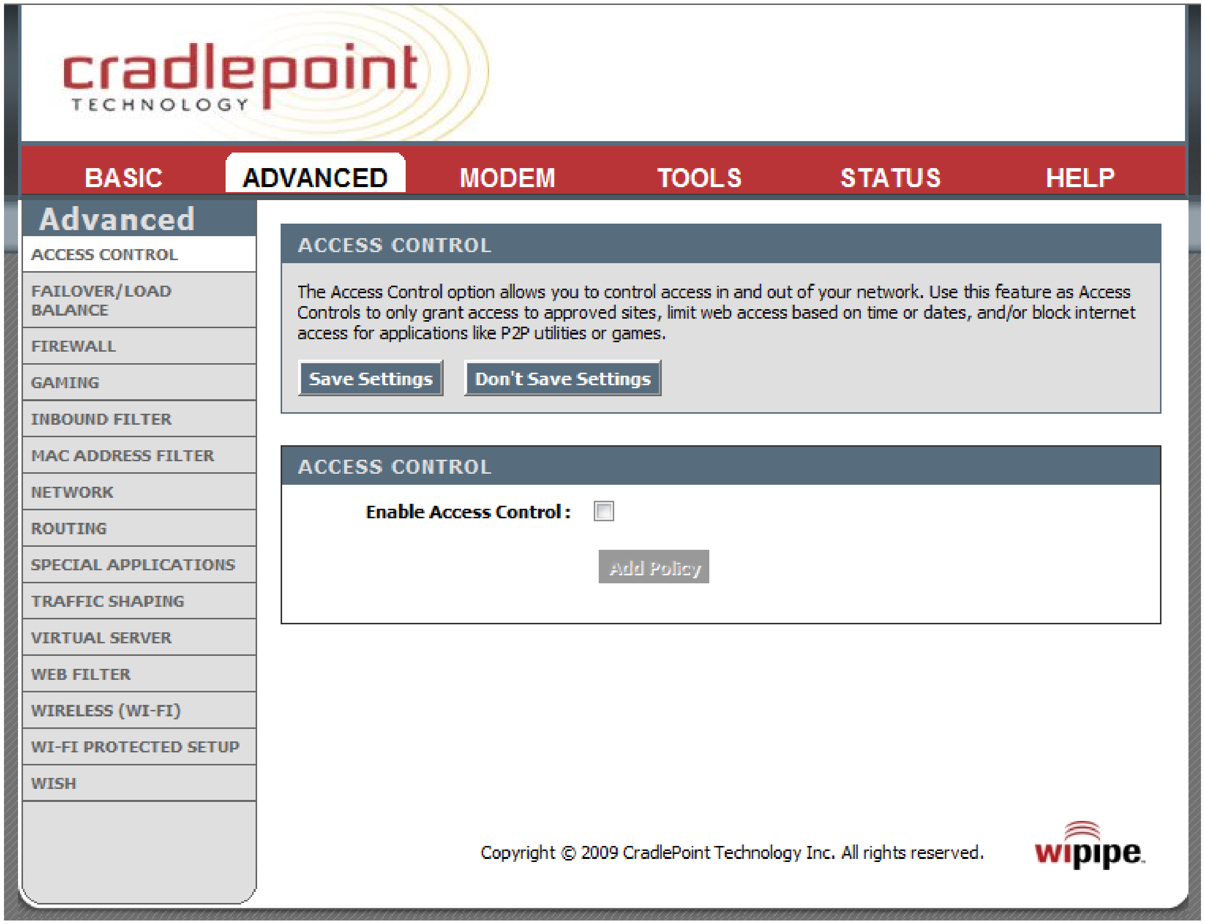
Second RADIUS server Shared Secret : radius_shared

Second MAC Address Authentication : ☑

5 ADVANCED TAB

The Advanced tab provides access to the 16 sub-menus for administering the following functions/tasks:

- Access Control
- Failover/Load Balance
- Firewall
- Gaming
- Inbound Filter
- Mac Address Filter
- Network
- Routing
- Special Applications
- Traffic Shaping
- Virtual Server
- Web Filter
- Wireless (WI-FI)
- WI-FI Protected Setup
- WISH



ACCESS CONTROL

The Access Control option allows you to control access in and out of your network. Use this feature as Access Controls to only grant access to approved sites, limit web access based on time or dates, and/or block internet access for applications like P2P utilities or games.

ACCESS CONTROL

Enable Access Control : □

Copyright © 2009 CradlePoint Technology Inc. All rights reserved.

5.1 Access Control

Use the Access Control sub-menu you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.

By default, the Access Control feature is disabled. If you enable Access Control, every device on the LAN must either have a static IP address (that is one that is not in the DHCP range) or must be in the Static DHCP Client List (see **Basic → DHCP** sub-menu.

When Access Control is disabled, every device on the WLAN is permitted to access the Internet. However, if you enable Access Control, every device on the WLAN that needs to access the Internet must have an Access Control rule that explicitly permits it to access the Internet. Devices that do not have an Access Control Rule cannot access the Internet.

5.1.1 Access Control

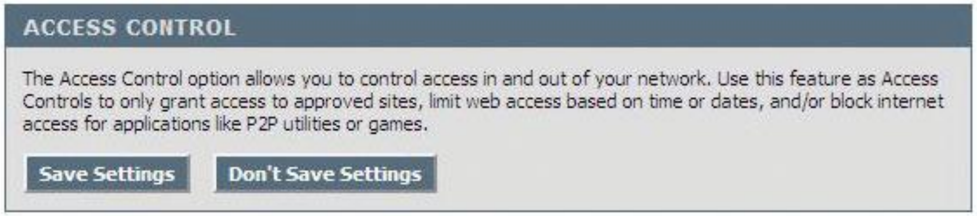
The Policy Wizard guides you through the steps of defining each access control policy. A policy is the "Who, What, When, and How" of access control -- whose computer will be affected by the control, what internet addresses are controlled, when will the control be in effect, and how is the control implemented. You can define multiple policies. The Policy Wizard starts when you click the button below and also when you edit an existing policy.

Enable Access Control. Click the **Enable Access Control** button to display the **Add New Policy** wizard.

5.1.2 Add New Policy

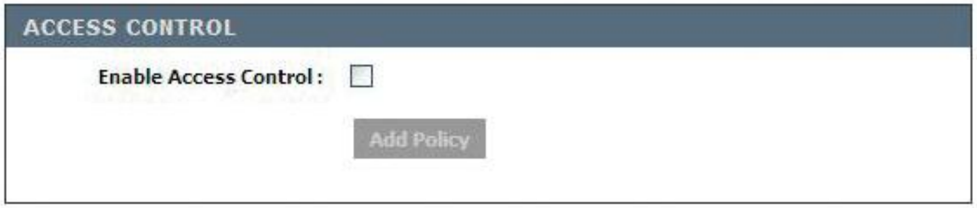
Step 1: Choose Policy Name. Create a name for this access control policy that is meaningful to you. Typically this would be a system name or user name such as **Rob's PC**.

(continued)



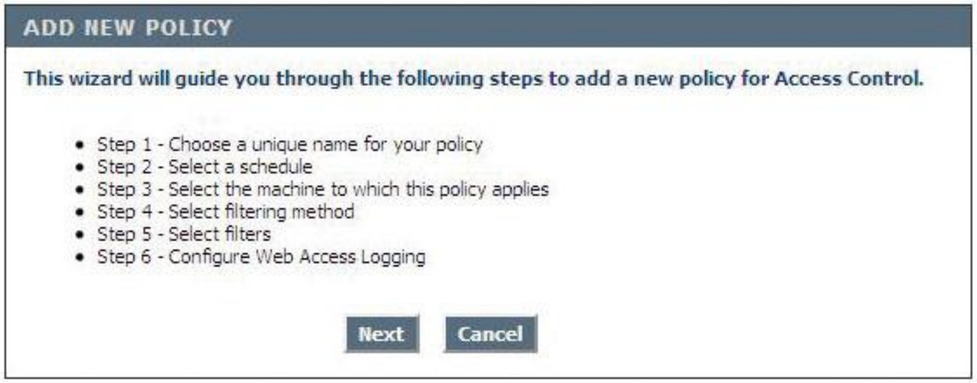
ACCESS CONTROL

The Access Control option allows you to control access in and out of your network. Use this feature as Access Controls to only grant access to approved sites, limit web access based on time or dates, and/or block internet access for applications like P2P utilities or games.



ACCESS CONTROL

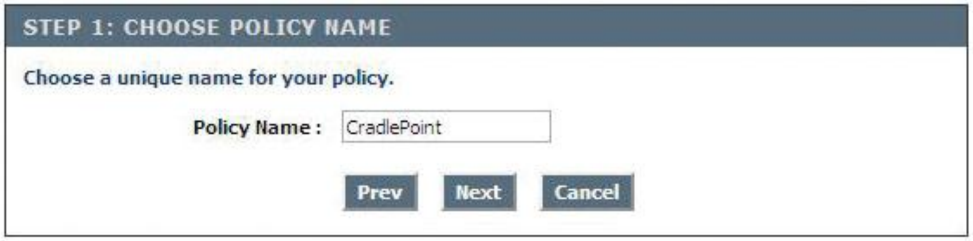
Enable Access Control : □



ADD NEW POLICY

This wizard will guide you through the following steps to add a new policy for Access Control.

- Step 1 - Choose a unique name for your policy
- Step 2 - Select a schedule
- Step 3 - Select the machine to which this policy applies
- Step 4 - Select filtering method
- Step 5 - Select filters
- Step 6 - Configure Web Access Logging

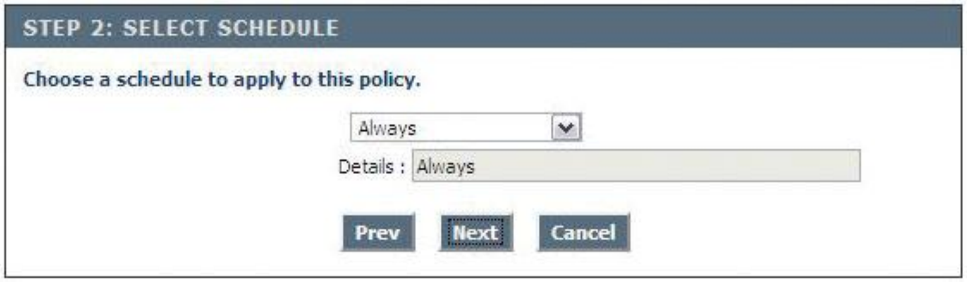


STEP 1: CHOOSE POLICY NAME

Choose a unique name for your policy.

Policy Name : CradlePoint

Step 2: Select Schedule. From the drop down menu, elect a schedule of times when you want the policy to apply: **Always**, **Never**, **Define a New Schedule** or a schedule that you've previously defined. If you do not see the schedule you need in the list of schedules, go to the **Tools → Schedules** sub-menu and create a new schedule.



STEP 2: SELECT SCHEDULE

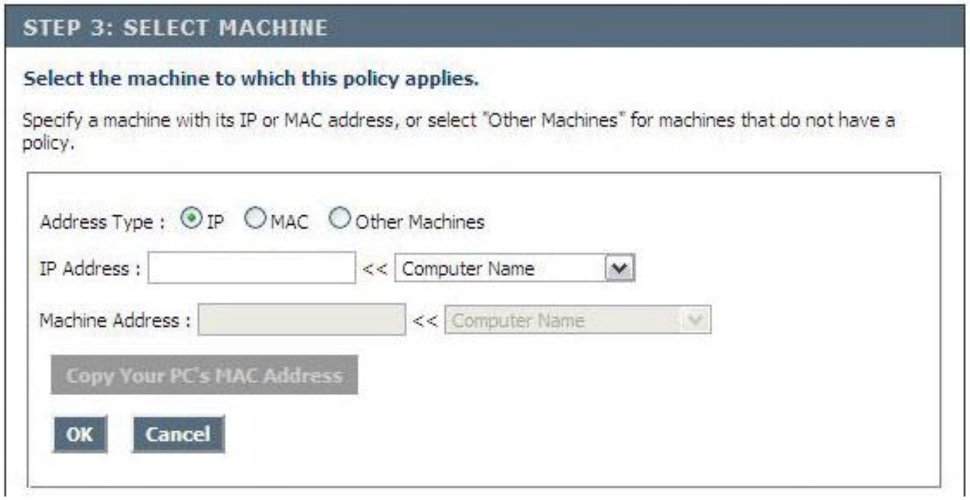
Choose a schedule to apply to this policy.

Always

Details : Always

Step 3: Select Machine. Select the machine to which this policy applies by clicking a radio button: **IP**, **MAC** or **Other Machines**. Depending on which radio button you've selected, enter either the local network IP address or MAC address of the machine that you want the access control rule to apply to. Click **OK**.

Example: 192.168.0.50. Make sure that this is a static IP address or the system is in the static DHCP Client list (See the **Basic → DHCP** sub-menu).



STEP 3: SELECT MACHINE

Select the machine to which this policy applies.

Specify a machine with its IP or MAC address, or select "Other Machines" for machines that do not have a policy.

Address Type : ● IP ○ MAC ○ Other Machines

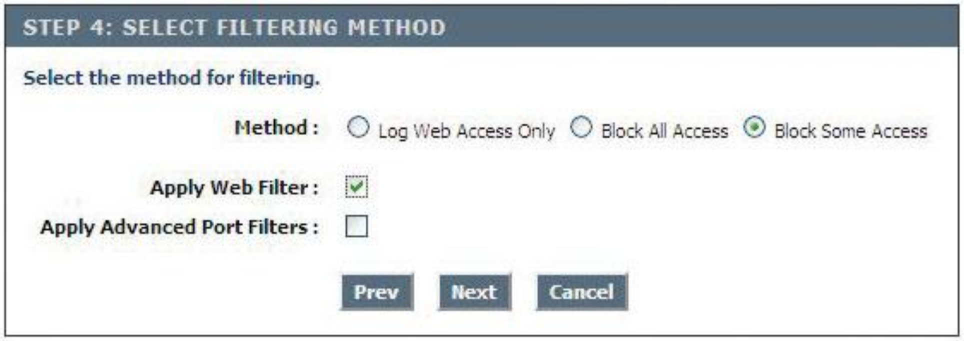
IP Address : << Computer Name

Machine Address : << Computer Name

Step 4: Select Filtering Method.

- Log Web Access Only. No filters will be applied, but web access will be logged.
- Block All Access. All access to the web will be blocked.
- Block Some Access. With this option enabled some access will be blocked. If the **Apply Web Filter** box is checked the specified system will only have access to the Web sites listed in the **Advanced → Web Filter** sub-menu.

(continued)



STEP 4: SELECT FILTERING METHOD

Select the method for filtering.

Method : ○ Log Web Access Only ○ Block All Access ● Block Some Access

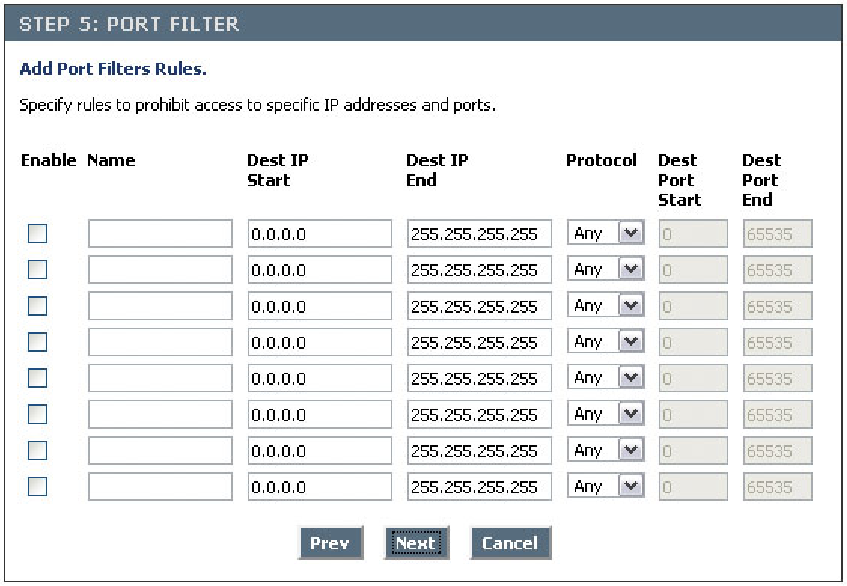
Apply Web Filter : ☑

Apply Advanced Port Filters : □

Step 5: Port Filter. By clicking the **Apply Advanced Port Filter** button you can specify that the rule enables access only to specific IP addresses and ports.

Step 6: Configure Web Access Logging. If this option is enabled, all of the Web sites visited by the specified machine will be logged.

(continued)

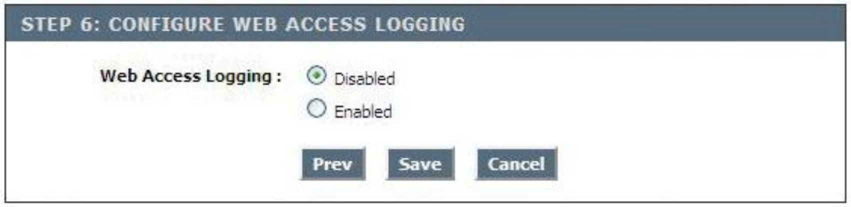


STEP 5: PORT FILTER

Add Port Filters Rules.

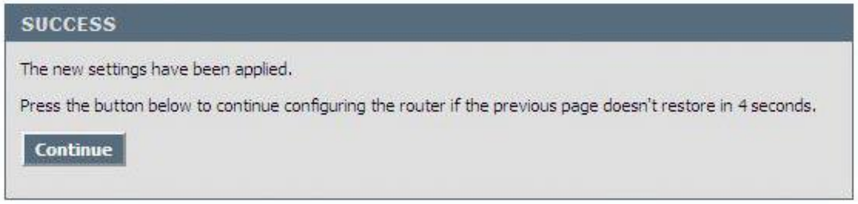
Specify rules to prohibit access to specific IP addresses and ports.

Enable	Name	Dest IP Start	Dest IP End	Protocol	Dest Port Start	Dest Port End
☐		0.0.0.0	255.255.255.255	Any	0	65535
☐		0.0.0.0	255.255.255.255	Any	0	65535
☐		0.0.0.0	255.255.255.255	Any	0	65535
☐		0.0.0.0	255.255.255.255	Any	0	65535
☐		0.0.0.0	255.255.255.255	Any	0	65535
☐		0.0.0.0	255.255.255.255	Any	0	65535
☐		0.0.0.0	255.255.255.255	Any	0	65535
☐		0.0.0.0	255.255.255.255	Any	0	65535



STEP 6: CONFIGURE WEB ACCESS LOGGING

Web Access Logging : ● Disabled ○ Enabled



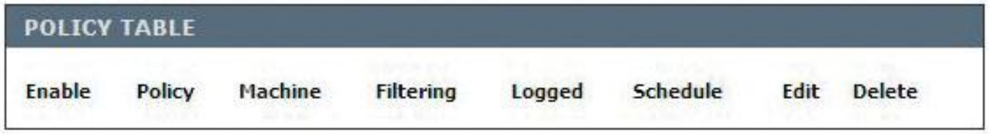
SUCCESS

The new settings have been applied.

Press the button below to continue configuring the router if the previous page doesn't restore in 4 seconds.

5.1.3 Policy Table

This section shows the current Access Control rules. Click the **Enable** check box at the left to directly activate or de-activate the entry. An entry can be changed by clicking the **Edit** icon or can be deleted by clicking the **Delete** Policy Table section icon. When you click the **Edit** icon, the item is highlighted, and the **Policy Table** section is activated for editing.



POLICY TABLE

Enable	Policy	Machine	Filtering	Logged	Schedule	Edit	Delete

After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with all configuration settings, click the **Reboot the Device** button.

5.2 Failover/Load Balance

The MBR1200 can establish an uplink via the ethernet WAN port or any modems plugged into the USB, ExpressCard or CardBus ports. Although all of these devices may be plugged in, only one of them establishes a link at a time unless load balancing is enabled. If the WAN connection fails the router will automatically attempt to bring up a new link on another device. This feature is called failover. You can also manually disconnect and re-connect specific ports using icons in the **Control** column. The priority table can be saved permanently via the **Save** button. Priority changes take effect immediately even if they are not saved.

5.2.1 Ethernet WAN Failure Detection

WAN failure detection works by detecting the presence of traffic on the ethernet WAN link. (Note that this only applies to the ethernet WAN link, not the modems.) If the link is idle for too long the router will attempt to ping a target IP address. If the ping does not reply, the router assumes the link is down and attempts to fail over to a modem.

Enable. This enables failure detection on the Ethernet link. Even when this is disabled, unplugging the Ethernet cable at the WAN port will trigger failover to a modem.

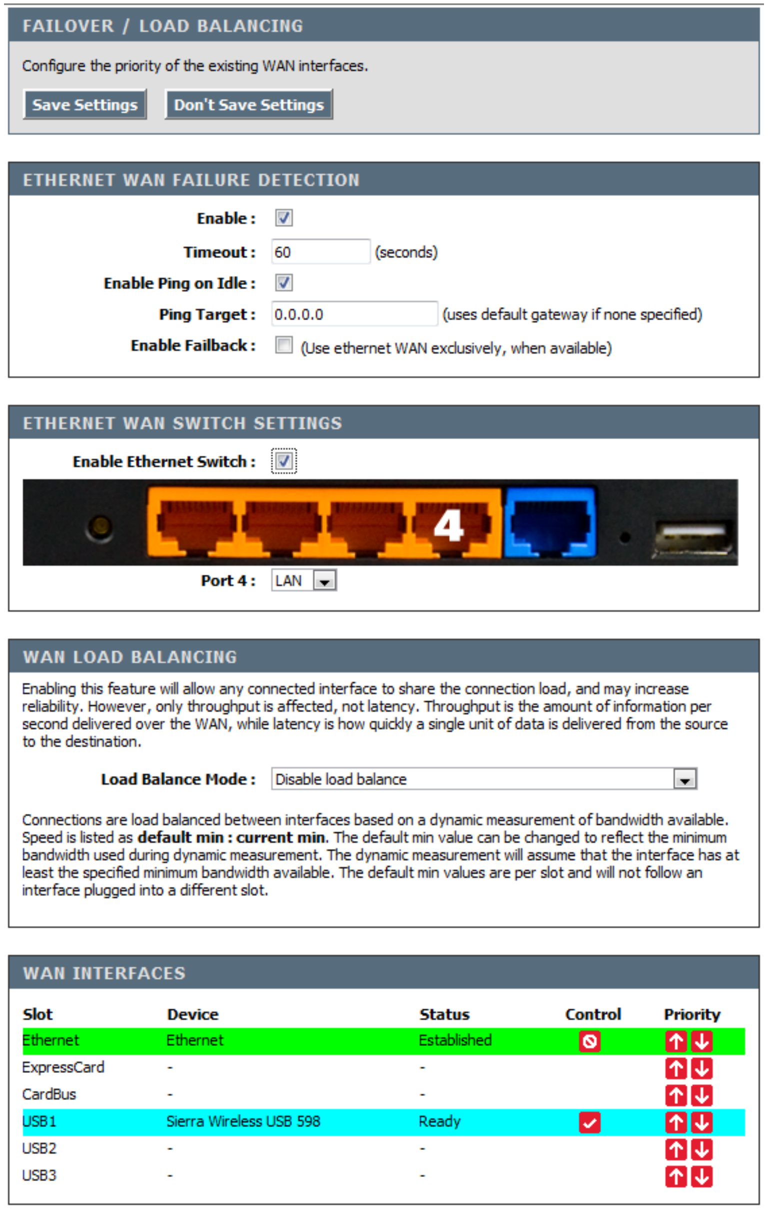
Timeout. Enter in this field the length of time that the ping target may be unresponsive before the MBR1200 will switch to the next failover connection.

Enable Ping on Idle. When enabled, the router will send a ping after the link idle timeout. If the ping gets a reply, the router will restart the idle timer, otherwise it will failover to a modem.

Ping Target. The default ping target is the router's gateway. You may specify a different IP address as a target here.

Enable Failback. This enables the Ethernet WAN connection to be monitored for usability. If the connection is usable, other WAN connections are disconnected and the Ethernet WAN connection is used exclusively.

(continued)



FAILOVER / LOAD BALANCING

Configure the priority of the existing WAN interfaces.

ETHERNET WAN FAILURE DETECTION

Enable : ☑

Timeout : 60 (seconds)

Enable Ping on Idle : ☑

Ping Target : 0.0.0.0 (uses default gateway if none specified)

Enable Failback : □ (Use ethernet WAN exclusively, when available)

ETHERNET WAN SWITCH SETTINGS

Enable Ethernet Switch : ☑

Port 4 : LAN

WAN LOAD BALANCING

Enabling this feature will allow any connected interface to share the connection load, and may increase reliability. However, only throughput is affected, not latency. Throughput is the amount of information per second delivered over the WAN, while latency is how quickly a single unit of data is delivered from the source to the destination.

Load Balance Mode : Disable load balance

Connections are load balanced between interfaces based on a dynamic measurement of bandwidth available. Speed is listed as **default min : current min**. The default min value can be changed to reflect the minimum bandwidth used during dynamic measurement. The dynamic measurement will assume that the interface has at least the specified minimum bandwidth available. The default min values are per slot and will not follow an interface plugged into a different slot.

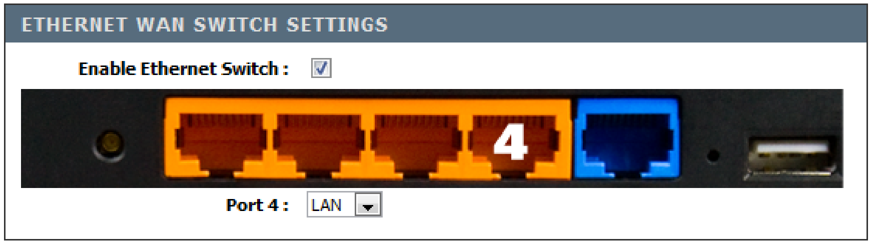
WAN INTERFACES

Slot	Device	Status	Control	Priority
Ethernet	Ethernet	Established	⊘	↑↓
ExpressCard	-	-		↑↓
CardBus	-	-		↑↓
USB1	Sierra Wireless USB 598	Ready	✓	↑↓
USB2	-	-		↑↓
USB3	-	-		↑↓

5.2.2 Ethernet WAN Switch Settings

Enable Ethernet Switch. This enables and disables the WAN Ethernet switch. When the switch is disabled, wired Ethernet connections will work.

Port 4: The user may convert port 4 from LAN to WAN, thus creating a secondary WAN Ethernet port.



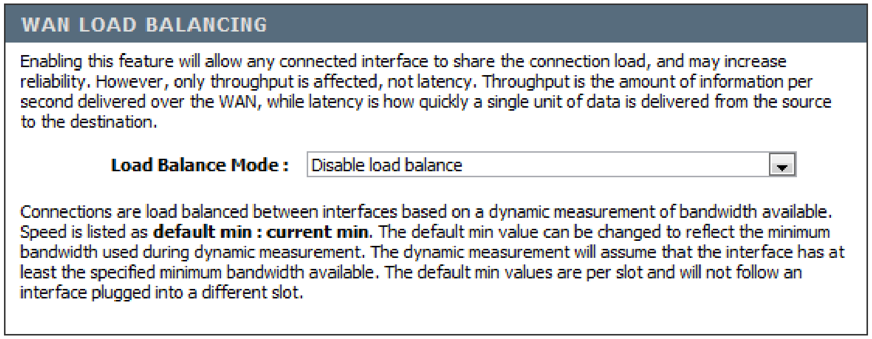
ETHERNET WAN SWITCH SETTINGS

Enable Ethernet Switch : ☑

Port 4 : LAN

5.2.3 WAN Load Balancing

This feature allows you to increase the data transfer throughput by allowing any connected interface to share the connection load. If load balancing is active, all configurable services will be associated with the primary interface: WAN 1. For example, if you have configured the router to accept connections on port 80 to be forwarded to a certain host, only WAN 1 will be effected. If the primary interface is disconnected, primary services will failover to the next available interface.



WAN LOAD BALANCING

Enabling this feature will allow any connected interface to share the connection load, and may increase reliability. However, only throughput is affected, not latency. Throughput is the amount of information per second delivered over the WAN, while latency is how quickly a single unit of data is delivered from the source to the destination.

Load Balance Mode : Disable load balance

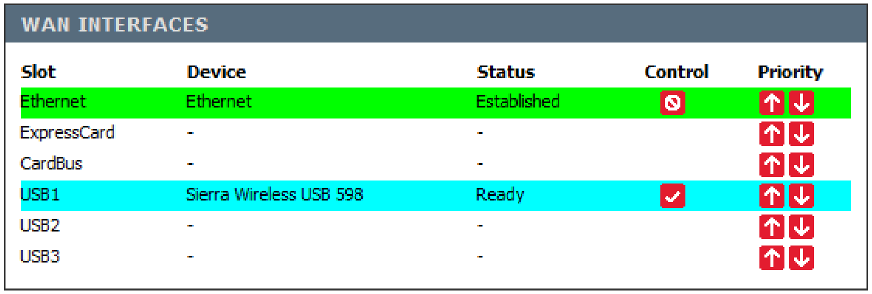
Connections are load balanced between interfaces based on a dynamic measurement of bandwidth available. Speed is listed as **default min : current min**. The default min value can be changed to reflect the minimum bandwidth used during dynamic measurement. The dynamic measurement will assume that the interface has at least the specified minimum bandwidth available. The default min values are per slot and will not follow an interface plugged into a different slot.

5.2.4 WAN Interfaces

This section allows you to:

- Change the failover order of devices (aka interfaces)
- Monitor their status
- Take the active link down
- Bring a link up on another device

The device at the top of the list has the highest priority. This is the device which the router will attempt to start when it boots up. If the link cannot be brought up on this device, or if it fails after boot up, the router will attempt to bring the link up on the next available device. Whenever a link fails on a device, the router will always move down to the next device down in the list, and wrap around again to the top.



WAN INTERFACES

Slot	Device	Status	Control	Priority
Ethernet	Ethernet	Established	⊘	↑ ↓
ExpressCard	-	-		↑ ↓
CardBus	-	-		↑ ↓
USB1	Sierra Wireless USB 598	Ready	✓	↑ ↓
USB2	-	-		↑ ↓
USB3	-	-		↑ ↓

Slot. The slot is the physical port the modem or Ethernet cable is plugged into.

Device. This shows a description of the device.

Status. This is the link status of a device, which is one of the following:

- **Ready**. This means the device is plugged in an available but not active. *(continued)*

- **Establishing**. This means the router is attempting to bring up the link over the device.
- **Established**. This means the link is up and running on the device.
- **Suspended**. This means the router will not attempt to bring up the link over the device until a timer expires. This only applies to modems, which must conform to carrier specifications about how often they may attempt to connect to the network. The timeout depends on how many previous connection attempts have failed in a row.

Control. The device which has an active link will show a circle-and-slash icon. If you click on this icon the router will bring the link down. It will not automatically failover in this case. If you bring the link down, the modem will remain disconnected until you use the control to enable it again. The router will not attempt to automatically connect to a modem that has been manually disconnected.

All other available devices will have a check mark icon. If you click on this icon the router will attempt to bring the link up over this device. If necessary, it will first bring the active link down. Failover will proceed to the next device down on the list.

Priority. Click on the **up-arrow** and **down-arrow** icons to change the priority of the device.

5.3 Firewall

Use the Firewall sub-menu to protect your network from the outside world. The MBR1200 provides a tight firewall by virtue of the way NAT works. Unless you configure the router to the contrary, the NAT does not respond to unsolicited incoming requests on any port, thereby making your LAN invisible to public Internet view. However, some network applications cannot run with a tight firewall. Those applications need to selectively open ports in the firewall to function correctly.

5.3.1 Firewall Settings

Enable SPI. SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. When SPI is enabled, the extra state information will be reported on the **Status → Active Sessions** sub-menu.

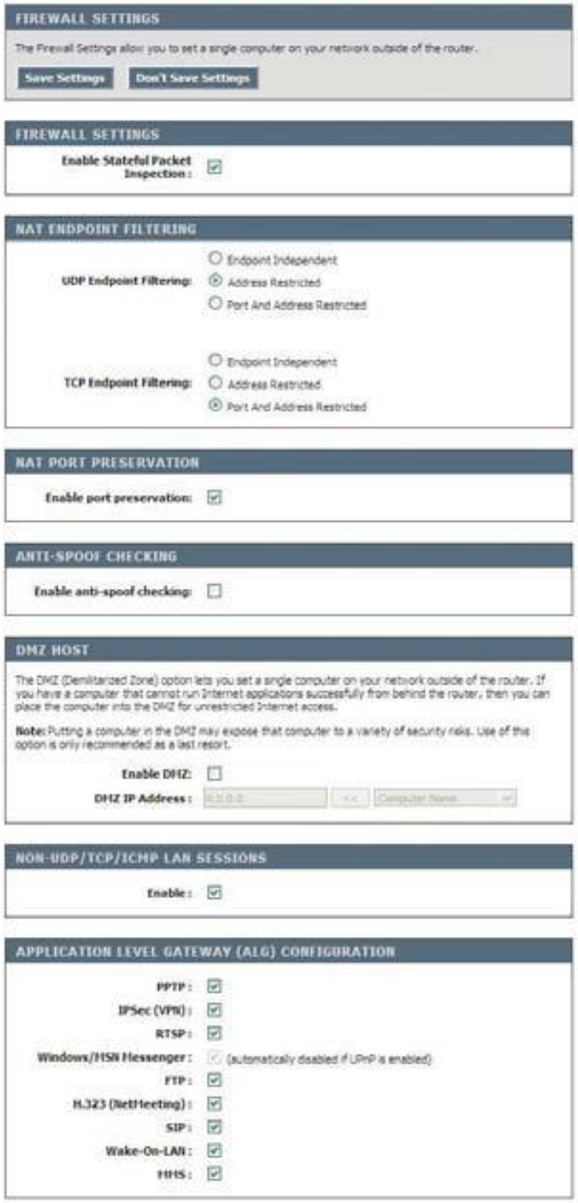
Whether SPI is enabled or not, the router always tracks TCP connection states and ensures that each TCP packet's flags are valid for the current state.

5.3.2 NAT Endpoint Filtering

The NAT Endpoint Filtering options control how the router’s NAT manages incoming connection requests to ports that are already being used.

UDP Endpoint Filtering/TCP Endpoint Filtering. The **UDP Endpoint Filtering** check box controls endpoint filtering for packets of the UDP protocol and the **TCP Endpoint Filtering** check box controls endpoint filtering for packets of the TCP protocol. Select a NAT Endpoint Filtering option:

- **Endpoint Independent.** Once a LAN-side application has created a connection through a specific port, the NAT will forward any incoming connection requests with the same port to the LAN-side application regardless of their origin. This is the least restrictive option, giving the best connectivity and allowing some applications (P2P applications in particular) to behave almost as if they are directly connected to the Internet.
- **Address Restricted.** The NAT forwards incoming connection requests to a LAN-side host only when they come from the same IP address with which a connection was established. This allows the remote application to send data back through a port different from the one used when the outgoing session was created. *(continued)*



FIREWALL SETTINGS

The Firewall Settings allow you to set a single computer on your network outside of the router.

FIREWALL SETTINGS

Enable Stateful Packet Inspection : ☑

NAT ENDPOINT FILTERING

UDP Endpoint Filtering: ○ Endpoint Independent ● Address Restricted ○ Port And Address Restricted

TCP Endpoint Filtering: ○ Endpoint Independent ○ Address Restricted ● Port And Address Restricted

NAT PORT PRESERVATION

Enable port preservation: ☑

ANTI-SPOOF CHECKING

Enable anti-spoof checking: □

DMZ HOST

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

Enable DMZ: □

DMZ IP Address : 0.0.0.0 << Computer Name

NON-UDP/TCP/ICMP LAN SESSIONS

Enable : ☑

APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION

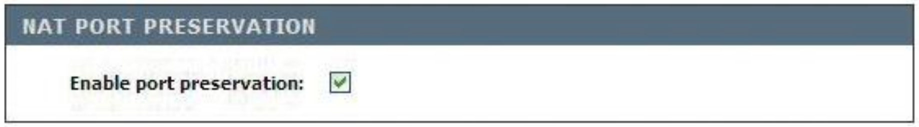
PPTP : ☑
IPSec (VPN) : ☑
RTSP : ☑
Windows/MSN Messenger : ☑ (automatically disabled if UPnP is enabled)
FTP : ☑
H.323 (NetMeeting) : ☑
SIP : ☑
Wake-On-LAN : ☑
MMS : ☑

- **Port And Address Restricted.** The NAT does not forward any incoming connection requests with the same port address as an already establish connection.

NOTE: Some of these options can interact with other port restrictions. Endpoint Independent Filtering takes priority over inbound filters or schedules, so it is possible for an incoming session request related to an outgoing session to enter through a port in spite of an active inbound filter on that port. However, packets will be rejected as expected when sent to blocked ports (whether blocked by schedule or by inbound filter) for which there are no active sessions. Port and Address Restricted Filtering ensures that inbound filters and schedules work precisely, but prevents some level of connectivity, and therefore might require the use of port triggers, virtual servers, or gaming to open the ports needed by the application. Address Restricted Filtering gives a compromise position, which avoids problems when communicating with certain other types of NAT router (symmetric NATs in particular) but leaves inbound filters and scheduled access working as expected.

5.3.3 NAT Port Preservation

Enable Port Preservation. (Default: enabled). NAT Port preservation tries to ensure that, when a LAN host makes an Internet connection, the same LAN port is also used as the Internet visible port. This ensures best compatibility for internet communications. Under some circumstances it may be desirable to turn off this feature.

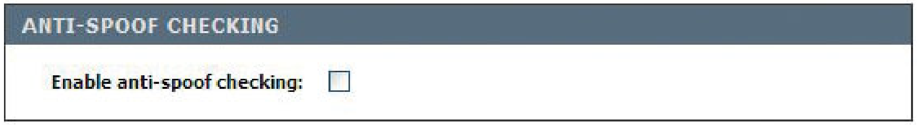


NAT PORT PRESERVATION

Enable port preservation: ☑

5.3.4 Anti-Spoof Checking

Enable Anti-Spoof Checking. Enabling this option can provide protection from certain kinds of “spoofing” attacks. However, enable this option with care. With some modems, the WAN connection may be lost when this option is enabled. In that case, it may be necessary to change the LAN subnet to something other than 192.168.0.x (**192.168.2.x**, for example), to re-establish the WAN connection.

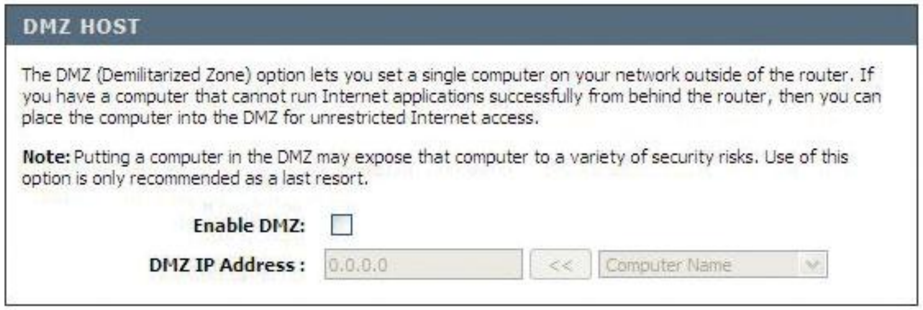


ANTI-SPOOF CHECKING

Enable anti-spoof checking: □

5.3.5 DMZ Host

Use the DMZ Host section when you want to expose a computer to the outside world for certain types of applications. This option will expose the chosen computer completely to the outside world. Only one machine can be put in the DMZ. NOTE: In general, the DMZ host should be used only if there are no other alternatives, because it is much more exposed to attacks than any other system on the LAN. Thought should be given to using other configurations instead: a virtual server, a gaming rule or a port trigger. *(continued)*



DMZ HOST

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

Enable DMZ: □

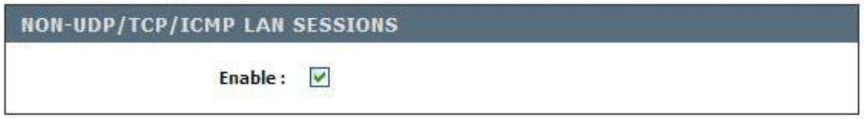
DMZ IP Address : 0.0.0.0

Enable DMZ. If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer. NOTE: Placing a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

DMZ IP Address. Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains its IP address automatically using DHCP, be sure to make a static reservation on the **Basic → DHCP** sub-menu so that the IP address of the DMZ machine does not change.

5.3.6 NON-UDP/TCP/ICMP LAN Sessions

When a LAN application that uses a protocol other than UDP, TCP, or ICMP initiates a session to the Internet, the router's NAT can track such a session, even though it does not recognize the protocol. This feature is useful because it enables certain applications (most importantly a single VPN connection to a remote host) without the need for an ALG.



NON-UDP/TCP/ICMP LAN SESSIONS

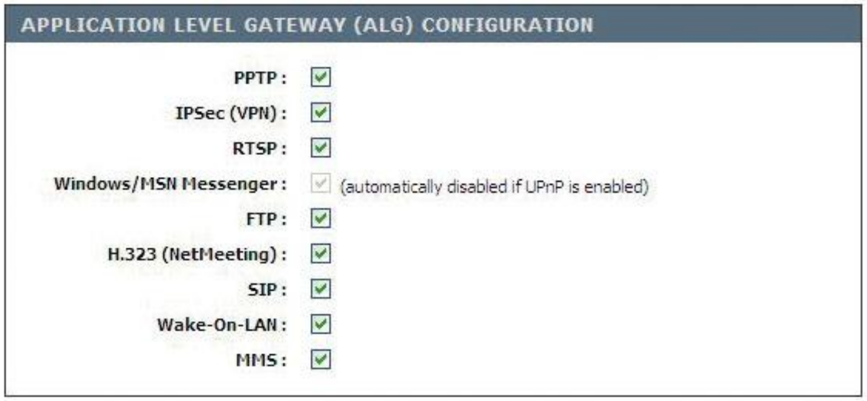
Enable : ☑

NOTE: this feature does not apply to the DMZ host (if one is enabled). The DMZ host always handles these kinds of sessions.

Enable. (Default: enabled). Allows single VPN connections to a remote host. But, for multiple VPN connections, the appropriate VPN ALG must be used. Disabling this option, however, only disables VPN if the appropriate VPN ALG is also disabled.

5.3.7 Application Level Gateway (ALG) Configuration

Here you can enable or disable ALGs. Some protocols and applications require special handling of the IP payload to make them work with network address translation (NAT). Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.



APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION

PPTP : ☑

IPSec (VPN) : ☑

RTSP : ☑

Windows/MSN Messenger : ☑ (automatically disabled if UPnP is enabled)

FTP : ☑

H.323 (NetMeeting) : ☑

SIP : ☑

Wake-On-LAN : ☑

MMS : ☑

PPTP. Allows multiple machines on the LAN to connect to their corporate networks using PPTP protocol. When the PPTP ALG is enabled, LAN computers can establish PPTP VPN connections either with the same or with different VPN servers. When the PPTP ALG is disabled, the router allows VPN operation in a restricted way -- LAN computers are typically able to establish VPN tunnels to different VPN Internet servers but not to the same server. The advantage of disabling the PPTP ALG is to increase VPN performance. Enabling the PPTP ALG also allows incoming VPN connections to a LAN side VPN server (refer to **Advanced → Virtual Server**).

IPSec (VPN). Allows multiple VPN clients to connect to their corporate networks using IPSec. Some VPN clients support traversal of IPSec through NAT. This option may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try disabling this option. *(continued)*

Check with the system administrator of your corporate network whether your VPN client supports NAT traversal.

Note that L2TP VPN connections typically use IPSec to secure the connection. To achieve multiple VPN pass-through in this case, the IPSec ALG must be enabled.

RTSP. Allows applications that use Real Time Streaming Protocol to receive streaming media from the Internet. EVDO QuickTime and Real Player are some of the common applications using this protocol.

Windows/MSN Messenger. Supports use on LAN computers of Microsoft Windows Messenger (the Internet messaging client that ships with Micro-soft Windows) and MSN Messenger. The SIP ALG must also be enabled when the Windows Messenger ALG is enabled. Required if you don't have UPnP-enabled chat program.

FTP. Allows FTP clients and servers to transfer data across NAT. Refer to the **Advanced → Virtual Server** sub-menu if you want to host an FTP server.

H.323 (NetMeeting). Allows H.323 (specifically, Microsoft NetMeeting) clients to communicate across NAT. NOTE: You must set up a virtual server for Net-Meeting. Refer to the **Advanced → Virtual Server** sub-menu for information on how to set up a virtual server.

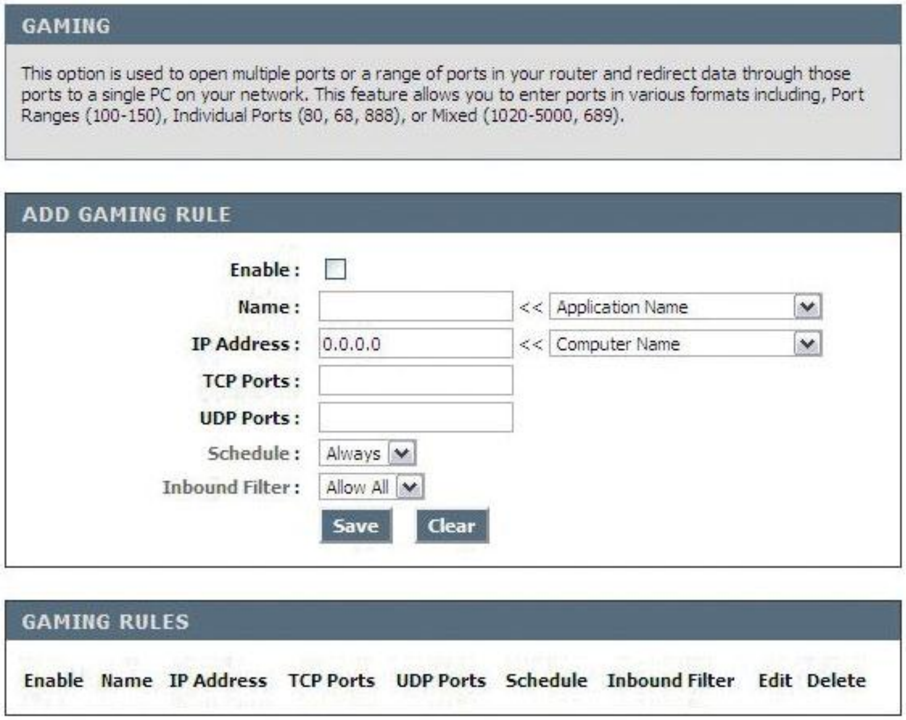
SIP. Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.

Wake-On-LAN. Enables forwarding of "magic packets" (that is, specially formatted wake-up packets) from the WAN to a LAN computer or other device that is "Wake on LAN" (WOL) capable. The WOL device must be defined as such on the **Advanced → Virtual Server** sub-menu. The LAN IP address for the virtual server is typically set to the broadcast address 192.168.0.255. The computer on the LAN whose MAC address is contained in the magic packet will be awakened.

MMS. Allows Windows Media Player, using MMS protocol, to receive streaming media from the Internet.

After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with all configuration settings, click the **Reboot the Device** button.

5.4 Gaming



GAMING

This option is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in various formats including, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689).

ADD GAMING RULE

Enable :	□	
Name :		<< Application Name
IP Address :	0.0.0.0	<< Computer Name
TCP Ports :		
UDP Ports :		
Schedule :	Always	
Inbound Filter :	Allow All	

GAMING RULES

Enable	Name	IP Address	TCP Ports	UDP Ports	Schedule	Inbound Filter	Edit	Delete

Multiple connections are required by some applications, such as internet games, video conferencing, Internet telephony, and others. These applications have difficulties working through NAT (Network Address Translation). This section is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. You can enter ports in various formats including, **Port Ranges (100-150)**, **Individual Ports (80, 68, 888)**, or **Mixed (1020-5000, 689)**.

Example: Suppose you are hosting an online game server that is running on a PC with a private IP Address of 192.168.0.50. This game requires that you open multiple ports (6159-6180, 99) on the router so Internet users can connect.

5.4.1 Add Gaming Rule

Use this section to add a Gaming Rule to the following list.

Enable. Specifies whether the entry will be active or inactive.

Name. Give the rule a name that is meaningful to you, for example **Game Server**. You can also select from a list of popular games, and many of the remaining configuration values will be filled in accordingly. However, you should check whether the port values have changed since this list was created, and you must fill in the IP address field.

IP Address. Enter the local network IP address of the system hosting the server, for example **192.168.0.50**. You can select a computer from the list of DHCP clients in the **Computer Name** drop-down menu, or you can manually enter the IP address of the server computer.

TCP Ports. Enter the TCP ports to open (for example **6159-6180, 99**).

UDP Ports. Enter the UDP ports to open (for example **6159-6180, 99**).

Schedule. Select a schedule for the times when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the **Tools → Schedules** sub-menu and create a new schedule.

Inbound Filter. Select a filter that controls access as needed for this rule. If you do not see the filter you need in the list of filters, go to the **Advanced → Inbound Filter** sub-menu and create a new filter.

Save/Update. Record the changes you have made. *(continued)*

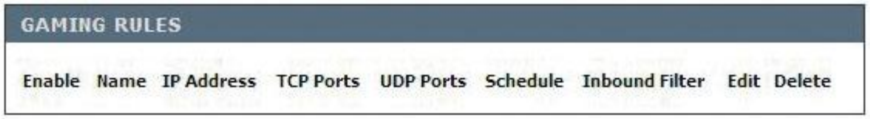
Clear. Re-initialize this area of the screen, discarding any changes you have made.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

With the above example values filled in and this Gaming Rule enabled, all TCP and UDP traffic on ports 6159 through 6180 and port 99 is passed through the router and redirected to the Internal Private IP Address of your Game Server at 192.168.0.50

NOTE: different LAN computers cannot be associated with Gaming rules that contain any ports in common. Such rules would contradict each other.

5.4.2 Gaming Rules



GAMING RULES

Enable	Name	IP Address	TCP Ports	UDP Ports	Schedule	Inbound Filter	Edit	Delete

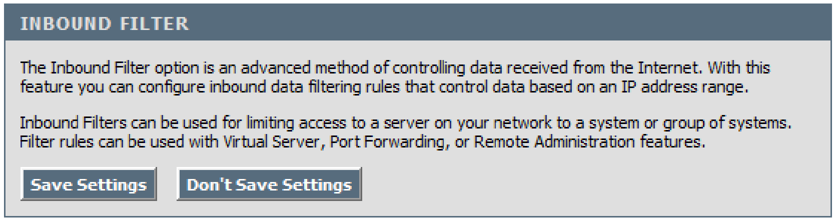
This is a list of the defined Gaming Rules. Click the **Enable** check box at the left to directly activate or de-activate the entry. An entry can be changed by clicking the **Edit** icon or can be deleted by clicking the **Delete** icon. When you click the **Edit** icon, the item is highlighted, and the **Gaming Rules** section is activated for editing.

After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with all configuration settings, click the **Reboot the Device** button.

5.5 *Inbound Filters*

(Default: No filters). When you use the Virtual Server, Gaming, or Remote Administration features to open specific ports to traffic from the Internet, you could be increasing the exposure of your LAN to cyberattacks from the Internet. In these cases, you can use Inbound Filters to limit that exposure by specifying the IP addresses of internet hosts that you trust to access your LAN through the ports that you have opened. You might, for example, only allow access to a game server on your home LAN from the computers of friends whom you have invited to play the games on that server.

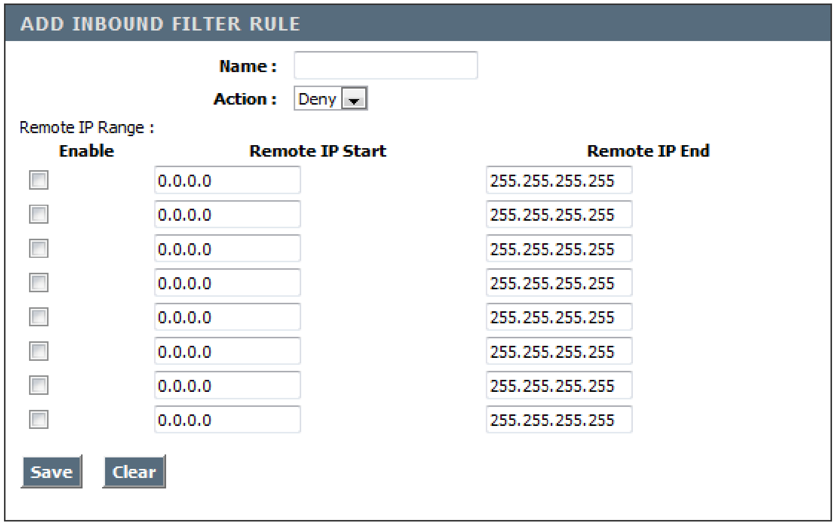
Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Gaming, or Remote Administration features. Each filter can be used for several functions; for example a "Game Clan" filter might allow all of the members of a particular gaming group to play several different games for which gaming entries have been created. At the same time an "Admin" filter might only allows systems from your office network to access the WAN admin pages and an FTP server you use at home. If you add an IP address to a filter, the change is effected in all of the places where the filter is used.



INBOUND FILTER

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range.

Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Port Forwarding, or Remote Administration features.



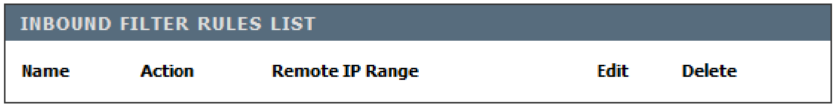
ADD INBOUND FILTER RULE

Name :

Action : Deny ▾

Remote IP Range :

Enable	Remote IP Start	Remote IP End
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255



INBOUND FILTER RULES LIST

Name	Action	Remote IP Range	Edit	Delete

5.5.1 Add Inbound Filter Rule

Name. Enter a name for the rule that is meaningful to you.

Action. The rule can be set to either ALLOW or DENY applicable messages. Defines the range of Internet addresses this rule applies to. Select the protocol used for this rule.

Enable. Enables inbound filtering for the IP Range you specify.

Remote IP Start/Remote IP End. Define the ranges of Internet addresses this rule applies to. For a single IP address, enter the same address in both the **Start** and **End** boxes. Up to eight ranges can be entered. The **Enable** check box allows you to turn on or off specific entries in the list of ranges.

Save/Update. Record the changes you have made.

Clear. Re-initialize this area of the screen, discarding any changes you have made. When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

(continued)

5.5.2 Inbound Filter Rules List

INBOUND FILTER RULES LIST

Name	Action	Remote IP Range	Edit	Delete

This section lists the current Inbound Filter rules. Click the **Enable** check box at the left to directly activate or de-activate the entry. An entry can be changed by clicking the **Edit** icon or can be deleted by clicking the **Delete** Inbound Filters Rule List section icon. When you click the **Edit** icon, the item is highlighted, and the **Inbound Filter Rules** section is activated for editing.

After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with all configuration settings, click the **Reboot the Device** button.

5.5.3 Configuring an Inbound Filter Rule

When the Rule List is empty or none of the rules are enabled, all inbound data that corresponds to a connection that originated from inside the router or which corresponds to a **Virtual Server**, **Gaming**, or **Special Application Rule** is ALLOWED by default. When rules are configured, the router compares incoming data packets against the rules in the list. It is very important to understand that the router examines each rule one by one in the order that they are listed in the Rule list until it finds a match. The packet will either be DENIED (Dropped) or ALLOWED. Once a match has been made, no further rules will be examined for that packet. If no rules match the data packet, it is ALLOWED. This means that to allow only a specific subset of traffic usually requires more than one rule to be entered.

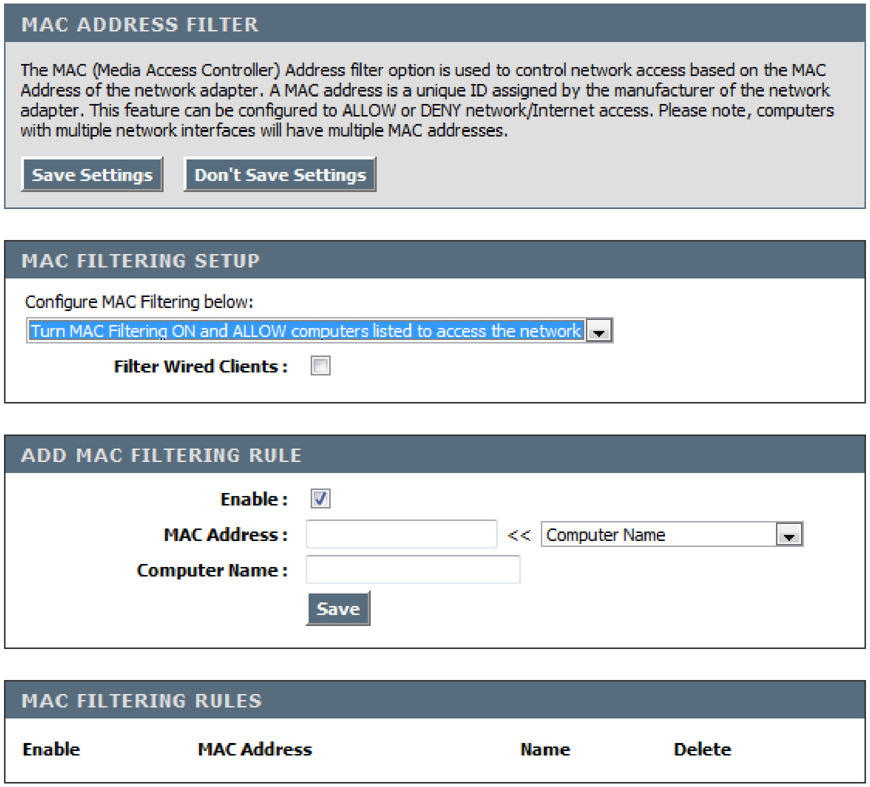
Example: You have configured a game server, using the **Advanced → Gaming** sub-menu, to play HALO: Combat Evolved with some friends. You would like to limit the access to your network and server to specific times of the day and only to your friends.

Next you would define a schedule on the **Tools → Schedule** sub-menu, called Game time, which specifies a schedule of Friday and Saturday between 7 PM and 11 PM. This example will assume all of your friends use the same service provider and have IP addresses 67.150.220.117, 67.150.231.43, and 67.150.231.75. You have an option of defining a set of rules to match each one of these addresses individually or you may just decide that using an IP range that covers all of them is sufficient for your needs.

The first rule is to configure a **DENY** rule that will catch all of the traffic that arrives on these ports but does not match data from the sources you want to have access to your network. It is important to enter the **DENY** rule first since all subsequent rules will be added higher in the list and will be checked first. Notice that it covers all **Source IP Address**, **Source Ports**, and **Times (Always)**, but is specifically tied to the Public Ports defined in the **Game Rule List**. This is because you do not want to accidentally block traffic for other applications. It is a good idea to turn on the log for this rule so that you can check in the log for anything that is filtered inappropriately. Next configure the **ALLOW** rules.

5.6 MAC Address Filter

Use the MAC (Media Access Control) Address filter sub-menu to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of a networking device. This feature can be configured to ALLOW or DENY network/Internet access.



MAC ADDRESS FILTER

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access. Please note, computers with multiple network interfaces will have multiple MAC addresses.

MAC FILTERING SETUP

Configure MAC Filtering below:

Turn MAC Filtering ON and ALLOW computers listed to access the network

Filter Wired Clients : □

ADD MAC FILTERING RULE

Enable : ☑

MAC Address : ______ << Computer Name

Computer Name : ______

MAC FILTERING RULES

Enable	MAC Address	Name	Delete

5.6.1 MAC Filtering Setup

Configure MAC Filtering Below. (Default: MAC Filtering Off). When MAC Filtering ON, depending on the mode selected, computers are granted or denied network access based on their MAC address.

- Turn MAC Filtering ON and ALLOW computers listed to access the network. When **ALLOW** is selected; only computers with MAC addresses listed in the MAC Address List are granted network access.
- Turn MAC Filtering ON and DENY computers listed to access the network. When **DENY** is selected, any computer with a MAC address listed in the MAC Address List will not be granted network access.

Filter Wired Clients. When check box is selected, MAC Filtering is applied to wired clients connected to the MBR1200 in addition to wireless clients.

5.6.2 ADD MAC Filtering Rule

Enable. MAC address entries are activated or deactivated with this check box.

MAC Address. Enter the MAC address of the desired computer or connect to the router from the desired computer and click **Copy Your PC's MAC Address** button.

Computer Name. Enter the name of the device or computer to which this MAC Address Filter Rule applies.

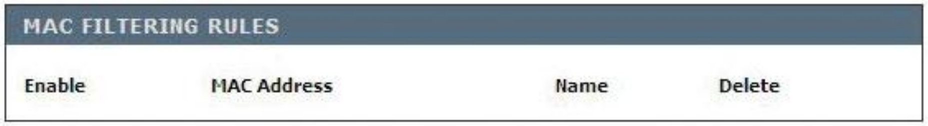
Save. Record the changes you have made.

Clear. Re-initialize this area of the screen, discarding any changes you have made.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

(continued)

5.6.3 MAC Filtering Rules



MAC FILTERING RULES

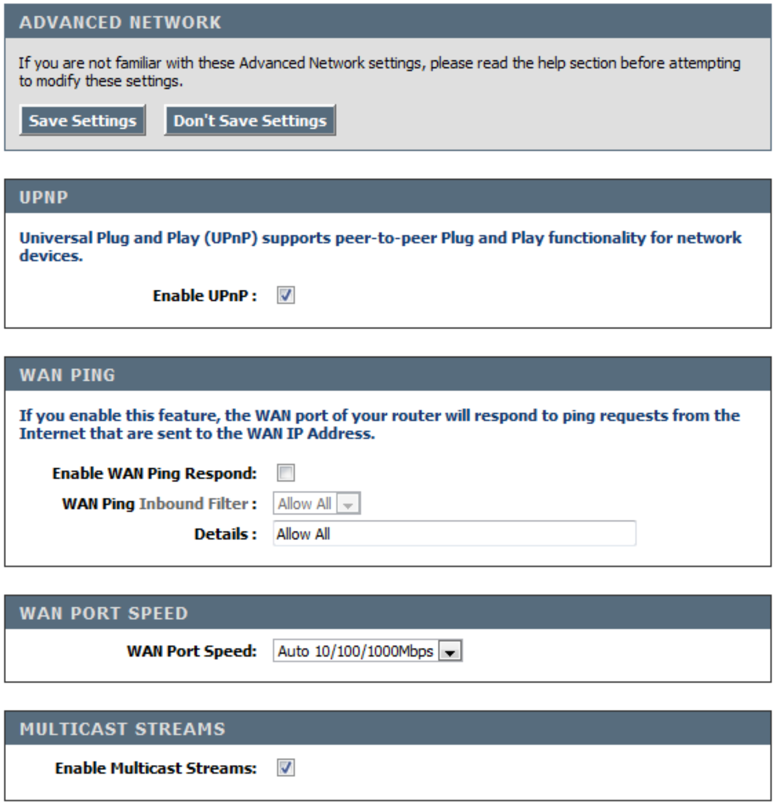
Enable	MAC Address	Name	Delete

This section lists the network devices that are under control of MAC filtering. Click the **Enable** check box at the left to directly activate or deactivate the entry. An entry can be changed by clicking the **Edit** icon or can be deleted MAC Filtering Rules section by clicking the **Delete** icon. When you click the **Edit** icon, the item is highlighted, and the **MAC Filtering Rules** section is activated for editing.

After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with all configuration settings, click the **Reboot the Device** button.

5.7 Network

The Network configuration is used to enable several special settings for the router. UPnP, WAN Ping response, WAN Port Speed, Multicast Streams, and PPoE Pass Through can be enabled or disabled.



If you are not familiar with these Advanced Network settings, please read the help section before attempting to modify these settings.

Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

Enable UPnP : ☑

If you enable this feature, the WAN port of your router will respond to ping requests from the Internet that are sent to the WAN IP Address.

Enable WAN Ping Respond: □

WAN Ping Inbound Filter : Allow All

Details : Allow All

WAN Port Speed: Auto 10/100/1000Mbps

Enable Multicast Streams: ☑

5.7.1 UPNP

Enable UPnP. Enables UPnP (Universal Plug and Play) functionality.

5.7.2 WAN Ping

Pinging public WAN IP addresses is a common method used by hackers to test whether your WAN IP address is valid.

Enable WAN Ping Respond. If you leave this option unchecked, you are causing the router to ignore ping commands for the public WAN IP address of the router.

WAN Ping Inbound Filter. Select a filter that controls which WAN computers can use the ping feature. If you do not see the filter you need in the list of filters, go to the **Advanced → Inbound Filter** sub-menu and create a new filter.

Details. This filter designates certain IP addresses from other computers or devices so that these IP addresses are either specifically allowed to communicate to the router, or are specifically blocked. This limits the range of IPs that can connect to the router, or block ones that are known to be from an attacking network.

5.7.3 WAN Port Speed

WAN Port Speed. Normally, this is set to **Auto**. If you have trouble connecting to the WAN, try the other settings.

5.7.4 Multicast Streams

The router uses the IGMP protocol to support efficient multicasting --transmission of identical content, such as multimedia, from a source to a number of recipients.

Enable Multicast Streams. This option must be enabled if any applications on the LAN participate in a multicast group. If you have a multimedia LAN application that is not receiving content as expected, try enabling this option.

5.8 Routing

Use the Routing sub-menu to define fixed routes.

5.8.1 Add Route

Adds a new route to the IP routing table or edits an existing route.

Enable. Specifies whether the entry will be enabled or disabled.

Destination IP. The IP address or network that the packets will be attempting to access. NOTE: 192.168.1.0 with a Netmask of 255.255.255.0 means traffic will be routed to the entire 192.168.1.x network.

Netmask. Used to specify which portion of the **Destination IP** signifies the network trying to be accessed and which part signifies the host that the packets will be routed to. NOTE: 255.255.255.255 is used to signify only the host that was entered in the Destination IP field.

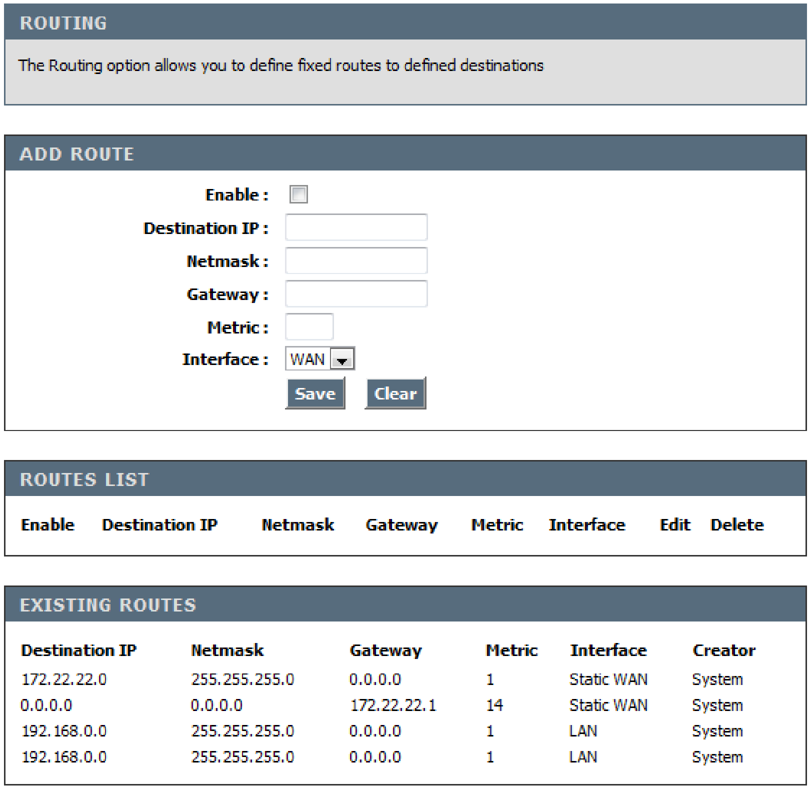
Gateway. Specifies the next hop to be taken if this route is used. A gateway of 0.0.0.0 implies there is no next hop, and the IP address matched is directly connected to the router on the interface specified: **LAN** or **WAN**.

Metric. The route metric is a value from 1 to 16 that indicates the cost of using this route. A value of 1 is the lowest cost, and 15 is the highest cost. A value of 16 indicates that the route is not reachable from this router. When trying to reach a particular destination, computers on your network will select the best route, ignoring unreachable routes.

Interface. Specifies the interface, **LAN** or **WAN**, that the IP packet must use to transit out of the router when this route is used.

Save/Update. Record the changes you have made.

Clear. Re-initialize this area of the screen, discarding any changes you have made.



ROUTING

The Routing option allows you to define fixed routes to defined destinations

ADD ROUTE

Enable :	☐
Destination IP :	
Netmask :	
Gateway :	
Metric :	
Interface :	WAN

ROUTES LIST

Enable	Destination IP	Netmask	Gateway	Metric	Interface	Edit	Delete

EXISTING ROUTES

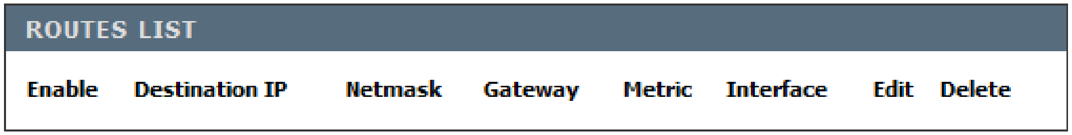
Destination IP	Netmask	Gateway	Metric	Interface	Creator
172.22.22.0	255.255.255.0	0.0.0.0	1	Static WAN	System
0.0.0.0	0.0.0.0	172.22.22.1	14	Static WAN	System
192.168.0.0	255.255.255.0	0.0.0.0	1	LAN	System
192.168.0.0	255.255.255.0	0.0.0.0	1	LAN	System

(continued)

5.8.2 Routes List

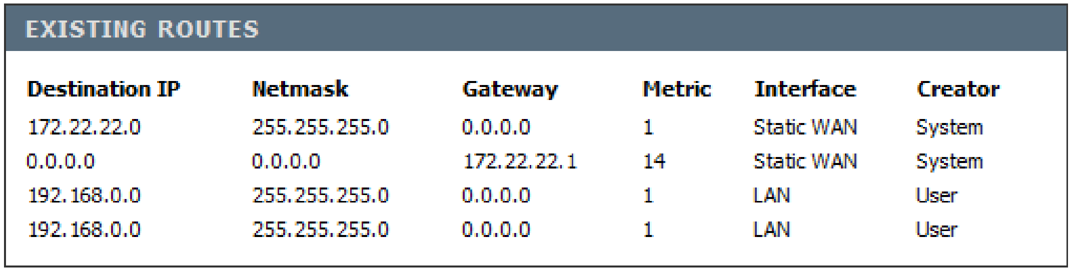
The section shows the current routing table entries. Certain required routes are predefined and cannot be changed. Routes that you add can be changed by clicking the **Edit** icon or can be deleted by clicking the **Delete** icon. When Routes List section you click the **Edit** icon, the item is highlighted, and the **Routes List** section is activated for editing. Click the **Enable** check box at the left to directly activate or de-activate the entry.

The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with all configuration settings, click the **Reboot the Device** button.



ROUTES LIST

Enable	Destination IP	Netmask	Gateway	Metric	Interface	Edit	Delete



EXISTING ROUTES

Destination IP	Netmask	Gateway	Metric	Interface	Creator
172.22.22.0	255.255.255.0	0.0.0.0	1	Static WAN	System
0.0.0.0	0.0.0.0	172.22.22.1	14	Static WAN	System
192.168.0.0	255.255.255.0	0.0.0.0	1	LAN	User
192.168.0.0	255.255.255.0	0.0.0.0	1	LAN	User

5.8.3 Existing Routes

Shows the routes that are in place already, some of which will be dynamically generated by the system and labeled “System” the Creator field). Those created by the user will be labeled “User” in the Creator field. To overwrite these values, simply click on the field of information you wish to change and re-enter the route information with the desired value changed.

5.9 Special Applications (Application Rules)

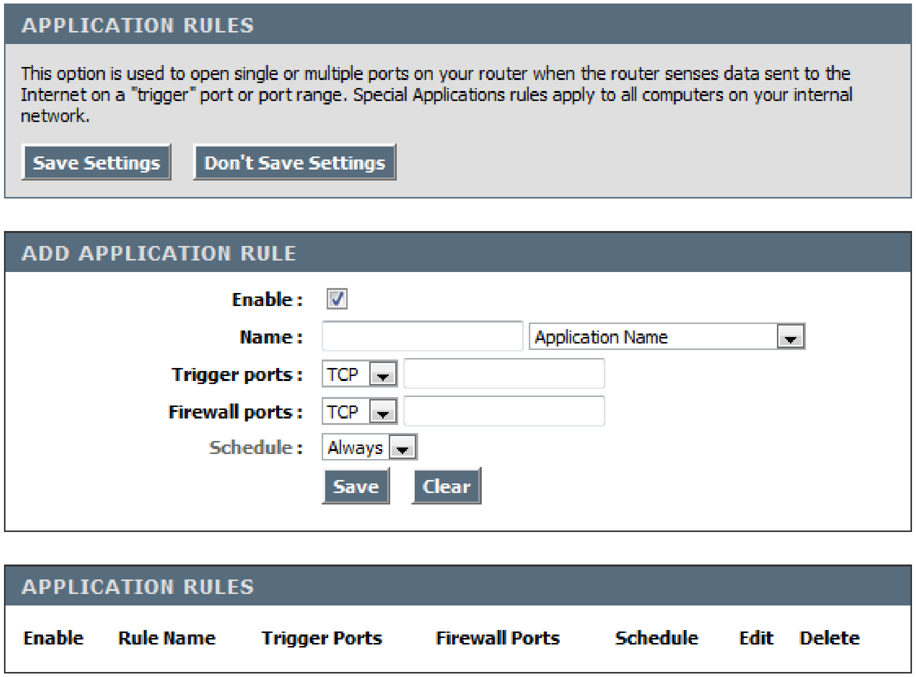
An application rule is used to open single or multiple ports on your router when the router senses data sent to the Internet on a "trigger" port or port range. An application rule applies to all computers on your internal network.

You can enable or disable Application Level Gateways (ALG's). Some protocols and applications require special handling of the IP payload to make them work with network address translation. Each ALG provides special handling for a specific protocol or application. ALG's for the following common applications are enabled by default, but can be turned off.

Example: You need to configure your router to allow a software application running on any computer on your network to connect to a web-based server or another user on the Internet.

5.9.1 Add Application Rule

Enable. (Default: No special applications rules). Opens single or multiple ports on the router when the router senses data sent to the Internet on a "trigger" port or port range. **Special Applications** rules apply to all computers on the network.



APPLICATION RULES

This option is used to open single or multiple ports on your router when the router senses data sent to the Internet on a "trigger" port or port range. Special Applications rules apply to all computers on your internal network.

ADD APPLICATION RULE

Enable : ☑
Name : Application Name
Trigger ports : TCP
Firewall ports : TCP
Schedule : Always

APPLICATION RULES

Enable	Rule Name	Trigger Ports	Firewall Ports	Schedule	Edit	Delete

Name. Enter a name for the Special Application Rule, for example **Game App**, which will help you identify the rule in the future. Alternatively, you can select from a drop down menu of common **applications**, and the remaining configuration values will be filled in accordingly.

Trigger Port. Enter the outgoing port range used by your application (for example **6500-6700**).

Trigger Traffic Type. Select the outbound protocol used by your application (for example **Both**).

Firewall Ports. Enter the port range that you want to open up to Internet traffic. (for example **6000-6200**).

Firewall Traffic Type. Select the protocol used by the Internet traffic coming back into the router through the opened port range (for example **Both**).

Schedule. Select a schedule for when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the **Tools → Schedules** sub-menu and create a new schedule.

Save/Update. Record the changes you have made.

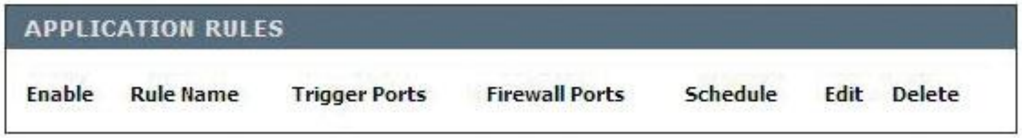
Clear. Re-initialize this area of the screen, discarding any changes you have made. *(continued)*

With the above example application rule enabled, the router will open up a range of ports from 6000-6200 for incoming traffic from the Internet, whenever any computer on the internal network opens up an application that sends data to the Internet using a port in the range of 6500-6700.

When you're done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

5.9.2 Applications Rules

The section shows the current routing table entries. Certain required routes are predefined and cannot be changed. Routes that you add can be changed by clicking the **Edit** icon or can be deleted by clicking the **Delete** icon. When you click the **Edit** icon, the item is highlighted, and the **Application Rules** section is activated for editing. Click the **Enable** check box at the left to directly activate or de-activate the entry.



APPLICATION RULES

Enable	Rule Name	Trigger Ports	Firewall Ports	Schedule	Edit	Delete

After you've completed all modifications or deletions, you must click **the Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with all configuration settings, click the **Reboot the Device** button.

5.10 Traffic Shaping

Use the Traffic Shaping sub-menu to configure CradlePoint's Traffic Shaping Technology, which allows control of the amount of traffic sent and received across the WAN port(s). The Traffic Shaping feature helps improve your network performance by prioritizing applications.

5.10.1 Traffic Shaping Setup

Enable Traffic Shaping. When this option is enabled, the router restricts the flow of outbound traffic so as not to exceed the WAN uplink bandwidth.

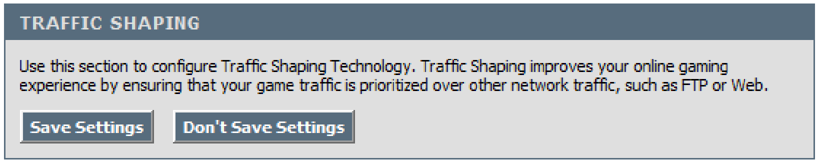
Automatic Classification. This option is enabled by default so that your router will automatically determine which programs should have network priority. For best performance, use the **Automatic Classification** option to automatically set the priority for your applications.

Dynamic Fragmentation. This option should be enabled when you have a slow Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones by breaking the large packets into several smaller packets.

Automatic Uplink Speed. When enabled, this option causes the router to automatically measure the useful uplink and downlink bandwidth each time the WAN interface is re-established (after a reboot, for example).

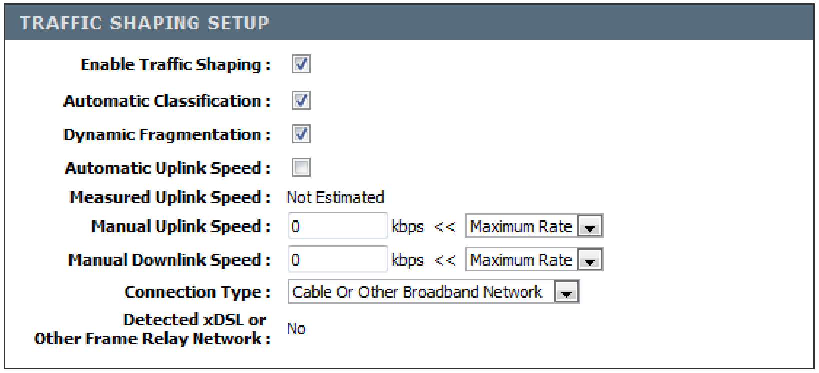
Measured Uplink Speed. This is the uplink speed measured when the WAN interface was last re-established. The value may be lower than that reported by your ISP as it does not include all of the network protocol overheads associated with your ISP's network. Typically, this figure will be between 87% and 91% of the stated uplink speed for xDSL connections and around 5 Kbps lower for cable network connections.

(continued)



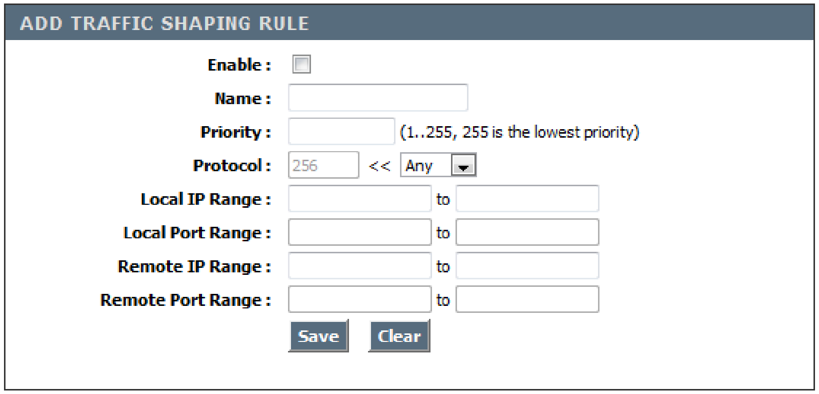
TRAFFIC SHAPING

Use this section to configure Traffic Shaping Technology. Traffic Shaping improves your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.



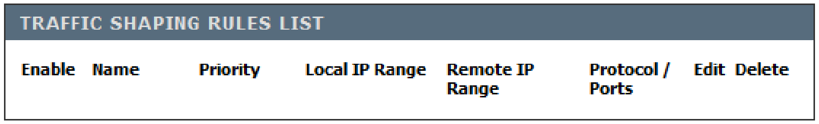
TRAFFIC SHAPING SETUP

Enable Traffic Shaping :	☑
Automatic Classification :	☑
Dynamic Fragmentation :	☑
Automatic Uplink Speed :	□
Measured Uplink Speed :	Not Estimated
Manual Uplink Speed :	0 kbps << Maximum Rate
Manual Downlink Speed :	0 kbps << Maximum Rate
Connection Type :	Cable Or Other Broadband Network
Detected xDSL or Other Frame Relay Network :	No



ADD TRAFFIC SHAPING RULE

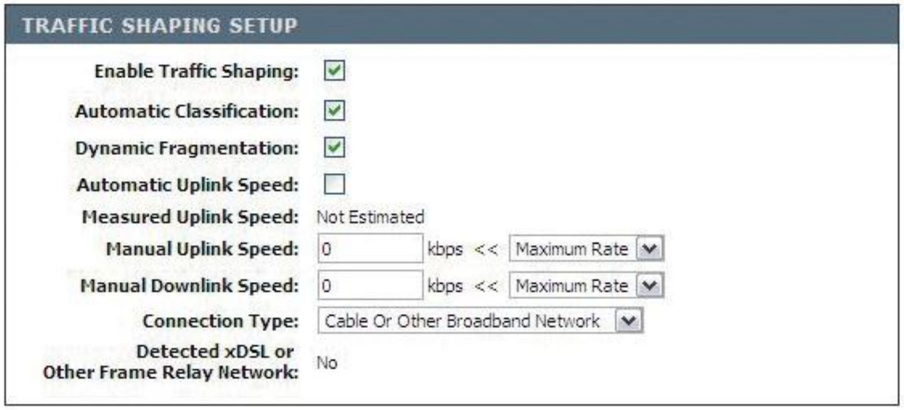
Enable :	□
Name :	
Priority :	(1..255, 255 is the lowest priority)
Protocol :	256 << Any
Local IP Range :	to
Local Port Range :	to
Remote IP Range :	to
Remote Port Range :	to



TRAFFIC SHAPING RULES LIST

Enable	Name	Priority	Local IP Range	Remote IP Range	Protocol / Ports	Edit	Delete

Manual Uplink Speed/Manual Downlink Speed. If Automatic Uplink Speed is disabled, these options allow you to set the uplink/downlink speeds manually. **Uplink speed** is the speed at which data can be transferred from the router to your ISP. **Downlink speed** is the speed at which data can be transferred from your ISP to the router. These are determined by your ISP. ISP's often specify speed as a downlink/uplink pair; for example, 1.5 Mbps/284 Kbps. In this case, for the uplink speed you would enter **1.5 Mbps** (or choose **1024 Kbps** from the drop down menu [the speed chosen has to be equal to or below your connection's rated speed]) and for the uplink speed you would enter **284 Kbps** (or choose **284 Kbps** from the drop down menu [the speed chosen has to be equal to or below your connection's rated speed]).



TRAFFIC SHAPING SETUP

Enable Traffic Shaping:	☑
Automatic Classification:	☑
Dynamic Fragmentation:	☑
Automatic Uplink Speed:	□
Measured Uplink Speed:	Not Estimated
Manual Uplink Speed:	0 kbps << Maximum Rate
Manual Downlink Speed:	0 kbps << Maximum Rate
Connection Type:	Cable Or Other Broadband Network
Detected xDSL or Other Frame Relay Network:	No

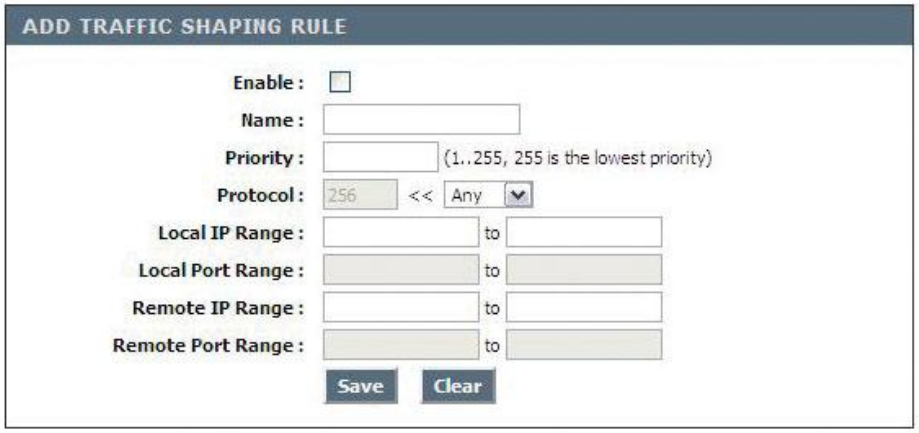
Alternatively you can test your uplink speed with a service such as **www.dslreports.com**. NOTE: not matter how a site, such as DSL reports, because they do not consider as many network protocol overheads, will generally note speeds slightly lower than the **Measured Uplink Speed** or the ISP rated speed.

Connection Type. By default, the router automatically determines whether the underlying connection is an xDSL/Frame-relay network or some other connection type (such as cable modem or Ethernet), and it displays the result as **Detected xDSL or Frame Relay Network**. If you have an unusual network connection in which you are actually connected via xDSL but for which you configure either **Static** or **DHCP** in the WAN settings, setting this option to **xDSL** or **Other Frame Relay Network** ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance. Choosing **xDSL** or **Other Frame Relay Network** causes the measured uplink speed to be reported slightly lower than before on such connections, but gives much better results.

Detected xDSL or Other Frame Relay Network. When **Connection Type** is set to **Auto-detect**, the automatically detected connection type is displayed here.

(continued)

5.10.2 Add Traffic Shaping Rule



ADD TRAFFIC SHAPING RULE

Enable :	□
Name :	
Priority :	(1..255, 255 is the lowest priority)
Protocol :	256 << Any
Local IP Range :	to
Local Port Range :	to
Remote IP Range :	to
Remote Port Range :	to

A Traffic Shaping Rule identifies a specific message flow and assigns a priority to that flow. For most applications, automatic classification will be adequate, and specific Traffic Shaping Rules will not be required.

Traffic Shaping supports overlaps between rules, where more than one rule can match for a specific message flow. If more than one rule is found to match the rule with the highest priority will be used.

Enable. Specifies whether the entry will be active or inactive.

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

Priority. The priority of the message flow is entered here--1 receives the highest priority (most urgent) and 255 receives the lowest priority (least urgent).

Protocol. The protocol used by the messages.

Local IP Range. The rule applies to a flow of messages whose LAN-side IP address falls within the range set here.

Local Port Range. The rule applies to a flow of messages whose LAN-side port number is within the range set here.

Remote IP Range. The rule applies to a flow of messages whose WAN-side IP address falls within the range set here.

Remote Port Range. The rule applies to a flow of messages whose WAN-side port number is within the range set here.

Save/Update. Record the changes you have made.

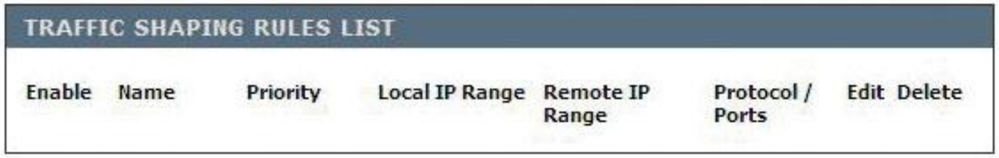
Clear. Re-initialize this area of the screen, discarding any changes you have made.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

(continued)

5.10.3 Traffic Shaping Rules List

This section lists all the defined Traffic Shaping Rules. Click the **Enable** check box at the left to directly activate or de-activate the entry. An entry can be changed by clicking the **Edit** icon or can be deleted by clicking the **Delete** icon. When you click the **Edit** icon, the item is highlighted, and the **Traffic Shaping Rules List** section is activated for editing



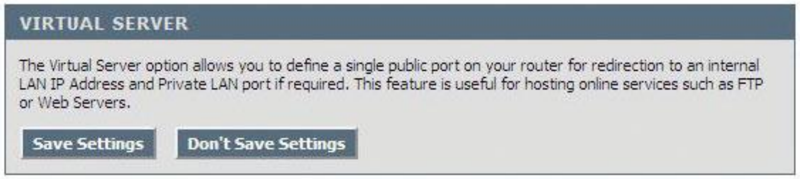
TRAFFIC SHAPING RULES LIST

Enable	Name	Priority	Local IP Range	Remote IP Range	Protocol / Ports	Edit	Delete

After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with all configuration settings, click the **Reboot the Device** button.

5.11 Virtual Server

The Virtual Server option gives Internet users access to services on a LAN. This feature is useful for hosting online services such as **FTP**, **Web**, or **Game Servers**. For each Virtual Server, the user defines a public port on the router for redirection to an internal LAN IP Address and LAN port.



VIRTUAL SERVER

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

5.11.1 Add Virtual Server Rule

Enable. Click the check box to enable (default = No Virtual Server rules).

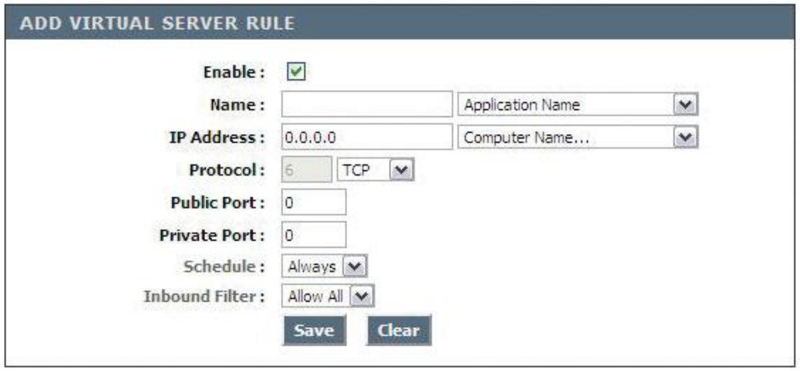
Name. Name of the virtual server, such as **Web Server**. Several well-known types of virtual server are available from the "Application Name" drop-down list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.

IP Address. The IP address of the system on your internal network that will provide the virtual service, such as **192.168.0.50**. You can select a computer from the list of DHCP clients in the "Computer Name" drop-down menu, or you can manually enter the IP address of the server computer.

Protocol. Select the protocol used by the service, **TCP**, **UDP** or **Both**. To specify any other protocol, select "Other" from the list, then enter the corresponding protocol number (as assigned by the IANA) in the **Protocol** box.

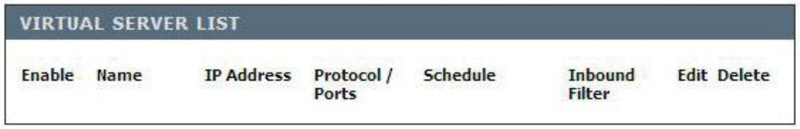
Public Port. The port that will be accessed from the Internet.

Private Port. The port that will be used on your internal network.



ADD VIRTUAL SERVER RULE

Enable :	☑	
Name :		Application Name
IP Address :	0.0.0.0	Computer Name...
Protocol :	6	TCP
Public Port :	0	
Private Port :	0	
Schedule :	Always	
Inbound Filter :	Allow All	



VIRTUAL SERVER LIST

Enable	Name	IP Address	Protocol / Ports	Schedule	Inbound Filter	Edit	Delete

Schedule. Select a schedule for when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the **Tools → Schedules** sub-menu and create a new schedule.

Inbound Filter. Select a filter that controls access as needed for this virtual server. If you do not see the filter you need in the list of filters, go to the **Advanced → Inbound Filter** sub-menu and create a new filter.

Save/Update. Record the changes you have made.

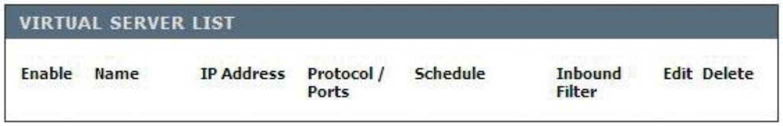
Clear. Re-initialize this area of the screen, discarding any changes you have made.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

(continued)

5.11.2 Virtual Server List

This is a list of the defined Virtual Servers. Click the Enable checkbox at the left to directly activate or de-activate the entry. An entry can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the **Edit Virtual Servers** section is activated for editing.



VIRTUAL SERVER LIST

Enable	Name	IP Address	Protocol / Ports	Schedule	Inbound Filter	Edit	Delete

After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with all configuration settings, click the **Reboot the Device** button.

NOTE: You might have trouble accessing a virtual server using its public identity (WAN-side IP-address of the gateway or its dynamic DNS name) from a machine on the LAN. Your requests may not be looped back or you may be redirected to the "Forbidden" page.

This will happen if you have an Access Control Rule configured for this LAN machine.

The requests from the LAN machine will not be looped back if Internet access is blocked at the time of access. To work around this problem, access the LAN machine using its LAN-side identity.

Requests may be redirected to the "Forbidden" page if web access for the LAN machine is restricted by an Access Control Rule. Add the WAN-side identity (WAN-side IP-address of the router or its dynamic DNS name) on the **Advanced → Web Filter** screen to work around this problem.

Example:

You are hosting a Web Server on a Laptop or PC that has Private IP Address of 192.168.0.50 and your ISP is blocking Port 80.

1. Name the Virtual Server Rule (e.g., **Web Server**)
2. Enter in the IP Address of the machine on your LAN – **192.168.0.50**
3. Enter the Private Port as [**80**]
4. Enter the Public Port as [**8888**]
5. Select the Protocol -**TCP**
6. Ensure the schedule is set to **Always**
7. Check the **Save** box to add the settings
8. Repeat these steps for each **Virtual Server Rule** you wish to add. After the list is complete, click **Save Settings** at the top of the page.

With this Virtual Server Rule all Internet traffic on Port 8888 will be redirected to an internal web server on port 80 at IP Address 192.168.0.50.

5.12 Web Filter (Website Filter)

Use the Web Filter section to enable OpenDNS and add Websites to be used for Access Control (**Advanced → Access Control** sub-menu). OpenDNS is web-based service that helps Web sites load faster, while providing antiphishing and Web content filtering. (www.openDNS.com)

By default, Website Filter is enabled, however no filtering is done until the list is populated. Also, since Access Control is disabled by default, no filtering is done until Access Control is also enabled (**Advanced → Access Control** sub-menu).

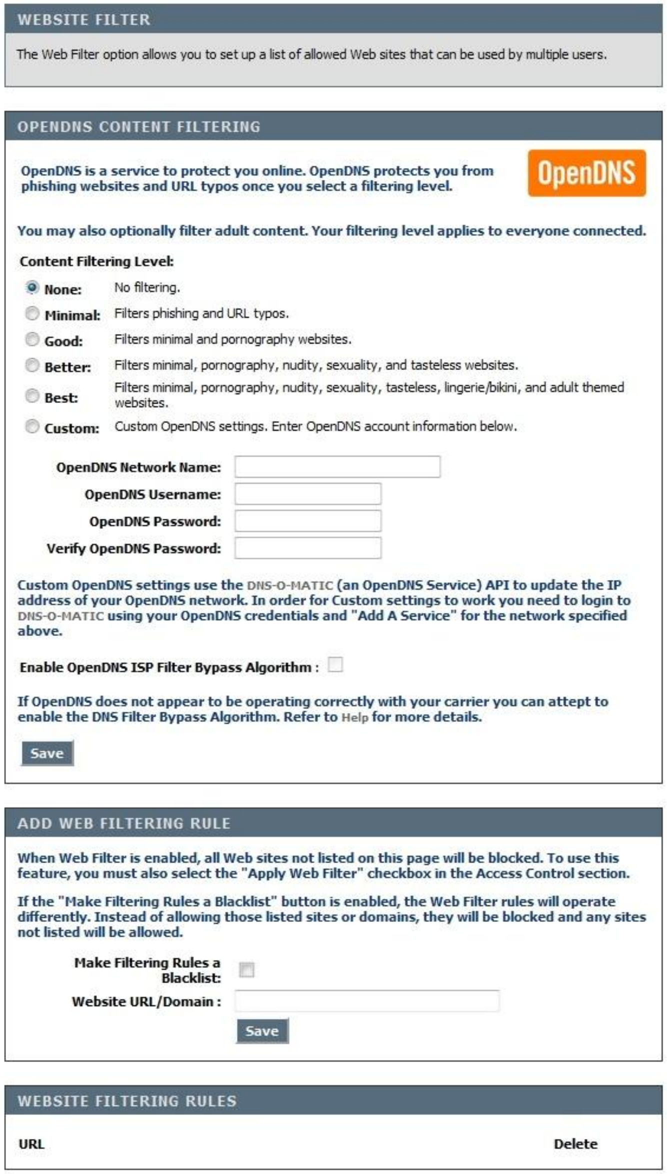
5.12.1 OpenDNS Content Filtering

This feature allows you to filter Web sites through the uses of OpenDNS. Different selectable qualities are chosen to enable Web filtering for everyone connected to the device. This does change your router's DNS settings to use the OpenDNS servers.

- None. Disables Web filtering that uses OpenDNS, but will enable manual Web site white listing in the next subsection.
- Minimal. Filters phishing and URL typos.
- Good. Filters any Web site containing pornography as well as enable typo and phishing redirection.
- Better. Filters more nudity, sexuality, and tasteless content.
- Best. Filters more nudity, sexuality, and tasteless content. Selecting "Best" will filter all content which is deemed adult content by OpenDNS
- Custom. Uses Custom OpenDNS settings. Enter OpenDNS account information. Enter OpenDNS account details to enable the router to dynamically update the dynamic WAN IP address with OpenDNS. Also ensure your network is associated to your account at DNS-O-MATIC (an OpenDNS service).

OpenDNS ISP Filter Bypass Algorithm. Some ISPs filter OpenDNS requests and redirect them to different DNS servers. Enabling this will attempt to bypass those filters when using an OpenDNS Content Filtering Level.

(continued)



WEBSITE FILTER

The Web Filter option allows you to set up a list of allowed Web sites that can be used by multiple users.

OPENDNS CONTENT FILTERING

OpenDNS is a service to protect you online. OpenDNS protects you from phishing websites and URL typos once you select a filtering level.

You may also optionally filter adult content. Your filtering level applies to everyone connected.

Content Filtering Level:

● None: No filtering.
○ Minimal: Filters phishing and URL typos.
○ Good: Filters minimal and pornography websites.
○ Better: Filters minimal, pornography, nudity, sexuality, and tasteless websites.
○ Best: Filters minimal, pornography, nudity, sexuality, tasteless, lingerie/bikini, and adult themed websites.
○ Custom: Custom OpenDNS settings. Enter OpenDNS account information below.

OpenDNS Network Name:
OpenDNS Username:
OpenDNS Password:
Verify OpenDNS Password:

Custom OpenDNS settings use the DNS-O-MATIC (an OpenDNS Service) API to update the IP address of your OpenDNS network. In order for Custom settings to work you need to login to DNS-O-MATIC using your OpenDNS credentials and "Add A Service" for the network specified above.

Enable OpenDNS ISP Filter Bypass Algorithm : □

If OpenDNS does not appear to be operating correctly with your carrier you can attept to enable the DNS Filter Bypass Algorithm. Refer to Help for more details.

ADD WEB FILTERING RULE

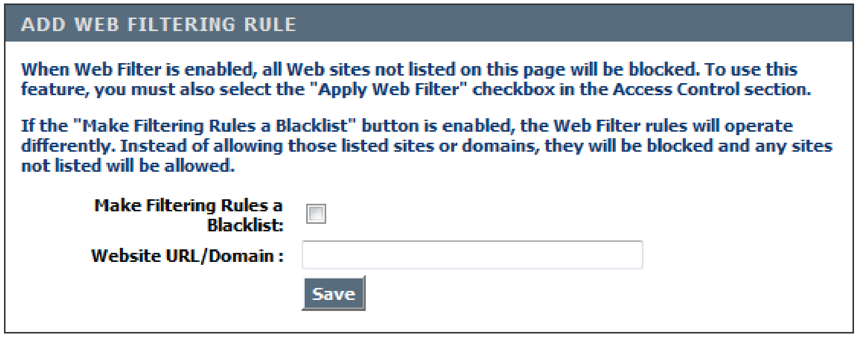
When Web Filter is enabled, all Web sites not listed on this page will be blocked. To use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section.

If the "Make Filtering Rules a Blacklist" button is enabled, the Web Filter rules will operate differently. Instead of allowing those listed sites or domains, they will be blocked and any sites not listed will be allowed.

Make Filtering Rules a Blacklist: □
Website URL/Domain :

WEBSITE FILTERING RULES

URL	Delete



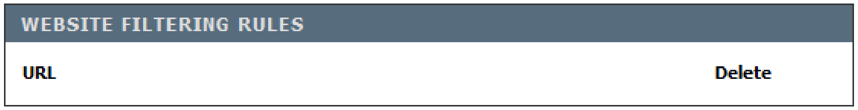
ADD WEB FILTERING RULE

When Web Filter is enabled, all Web sites not listed on this page will be blocked. To use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section.

If the "Make Filtering Rules a Blacklist" button is enabled, the Web Filter rules will operate differently. Instead of allowing those listed sites or domains, they will be blocked and any sites not listed will be allowed.

Make Filtering Rules a Blacklist: □

Website URL/Domain :



WEBSITE FILTERING RULES

URL	Delete

5.12.2 Add Web Filtering Rule

This section is where you add the Web sites to be used for Access Control.

Make Filtering Rules a Blacklist. If the **Make Filtering Rules a Blacklist** button is enabled, the Web Filter rules will operate differently. Instead of allowing those listed sites or domains, they will be blocked and any sites not listed will be allowed.

Website URL/Domain. Enter the URL (address) of the Web Site that you want to allow; for example: **google.com**. Do not enter the **http://** preceding the URL. Enter the most inclusive domain; for example, enter **kyocera.com** and access will be permitted to both **www.kyocera.com** and **support.kyocera.com**.

Save. Record the changes you have made into the following list.

NOTE: Many web sites construct pages with images and content from other web sites. Access will be forbidden if you do not enable all the web sites used to construct a page. For example, to access **my.yahoo.com**, you need to enable access to **yahoo.com**, **yimg.com**, and **doubleclick.net**.

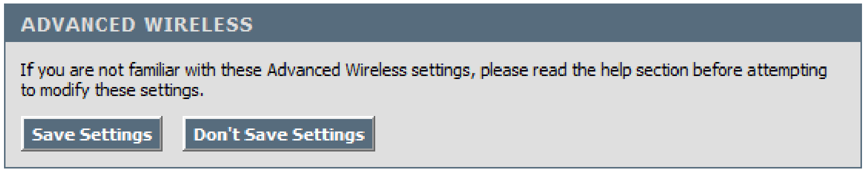
NOTE: To activate this feature, you must select **Apply Web Filter** in the **Advanced → Access Control** sub-menu.

5.12.3 Website Filtering Rules

The section lists the currently allowed web sites. The Web sites listed here are used when the Web Filter option is enabled in the **Advanced → Access Control** sub-menu.

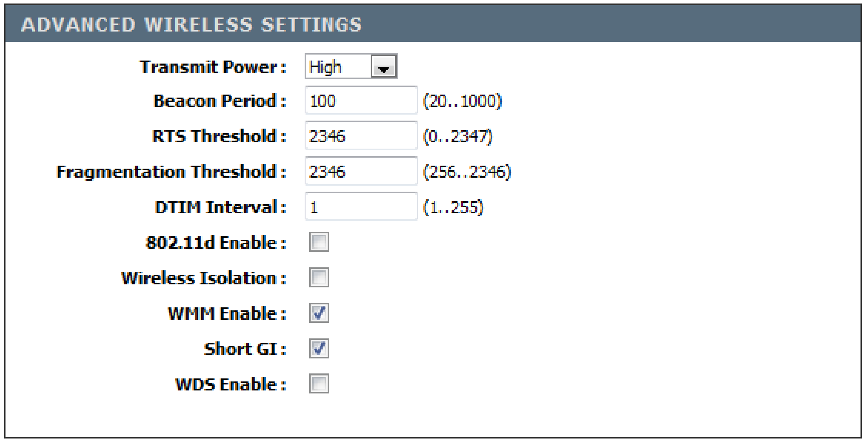
5.13 Wireless (WI-FI)

Use the Advanced Wireless sub-menu for detailed configuration of radio parameters for the 802.11b/g/n Wireless LAN.



ADVANCED WIRELESS

If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings.



ADVANCED WIRELESS SETTINGS

Transmit Power :	High	
Beacon Period :	100	(20..1000)
RTS Threshold :	2346	(0..2347)
Fragmentation Threshold :	2346	(256..2346)
DTIM Interval :	1	(1..255)
802.11d Enable :	□	
Wireless Isolation :	□	
WMM Enable :	☑	
Short GI :	☑	
WDS Enable :	□	

5.13.1 Advanced Wireless Settings

Transmit Power. Normally the wireless transmitter operates at 100% power (drop down menu: **High**). 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.

Beacon Period. Beacons are packets sent by a wireless router to synchronize wireless devices. Specify a **Beacon Period** value between 20 and 1000 milliseconds. The default value is set to **100 milliseconds**.

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 of **2346 bytes**.

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 of **2346 bytes**. Setting the Fragmentation value too low may result in poor performance.

DTIM Interval. 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**.

(continued)

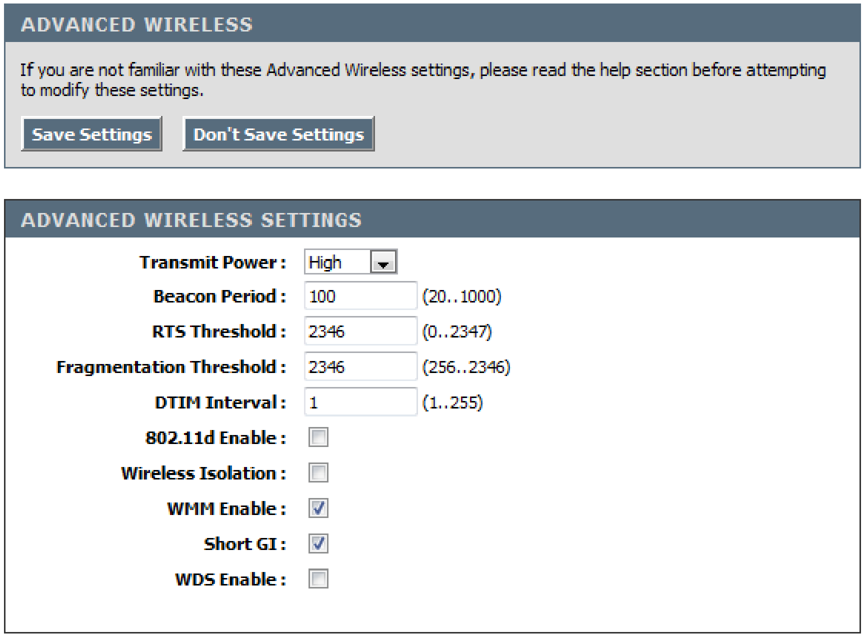
802.11d Enable. Enables 802.11d operation. 802.11d is a wireless specification for operation in additional regulatory domains. This supplement to the 802.11 specifications defines the physical layer requirements (channelization, hopping patterns, new values for current MIB attributes, and other requirements to extend the operation of 802.11 WLANs to new regulatory domains (countries). The current 802.11 standard defines operation in only a few regulatory domains (countries). This supplement adds the requirements and definitions necessary to allow 802.11 WLAN equipment to operate in markets not served by the current standard. Enable this option if you are operating in one of these “additional regulatory domains”.

Wireless Isolation. Enabling Wireless Isolation prevents associated wireless clients from communicating with each other.

WMM Enable. Enabling WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.

Short GI. Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

WDS Enable. Not Supported in the MBR1200.



ADVANCED WIRELESS

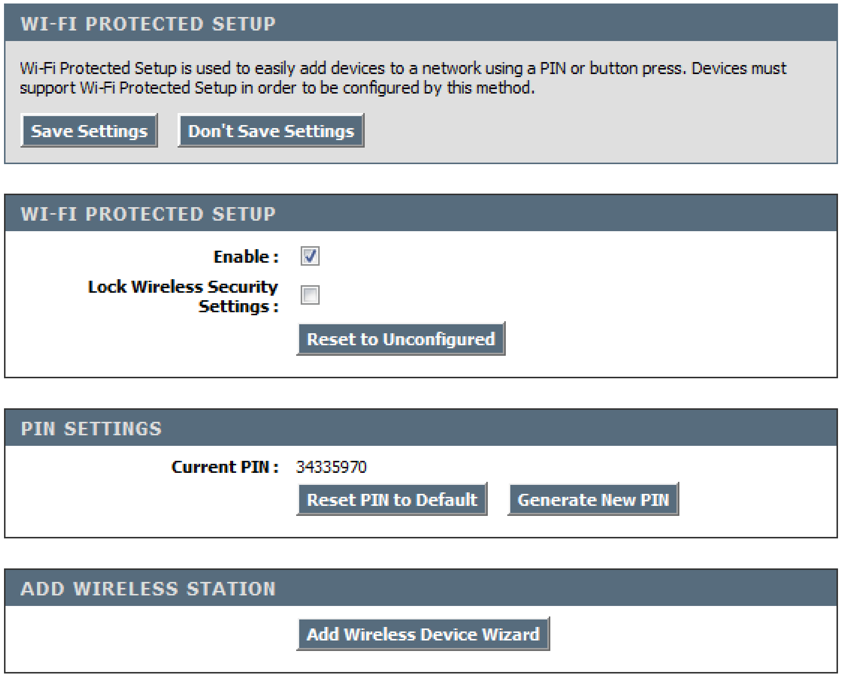
If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings.

ADVANCED WIRELESS SETTINGS

Transmit Power :	High	
Beacon Period :	100	(20..1000)
RTS Threshold :	2346	(0..2347)
Fragmentation Threshold :	2346	(256..2346)
DTIM Interval :	1	(1..255)
802.11d Enable :	□	
Wireless Isolation :	□	
WMM Enable :	☑	
Short GI :	☑	
WDS Enable :	□	

5.14 WI-FI Protected Setup

Use Wi-Fi Protected Setup sub-menu to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.



WI-FI PROTECTED SETUP

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

WI-FI PROTECTED SETUP

Enable : ☑

Lock Wireless Security Settings : □

PIN SETTINGS

Current PIN : 34335970

ADD WIRELESS STATION

5.14.1 WI-FI Protected Setup

Enable. Enable the Wi-Fi Protected Setup feature.

Lock Wireless Security Settings. Locking the wireless security settings prevents the settings from being changed by any new external registrar using its PIN. Devices can still be added to the wireless network using Wi-Fi Protected Setup. It is still possible to change wireless network settings with **Manual Wireless Network Setup**, **Wireless Network Setup Wizard**, or an existing external WLAN Manager Registrar.

Reset to Unconfigured. Click the **Reset to Unconfigured** button to set the PIN back to the factory default pin which is listed on the end panel of the MBR1200 box and on the label affixed to the bottom of the MBR1200 unit.

5.14.2 Pin Settings

A PIN is a unique number that can be used to add the router to an existing network or to create a new network. The default PIN may be printed on the bottom of the router. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator ("admin" account) can change or reset the PIN.

Current PIN. Shows the current value of the router's PIN.

Reset PIN to Default. Restore the default PIN of the router.

Generate New PIN. Create a random number that is a valid PIN. This becomes the router's PIN. You can then copy this PIN to the user interface of the registrar.

5.14.3 Add Wireless Station

This Wizard helps you add wireless devices to the wireless network using the Wi-Fi Protected Setup protocol.

(continued)

The wizard will prompt you to enter the PIN for the device, or ask you to press the configuration button on the device. If the device supports Wi-Fi Protected Setup and has a configuration button, you can add it to the network by pressing the configuration button on the device and then the on the router within 60 seconds. The status LED on the router will flash three times if the device has been successfully added to the network.

There are several ways to add a wireless device to your network. Access to the wireless network is controlled by a “registrar”. A registrar only allows devices onto the wireless network if you have entered the PIN, or pressed a special Wi-Fi Protected Setup button on the device. The router acts as a registrar for the network, although other devices may act as a registrar as well.

Clicking the **Add Wireless Device Wizard** button starts the wizard.

“PIN” Option

Welcome to the Add Wireless Device Wizard. Click **Next**.

Step 1: Select Configuration Method for Your Wireless Network. Choose configuration method that your wireless device is capable of supporting (refer to the documentation that came with your wireless adapter).

Select **PIN**. Select this option if your wireless device supports PIN. (Push Button instructions follow in next section).

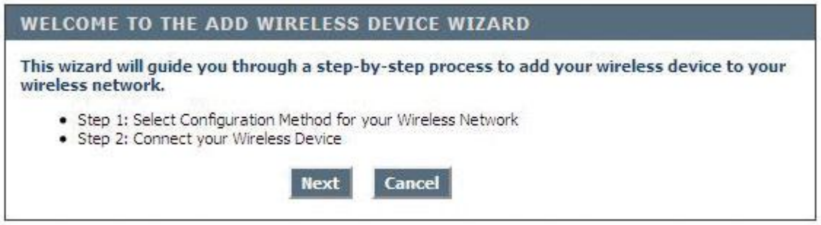
Click **Next**.

Step 2: Connect Your Wireless Device. Enter the PIN of your wireless device, then click on the **Connect** button.

The PIN method of WPS allows a device to search for the Wi-Fi device attached to that PIN number and setup a connection and security between that device and the router.

All devices supporting the WPS PIN method will have a PIN number associated to them in product packaging, documentation or labeling.

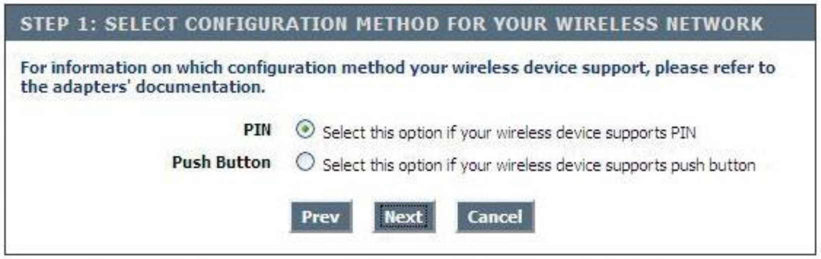
(continued)



WELCOME TO THE ADD WIRELESS DEVICE WIZARD

This wizard will guide you through a step-by-step process to add your wireless device to your wireless network.

- Step 1: Select Configuration Method for your Wireless Network
- Step 2: Connect your Wireless Device

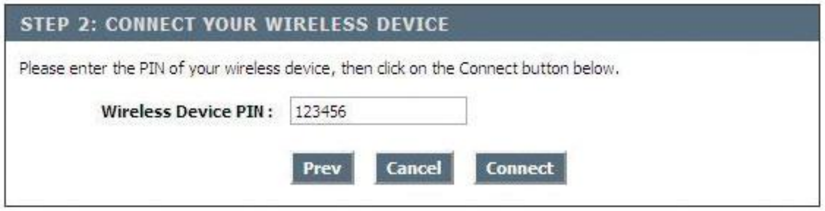


STEP 1: SELECT CONFIGURATION METHOD FOR YOUR WIRELESS NETWORK

For information on which configuration method your wireless device support, please refer to the adapters' documentation.

PIN ● Select this option if your wireless device supports PIN

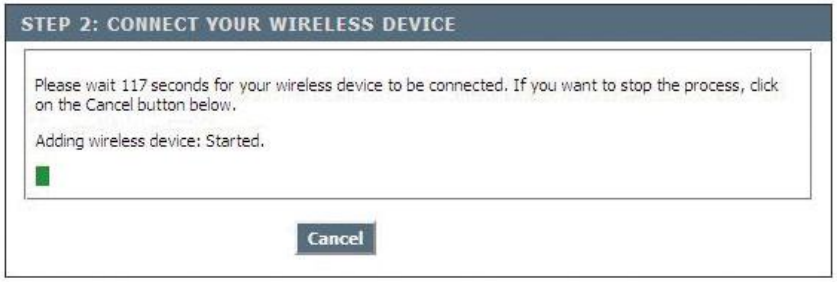
Push Button ○ Select this option if your wireless device supports push button



STEP 2: CONNECT YOUR WIRELESS DEVICE

Please enter the PIN of your wireless device, then click on the Connect button below.

Wireless Device PIN : 123456



STEP 2: CONNECT YOUR WIRELESS DEVICE

Please wait 117 seconds for your wireless device to be connected. If you want to stop the process, click on the Cancel button below.

Adding wireless device: Started.

"PUSH BUTTON" Option

Welcome to the Add Wireless Device Wizard. Click **Next**.

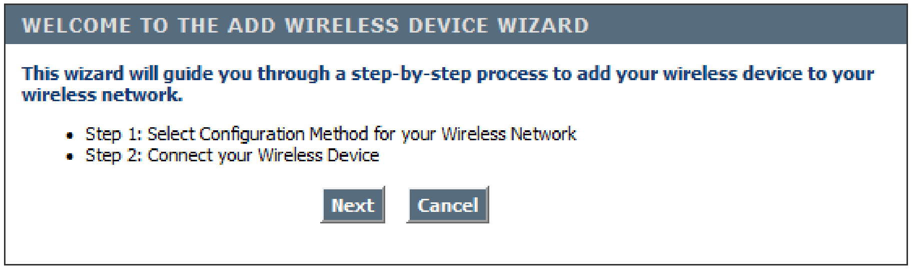
Step 1: Select Configuration Method for Your Wireless Network. Choose configuration method that your wireless device is capable of supporting (refer to the documentation that came with your wireless adapter).

Select **Push Button**. Select this option if your wireless device supports push button. (PIN instructions in previous section) Click **Next**.

Click **Next**

Step 2: Connect Your Wireless Device. Push the button on your wireless device, then click on the **Connect button**.

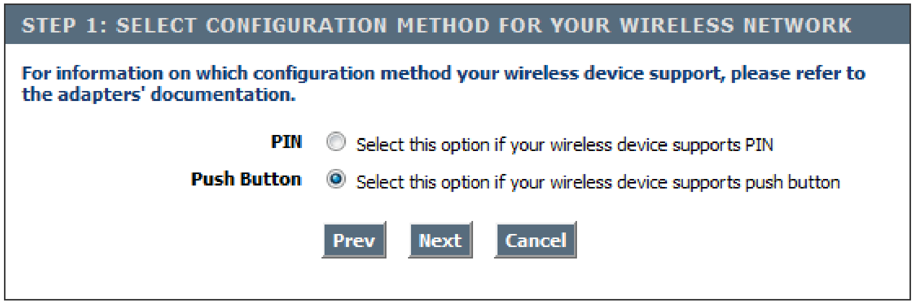
When you use the push button method, the MBR1200 and another WPS device will enter their "discoverable" mode and find each other to set up a connection and security.



WELCOME TO THE ADD WIRELESS DEVICE WIZARD

This wizard will guide you through a step-by-step process to add your wireless device to your wireless network.

- Step 1: Select Configuration Method for your Wireless Network
- Step 2: Connect your Wireless Device

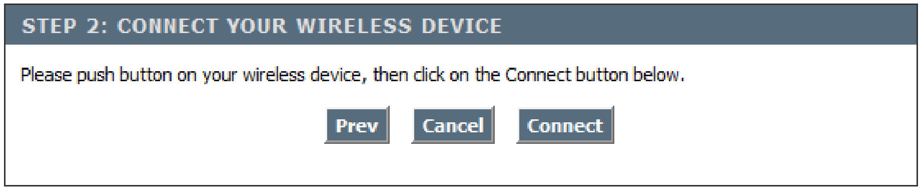


STEP 1: SELECT CONFIGURATION METHOD FOR YOUR WIRELESS NETWORK

For information on which configuration method your wireless device support, please refer to the adapters' documentation.

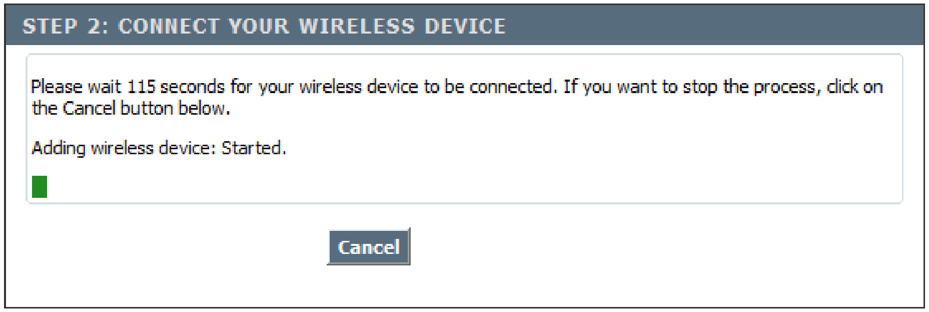
PIN ○ Select this option if your wireless device supports PIN

Push Button ● Select this option if your wireless device supports push button



STEP 2: CONNECT YOUR WIRELESS DEVICE

Please push button on your wireless device, then click on the Connect button below.



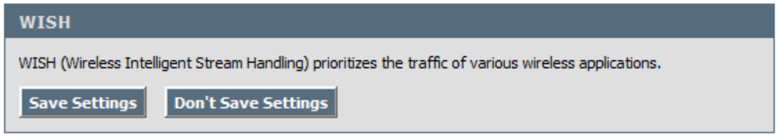
STEP 2: CONNECT YOUR WIRELESS DEVICE

Please wait 115 seconds for your wireless device to be connected. If you want to stop the process, click on the Cancel button below.

Adding wireless device: Started.

5.15 WISH

Use the WISH (Wireless Intelligent Stream Handling) sub-menu to prioritize traffic for various wireless applications, specific application protocols and specific computers on the wireless network.

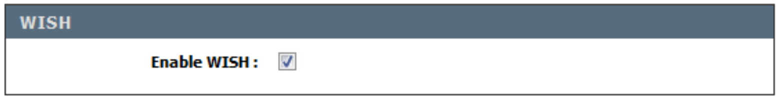


WISH

WISH (Wireless Intelligent Stream Handling) prioritizes the traffic of various wireless applications.

5.15.1 WISH

Enable WISH. Enable this option if you want to allow WISH to prioritize your traffic.



WISH

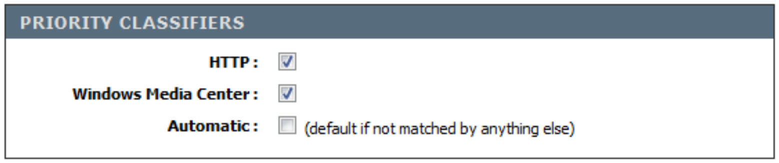
Enable WISH : ☑

5.15.2 Priority Classifiers

HTTP. Allows the router to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.

Windows Media Center. Enables the router to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360.

Automatic. When enabled, this option causes the router to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behavior that the streams exhibit. This acts to de-prioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.



PRIORITY CLASSIFIERS

HTTP : ☑

Windows Media Center : ☑

Automatic : □ (default if not matched by anything else)

5.15.3 Add Wish Rule

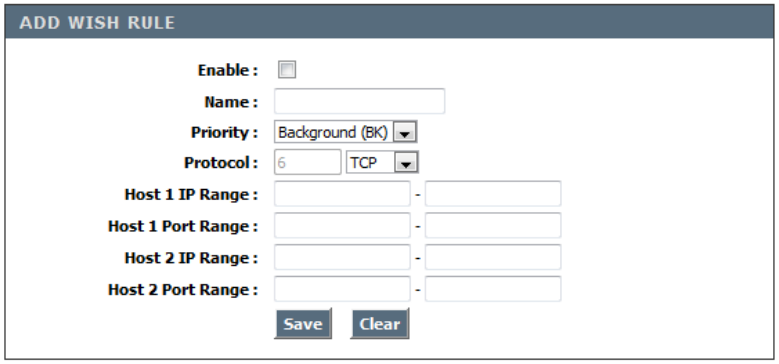
A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific WISH Rules are not required.

WISH supports overlaps between rules. If more than one rule matches for a specific message flow, the rule with the highest priority will be used.

Enable. Specifies whether the entry will be active or inactive.

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

(continued)



ADD WISH RULE

Enable : □

Name :

Priority : Background (BK)

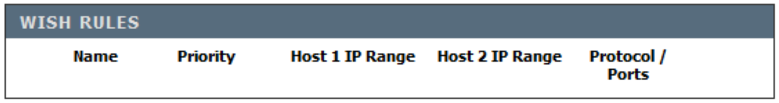
Protocol : 6 TCP

Host 1 IP Range : -

Host 1 Port Range : -

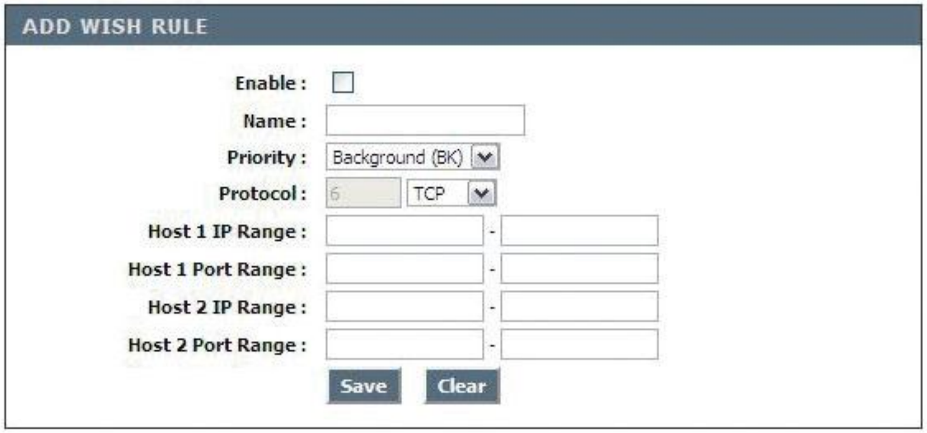
Host 2 IP Range : -

Host 2 Port Range : -



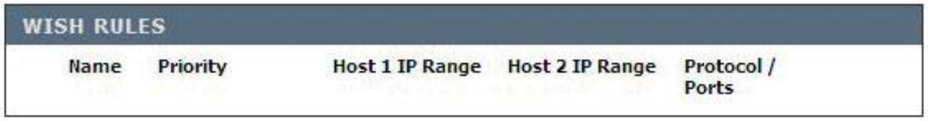
WISH RULES

Name	Priority	Host 1 IP Range	Host 2 IP Range	Protocol / Ports



ADD WISH RULE

Enable :	□
Name :	
Priority :	Background (BK)
Protocol :	6 TCP
Host 1 IP Range :	-
Host 1 Port Range :	-
Host 2 IP Range :	-
Host 2 Port Range :	-



WISH RULES

Name	Priority	Host 1 IP Range	Host 2 IP Range	Protocol / Ports

Priority. The priority of the message flow is entered here. Four priorities are defined:

- BK: Background (least urgent).
- BE: Best Effort.
- VI: Video.
- VO: Voice (most urgent).

Protocol. The protocol used by the messages.

Host 1 IP Range. The rule applies to a flow of messages for which one computer's IP address falls within the range set here.

Host 1 Port Range. The rule applies to a flow of messages for which Host 1's port number is within the range set here.

Host 2 IP Range. The rule applies to a flow of messages for which the other computer's IP address falls within the range set here.

Host 2 Port Range. The rule applies to a flow of messages for which Host 2's port number is within the range set here.

Save/Update. Record the changes you have made.

Clear. Re-initialize this area of the screen, discarding any changes you have made. When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

5.15.4 WISH Rules

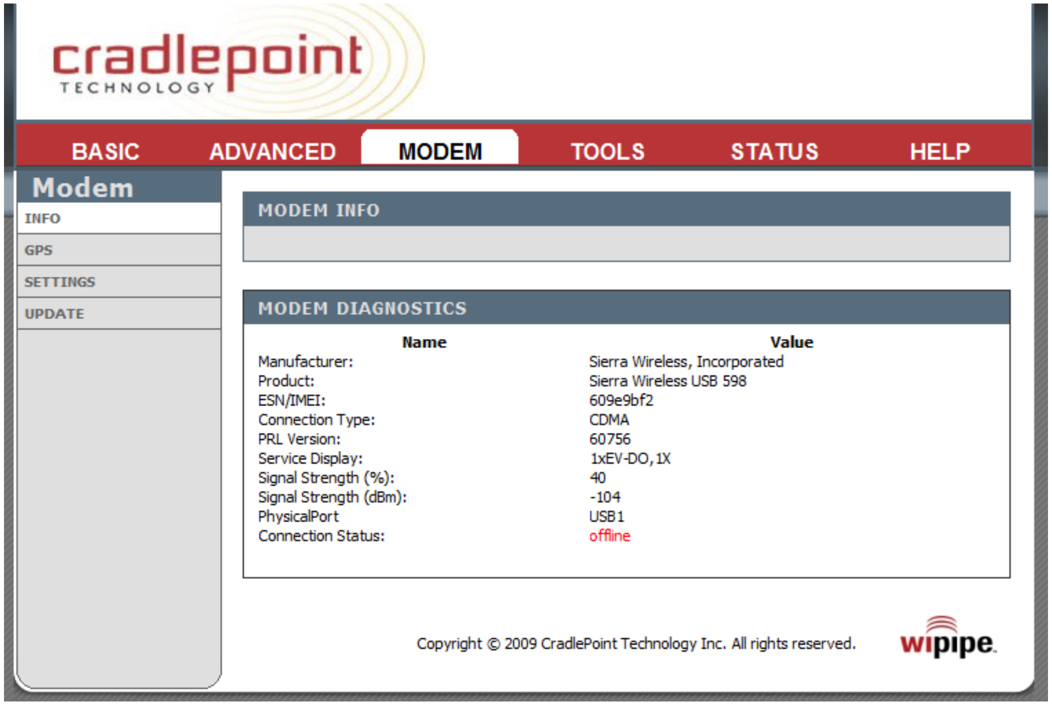
This section lists the WISH rules. Click the **Enable** check box at the left to directly activate or de-activate the entry. An entry can be changed by clicking the **Edit** icon or can be deleted by clicking the **Delete** icon. When you click the **Edit** icon, the item is highlighted, and the WISH Rules section is activated for editing.

After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with all configuration settings, click the **Reboot the Device** button.

6 MODEM TAB

The Modem Tab provides access to 4 sub-menus for displaying information and controlling settings for any attached phones or modems.

- Info
- GPS
- Settings
- Update



MODEM INFO

MODEM DIAGNOSTICS

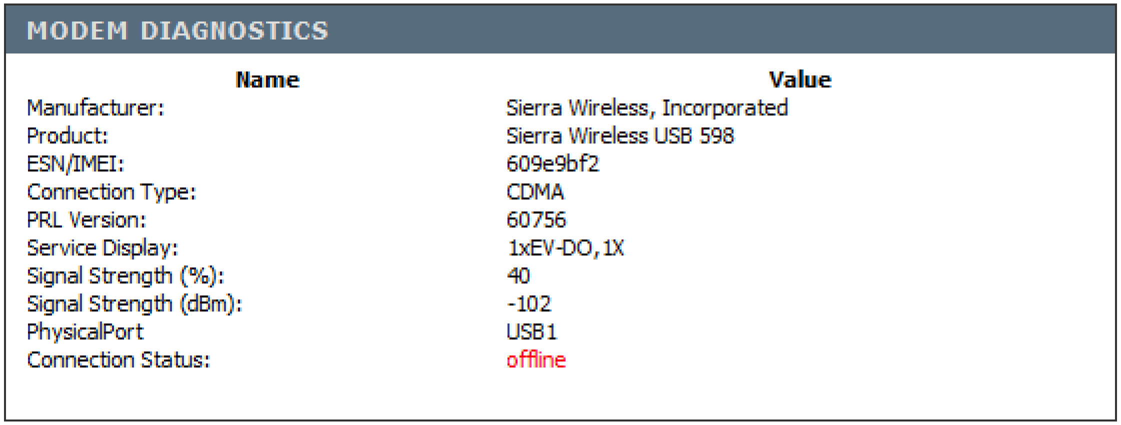
Name	Value
Manufacturer:	Sierra Wireless, Incorporated
Product:	Sierra Wireless USB 598
ESN/IMEI:	609e9bf2
Connection Type:	CDMA
PRL Version:	60756
Service Display:	1xEV-DO, 1X
Signal Strength (%):	40
Signal Strength (dBm):	-104
PhysicalPort	USB1
Connection Status:	offline

Copyright © 2009 CradlePoint Technology Inc. All rights reserved.

6.1 Info

This page displays information about any attached phones or modems. The amount of information displayed depends on the particular phone/modem, but generally from a dozen to two dozen values are displayed. To understand what particular values such as "Home Address" or "Network Access Identifier" mean, please review information provided by your carrier. Of particular interest are the Signal Strength readings, these let you know the quality of the attached phone/modem connection to your carrier. You may be able to move the location of the router or modem to increase your Signal Strength. Please note that if any of the values are displayed in red, you will need to correct the condition before you can access the WAN link across that phone/modem.

If your phone/modem does not support reading diagnostics such as Signal Strength while it is connected to the carrier's network, a "Refresh" button will show up on the page. If you press this button, any current data connection will be terminated, new readings will be presented, and a new data connection will be made. This is equivalent to pressing the router's external Signal Strength (SGNL) button. Again, note that the data connection will be lost and any attached devices will be momentarily interrupted if they are accessing the WAN using the phone/modem.



MODEM DIAGNOSTICS

Name	Value
Manufacturer:	Sierra Wireless, Incorporated
Product:	Sierra Wireless USB 598
ESN/IMEI:	609e9bf2
Connection Type:	CDMA
PRL Version:	60756
Service Display:	1xEV-DO,1X
Signal Strength (%):	40
Signal Strength (dBm):	-102
PhysicalPort	USB1
Connection Status:	offline

6.2 GPS

Some modems and handsets export GPS data. The router can display the GPS data directly, load the GPS data into an online mapping service and export the GPS data over the network in real time. Use the **Modem → GPS** page to adjust how your router displays and exports GPS data from supported devices.

6.2.1 Last Known Position

This section displays the latest update of GPS data the page has received. The best way to get an accurate GPS reading from the router is to use the GPS Network Access feature.

6.2.2 Data Update Settings

Update Method determines how the web page's GPS data is updated from the router.

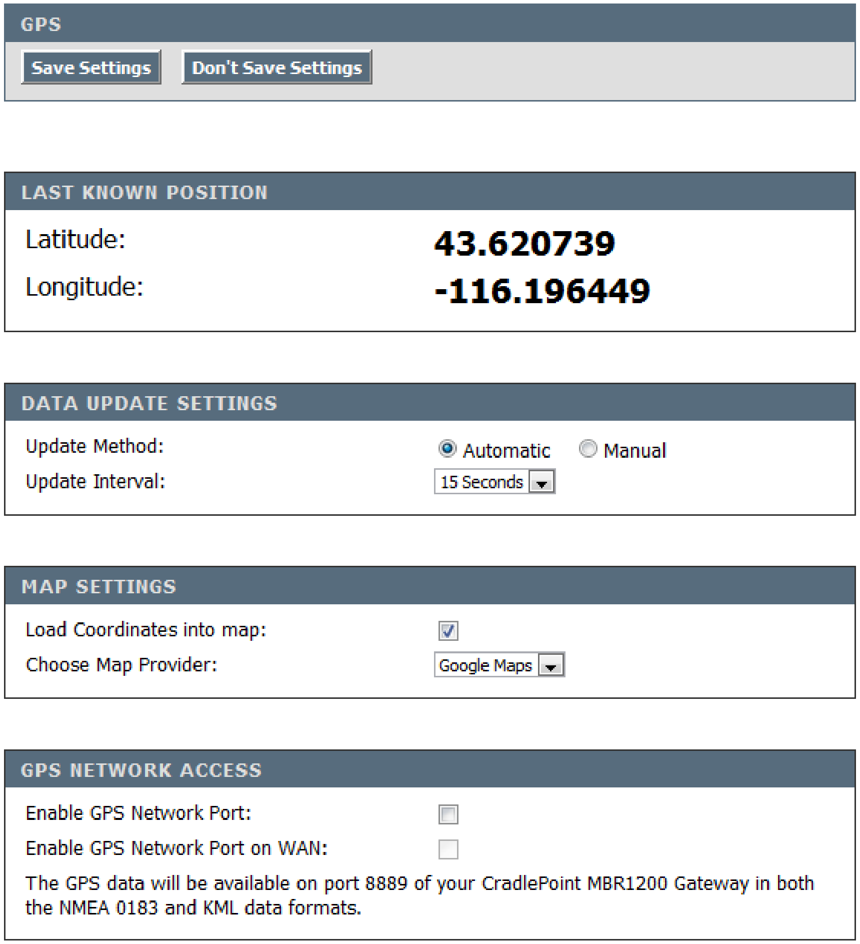
Automatic. When chosen the page will update itself at a specified interval.

Update Interval. (Default: every 15 seconds). Changed by using the **Update Interval** drop down box that is displayed when the Automatic update method is chosen.

Manual. You must tell the page to update itself. When the Manual method is chosen a button titled **Update** will be displayed. When the Update button is pushed the page will update its GPS data.

These selections can be saved by clicking the **Save Settings** button at the top of the page.

(continued)



LAST KNOWN POSITION

Latitude:	43.620739
Longitude:	-116.196449

DATA UPDATE SETTINGS

Update Method:	● Automatic ○ Manual
Update Interval:	15 Seconds

MAP SETTINGS

Load Coordinates into map:	☑
Choose Map Provider:	Google Maps

GPS NETWORK ACCESS

Enable GPS Network Port:	□
Enable GPS Network Port on WAN:	□

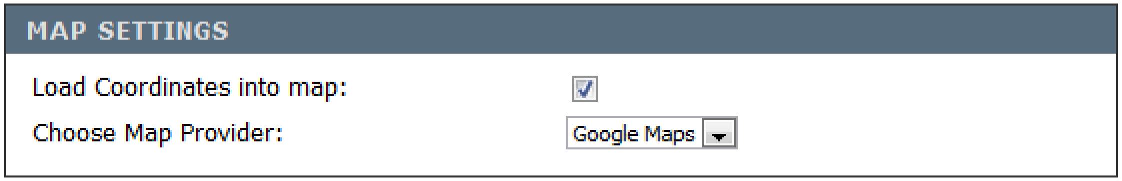
The GPS data will be available on port 8889 of your CradlePoint MBR1200 Gateway in both the NMEA 0183 and KML data formats.

6.2.3 Map Settings

Load Coordinates into map. (Default: enabled). GPS page reads valid GPS coordinates from the router and displays the location using an online mapping service in a separate browser window.

Choose Map Provider. Drop down enables you to choose which online mapping service you have the GPS coordinates sent to.

These selections can be saved by clicking the Save **Settings** button at the top of the page.



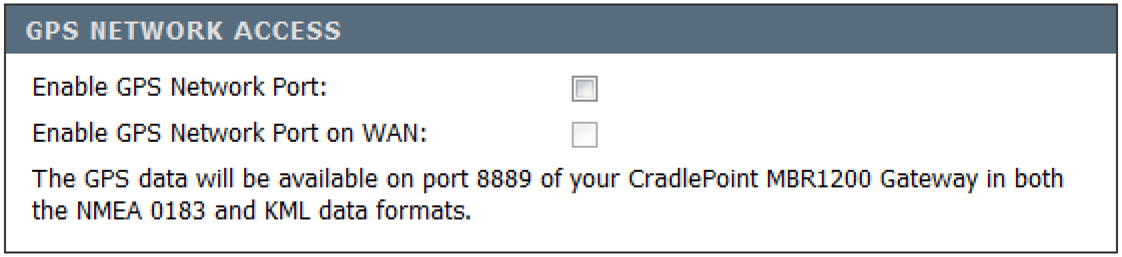
MAP SETTINGS

Load Coordinates into map: ☑

Choose Map Provider: Google Maps

6.2.4 GPS Network Access

Enable GPS Network Port. (Default: disabled). When checked the router makes live GPS data available over the local/wireless network. The GPS data can be read from port 8889 of the router when this option is enabled.



GPS NETWORK ACCESS

Enable GPS Network Port: □

Enable GPS Network Port on WAN: □

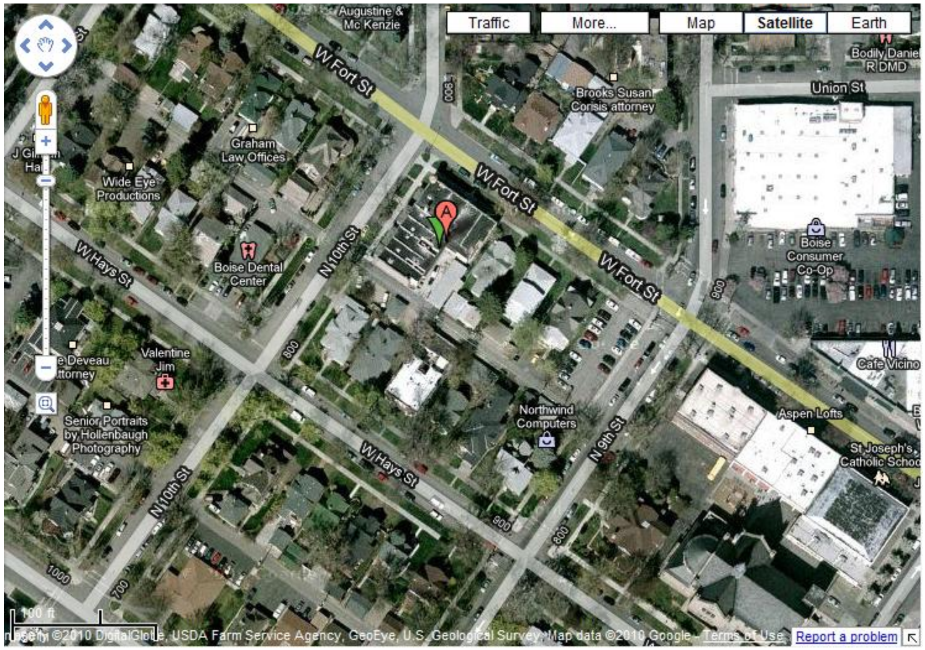
The GPS data will be available on port 8889 of your CradlePoint MBR1200 Gateway in both the NMEA 0183 and KML data formats.

Note: You may need to enable pop ups in your browser to view the map as it updates.

Enable GPS Network Port on WAN. (Default: disabled). When checked the router makes live GPS data available to the WAN.

GPS data is presented in both NMEA 0183 sentences and Keyhole Markup Language (KML) formatted data. To get NMEA data into a GPS aware application you may need an extra piece of software that can bridge the network NMEA data into a virtual serial port that the GPS application connects to. HTTP requests to the GPS port will return data formatted in KML for use in KML enabled GPS applications. Both NMEA and KML data can be requested simultaneously by multiple users.

This selection is saved by clicking the **Save Settings** button at the top of the page. After saving this option you must reboot the router for the change to have effect.



6.3 Settings

Advanced modem settings is a method for customizing a limited set of modem settings. Currently, this includes controlling the AT dial commands and entering a modem password if required by the device.

6.3.1 Global Mode Settings

This section allows for customization of Global Modem Settings.

Reconnect Mode. Typically modem connections are not always on. The CradlePoint router allows you to set the reconnection mode. The settings are:

- **Always on.** A connection to the Internet is always maintained.
- **On demand.** A connection to the Internet is made as needed.
- **Manual.** You have to open up the Web-based management interface and click the Connect button manually any time that you wish to connect to the Internet.

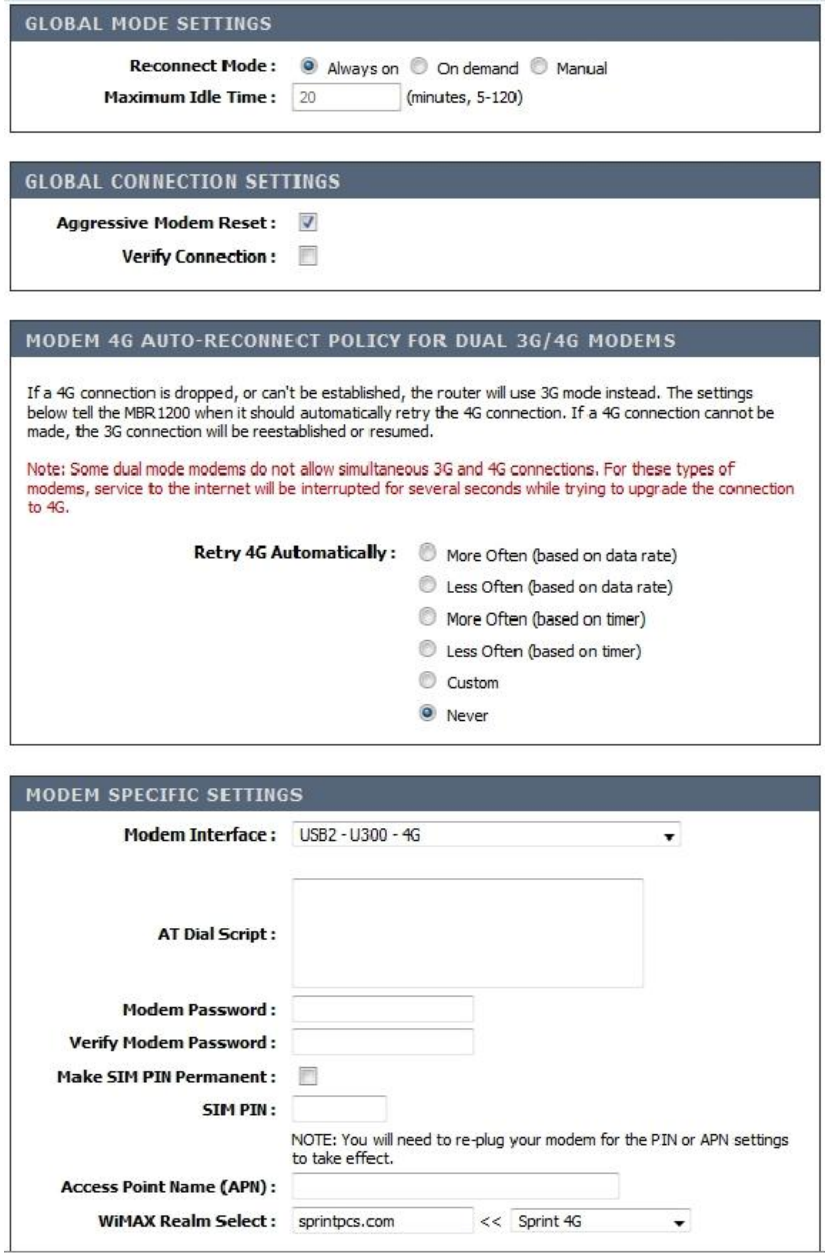
Maximum Idle Time. Time interval (in minutes) the machine can be idle before the modem connection is disconnected. The Maximum Idle Time value is only used for the **On demand** and **Manual** reconnect modes.

6.3.2 Global Connection Settings

This section is for changing the connection settings for any modem plugged into the router.

Aggressive Modem Reset. Some modems tend to become unresponsive or unable to maintain a connection for a long period of time. This setting uses more aggressive techniques to get the modem to reset and reconnect.

(continued)



GLOBAL MODE SETTINGS

Reconnect Mode : ● Always on ○ On demand ○ Manual

Maximum Idle Time : 20 (minutes, 5-120)

GLOBAL CONNECTION SETTINGS

Aggressive Modem Reset : ☑

Verify Connection : □

MODEM 4G AUTO-RECONNECT POLICY FOR DUAL 3G/4G MODEMS

If a 4G connection is dropped, or can't be established, the router will use 3G mode instead. The settings below tell the MBR1200 when it should automatically retry the 4G connection. If a 4G connection cannot be made, the 3G connection will be reestablished or resumed.

Note: Some dual mode modems do not allow simultaneous 3G and 4G connections. For these types of modems, service to the internet will be interrupted for several seconds while trying to upgrade the connection to 4G.

Retry 4G Automatically :
○ More Often (based on data rate)
○ Less Often (based on data rate)
○ More Often (based on timer)
○ Less Often (based on timer)
○ Custom
● Never

MODEM SPECIFIC SETTINGS

Modem Interface : USB2 - U300 - 4G

AT Dial Script :

Modem Password :

Verify Modem Password :

Make SIM PIN Permanent : □

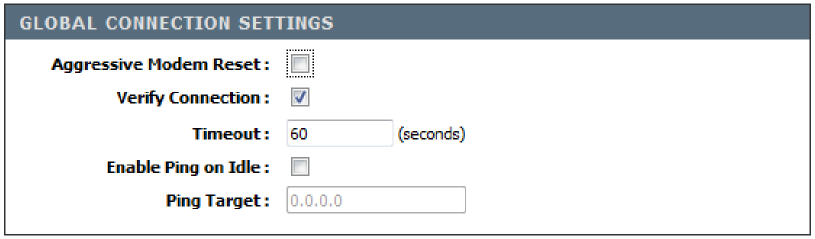
SIM PIN :

NOTE: You will need to re-plug your modem for the PIN or APN settings to take effect.

Access Point Name (APN) :

WiMAX Realm Select : sprintpcs.com << Sprint 4G

MODEM



GLOBAL CONNECTION SETTINGS

Aggressive Modem Reset :	□
Verify Connection :	☑
Timeout :	60 (seconds)
Enable Ping on Idle :	□
Ping Target :	0.0.0.0

Verify Connection. This setting causes the router to periodically verify that the modem connection to the Internet is still active. Due to the nature of cellular networks, there are times the modem will report it is still active but data will not be able to flow across the connection. This setting enables the router to detect this condition (either actively or passively) and restart the connection if there is a problem.

Timeout. This is how often the router will check to see if the modem connection is still active. It does this by seeing if any new data was received over the connection during the previous Timeout seconds. This is the passive mode of connection verification.

Enable Ping on Idle. This setting configures the router to send a ping packet when no data was received during the previous timeout period. If the connection is still active, a response should be received. This is the active mode of connection verification.

Ping Target. This setting controls which IP address will be pinged.

6.3.3 Modem 4G Auto-Reconnect Policy for DUAL 3G/4G Modems

If a 4G connection is dropped, or can't be established, the router will use 3G mode instead. The settings tell the MBR1200 when it should automatically retry the 4G connection. If a 4G connection cannot be made, the 3G connection will be reestablished or resumed.

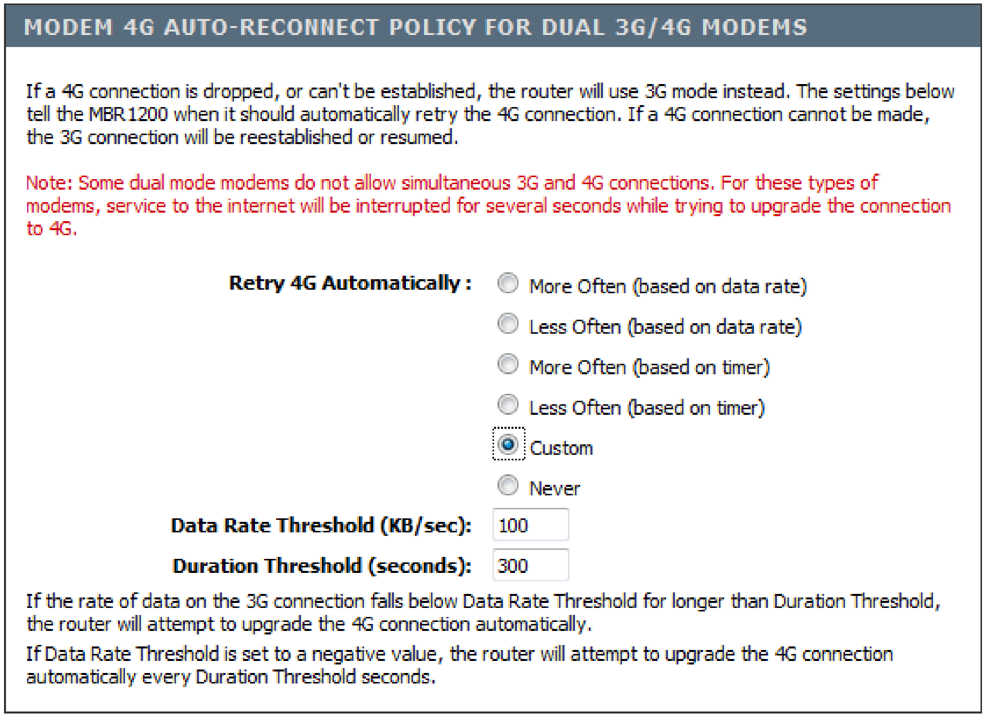
Retry 4G Automatically.

- More Often (based on data rate)
- Less Often (based on data rate)
- More Often (based on timer)
- Less Often (based on timer)
- Never (Default)
- Custom

Data Rate Threshold (KB/Sec). Select Data Rate Threshold.

Duration Threshold (seconds). Select Duration Threshold.

If the rate of data on the 3G connection falls below **Data Rate Threshold** for longer than the **Duration Threshold**, the router will attempt to upgrade the 4G connection automatically.



MODEM 4G AUTO-RECONNECT POLICY FOR DUAL 3G/4G MODEMS

If a 4G connection is dropped, or can't be established, the router will use 3G mode instead. The settings below tell the MBR1200 when it should automatically retry the 4G connection. If a 4G connection cannot be made, the 3G connection will be reestablished or resumed.

Note: Some dual mode modems do not allow simultaneous 3G and 4G connections. For these types of modems, service to the internet will be interrupted for several seconds while trying to upgrade the connection to 4G.

Retry 4G Automatically : ○ More Often (based on data rate)
○ Less Often (based on data rate)
○ More Often (based on timer)
○ Less Often (based on timer)
● Custom
○ Never

Data Rate Threshold (KB/sec): 100

Duration Threshold (seconds): 300

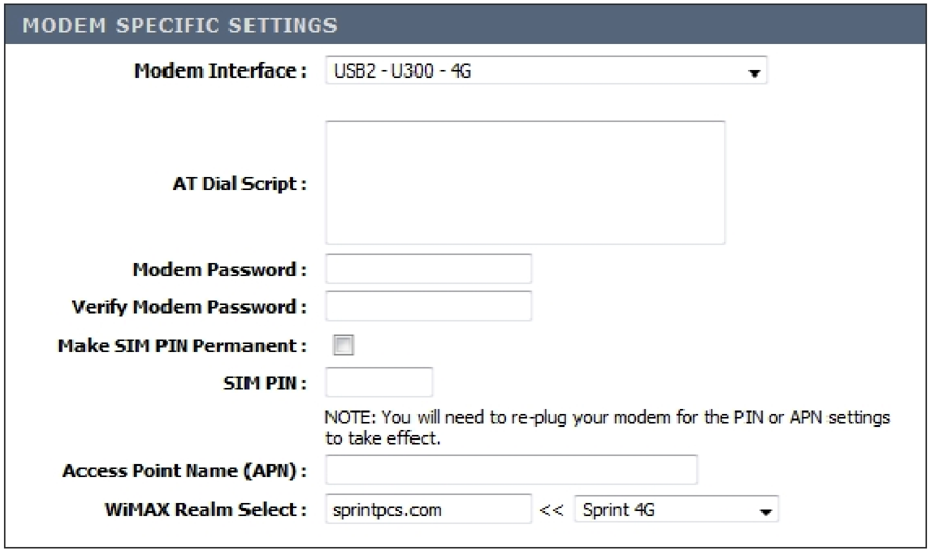
If the rate of data on the 3G connection falls below Data Rate Threshold for longer than Duration Threshold, the router will attempt to upgrade the 4G connection automatically.

If Data Rate Threshold is set to a negative value, the router will attempt to upgrade the 4G connection automatically every Duration Threshold seconds.

If the **Data Rate Threshold** is set to a negative value, the router will attempt to upgrade the 4G connection automatically every **Duration Threshold Seconds**.

NOTE: Some dual mode modems do not allow simultaneous 3G and 4G connections. For these types of modems, service to the internet will be interrupted for several seconds while trying to upgrade the connection to 4G.

6.3.4 Modem Specific Settings



MODEM SPECIFIC SETTINGS

Modem Interface : USB2 - U300 - 4G

AT Dial Script :

Modem Password :

Verify Modem Password :

Make SIM PIN Permanent : □

SIM PIN :

NOTE: You will need to re-plug your modem for the PIN or APN settings to take effect.

Access Point Name (APN) :

WiMAX Realm Select : sprintpcs.com << Sprint 4G

This section allows customization of the AT dial commands

Modem Interface. Use the drop down menu to specify which modem interface you want to adjust settings for (i.e., **USB1**, **USB2**, **USB3**, **Cardbus**, **ExpressCard**).

AT Dial Script. 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

AT+CGDCONT=2,"IP","isp.cingular"

ATDT*99***2#

Modem Password. Enter the modem password, if required

Verify Modem Password. Enter the modem password again to ensure it was entered correctly.

Disable Automatic Dialing. If you check this box then a modem won't dial unless you start it manually. Otherwise a modem will dial automatically (if it is the highest priority available device).

Make SIM PIN Permanent. If **Make SIM PIN Permanent** is selected the entered PIN will be remembered between reboots. If a modem is plugged in when this is selected the router will make a permanent association between the PIN and the current modem. When a PIN is associated with a modem the PIN will be automatically entered for you when the associated modem is plugged in. If you choose Permanent PIN but there is no modem plugged in at the time then no modem is associated with any PIN. The next time a modem is plugged in and a valid PIN is entered for the modem the router will remember that association.

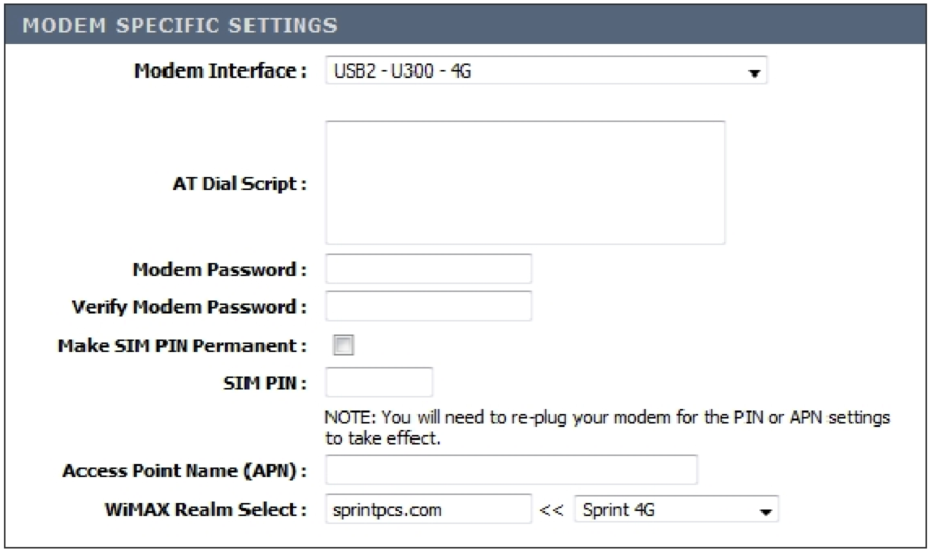
SIM PIN. Enter your **PIN number** here. If Permanent PIN is not selected, this PIN number will be used with any modem plugged in until the router is rebooted.

Access Point Name (APN). Some wireless carriers provide multiple Access Point Names that a modem can connect to. If you wish to specify an APN, enter it into this field. Some examples of APN are **isp.cingular**, **ecp.tmobile.com** and **vpn.com**. This APN will be set in the first profile position (see **Modem Diagnostics**). The modem must be removed and reinserted for this change to take affect (or the router rebooted). This APN is associated with the modem in the interface referred to in the **Modem Interface** drop down menu, so multiple APNs may be entered.

(continued)

Band Select. This function is currently supported only on Sierra Wireless modems. It allows you to select specific frequency bands to use, either GSM (2.5G network) or WCDMA (3G network) settings, or the use of "Autoband", which is automatic band selection. Depending on your location, different network selections will be shown based on the bands the particular modem supports and the router recognizes. If you select one of the WCDMA settings such as "WCDMA/GSM NA (North America)", the modem will use the 3G network in preference to the 2.5G network. *This change is persistent and stays with the modem, even if you unplug it and move it to a PC.* The band currently selected by the modem will be marked with an asterisk (*) in the drop-down list.

WiMAX Realm Select. If you are using a 4G modem you must select the WiMAX realm. This allows you to connect to your carrier: ie. Sprint.

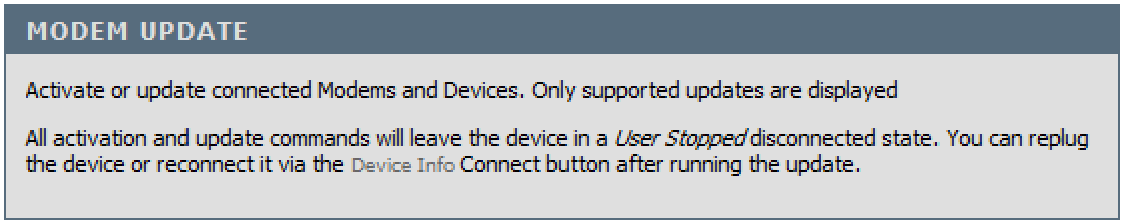


MODEM SPECIFIC SETTINGS

Modem Interface :	USB2 - U300 - 4G
AT Dial Script :	
Modem Password :	
Verify Modem Password :	
Make SIM PIN Permanent :	□
SIM PIN :	
	NOTE: You will need to re-plug your modem for the PIN or APN settings to take effect.
Access Point Name (APN) :	
WiMAX Realm Select :	sprintpcs.com << Sprint 4G

6.4 Update

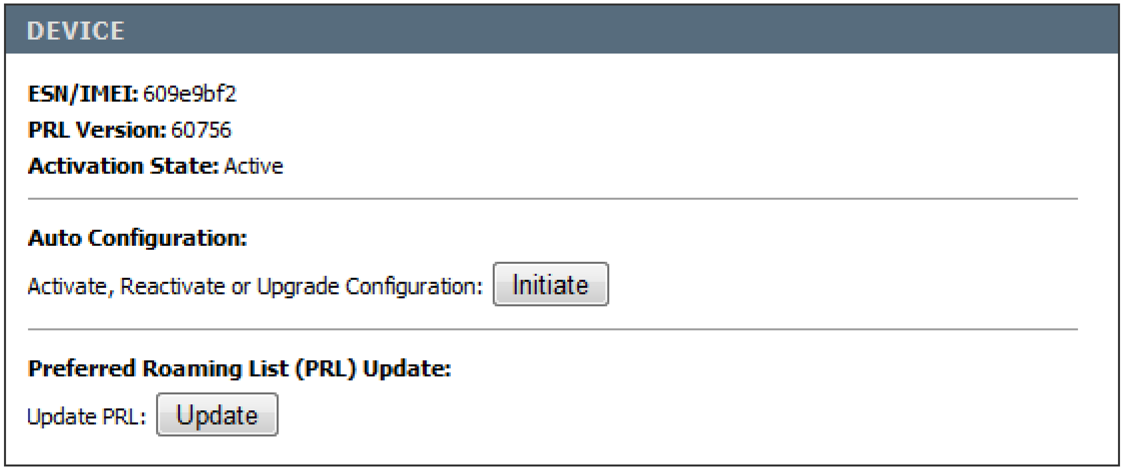
Some modems can be activated and updated while plugged into the router. Activation and updates vary by modem model and service provider. All supported methods are displayed. If no methods are displayed for your device you will need to activate and update your device externally.



MODEM UPDATE

Activate or update connected Modems and Devices. Only supported updates are displayed

All activation and update commands will leave the device in a *User Stopped* disconnected state. You can replug the device or reconnect it via the Device Info Connect button after running the update.



DEVICE

ESN/IMEI: 609e9bf2

PRL Version: 60756

Activation State: Active

Auto Configuration:

Activate, Reactivate or Upgrade Configuration: Initiate

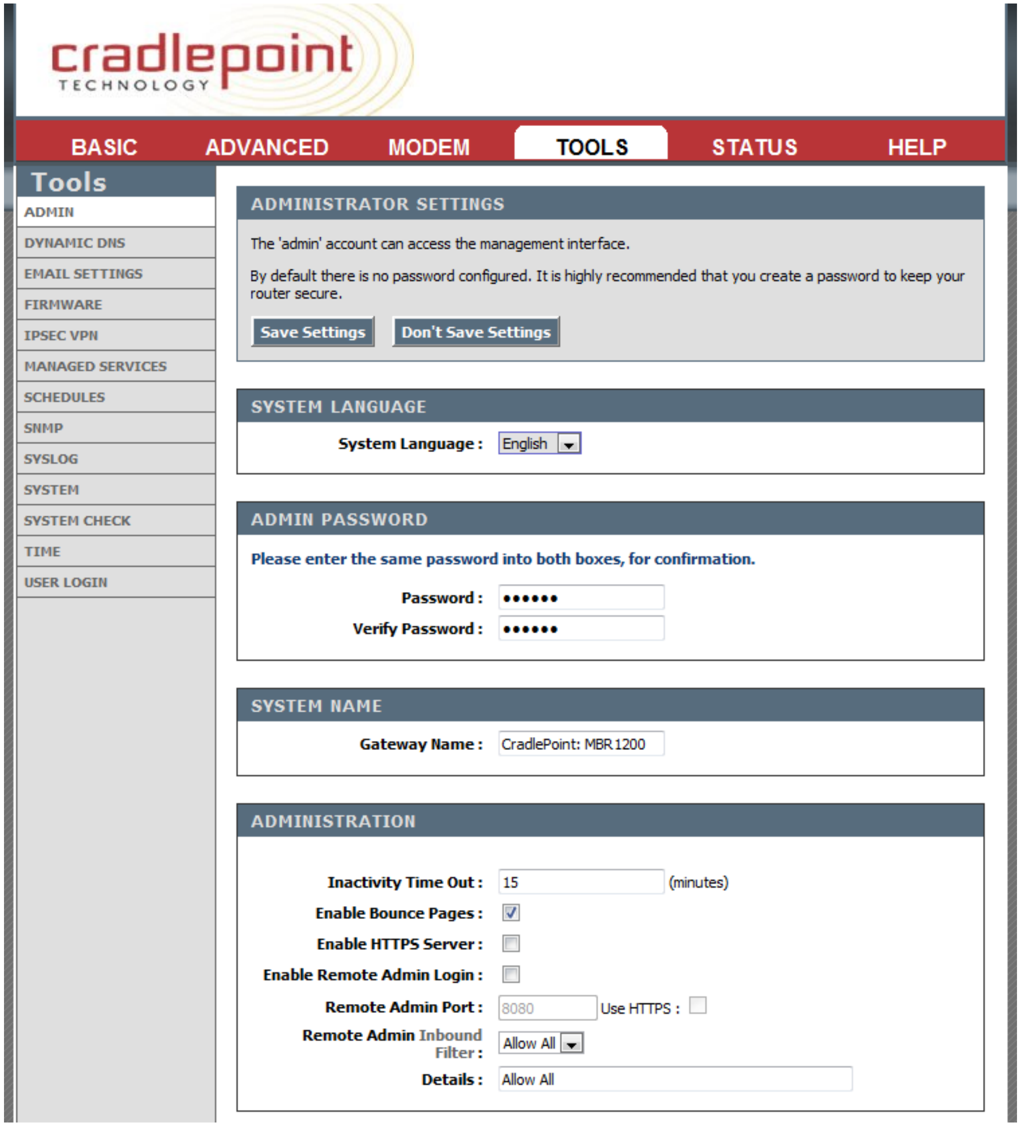
Preferred Roaming List (PRL) Update:

Update PRL: Update

7 TOOLS TAB

The Advanced tab provides access to 13 sub-menus for administering advanced functions/tasks important in enterprises and larger organizations. Specifically, for IT organizations that use a number of MBR1200 units to provide wireless data connectivity for employees, the Tools tab allows you to enable the remote devices to be an extension of your network, and abide by the policies set within your department. Included are a number of features that allow the unit to provide security, supportability, and EVDO handset behavior regardless where a remote employee is located.

- Admin
- Dynamic DNS
- Email Settings
- Firmware
- IPSec VPN
- Managed Services
- Schedules
- SNMP
- SysLog
- System
- System Check
- Time
- User Log



ADMINISTRATOR SETTINGS

The 'admin' account can access the management interface.

By default there is no password configured. It is highly recommended that you create a password to keep your router secure.

SYSTEM LANGUAGE

System Language : English

ADMIN PASSWORD

Please enter the same password into both boxes, for confirmation.

Password : ••••••

Verify Password : ••••••

SYSTEM NAME

Gateway Name : CradlePoint: MBR1200

ADMINISTRATION

Inactivity Time Out : 15 (minutes)

Enable Bounce Pages : ☑

Enable HTTPS Server : □

Enable Remote Admin Login : □

Remote Admin Port : 8080 Use HTTPS : □

Remote Admin Inbound Filter : Allow All

Details : Allow All

7.1 Admin (Administrative Settings).

Use the Admin sub-menu to set a password for access to the Web-based management. The default Admin and Internet Access (User) passwords are the last six characters of the MAC address (NOTE: all letters in the MAC address should be entered as lower case). This screen may also be used by the individual who first activates the unit.

7.1.1 System Language

System Language. Select **English** or **Spanish**.

7.1.2 Admin Password

Password. Type password in this field that you want to use to grant access to Web based management interface. Default: Last 6 characters of the MBR1200's MAC address.

NOTE: all letters in the MAC address should be entered as lower case.

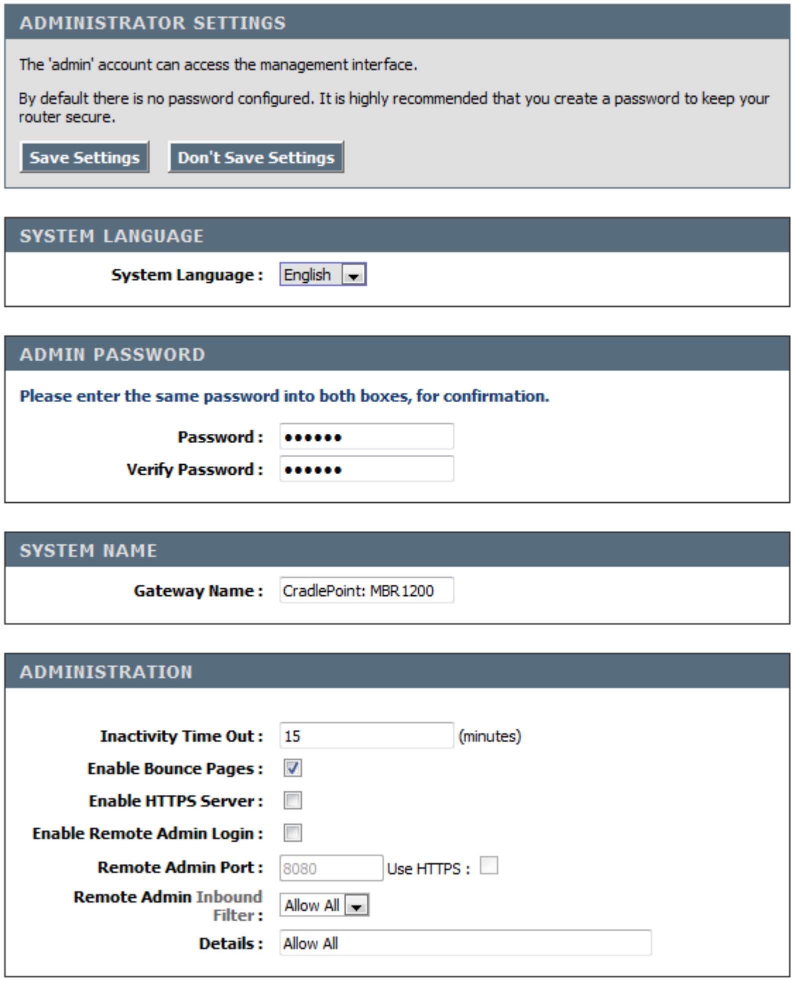
Verify Password. Re-type the password to ensure it was entered correctly.

7.1.3 System Name

Gateway Name. The name of the router can be changed here. Default (CradlePoint: MBR1200).

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

(continued)



ADMINISTRATOR SETTINGS

The 'admin' account can access the management interface.

By default there is no password configured. It is highly recommended that you create a password to keep your router secure.

SYSTEM LANGUAGE

System Language : English

ADMIN PASSWORD

Please enter the same password into both boxes, for confirmation.

Password : ••••••

Verify Password : ••••••

SYSTEM NAME

Gateway Name : CradlePoint: MBR1200

ADMINISTRATION

Inactivity Time Out : 15 (minutes)

Enable Bounce Pages : ☑

Enable HTTPS Server : □

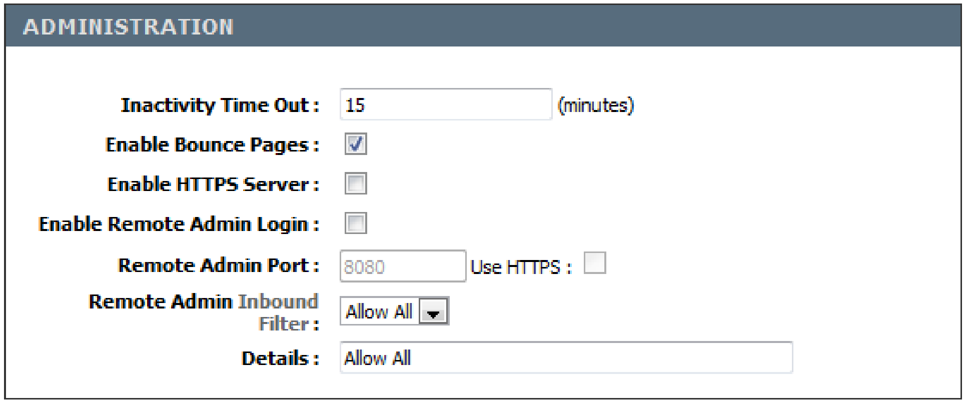
Enable Remote Admin Login : □

Remote Admin Port : 8080 Use HTTPS : □

Remote Admin Inbound Filter : Allow All

Details : Allow All

7.1.4 Administration



ADMINISTRATION

Inactivity Time Out :	15 (minutes)
Enable Bounce Pages :	☑
Enable HTTPS Server :	□
Enable Remote Admin Login :	□
Remote Admin Port :	8080 Use HTTPS : □
Remote Admin Inbound Filter :	Allow All
Details :	Allow All

Inactivity Time Out. If the router does not detect any administrative activity (from WAN or LAN) during this number of minutes, it logs the administrator off.

Enable Bounce Pages. Enabling this option allows users of wireless devices attempting to connect to the MBR1200 to see bounce pages that display error message pages. For example, users would see a “phone or modem not connected” page, a “require user login” page or other error pages.

NOTE: To avoid issues with some applications, you may have to leave this check box unselected.

Enable HTTPS Server. Enabling this option makes it possible to perform management with the Secure HTTP (HTTPS) protocol.

Enable Remote Management. Enabling this allows you to manage the router from anywhere with an Internet connection. Disabling Remote Admin Login allows you to manage the router only from computers on your LAN. Default: off.

Remote Admin Port. The port that will be accessed from the Internet. This allows you to make modifications to ensure that there is no conflict with other enterprise software. Default: Port 8080. For example, if you specify port 1080 here, then, to access the router from the Internet, you would use a URL of the form: **http://my.domain.com:1080/**.

Use HTTPS. Setting this option requires all remote administration to use the Secure HTTP (HTTPS) protocol. For example, if you specify port 1080 above, then, to access the router from the Internet, you would use a URL of the form: **https://my.domain.com:1080/**.

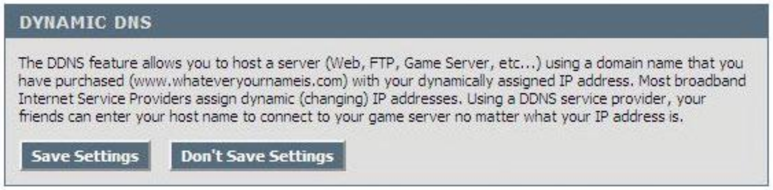
Remote Inbound Filter. Select a filter that controls access as needed for this admin port. If you do not see the filter you need in the list of filters, go to the **Advanced → Inbound Filter** sub-menu and create a new filter.

Details. The text field description of the inbound filter you want to select. When you populate a new inbound filter rule, you attribute to it a descriptor, which is what is shown here.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

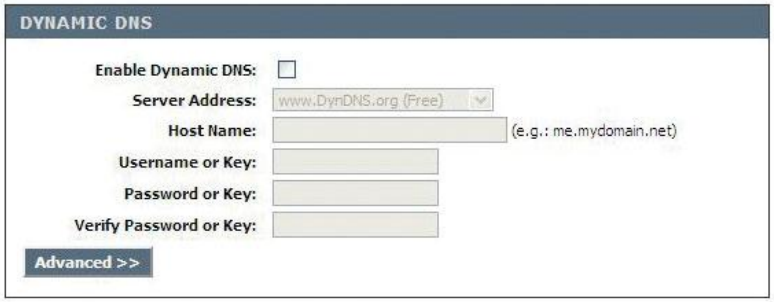
7.2 Dynamic DNS

Use the Dynamic DNS feature sub-menu to host a server (Web, FTP, Game Server, etc.) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a Dynamic DNS service provider, the router can be addressed by Host Name, regardless of the assigned IP address.



DYNAMIC DNS

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.



DYNAMIC DNS

Enable Dynamic DNS:	□
Server Address:	www.DynDNS.org (Free)
Host Name:	(e.g.: me.mydomain.net)
Username or Key:	
Password or Key:	
Verify Password or Key:	

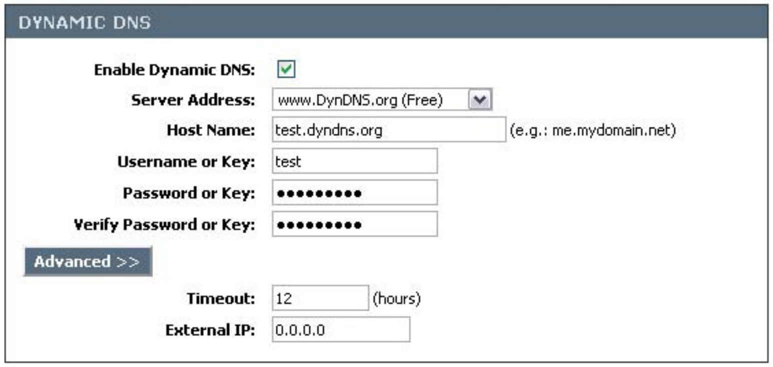
7.2.1 Dynamic DNS

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

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

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

Host Name. Enter the host name, fully qualified; for example: **myhost.mydomain.net**.



DYNAMIC DNS

Enable Dynamic DNS:	☑
Server Address:	www.DynDNS.org (Free)
Host Name:	test.dyndns.org (e.g.: me.mydomain.net)
Username or Key:	test
Password or Key:	•••••••••
Verify Password or Key:	•••••••••
Timeout:	12 (hours)
External IP:	0.0.0.0

Username or Key. Enter the username or key provided by the Dynamic DNS service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

Password or Key. Enter the password or key provided by the Dynamic DNS service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

Verify Password or Key. Re-type the password or key provided by the Dynamic DNS service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

Advanced. Click the **Advanced >>** button to access the following functions:

Timeout. The time between periodic updates to the Dynamic DNS, if the dynamic IP address has not change. The timeout period is entered in hours. NOTE: this option will automatically disable if Username and Password or keys are incorrect.

External IP. This allows you to specify the IP that should be sent to the DynDNS server, and a time frame in which it should time out and send the information again. Thus, if you pick a time out of 6 hours, the IP will send a new update every 6 hours. *(continued)*

NOTE. If a dynamic DNS update fails for any reason (for example, when incorrect parameters are entered), the router automatically disables the Dynamic DNS feature and records the failure in the log.

NOTE: After configuring the router for dynamic DNS, you can open a browser and navigate to the URL for your domain (for example **http://www.mydomain.info**) and the router will attempt to forward the request to port 80 on your LAN. If, however, you do this from a LAN-side computer and there is no virtual server defined for port 80, the router will return the router's configuration home page. Refer to the **Advanced → Virtual Server** configuration page to set up a virtual server.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

7.3 Email Settings

Use the Email sub-menu to send the system log files, router alert messages, and firmware update notification to your email account or any email account you specify.

7.3.1 Enable

Enable Email Notification. When this option is enabled, router activity logs are emailed to a designated email address.

7.3.2 Email Settings

From Email Address. This email address will appear as the sender when you receive a log file or firmware upgrade notification via email.

To Email Address. Enter the email address where you want the email sent.

SMTP Server Address. Enter the SMTP server address for sending email.

SMTP Server Port. Enter the SMTP server port for sending email.

Enable Authentication. If your SMTP server requires authentication, select this option.

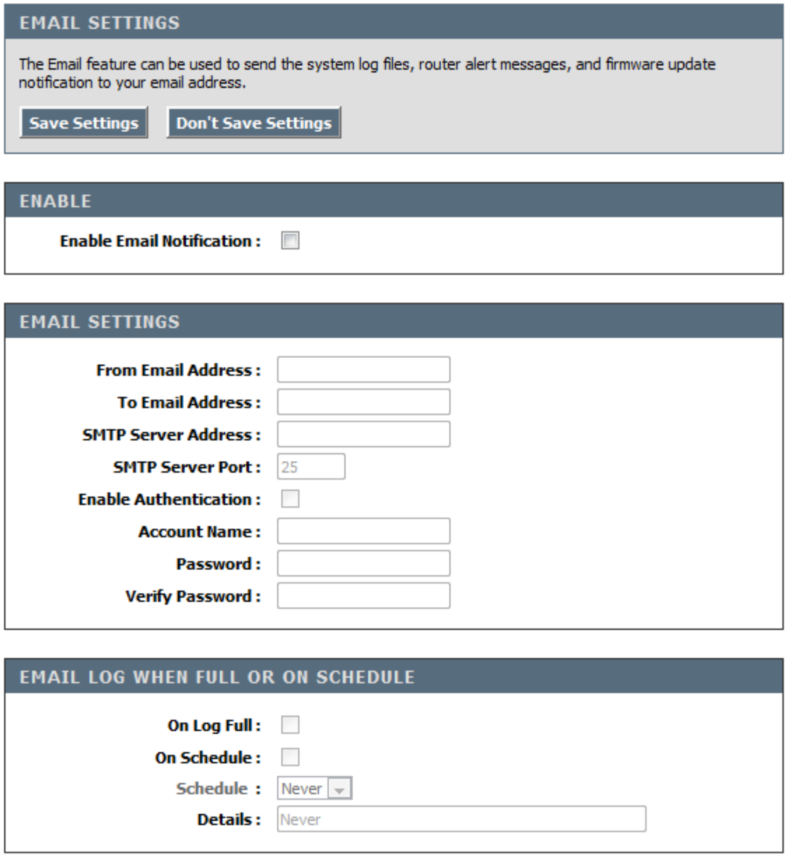
Account Name. Enter your account for sending email.

Password. Enter the password associated with the account.

Verify Password. Re-type the password associated with the account.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

(continued)



EMAIL SETTINGS

The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address.

ENABLE

Enable Email Notification : □

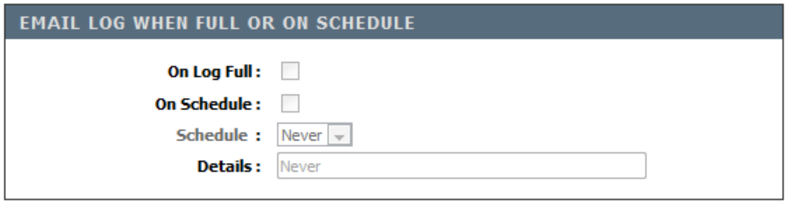
EMAIL SETTINGS

From Email Address :
To Email Address :
SMTP Server Address :
SMTP Server Port : 25
Enable Authentication : □
Account Name :
Password :
Verify Password :

EMAIL LOG WHEN FULL OR ON SCHEDULE

On Log Full : □
On Schedule : □
Schedule : Never
Details : Never

7.3.3 Email Log When Full or on Schedule



EMAIL LOG WHEN FULL OR ON SCHEDULE

On Log Full : □

On Schedule : □

Schedule : Never

Details : Never

On Log Full. When this option is selected, logs will be sent via email when the log is full.

On Schedule. Selecting this option will send the logs via email according to schedule.

Schedule. This option is enabled when On Schedule is selected. You can select a schedule from the list of defined schedules. To create a schedule, go to the **Tools → Schedules** sub-menu. NOTE: Normally email is sent at the start time defined for a schedule, and the schedule end time is not used. However, rebooting the router during the schedule period will cause additional emails to be sent.

Details. The text field description of the inbound filter you want to select. When you populate a new inbound filter rule, you attribute to it a descriptor, which is what is shown here.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

7.4 Firmware

Use the Firmware Upgrade sub-menu to update your router to the latest firmware to improve functionality and performance. To check for the latest firmware, click the **Check Online Now** button. If you would like to be notified when new firmware is released, place a check-mark in the box next to **Email Notification of Newer Firmware Version**. NOTE: You must enter a destination email address in the **Tools → E-mail** submenu in order to receive email notifications of firmware updates.

7.4.1 Firmware Information

This section displays the Current Firmware Version and the Latest Firmware Version. To check for the latest version, click the **Check Online Now for Latest Firmware Version** button. To verify the latest firmware version, the MBR1200 checks the Internet.

7.4.2 Manually Upgrade Firmware

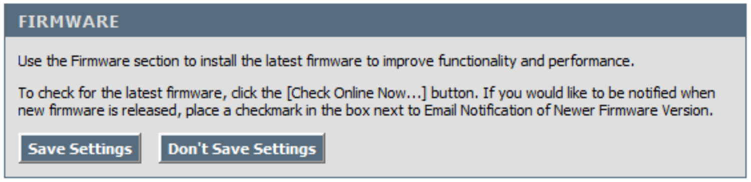
Upload Firmware. To update the firmware, follow these steps:

1. Click the **Browse** button to locate the update file on your computer.
2. Once you have found the file to be used, click the **Upload** button to start the firmware update process.
3. Wait for the router to reboot.
4. Confirm updated firmware revision on the **Status → Device Info** submenu.

7.4.3 Manually Upgrade WIMAX Modem Driver File

Upload WiMAX Modem Driver File. To update the driver follow these steps:

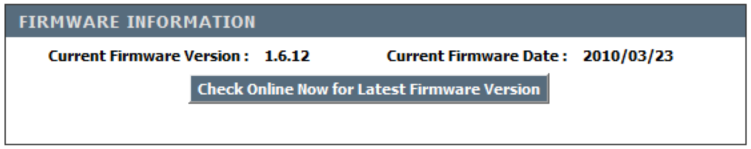
1. Click the **Browse** button to locate the update file on your computer.
2. Once you have found the file to be used, click the **Upload** button to start the driver update process.
3. Wait for the modem to reboot.
4. Confirm updated firmware revision on the **Tools → Firmware** submenu.



FIRMWARE

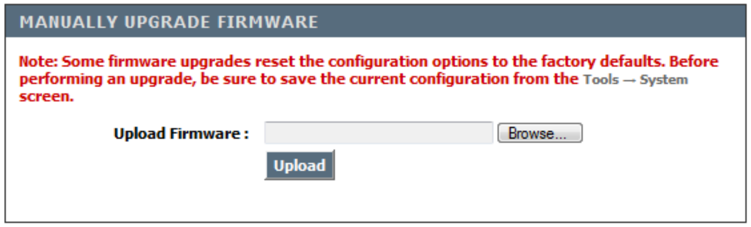
Use the Firmware section to install the latest firmware to improve functionality and performance.

To check for the latest firmware, click the [Check Online Now...] button. If you would like to be notified when new firmware is released, place a checkmark in the box next to Email Notification of Newer Firmware Version.



FIRMWARE INFORMATION

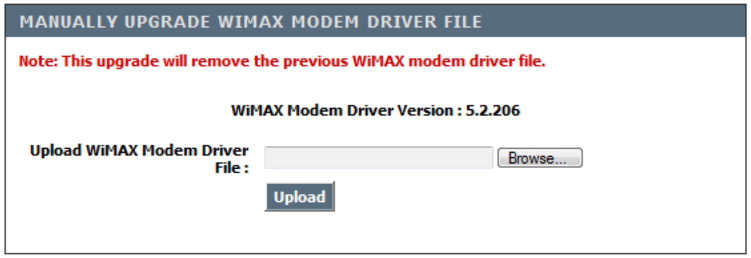
Current Firmware Version : 1.6.12 Current Firmware Date : 2010/03/23



MANUALLY UPGRADE FIRMWARE

Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the Tools → System screen.

Upload Firmware :

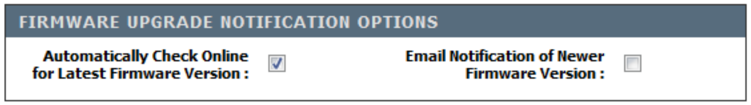


MANUALLY UPGRADE WIMAX MODEM DRIVER FILE

Note: This upgrade will remove the previous WiMAX modem driver file.

WiMAX Modem Driver Version : 5.2.206

Upload WiMAX Modem Driver File :



FIRMWARE UPGRADE NOTIFICATION OPTIONS

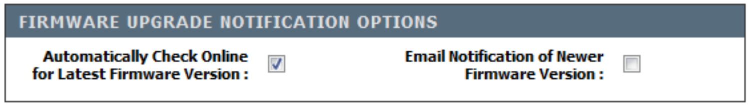
Automatically Check Online for Latest Firmware Version : ☑

Email Notification of Newer Firmware Version : □

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

(continued)

7.4.4 Firmware Upgrade Notification Options



FIRMWARE UPGRADE NOTIFICATION OPTIONS

Automatically Check Online for Latest Firmware Version :	☑	Email Notification of Newer Firmware Version :	□

Automatically Check Online for Latest Firmware Version. When this option is enabled, your router will check online periodically to see if there is a newer version of firmware available. When new firmware is available, you will see an additional button that initiates a one button update. Simply click the button to download and update the router in one click.

Email Notification of Newer Firmware Version. When a newer version of firmware is available, a notice will be set to the email address listed under the **Tools → Email** sub-menu.

7.4.5 Firmware Update Notes

When a new firmware update file is loaded into the router, the following checks are made to insure that the new file is correct.

1. Before the new firmware update is loaded into its permanent location (the NVRAM), it is first downloaded into a temporary (RAM) area for checking.
2. The downloaded file is first checked against a checksum to insure that the entire file has been downloaded and no data errors have occurred.
3. Each firmware file is encoded with a special product identification, which must match the current code in the router. If the two identifiers match the update is allowed to proceed. If either of these checks fail, the firmware update file is rejected and a failure message given to the user.
4. After the new firmware file passes both of these checks, the code is written to the permanent location (NVRAM). Power to the unit must be maintained during this critical step; do not turn off unit. As the router writes the new code into the permanent location (NVRAM), the user is presented with a screen on the browser which counts down for 60 seconds. After the 60-second countdown, the unit automatically reboots and reinitializes.

7.4.6 Firmware Update via the USB

The MBR1200 supports software upgrades via the USB port. A USB storage device (thumb drive) is preloaded with the new software .bin file.

Requirements:

- CradlePoint MBR1200 Binary firmware file (i.e. u_mbr1200_2010_03_23.bin) From: http://www.cradlepoint.com/support/mbr1200
- 4G Modem Binary firmware file (i.e. u_ modem _5_2_206.bin) From: http://www.cradlepoint.com/support/mbr1200
- CradlePoint MBR1200
- USB "Thumb drive" mass storage device formatted FAT or FAT32.

Router Firmware Update – USB Procedure:

- Remove the date code from the binary file. Example: u_mbr1200_2010_01_22.bin to **u_mbr1200.bin**.
- Copy the u_mbr1200.bin file to the USB Thumb Drive. This must be in the root not in a folder.
- Power on a MBR1200 and wait for the WLAN and POWER lights to go solid green.
- Plug-in the USB Thumb Drive into the USB port on the MBR1200
- The EC light will come on and blink while it is reading the binary file off the USB Thumb Drive
- When the EC light goes solid for 3 seconds or more, pull the USB thumb drive.
- At this point, the router will read the file, error check it and will load it. The router will reboot itself and will be running the new firmware

NOTE: If the file is corrupt, the MBR1200 will reboot and will not load the new firmware. It is recommend that when you are doing these en mass, the first few are manually checked by logging into the router with a computer and going to http://192.168.0.1, login with the default password, and then check the "Status" tab which will show the current router firmware version. The default password is the last 6 character of the MAC address, which is located on a sticker on the bottom.

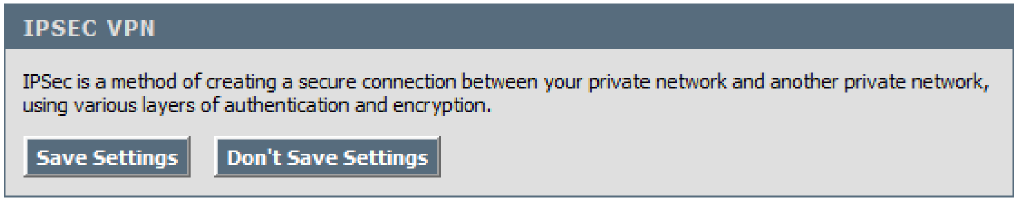
Modem File Update – USB Procedure:

- Remove the date code from the binary file. Example: u_modem_2009_11_16 to **u_ modem.bin**.
- Copy the u_modem.bin file to the USB Thumb Drive. This must be in the root not in a folder.
- Power on a MBR1200 and wait for the WLAN and POWER lights to go solid green.
- Plug-in the USB Thumb Drive into the USB port on the MBR1200
- The EC light will come on and blink while it is reading the binary file off the USB Thumb Drive
- When the EC light goes solid for 3 seconds or more, pull the USB thumb drive.
- At this point, the router will read the file, error check it and will load it. The router will reboot itself and will be running the new firmware

NOTE: If the file is corrupt, the MBR1200 will reboot and will not load the modem file. It is recommend that when you are doing these en mass, the first few are manually checked by logging into the router with a computer and going to http://192.168.0.1, login with the default password, and then check the "Status" tab which will show the current router firmware version. The default password is the last 6 character of the MAC address, which is located on a sticker on the bottom.

7.5 IPsec VPN

Use the IPsec sub-menus to set policies that are used to create a secure connection to a private network or allow others to connect in a very secure way.



IPSEC VPN

IPSec is a method of creating a secure connection between your private network and another private network, using various layers of authentication and encryption.

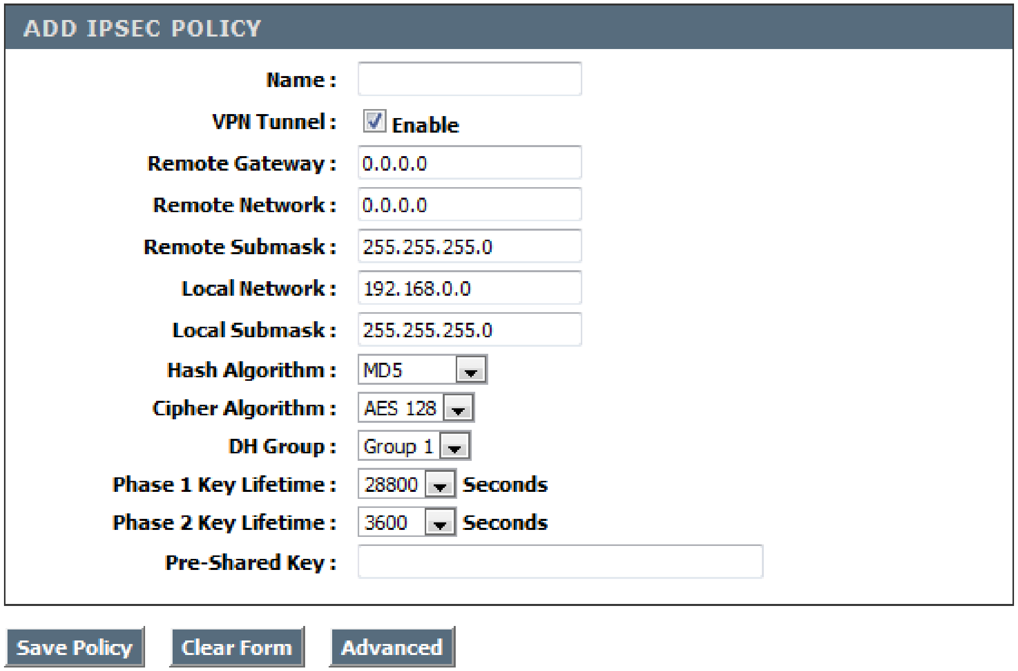
7.5.1 Add IPsec Policy

In this section you can add and edit IPSec policies to connect via private networks. Please note that the policies must match between routers when creating a connection. In other words, while the names of the policies can be different, the Hash, Cipher, Group, Timeouts, Pre-shared keys, or manual settings must correspond for a successful connection.

Name. Add a name to identify the polity and distinguish one policy from another.

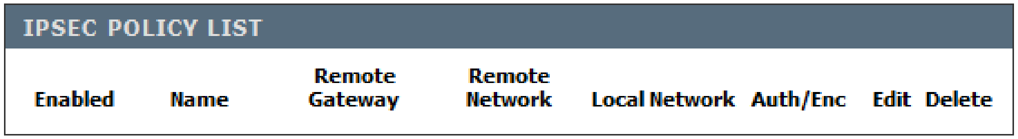
VPN Tunnel. Tunnel mode allows a remote network to appear as though it is a part of the local network. All machines behind the remote LAN will be visible to the local network. Transport mode, enabled by un-checking the VPN Tunnel check box, creates an encrypted connection terminating at the remote network's router. Inbound connections are then forwarded to the appropriate machine on the remote LAN. Please note: Transport mode requires the additional step of a configured port forward policy. Only data sent and received across networks with an IPSec policy will be encrypted for both Tunnel and Transport.

Log messages related to IPSec VPN can be found on the **Status → Logs** page. To reduce the number of log messages generated by IPSec negotiations un-check the **Firewall & Security** checkbox in the **Log Options** section.



ADD IPSEC POLICY

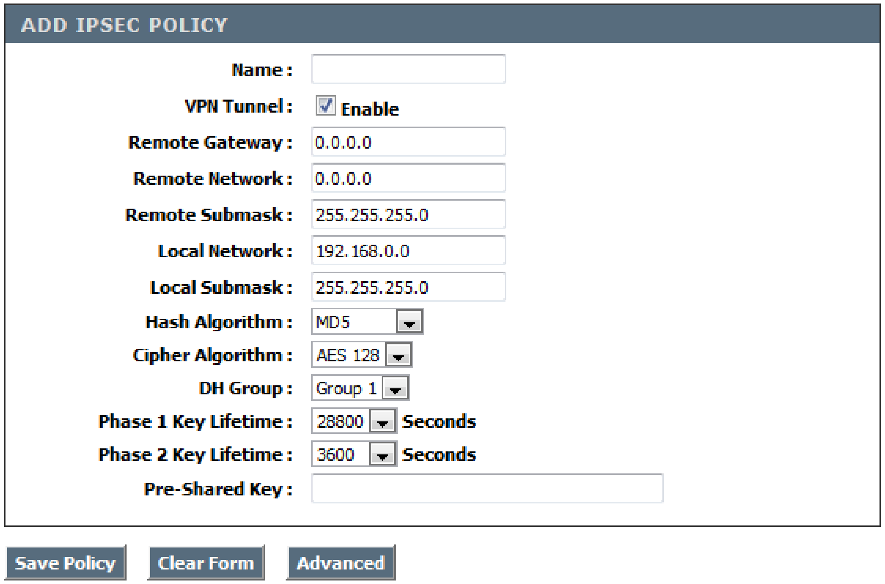
Name :	
VPN Tunnel :	☑ Enable
Remote Gateway :	0.0.0.0
Remote Network :	0.0.0.0
Remote Submask :	255.255.255.0
Local Network :	192.168.0.0
Local Submask :	255.255.255.0
Hash Algorithm :	MD5
Cipher Algorithm :	AES 128
DH Group :	Group 1
Phase 1 Key Lifetime :	28800 Seconds
Phase 2 Key Lifetime :	3600 Seconds
Pre-Shared Key :	



IPSEC POLICY LIST

Enabled	Name	Remote Gateway	Remote Network	Local Network	Auth/Enc	Edit	Delete

Remote Gateway. While this can be the WAN IP of the remote network it is recommended you use a dynamic DNS account host name. You can configure your DynDNS settings in the **Tools → Dynamic DNS** page. By using the remote router's dynamic DNS host name when configuring your IPSec policy updates of the remote WAN IP are compensated for while connecting to a VPN. *(continued)*



ADD IPSEC POLICY

Name :	
VPN Tunnel :	☑ Enable
Remote Gateway :	0.0.0.0
Remote Network :	0.0.0.0
Remote Submask :	255.255.255.0
Local Network :	192.168.0.0
Local Submask :	255.255.255.0
Hash Algorithm :	MD5
Cipher Algorithm :	AES 128
DH Group :	Group 1
Phase 1 Key Lifetime :	28800 Seconds
Phase 2 Key Lifetime :	3600 Seconds
Pre-Shared Key :	

Remote Network. This is the address of the remote LAN. The network IP addresses of the local and remote network must not be the same. Set, for example the local IP to 192.168.0.1 (default CradlePoint LAN IP) and the remote network to 192.168.30.1. In this case the IP specified in your policy for Remote Network should be 192.168.30.0. For CradlePoint routers, this IP can be configured in the **Basic → Network** page.

Remote Submask. This is the corresponding subnet mask of the remote network.

Local Network. As with the Remote Network configuration description above, this is the local network's IP address, which should be different from the Remote Network's LAN IP address. If your local IP is 192.168.0.1 the value specified in your policy for Local Network should be 192.168.0.0.

Local Submask. This is the corresponding subnet mask of the local network.

Hash Algorithm. The hash is used to compare, authenticate, and validate that data across the VPN arrives in its intended form and to derive keys used by IPSec. This section is used for both phase 1 and phase 2 of the IKE key negotiation. While the default configuration is MD5, for increased security SHA algorithms are recommended.

Cipher Algorithm. The cipher is used to encrypt messages used by IPsec. This selection is used for both Phase 1 and Phase 2 of the IKE key negotiation. The default cipher is AES.

DH Group. The DH (Diffie-Hellman) Group is a property of IKE. It 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. Mismatched group settings between policies when creating a VPN will cause your connection to the remote network to fail.

Phase 1 Key Lifetime. The lifetime of the generated keys of Phase 1 of the IPSec negotiation from IKE.

Phase 2 Key Lifetime. The lifetime of the generated keys of Phase 2 of the IPSec negotiation from IKE.

Pre-Shared Key. A secret password used to derive keys, which both parties will have to know.

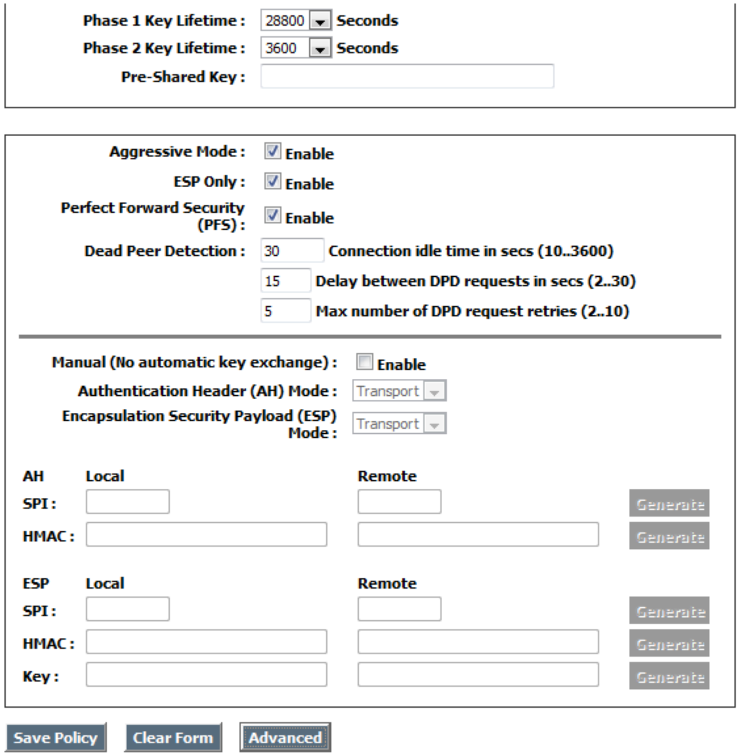
Save Policy. Adds a new policy to the IPSec Policy List. After adding the policy to the list you will need to save the settings at the top of this page before the policy will take effect.

Clear Form. While adding or updating a policy, the Clear Form button can be selected to reset the values to their default states.

Advanced. Shows you a menu to configure advanced settings.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent. *(continued)*

7.5.2 IPSEC Advanced Section



Phase 1 Key Lifetime : 28800 Seconds

Phase 2 Key Lifetime : 3600 Seconds

Pre-Shared Key :

Aggressive Mode : ☑ Enable

ESP Only : ☑ Enable

Perfect Forward Security (PFS) : ☑ Enable

Dead Peer Detection : 30 Connection idle time in secs (10..3600)

15 Delay between DPD requests in secs (2..30)

5 Max number of DPD request retries (2..10)

Manual (No automatic key exchange) : □ Enable

Authentication Header (AH) Mode : Transport

Encapsulation Security Payload (ESP) Mode : Transport

AH	Local	Remote	
SPI :			Generate
HMAC :			Generate

ESP	Local	Remote	
SPI :			Generate
HMAC :			Generate
Key :			Generate

This section includes advanced features to affect how IKE will behave. You can manually configure your IPSec policies rather than using those in the main section of this page. Some of these features can be used if you are having difficulties with IKE, using the CradlePoint IPSec VPN feature alongside a Linksys router, or working with legacy hardware. However, this section is meant for advanced users and should only be changed if you know what you are doing or a system administrator directs you to change something.

Aggressive Mode. Enables Aggressive Mode phase 1 negotiation in IKE. The IKE protocol has 2 modes of negotiating phase 1 - Identity Protection (main mode) and Aggressive. In Identity Protection 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. Un-checking this option tells IKE to use Identity Protection mode instead of Aggressive. Disabling Aggressive mode may be required for using IPSec alongside certain Linksys routers.

ESP Only. Enables **ESP Only** mode for IPSec. IPSec utilizes two protocols to secure communication through an IPSec tunnel: ESP and AH. Both protocols can be used together or separately.

If you are using any legacy hardware, which may expect AH, disable this feature. Enabling this option tells IPSec to only use the ESP protocol when securing the data. Only using ESP reduces the packet overhead but does not reduce security.

Perfect Forward Security (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.

Dead Peer Detection. 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. You can adjust the **delay between these DPD packets** to send as quickly as every 2 seconds up to 30 seconds apart. Additionally, you can specify the **Max number of DPD requests** to send at the time interval mentioned above.

(continued)

Manual (No automatic key exchange). Select this to enable **Manual Key Exchange**. This feature is useful if you experience difficulties with IKE or simply prefer not to use the form above for creating an IPSec policy. In those cases where you opt to use manual configuration instead, be sure you first generate both the local and remote values on one router then communicate the remote values as the remote network's local values and vice versa, so that the data here is exactly swapped in the remote router's IPSec settings. To populate the key fields simply select the **Generate** key to the right for AH, ESP, or Both

Authentication Header (AH) / Encapsulation Security Payload (ESP) Mode. Allows you to pick the mode AH/ESP should operate in for this policy – Transport or Tunnel. See VPN Tunnel description above for details.

AH/ESP SPI. These are hexadecimal numbers used to uniquely identify different IPsec tunnels between peers at the protocol level.

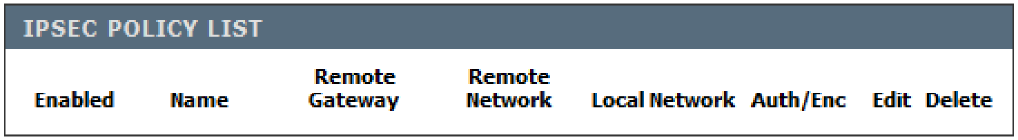
AH/ESP HMAC. These are the keys used by the AH/ESP protocol to authenticate the IP header protocol and the message payload.

ESP Keys. These are the keys used to encrypt and decrypt the messages being passed between peers.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

7.5.3 IPSEC Policy List

This section shows the currently defined IPsec Policies. An entry can be changed by clicking the **Edit** icon or can be deleted by clicking the **Delete** icon. When you click the **Edit** icon, the **Edit IPsec Policy** section is activated for editing.

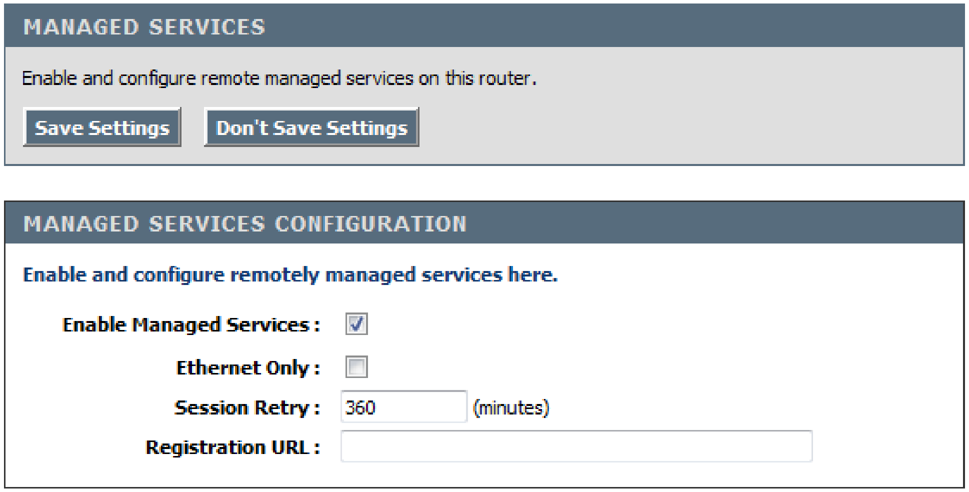


IPSEC POLICY LIST

Enabled	Name	Remote Gateway	Remote Network	Local Network	Auth/Enc	Edit	Delete

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

7.6 Managed Services



MANAGED SERVICES

Enable and configure remote managed services on this router.

MANAGED SERVICES CONFIGURATION

Enable and configure remotely managed services here.

Enable Managed Services :	☑
Ethernet Only :	□
Session Retry :	360 (minutes)
Registration URL :	

Use the Managed Services sub-menus to securely control your routers from anywhere on the Internet. You can manage their configuration, change their f/w, monitor their status and view their stored logs from any Internet-connected web browser. When this feature is enabled the router will automatically attempt to contact the management server whenever its WAN link comes up. All session management is done over the WAN link using an SSL-secured connection.

In order for the router to establish a session it must be registered with the server. Contact CradlePoint for details on how to create an account.

Enable Managed Services. Tell the router to attempt to establish a management session over the active WAN link.

Ethernet Only. A management session can involve non-trivial amounts of data transfer, especially for f/w upgrades. Since many modem plans impose data limits you may want to disable managed services when the modem is the primary WAN interface. By checking this box you ensure that the router will only establish a management session when Ethernet is the primary WAN link.

Session Retry. If a router is not yet registered with the server it will periodically retry to establish a session. This setting controls how long it will wait between retry attempts.

Registration URL. If you have contacted Cradlepoint about registering your router, you may have received an email with a URL link. Paste that link here, and the next time your router fails to start a session it will register via this link.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

7.7 Schedules

Use the Schedules sub-menu to create schedules employed to enforce rules. For example, if you want to restrict web access to Mon-Fri from 3 PM to 8 PM you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3 PM and End Time of 8 PM.

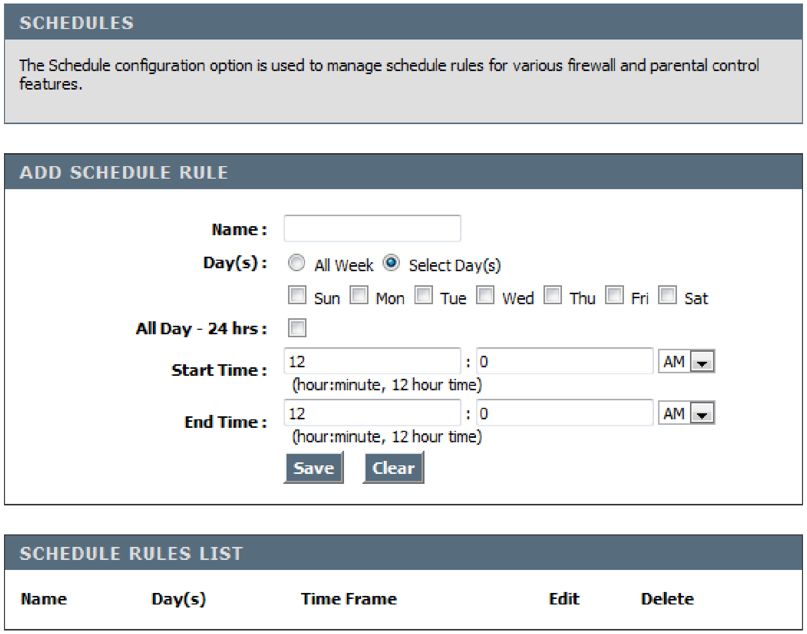
The schedules your create in this submenu are used in the other submenus that allow you to apply a time-based schedule, including

- Virtual Server
- Special Applications
- Gaming
- Parental Controls

7.7.1 Add Schedule Rule

Name. Name the schedule, such as **Weekday** rule.

Day(s). Place a check mark in the **All Week** radio button to select all seven days of the week or place a check mark in the **Select Day(s)** radio button, then put a check mark in the boxes next to the days of the week that you want your schedule to be in effect.



SCHEDULES

The Schedule configuration option is used to manage schedule rules for various firewall and parental control features.

ADD SCHEDULE RULE

Name :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

All Day - 24 hrs : □

Start Time : 12 : 0 AM
(hour:minute, 12 hour time)

End Time : 12 : 0 AM
(hour:minute, 12 hour time)

Save Clear

SCHEDULE RULES LIST

Name	Day(s)	Time Frame	Edit	Delete

All Day. Select this option if you want your schedule in effect all 24 hours for the selected day(s).

Start Time. If you don't use the **All Day** option, then enter the **Start Time**, which consists of two fields. Enter the hour of the Start Time in the first field and enter the minute of the Start Time in the second field. Email events only require a Start Time (an End Time is not required for email events).

End Time. Enter the **End Time**, which like the **Start Time** function, which consists of two fields. Enter the hour of the **End Time** in the first field and enter the minute of the **End Time** in the second field. Entering an **End Time** is required for most rules (but not for email events).

Save/Update. Record the changes you have made.

Clear. Re-initialize this area of the screen, discarding any changes you have made.

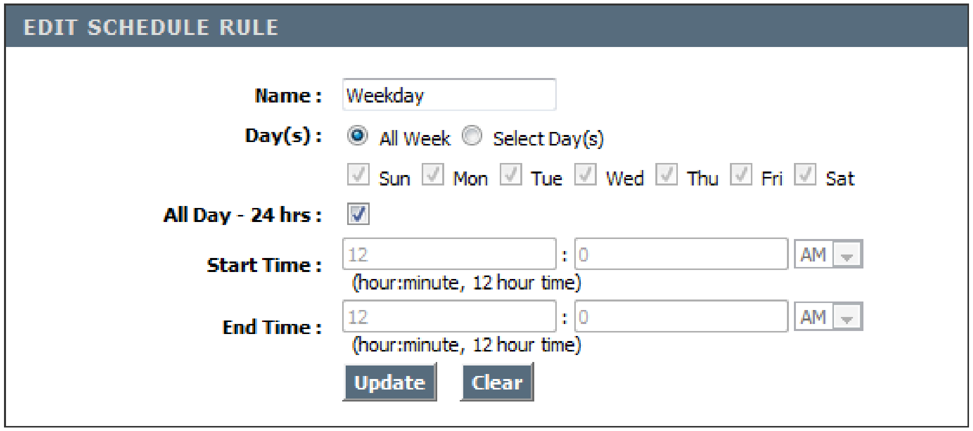
(continued)

7.7.2 Schedule Rules List.

This list displays all of the currently defined schedules. An entry can be changed by clicking the **Edit** icon or can be deleted by clicking the **Delete** icon. When you click the **Edit** icon, the item populates the **Edit Schedule Rule** and is activated for editing.

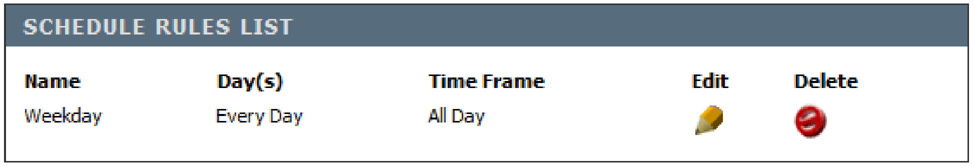
Update. Record the changes you have made.

The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with all configuration settings, click the **Reboot the Device** button.



EDIT SCHEDULE RULE

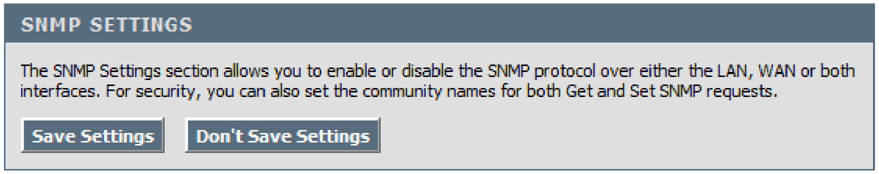
Name :	Weekday
Day(s) :	● All Week ○ Select Day(s)
	☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat
All Day - 24 hrs :	☑
Start Time :	12 : 0 AM (hour:minute, 12 hour time)
End Time :	12 : 0 AM (hour:minute, 12 hour time)



SCHEDULE RULES LIST

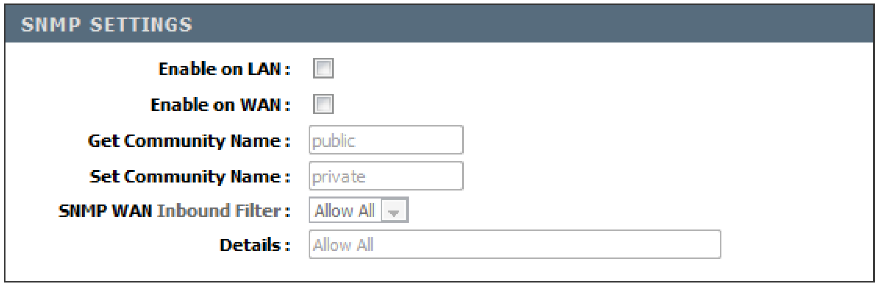
Name	Day(s)	Time Frame	Edit	Delete
Weekday	Every Day	All Day	✎	⊖

7.8 SNMP



SNMP SETTINGS

The SNMP Settings section allows you to enable or disable the SNMP protocol over either the LAN, WAN or both interfaces. For security, you can also set the community names for both Get and Set SNMP requests.



SNMP SETTINGS

Enable on LAN :	□
Enable on WAN :	□
Get Community Name :	public
Set Community Name :	private
SNMP WAN Inbound Filter :	Allow All
Details :	Allow All

Use the Simple Network Management Protocol (SNMP) Settings sub-menu to enable or disable the SNMP protocol over either the LAN, WAN, or both interfaces. For security, you can also set the community names for both Get and Set SNMP requests. SNMP version 1 is currently implemented. The supported MIB is the standard RFC 1213 MIB as maintained by the IETF. Additional Cellular-router MIB elements are available through CradlePoint's WIPIPE-MIB.

Enable on LAN. Enable SNMP on the local LAN ports so that a local device can manage the router.

Enable on WAN. Enable SNMP on the external WAN port so that an external device can manage the router.

Get Community Name. Variable length string which allows access to read-only data within this community group. The community names should never be "public" or "private". Community names are a maximum of 15 characters long. Names should contain at least one number and one capital letter. Access to the community name should be limited to the Administrator of realms.

Set Community Name. Variable length string which allows access to read and write data within this community group. The community names should never be "public" or "private". Community names are a maximum of 15 characters long. Names should contain at least one number and one capital letter. Access to the community name should be limited to the Administrator of realms.

SNMP WAN Inbound Filter. If SNMP is enabled on the WAN port you can create a filter that allows or denies specific IP ranges to connect to the SNMP server.

Details. This shows the details of the selected Inbound Filter rule.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

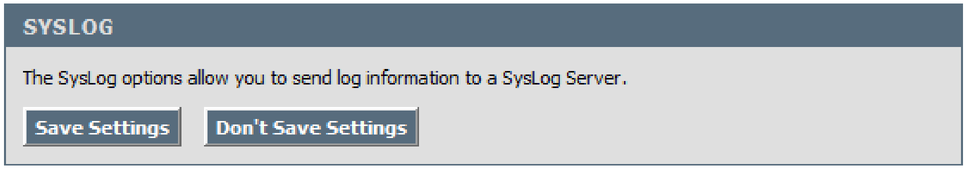
7.9 Syslog

Use the SYSLOG sub-menu to enable archive of log files to a Syslog Server.

Enable Logging to Syslog Server. (Default: off) Enable this option if you have a syslog server currently running on the LAN and wish to send log messages to it.

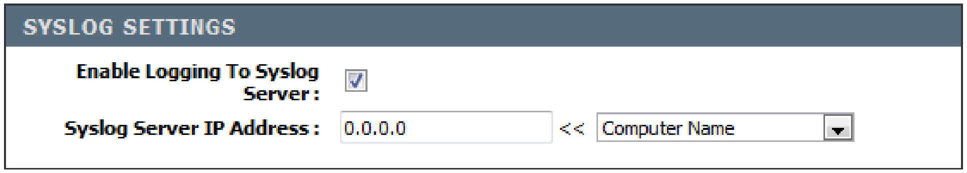
Syslog Server IP Address. Enter the LAN IP address of the Syslog Server.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.



SYSLOG

The SysLog options allow you to send log information to a SysLog Server.



SYSLOG SETTINGS

Enable Logging To Syslog Server : ☑

Syslog Server IP Address : 0.0.0.0 << Computer Name

7.10 System (System Settings)

Use the System Settings sub-menu to control to **Reboot the Device** function or to restore the router to the factory default settings.

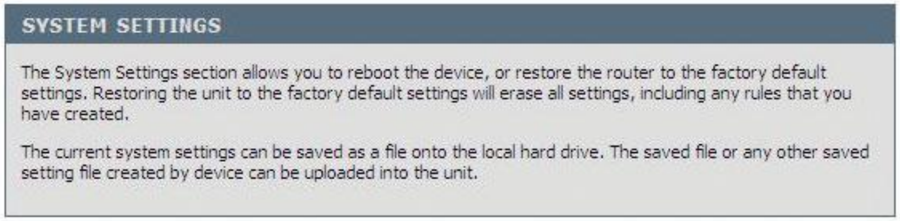
WARNING: Restoring the unit to the factory default settings will overwrite and erase any custom settings you have implemented that change the original factory default settings.

7.10.1 System Settings

Save Configuration. Click to save configuration information to a file on a local hard drive or any other target you choose.

Restore Configuration from File. Reads all configuration information from a Save Configuration file.

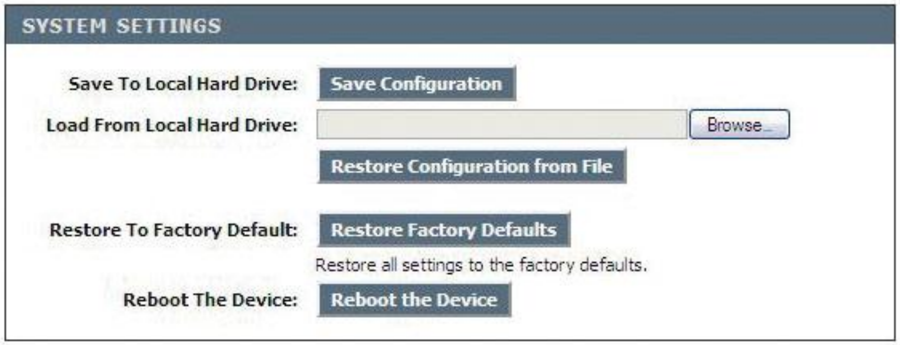
Restore to Factory Defaults. This option will restore all configuration settings back to the factory defaults. Any settings that have not been saved will be lost. If you want to save your router configuration settings, you can do so from the **Tools → Admin** sub-menu.



SYSTEM SETTINGS

The System Settings section allows you to reboot the device, or restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you have created.

The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by device can be uploaded into the unit.



SYSTEM SETTINGS

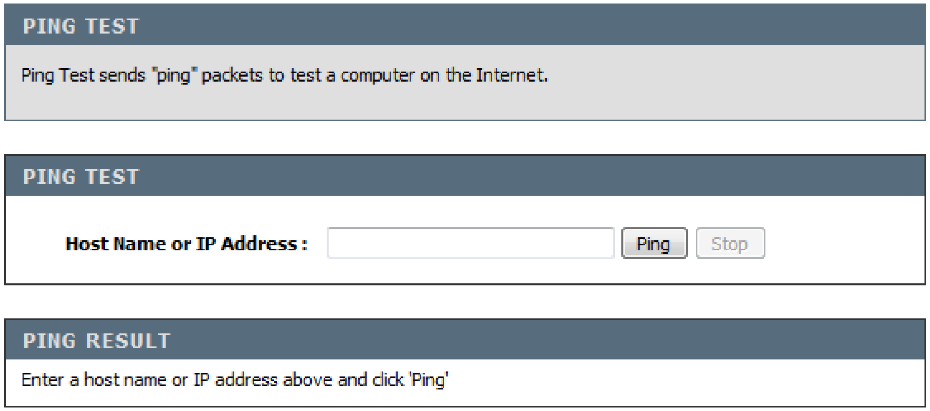
Save To Local Hard Drive:
Save Configuration
Load From Local Hard Drive:
Browse...
Restore Configuration from File
Restore To Factory Default:
Restore Factory Defaults
Reboot The Device:
Reboot the Device

Restore all settings to the factory defaults.

Reboot the Device. This will restart the router. Useful for restarting when you are not near the device. When you click the **Reboot the Device** button, you will be prompted to **Save Configuration**, which saves the configuration as described in **Save to Local Hard Drive**. This option preserves any custom settings you have implemented.

7.11 System Check (Ping Test)

Use the System Check sub-menu as a diagnostic tool to check connectivity from the router to another computer. This function can be used to verify a working connection across the WAN network or the local network. NOTE: the ping target must be configured to respond to ICMP ping requests.



PING TEST

Ping Test sends "ping" packets to test a computer on the Internet.

PING TEST

Host Name or IP Address :

PING RESULT

Enter a host name or IP address above and click 'Ping'

7.11.1 Ping Test

Host Name or IP Address. Enter either the IP address of the target computer or enter its fully qualified domain name.

- Ping. Start Pinging the specified host
- Stop. The host is pinged repeatedly until you click the **Stop** button.

7.11.2 Ping Result

Displays the results of the ping test. The ping test is an ICMP echo protocol. It's used to test response and path to a remote computer system, i.e., a ping to a URL "www.xxxxx.com" will tell you if there is a path and if the remote computer is responding. NOTE: Not all devices respond to pings.

Example:

- Host Name or IP Address:

www.whitehouse.gov

- Ping Result

Please wait, resolving www.whitehouse.gov....

Resolved to 205.161.7.102.

Response from 205.161.7.102 received in 7 milliseconds.

Response from 205.161.7.102 received in 6 milliseconds.

Response from 205.161.7.102 received in 7 milliseconds.

User stopped ping.

7.12 Time

Use the Time Configuration sub-menu to configure, update, and maintain the correct time on the internal system clock. The time can be configured manually or a network time server can be selected and the time updated via the Network Time Protocol (NTP).

7.12.1 Time Configuration.

Current Router Time. Displays the day, date and local time used by the MBR1200.

Time Zone. Select the local time zone.

Enable Daylight Saving. Check this option to adjust for daylight savings time.

Daylight Saving Offset. Select the time offset for daylight savings time.

Daylight Savings Dates. Set the month, week, day of week and time for the MBR1200 to switch to/from Daylight Savings Time.

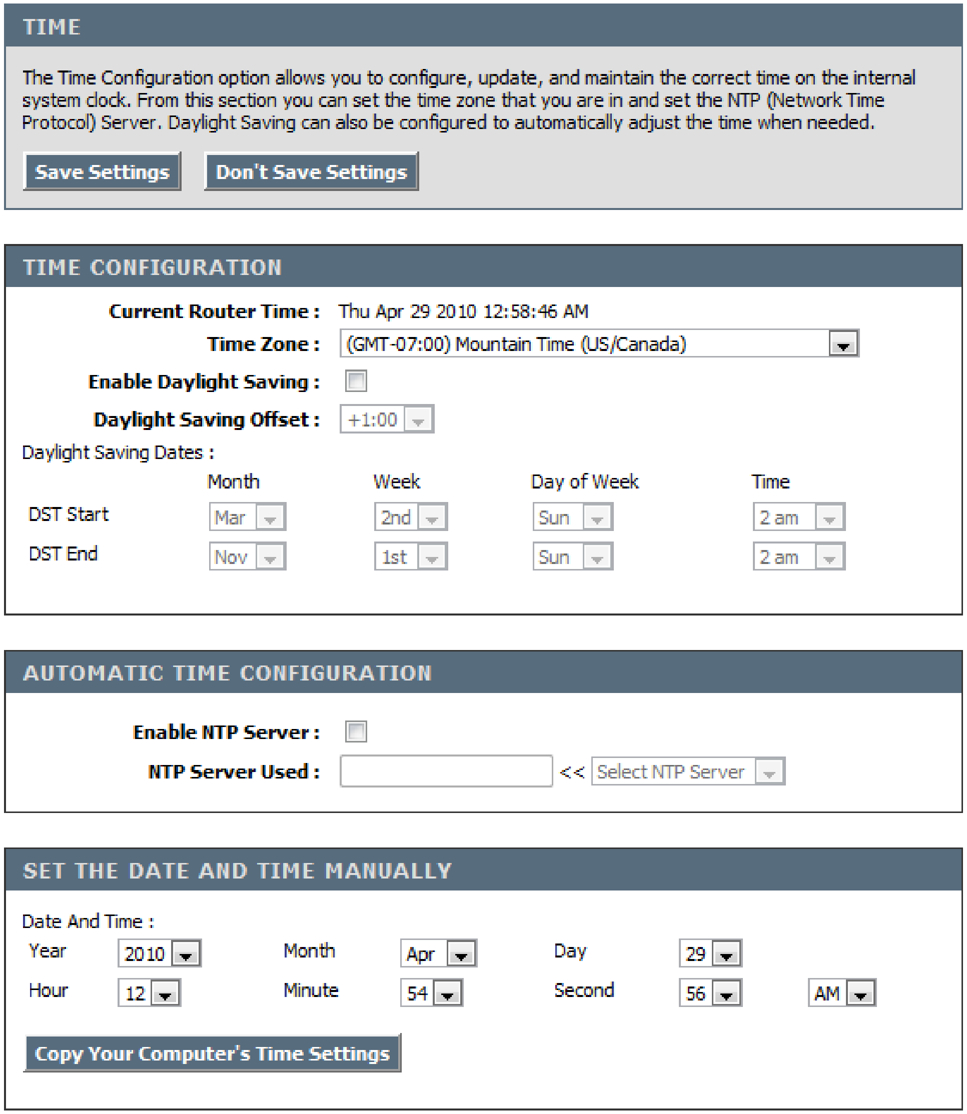
7.12.2 Automatic Time Configuration

Enabling this option allows the MBR1200 to contact network time servers to automatically adjust the MBR1200 clock. If you are using schedules or logs, this is the best way to ensure that the schedules and logs are accurate.

Enable NTP Server. Select this option if you want the router's clock synchronized to a Time Sever over the Internet.

NTP Server Used. Select a Time Server for synchronization. You can type in the address of a time server or select one from the drop down menu.

(continued)



TIME

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

TIME CONFIGURATION

Current Router Time : Thu Apr 29 2010 12:58:46 AM

Time Zone : (GMT-07:00) Mountain Time (US/Canada)

Enable Daylight Saving : □

Daylight Saving Offset : +1:00

Daylight Saving Dates :

	Month	Week	Day of Week	Time
DST Start	Mar	2nd	Sun	2 am
DST End	Nov	1st	Sun	2 am

AUTOMATIC TIME CONFIGURATION

Enable NTP Server : □

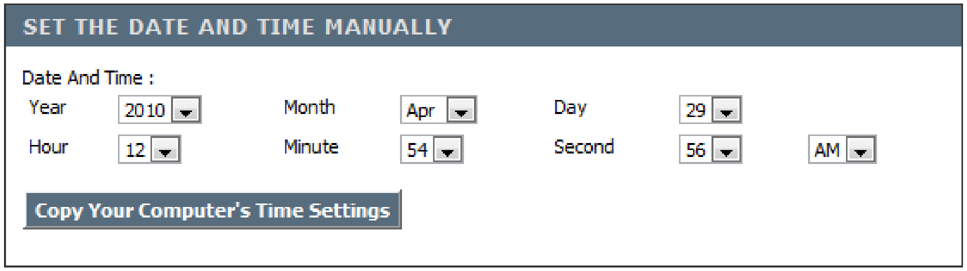
NTP Server Used : << Select NTP Server

SET THE DATE AND TIME MANUALLY

Date And Time :

Year	2010	Month	Apr	Day	29	
Hour	12	Minute	54	Second	56	AM

7.12.3 Set the Date and Time Manually



SET THE DATE AND TIME MANUALLY

Date And Time :

Year	2010	Month	Apr	Day	29	
Hour	12	Minute	54	Second	56	AM

If you do not have the NTP Server option in effect, you can either manually set the time for your router here or you can click the **Copy Your Computer's Time Settings** button to copy the time from the computer you are using.

NOTE: Be sure the computer's time is set correctly.

WARNING: If the router loses power for any reason, it cannot keep its clock running and will not have the correct time when it is started again. To maintain the correct time for schedules and logs, either you must enter the correct time after you restart the router or you must enable the NTP Server option.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

7.13 User Login

Use the User Login sub-menu to configure, update, and maintain a customized login page for other users to see when they log into the router.

7.13.1 User Login Settings

Require User Login. Select this option to enable or disable user login.

7.13.2 Internet Access Password

Password. Enter the password required for internet access.

Verify Password. Verify password required for internet access.

7.13.3 Customize Billboard

Enable Custom Billboard. Select this option if you want to provide the router with a new customized user login page.

Custom Billboard. Enter HTML into this section to create a customized user login page.

Preview. Select this button to preview the customized user login in the preview panel.

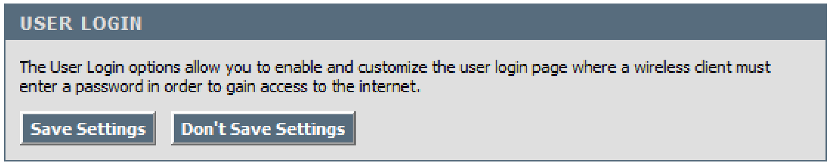
Load Default. Select this button to load a default or example customized user login.

NOTE. HTML links entered into customized bounce page will not be able to retrieve information on the WAN side of the router.

7.13.4 Preview Custom Billboard

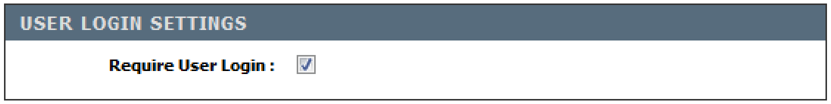
This area will show a preview of the customized user login.

When you are done editing the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.



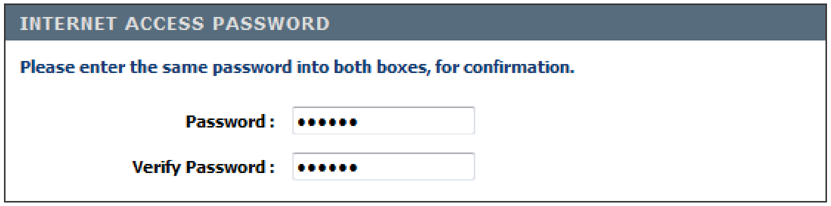
USER LOGIN

The User Login options allow you to enable and customize the user login page where a wireless client must enter a password in order to gain access to the internet.



USER LOGIN SETTINGS

Require User Login : ☑

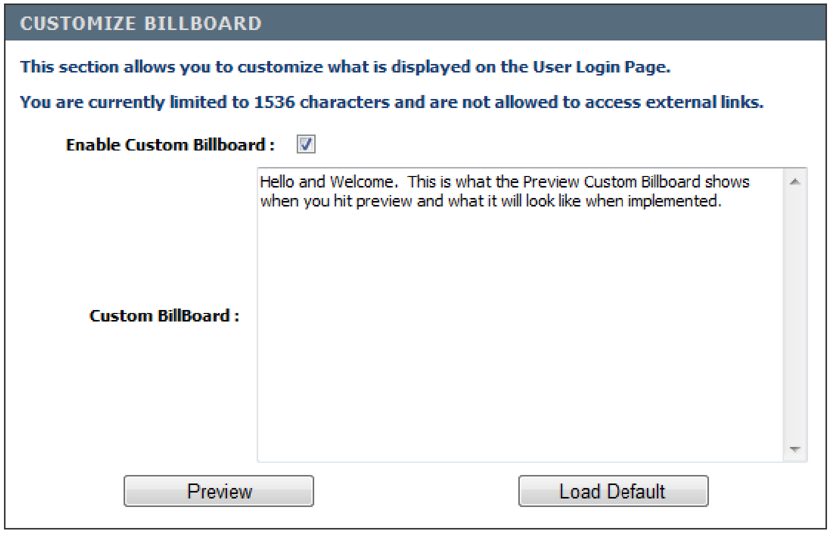


INTERNET ACCESS PASSWORD

Please enter the same password into both boxes, for confirmation.

Password : ••••••

Verify Password : ••••••



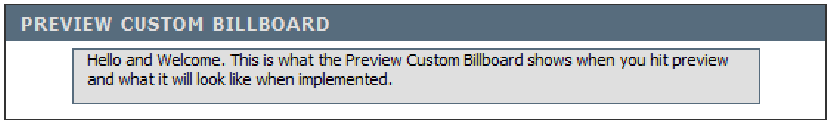
CUSTOMIZE BILLBOARD

This section allows you to customize what is displayed on the User Login Page.

You are currently limited to 1536 characters and are not allowed to access external links.

Enable Custom Billboard : ☑

Custom BillBoard : Hello and Welcome. This is what the Preview Custom Billboard shows when you hit preview and what it will look like when implemented.



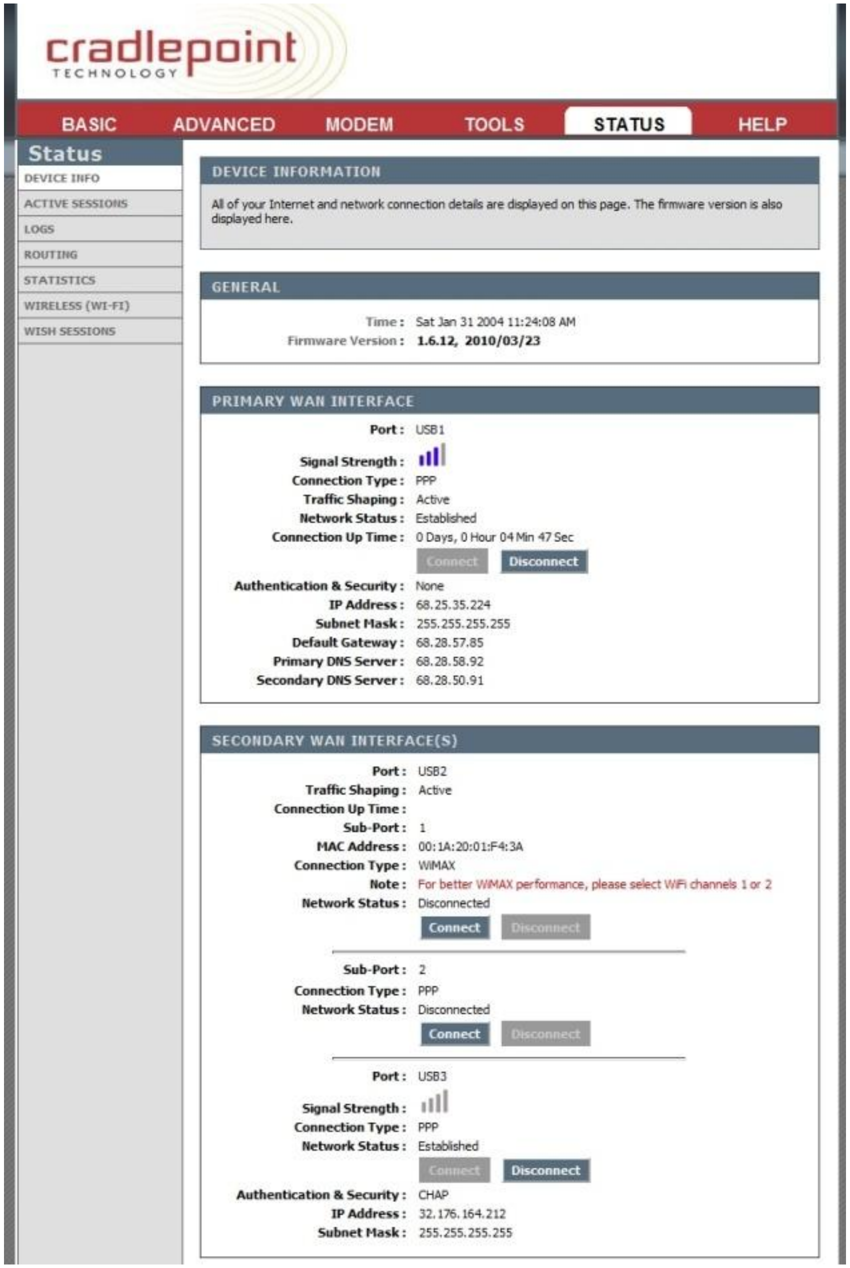
PREVIEW CUSTOM BILLBOARD

Hello and Welcome. This is what the Preview Custom Billboard shows when you hit preview and what it will look like when implemented.

8 STATUS TAB

The Status tab provides information about the current configuration settings of the MBR1200 router via 7 sub-menus:

- Device Info
- Active Sessions
- Logs
- Routing
- Statistics
- Wireless (Wi-Fi)
- WISH Sessions



DEVICE INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

GENERAL

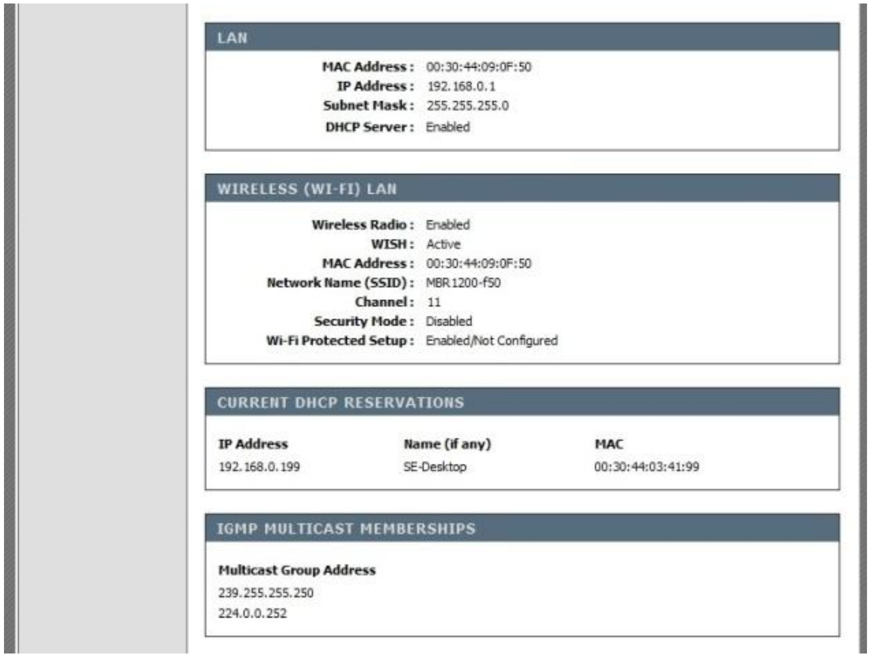
Time :	Sat Jan 31 2004 11:24:08 AM
Firmware Version :	**1.6.12, 2010/03/23**

PRIMARY WAN INTERFACE

Port :	USB1
Signal Strength :	▂▄▆█
Connection Type :	PPP
Traffic Shaping :	Active
Network Status :	Established
Connection Up Time :	0 Days, 0 Hour 04 Min 47 Sec
	Connect Disconnect
Authentication & Security :	None
IP Address :	68.25.35.224
Subnet Mask :	255.255.255.255
Default Gateway :	68.28.57.85
Primary DNS Server :	68.28.58.92
Secondary DNS Server :	68.28.50.91

SECONDARY WAN INTERFACE(S)

Port :	USB2
Traffic Shaping :	Active
Connection Up Time :	
Sub-Port :	1
MAC Address :	00:1A:20:01:F4:3A
Connection Type :	WIMAX
Note :	For better WiMAX performance, please select WiFi channels 1 or 2
Network Status :	Disconnected
	Connect Disconnect
Sub-Port :	2
Connection Type :	PPP
Network Status :	Disconnected
	Connect Disconnect
Port :	USB3
Signal Strength :	▂▄▆█
Connection Type :	PPP
Network Status :	Established
	Connect Disconnect
Authentication & Security :	CHAP
IP Address :	32.176.164.212
Subnet Mask :	255.255.255.255



LAN

MAC Address :	00:30:44:09:0F:50
IP Address :	192.168.0.1
Subnet Mask :	255.255.255.0
DHCP Server :	Enabled

WIRELESS (WI-FI) LAN

Wireless Radio :	Enabled
WISH :	Active
MAC Address :	00:30:44:09:0F:50
Network Name (SSID) :	MBR1200-f50
Channel :	11
Security Mode :	Disabled
Wi-Fi Protected Setup :	Enabled/Not Configured

CURRENT DHCP RESERVATIONS

IP Address	Name (if any)	MAC
192.168.0.199	SE-Desktop	00:30:44:03:41:99

IGMP MULTICAST MEMBERSHIPS

Multicast Group Address
239.255.255.250
224.0.0.252

8.1 Device Info

The Device Information sub-menu displays your Router settings. Options cannot be changed from this sub-menu. They can only be monitored.

NOTE: Some browsers have limitations that make it impossible to update the WAN status display when the status changes. Some browsers require that you refresh the display to obtain updated status. Some browsers report an error condition when trying to obtain WAN status.

8.1.1 General

Time. Displays the time and date that the router is set to.

Firmware Version. Displays the currently loaded firmware version.

8.1.2 WAN (Primary and Secondary Interface(s))

The information displayed will be for the currently active WAN connection. To change the failover priorities of the various WAN connections or to manually connect or disconnect a WAN connection go to the **Advanced → Failover** sub-menu. If the connection is DHCP, clicking the **DHCP Release** button unassigns the router's IP address. The router will not respond to IP messages from the WAN side until you click the **DHCP Renew** button or power-up the router again. Clicking the **DHCP Renew** button requests a new IP address from the ISP's server.

If the connection is via a modem, clicking the **Disconnect** button will cause the modem to hang up, and it will not dial again (regardless of the **Reconnect Mode** from the Global Settings section of the Modem Settings page) unless you re-plug it or click the **Connect** button.

Port. USB1, USB2, USB3, PC Card, Express Card or Ethernet.

Signal Strength. (USB, PC Card, Express Card only). Strength of wireless signal.

Connection Type. The Internet connection type that is being used.

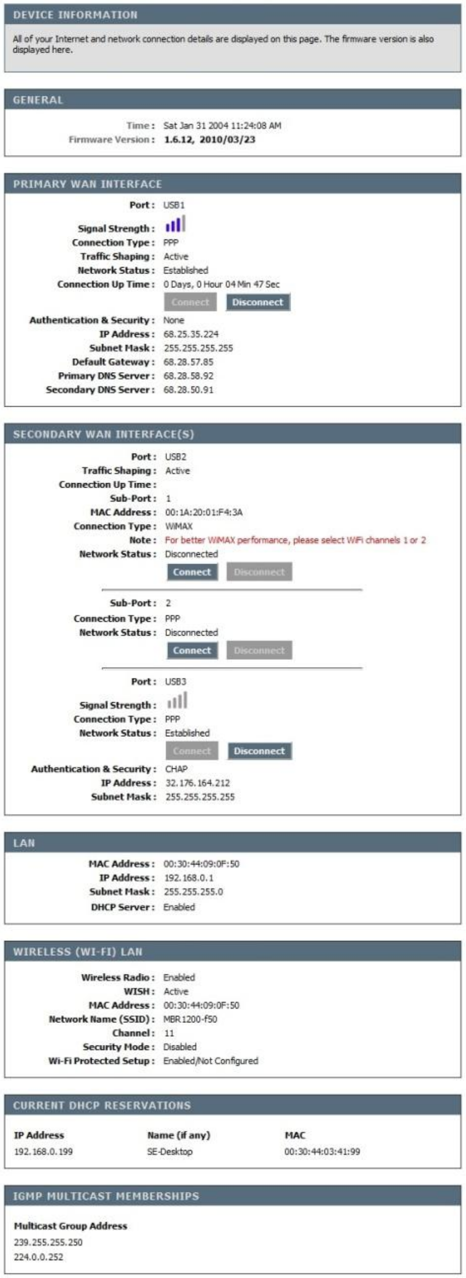
Traffic Shaping. Traffic Shaping is Active or Inactive.

Cable Status. (Ethernet Only). Connected or not.

Network Status. Network is Connected, Establishing, Suspended, or Established.

Connection Uptime. Amount of time the connection has been successfully connected.

Authentication & Security. Type of Authentication & Security in place. *(continued)*



DEVICE INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

GENERAL

Time : Sat Jan 31 2004 11:24:08 AM
Firmware Version : 1.6.12, 2010/03/23

PRIMARY WAN INTERFACE

Port : USB1
Signal Strength :
Connection Type : PPP
Traffic Shaping : Active
Network Status : Established
Connection Up Time : 0 Days, 0 Hour 04 Min 47 Sec

Authentication & Security : None
IP Address : 68.25.35.224
Subnet Mask : 255.255.255.255
Default Gateway : 68.28.57.85
Primary DNS Server : 68.28.58.92
Secondary DNS Server : 68.28.50.91

SECONDARY WAN INTERFACE(S)

Port : USB2
Traffic Shaping : Active
Connection Up Time :
Sub-Port : 1
MAC Address : 00:1A:20:01:F4:3A
Connection Type : WiMAX
Note : For better WiMAX performance, please select WiFi channels 1 or 2
Network Status : Disconnected

Sub-Port : 2
Connection Type : PPP
Network Status : Disconnected

Port : USB3
Signal Strength :
Connection Type : PPP
Network Status : Established

Authentication & Security : CHAP
IP Address : 32.176.164.212
Subnet Mask : 255.255.255.255

LAN

MAC Address : 00:30:44:09:0F:50
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WIRELESS (WI-FI) LAN

Wireless Radio : Enabled
WISH : Active
MAC Address : 00:30:44:09:0F:50
Network Name (SSID) : MBR1200-f50
Channel : 11
Security Mode : Disabled
Wi-Fi Protected Setup : Enabled/Not Configured

CURRENT DHCP RESERVATIONS

IP Address	Name (if any)	MAC
192.168.0.199	SE-Desktop	00:30:44:03:41:99

IGMP MULTICAST MEMBERSHIPS

Multicast Group Address
239.255.255.250
224.0.0.252

MAC Address. The MAC address that is seen over the Internet.

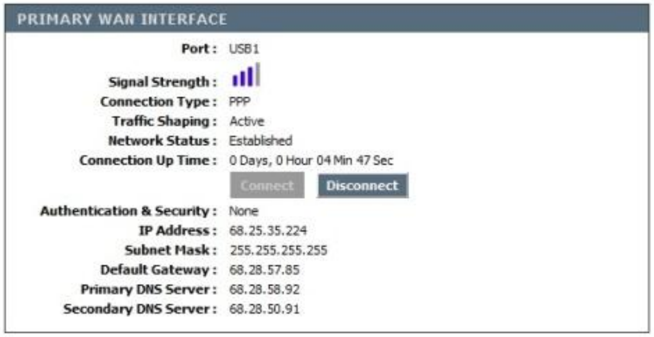
IP Address. The IP address being used on the WAN port.

Subnet Mask. The subnet mask used on the WAN port.

Default Gateway. The default gateway of the WAN port.

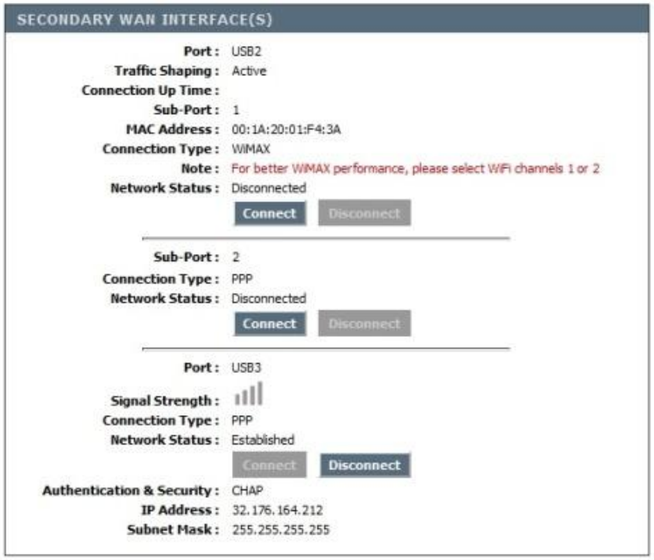
Primary DNS Server. The Primary DNS Server address.

Secondary DNS Server. The Secondary DNS Server address.



PRIMARY WAN INTERFACE

Port : USB1
Signal Strength :
Connection Type : PPP
Traffic Shaping : Active
Network Status : Established
Connection Up Time : 0 Days, 0 Hour 04 Min 47 Sec
Authentication & Security : None
IP Address : 68.25.35.224
Subnet Mask : 255.255.255.255
Default Gateway : 68.28.57.85
Primary DNS Server : 68.28.58.92
Secondary DNS Server : 68.28.50.91



SECONDARY WAN INTERFACE(S)

Port : USB2
Traffic Shaping : Active
Connection Up Time :
Sub-Port : 1
MAC Address : 00:1A:20:01:F4:3A
Connection Type : WIMAX
Note : For better WiMAX performance, please select WiFi channels 1 or 2
Network Status : Disconnected

Sub-Port : 2
Connection Type : PPP
Network Status : Disconnected

Port : USB3
Signal Strength :
Connection Type : PPP
Network Status : Established
Authentication & Security : CHAP
IP Address : 32.176.164.212
Subnet Mask : 255.255.255.255

8.1.3 LAN

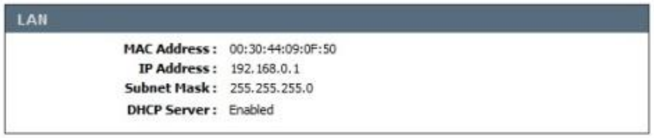
This area of the screen reflects configuration settings from the **Basic → Network** sub-menu.

MAC Address. The MAC address displayed for your wired network. It is the factory-assigned identifier of the LAN ports.

IP Address. IP Address of the router.

Subnet Mask. Subnet of the router.

DHCP Server. DHCP Server is Enabled or Disabled.



LAN

MAC Address : 00:30:44:09:0F:50
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

8.1.4 Wireless (Wi-Fi) LAN

This area of the screen reflects configuration settings from the **Basic → Wireless** page, the **Advanced → WISH** page and the **Advanced → Wi-Fi Protected Setup** page. The **MAC Address** is the factory-assigned identifier of the wireless card.

Wireless Radio. Wi-Fi is Enabled or Disabled.

WISH. WISH is Active or Inactive.

MAC Address. MAC address of the router.

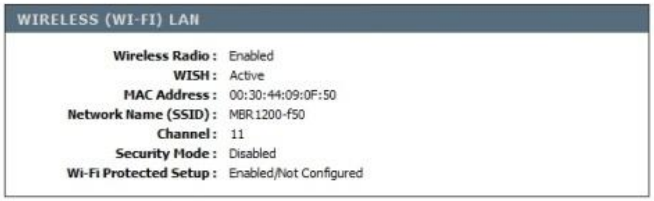
Network Name (SSID). Network Name of the router.

Channel. Wi-Fi channel that the router is broadcasting on.

Turbo Mode. Turbo Mode is Enabled or Disabled.

Security Mode. WEP, WPA, WPA2, etc.

Wi-Fi Protected Setup. Wi-Fi Protected Setup is Enabled or Configured.



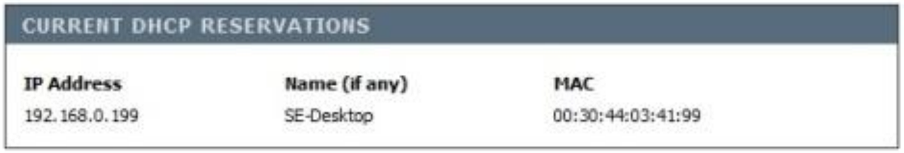
WIRELESS (WI-FI) LAN

Wireless Radio : Enabled
WISH : Active
MAC Address : 00:30:44:09:0F:50
Network Name (SSID) : MBR1200-f50
Channel : 11
Security Mode : Disabled
Wi-Fi Protected Setup : Enabled/Not Configured

(continued)

8.1.5 Current DHCP Reservation

This area of the screen continually updates to show all DHCP enabled computers and devices connected to the LAN side of your router. The detection "range" is limited to the address range as configured in DHCP Server. Computers that have an address outside of this range will not show. If the DHCP Client (i.e. a computer configured to Automatically obtain an address) supplies a Host Name then that will also be shown. Any computer or device that has a static IP address that lies within the detection "range" may show, however its host name will not.

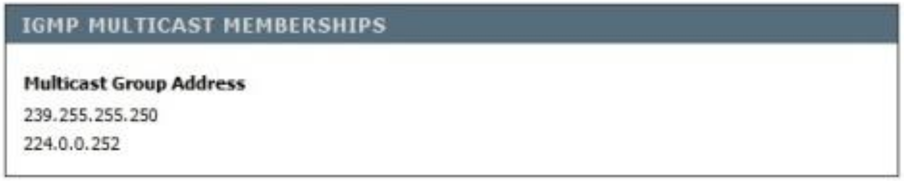


CURRENT DHCP RESERVATIONS

IP Address	Name (if any)	MAC
192.168.0.199	SE-Desktop	00:30:44:03:41:99

8.1.6 IGMP Multicast memberships

If IGMP is enabled, this area of the screen shows all multicast groups of which any LAN devices are members.



IGMP MULTICAST MEMBERSHIPS

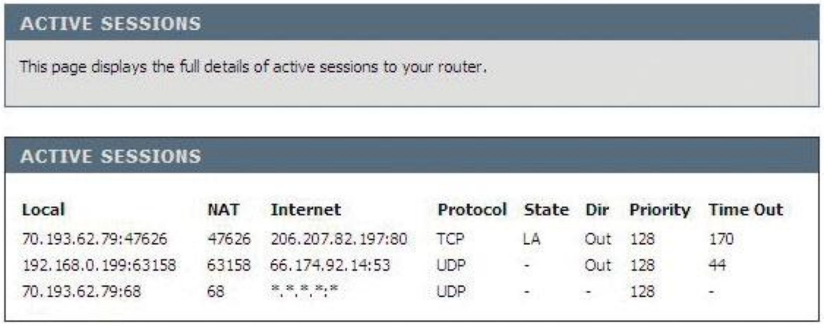
Multicast Group Address
239.255.255.250
224.0.0.252

8.2 Active Sessions

The Active Session sub-menu displays the full details of active sessions to your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN side computer.

Local. The IP address and, where appropriate, port number of the local application.

NAT. The port number of the LAN-side application as viewed by the WAN side application.



ACTIVE SESSIONS

This page displays the full details of active sessions to your router.

ACTIVE SESSIONS

Local	NAT	Internet	Protocol	State	Dir	Priority	Time Out
70.193.62.79:47626	47626	206.207.82.197:80	TCP	LA	Out	128	170
192.168.0.199:63158	63158	66.174.92.14:53	UDP	-	Out	128	44
70.193.62.79:68	68	*.*.*.*:*	UDP	-	-	128	-

Internet. The IP address and, where appropriate, port number of the application on the Internet.

Protocol. The communications protocol used for the conversation.

State. State for sessions that use the TCP protocol.

- NO: None -- This entry is used as a placeholder for a future connection that may occur.
- SS: SYN Sent -- One of the systems is attempting to start a connection.
- EST: Established -- The connection is passing data.
- FW: FIN Wait -- The client system has requested that the connection be stopped.
- CW: Close Wait -- The server system has requested that the connection be stopped.
- TW: Time Wait -- Waiting for a short time while a connection that was in FIN Wait is fully closed.
- LA: Last ACK -- Waiting for a short time while a connection that was in Close Wait is fully closed.
- CL: Closed -- The connection is no longer active but the session is being tracked in case there are any retransmitted packets still pending.

Dir. The direction of initiation of the conversation:

- Out. Initiated from LAN to WAN.
- In. Initiated from WAN to LAN.

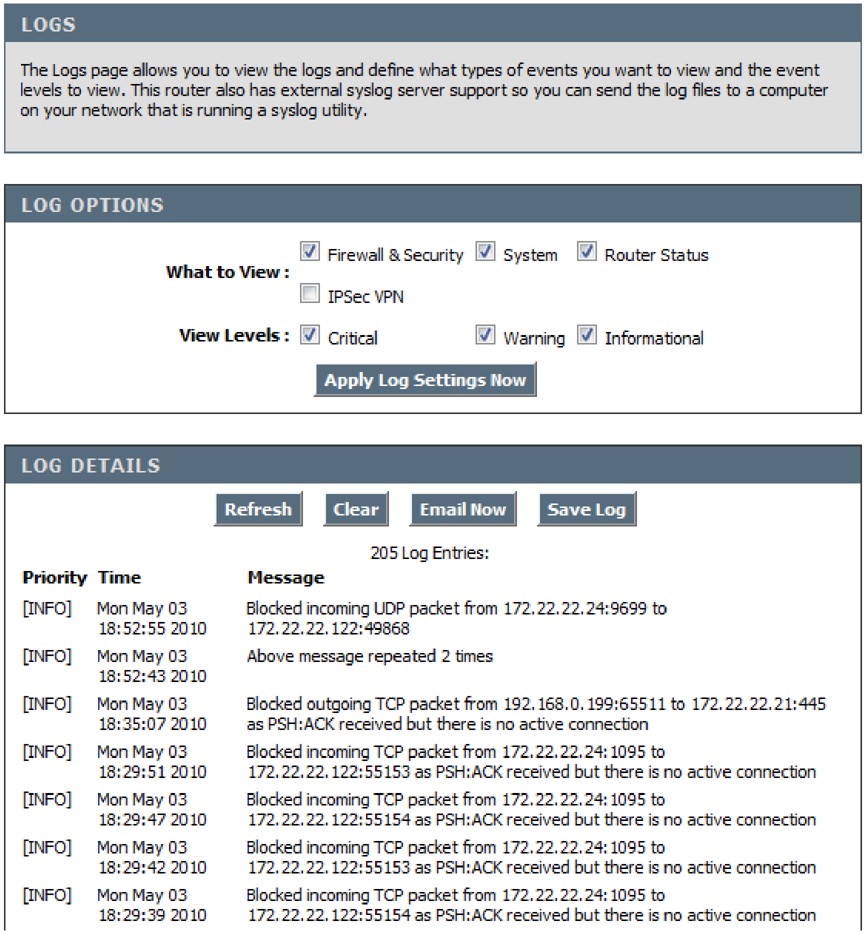
Priority. The preference given to outbound packets of this conversation by the QoS Engine logic. Smaller numbers represent higher priority.

Time Out. The number of seconds of idle time until the router considers the session terminated. The initial value of Time Out depends on the type and state of the connection.

- 300 seconds. UDP connections.
- 240 seconds. Reset or closed TCP connections. The connection does not close instantly so that lingering packets can pass or the connection can be re-established.
- 7800 seconds. Established or closing TCP connections.

8.3 Logs

The Logs sub-menu allows you to view the router logs. The router automatically logs (records) events of possible interest in its internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. You can decide what types of events you want to view and the level of the events to view. 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.



LOGS

The Logs page allows you to view the logs and define what types of events you want to view and the event levels to view. 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.

LOG OPTIONS

What to View : ☑ Firewall & Security ☑ System ☑ Router Status ☐ IPSec VPN

View Levels : ☑ Critical ☑ Warning ☑ Informational

LOG DETAILS

205 Log Entries:

Priority	Time	Message
[INFO]	Mon May 03 18:52:55 2010	Blocked incoming UDP packet from 172.22.22.24:9699 to 172.22.22.122:49868
[INFO]	Mon May 03 18:52:43 2010	Above message repeated 2 times
[INFO]	Mon May 03 18:35:07 2010	Blocked outgoing TCP packet from 192.168.0.199:65511 to 172.22.22.21:445 as PSH:ACK received but there is no active connection
[INFO]	Mon May 03 18:29:51 2010	Blocked incoming TCP packet from 172.22.22.24:1095 to 172.22.22.122:55153 as PSH:ACK received but there is no active connection
[INFO]	Mon May 03 18:29:47 2010	Blocked incoming TCP packet from 172.22.22.24:1095 to 172.22.22.122:55154 as PSH:ACK received but there is no active connection
[INFO]	Mon May 03 18:29:42 2010	Blocked incoming TCP packet from 172.22.22.24:1095 to 172.22.22.122:55153 as PSH:ACK received but there is no active connection
[INFO]	Mon May 03 18:29:39 2010	Blocked incoming TCP packet from 172.22.22.24:1095 to 172.22.22.122:55154 as PSH:ACK received but there is no active connection

8.3.1 Log Options

What to View. You can select the types of messages that you want to display from the log:

- Firewall & Security
- System
- Router Status
- IPSec VPN

View Levels. You can choose from three levels of message importance:

- Critical
- Warning
- Informational

Apply Log Settings Now. Filters the log results so that only the selected options appear.

8.3.2 Log Details

Refresh. Updates the log details on the screen so it displays any recent activity.

Clear. Clears all of the log contents.

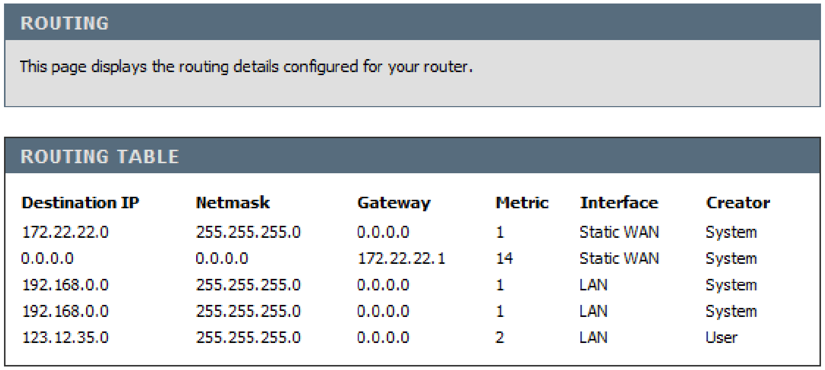
Email Now. This option will send a copy of the router log to the email address configured in the **Tools → Email** sub-menu.

Save Log. This option will save the router to a log file on your computer.

8.4 Routing

The routing section displays all of the routing details configured for your router.

A value of 0.0.0.0 for gateway means there is no next hop, and the IP address is directly connected to the router on the interface specified: LAN or WAN. A value of 0.0.0.0 in both the destination IP and netmask means that this is the default route.



ROUTING

This page displays the routing details configured for your router.

ROUTING TABLE

Destination IP	Netmask	Gateway	Metric	Interface	Creator
172.22.22.0	255.255.255.0	0.0.0.0	1	Static WAN	System
0.0.0.0	0.0.0.0	172.22.22.1	14	Static WAN	System
192.168.0.0	255.255.255.0	0.0.0.0	1	LAN	System
192.168.0.0	255.255.255.0	0.0.0.0	1	LAN	System
123.12.35.0	255.255.255.0	0.0.0.0	2	LAN	User

8.5 Statistics (Traffic Statistics)

The Statistics (Traffic Statistics) sub-menu displays basic statistics for the LAN, WAN and Wireless network interfaces.

8.5.1 Traffic Statistics

Refresh Statistics. Updates the screen with the latest router statistics.

Clear Statistics. Clears all of the values on the screen.

8.5.2 Wireless (Wi-Fi), LAN and WAN Statistics

Kbytes Sent. The number of packets transmitted to the local area network.

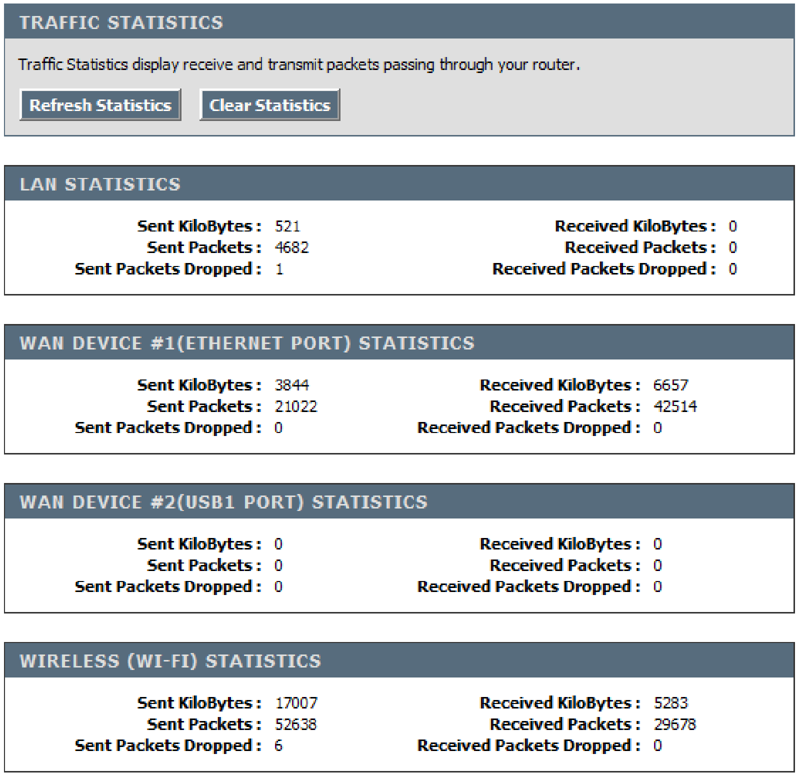
Kbytes Received. The number of packets received from the local area network.

TX Packets Dropped. The number of transmit packets not sent.

RX Packets Dropped. The number of receive packets not dropped.

Collisions. The number of collision packets on the LAN.

Errors. The number of packets received with errors on the LAN.



TRAFFIC STATISTICS

Traffic Statistics display receive and transmit packets passing through your router.

LAN STATISTICS

Sent KiloBytes :	521	Received KiloBytes :	0
Sent Packets :	4682	Received Packets :	0
Sent Packets Dropped :	1	Received Packets Dropped :	0

WAN DEVICE #1(ETHERNET PORT) STATISTICS

Sent KiloBytes :	3844	Received KiloBytes :	6657
Sent Packets :	21022	Received Packets :	42514
Sent Packets Dropped :	0	Received Packets Dropped :	0

WAN DEVICE #2(USB1 PORT) STATISTICS

Sent KiloBytes :	0	Received KiloBytes :	0
Sent Packets :	0	Received Packets :	0
Sent Packets Dropped :	0	Received Packets Dropped :	0

WIRELESS (WI-FI) STATISTICS

Sent KiloBytes :	17007	Received KiloBytes :	5283
Sent Packets :	52638	Received Packets :	29678
Sent Packets Dropped :	6	Received Packets Dropped :	0

8.6 Wireless (Wi-Fi)

The Wireless (Wi-Fi) sub-menu displays the number of wireless clients that are connected to the router, the MAC address of each system connecting wirelessly, and the IP address of each system connecting wirelessly. Control buttons allow the administrator to allow or deny access for each of the listed computers. If **Require User Login** has not been enabled (**Basic → Wizard** sub-menu), then the control buttons are not available on this submenu.

8.6.1 Number of Wireless Clients

This lists the client computers that are currently connected to the WLAN access point.

MAC Address. The Ethernet ID (MAC address) of the wireless client.

IP Address. The LAN-side IP address of the client.

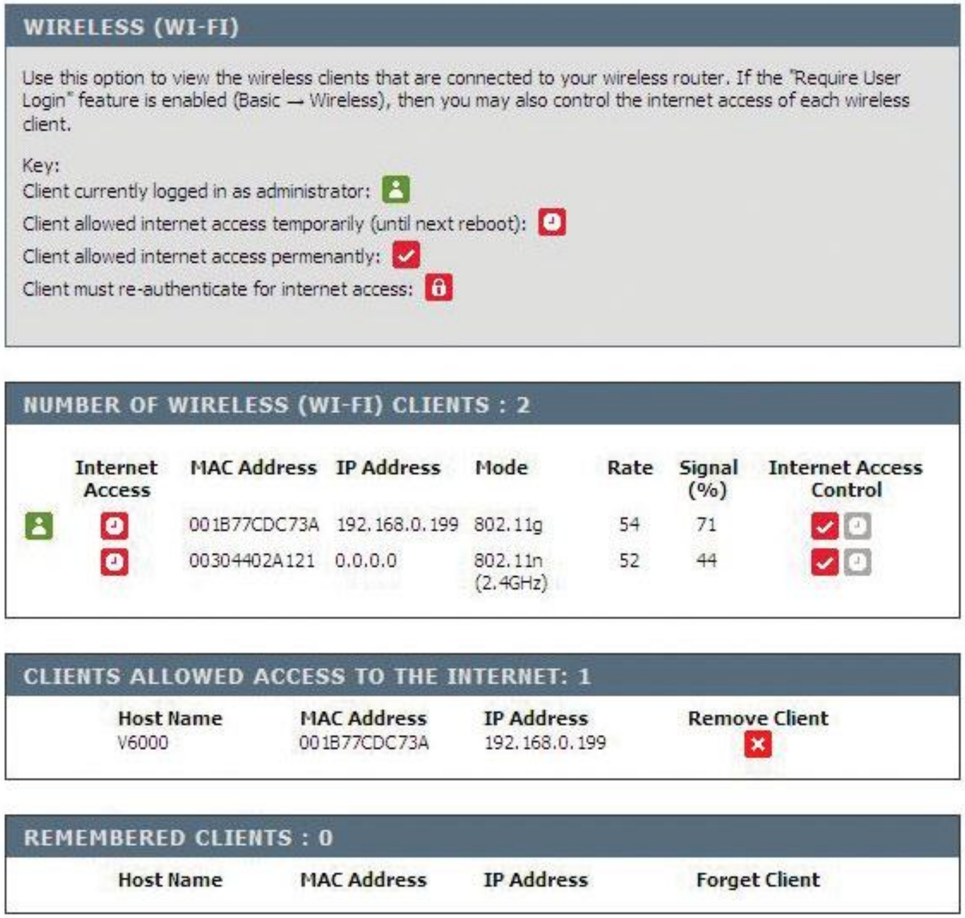
Mode. The transmission standard being used by the client. Values are 802.11a, 802.11b, 802.11g, or 802.11n.

Rate. The actual transmission rate of the client in megabits per second.

Signal. This is a relative measure of signal quality. The value is expressed as a percentage of theoretical best quality. 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.

If **Require User Login** is enabled then you can also control internet access privileges for the attached wireless clients.

(continued)



WIRELESS (WI-FI)

Use this option to view the wireless clients that are connected to your wireless router. If the "Require User Login" feature is enabled (Basic → Wireless), then you may also control the internet access of each wireless client.

Key:
Client currently logged in as administrator: 👤
Client allowed internet access temporarily (until next reboot): 🕒
Client allowed internet access permenantly: ✓
Client must re-authenticate for internet access: 🔒

NUMBER OF WIRELESS (WI-FI) CLIENTS : 2

	Internet Access	MAC Address	IP Address	Mode	Rate	Signal (%)	Internet Access Control
👤	🕒	001B77CDC73A	192.168.0.199	802.11g	54	71	✓ 🕒
	🕒	00304402A121	0.0.0.0	802.11n (2.4GHz)	52	44	✓ 🕒

CLIENTS ALLOWED ACCESS TO THE INTERNET: 1

Host Name	MAC Address	IP Address	Remove Client
V6000	001B77CDC73A	192.168.0.199	✕

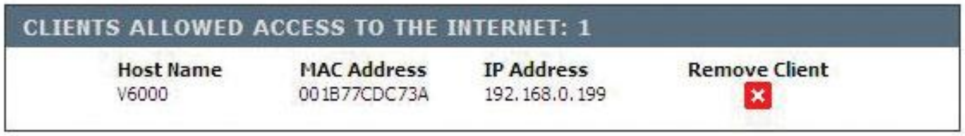
REMEMBERED CLIENTS : 0

Host Name	MAC Address	IP Address	Forget Client

8.6.2 Clients Allowed Access to the Internet

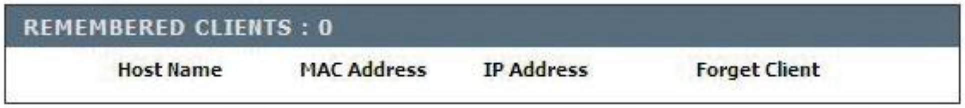
The control icons allow the administrator to grant access to the client computers. Access grants provide the same access as if a client went through the user login.

- Client allowed temporarily. Will have access until disconnected from the Wi-Fi network
- Client allowed permanently. Same as the **Remember Me** function in the user login process. Will have access each time connected to the Wi-Fi network.
- Client is not allowed. This client computer is denied access to the Wi-Fi network.



CLIENTS ALLOWED ACCESS TO THE INTERNET: 1

Host Name	MAC Address	IP Address	Remove Client
V6000	001B77CDC73A	192.168.0.199	☒



REMEMBERED CLIENTS : 0

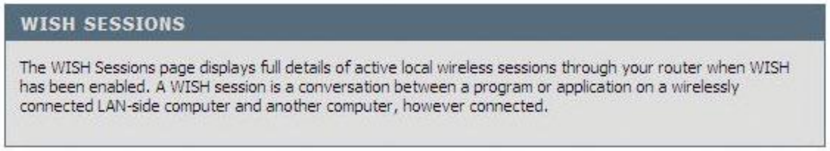
Host Name	MAC Address	IP Address	Forget Client

8.6.3 Remembered Clients

Once a Wi-Fi client has successfully logged into the Internet access side of the router, the MBR1200 can "remember" that Wi-Fi client by remembering its MAC address, eliminating the need to login each time. NOTE: Remembered Clients are "forgotten" if you reset the MBR1200 to its factory default.

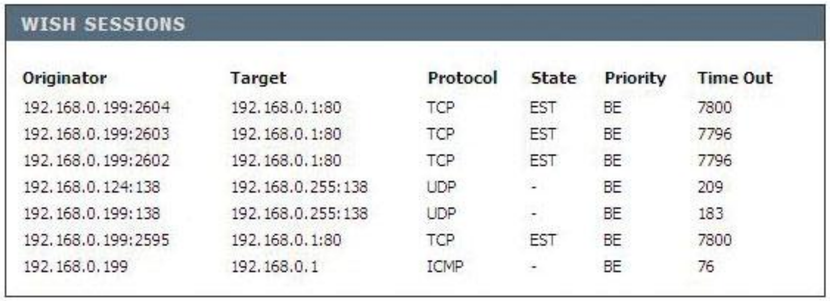
8.7 WISH Sessions

The WISH Sessions sub-menu displays full details of active local wireless sessions through your router when WISH has been enabled. A WISH session is a conversation between a program or application on a wirelessly connected LAN-side computer and another computer, however connected.



WISH SESSIONS

The WISH Sessions page displays full details of active local wireless sessions through your router when WISH has been enabled. A WISH session is a conversation between a program or application on a wirelessly connected LAN-side computer and another computer, however connected.



WISH SESSIONS

Originator	Target	Protocol	State	Priority	Time Out
192.168.0.199:2604	192.168.0.1:80	TCP	EST	BE	7800
192.168.0.199:2603	192.168.0.1:80	TCP	EST	BE	7796
192.168.0.199:2602	192.168.0.1:80	TCP	EST	BE	7796
192.168.0.124:138	192.168.0.255:138	UDP	-	BE	209
192.168.0.199:138	192.168.0.255:138	UDP	-	BE	183
192.168.0.199:2595	192.168.0.1:80	TCP	EST	BE	7800
192.168.0.199	192.168.0.1	ICMP	-	BE	76

Originator. The IP address and, where appropriate, port number of the computer that originated a network connection.

Target. The IP address and, where appropriate, port number of the computer to which a network connection has been made.

Protocol. The communications protocol used for the conversation.

State. State for sessions that use the TCP protocol.

- NO: None -- This entry is used as a placeholder for a future connection that may occur.
- SS: SYN Sent -- One of the systems is attempting to start a connection.
- EST: Established -- the connection is passing data.
- FW: FIN Wait -- The client system has requested that the connection be stopped.
- CW: Close Wait -- the server system has requested that the connection be stopped.
- TW: Time Wait -- Waiting for a short time while a connection that was in FIN Wait is fully closed.
- LA: Last ACK -- Waiting for a short time while a connection that was in Close Wait is fully closed.
- CL: Closed -- The connection is no longer active but the session is being tracked in case there are any retransmitted packets still pending.

Priority. The priority of the message flow is entered here. Four priorities are defined:

- BK: Background (least urgent).
- BE: Best Effort.
- VI: Video.
- VO: Voice (most urgent).

Time Out. The number of seconds of idle time until the router considers the session terminated. The initial value of Time Out depends on the type and state of the connection.

- 300 seconds. UDP connections.
- 240 seconds. Reset or closed TCP connections. The connection does not close instantly so that lingering packets can pass or the connection can be re-established.
- 7800 seconds. Established or closing TCP connections.

9 GLOSSARY

802.11

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

Access Control List

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

Access Point

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

ActiveX

A Microsoft specification for the interaction of software components.

Ad-hoc network

Peer-to-Peer network between wireless clients.

Address Resolution Protocol

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

ADSL

Asymmetric Digital Subscriber Line.

Advanced Encryption Standard

AES. Government encryption standard.

Alphanumeric

Characters A-Z and 0-9.

Antenna

Used to transmit and receive RF signals.

AppleTalk

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

AppleTalk Address Resolution Protocol

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

Application layer

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

ASCII

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

Attenuation

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

Authentication

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

Automatic Private IP Addressing

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

Backward Compatible

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

Bandwidth

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

Basic Input/Output System

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

Baud

Data transmission speed.

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.

DMZ

“Demilitarized Zone”. A computer that logically sits in a “no-mans-land” between the LAN and the WAN. The DMZ computer trades some of the protection of the router’s security mechanisms for the convenience of being directly addressable from the Internet.

DNS

Domain Name System: Translates Domain Names to IP addresses.

Domain name

A name that is associated with an IP address.

Download

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

DSL

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

Duplex

Sending and Receiving data transmissions at the same time.

Dynamic DNS service

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

Dynamic IP address

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

EAP

Extensible Authentication Protocol.

Email

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

Encryption

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

Ethernet

The most widely used technology for Local Area Networks.

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

Firmware

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

Fragmentation

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

FTP

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

Full-duplex

Sending and Receiving data at the same time.

Gain

The amount an amplifier boosts the wireless signal.

Gateway

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

Gbps

Gigabits per second.

Gigabit Ethernet

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

GUI

Graphical user interface.

H.323

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

Half-duplex

Data cannot be transmitted and received at the same time.

Hashing

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

Hexadecimal

Characters 0-9 and A-F.

Hop

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

Host

Computer on a network.

HTTP

Hypertext Transfer Protocol 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 is a WEB server and FTP server provided by Microsoft.

IKE

Internet Key Exchange is 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 which 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, that 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.

Mbps

Megabits per second.

MDI

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

MDIX

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

MIB

Management Information Base is 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 is used to secure data transmissions over PPTP connections.

MTU

Maximum Transmission Unit is 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 is 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 is the modulation technique for both 802.11a and 802.11g.

OSI

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

OSPF

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

Password

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

Personal Area Network

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

Physical layer

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

Ping

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

PoE

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

POP3

Post Office Protocol 3 is used for receiving email.

Port

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

PPP

Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line.

PPPoE

Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet.

PPTP

Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks.

Preamble

Used to synchronize communication timing between devices on a network.

QoS

Quality of Service.

RADIUS

Remote Authentication Dial-In User Service allows 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 it's 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 is 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.

SOHO

Small Office/Home Office.

SPI

Stateful Packet Inspection.

SSH

Secure Shell is a command line interface that allows for secure connections to remote computers.

SSID

Service Set Identifier is 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 is a utility used for transferring files that is simpler to use than FTP but with less features.

Throughput

The amount of data that can be transferred in a given time period.

Traceroute

A utility displays the routes between you computer and specific destination.

UDP

User Datagram Protocol.

Unicast

Communication between a single sender and receiver.

Universal Plug and Play

UPnP. A standard that allows network devices to discover each other and configure themselves to be a part of the network.

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.

URL

Uniform Resource Locator is 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.

Voice over IP

Sending voice information over the Internet as opposed to the PSTN

VoIP

Voice over IP.

Wake on LAN

Allows you to power up a computer though it's 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 is 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.

Wireless ISP

WISP. A company that provides a broadband Internet connection over a wireless connection.

WISP

Wireless Internet Service Provider.

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 Regulatory Information

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. This device must accept any interference received, including interference that may cause undesired operation. 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 and correct the interference by one or more 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 or television technician for help.*

Changes or modifications not expressly approved by CradlePoint, Inc. could void the user's authority to operate the product.

Radio Frequency Interference Requirement - Canada

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

10.2 Warranty Information

CradlePoint, Inc. warrants this product against defects in materials and workmanship to the original purchases (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.

Within thirty (30) days of receipt should the product fail for any reason other than damage due to customer negligence, purchaser may return the product to the point of purchase for a full refund of the purchase price.

If the purchaser wishes to upgrade or convert to another CradlePoint, Inc. product within the thirty (30) day period, purchaser may return the product and apply the full purchase price toward the purchase of the other product. Any other return will be subject to CradlePoint, Inc.'s existing return policy.

IN NO EVENT SHALL CRADLEPOINT'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS USER INTERFACE SOFTWARE, OR ITS DOCUMENTATION.

CradlePoint makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all user interface software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. CradlePoint reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity.

10.3 Specifications

MODEL NAME
MBR1200 Failsafe Gigabit Broadband N Router

WAN / INTERNET
3G/4G via Five Modem Ports (3 USB 2.0, 1 ExpressCard, 1 PC Card); One Ethernet Port (10/100/1000); One LAN Ethernet Port re-configurable to WAN for redundancy

LAN
WiFi 802.11 b/g/n, Four Ethernet Ports (10/100/1000)

ANTENNAS
internal WiFi antennas (300+ yards range), external antenna ports for optional antennas providing additional distance and performance

BUTTONS / SWITCHES
WiFi On/Off Switch, WPS Button (WiFi 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 (WiFi Protected Setup), Signal Strength

DIMENSIONS
9” x 5.1” x 1.57” (230mm x 130mm x 40mm)

CERTIFICATIONS
FCC, IC, CE, WiFi Alliance

OPERATING TEMPERATURE
0^{o}C to 50^{o}C

DETAILS

- 2.412 to 2.484 GHz WIFi 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, & WiMAX Cellular Network Devices
- Easy Management via HTTP and Remote Management via HTTP and SNMP
- Create, Manage, and Terminate Up To 5 IPSec VPN Sessions
- Supported VPN Implementations: MBR1x00 to MBR1x00, MBR1x00 to Cisco/Linksys Routers [1], MBR1x00 to Linux Systems [2]
- 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 [3]

[1] Tested against a Cisco 5500 running IKE Microcode: CNlite-MC-IPSEC-Admin-3.03 IPSec Microcode: CNlite-MC-IPSECm-MAIN-2.03

[2] Tested with Linux Kernel: 2.6.18 - 2.6.25; IKE (Racoon): 0.7.0 and 0.7.1

[3] No Stream Compression, LT2TP or PPTP Support

http://www.cradlepoint.com/