

Cable Modem/Router

Cable Modem *plus*
Dual-band Wireless-AC Router

U S E R M A N U A L



NOTICE

This document contains proprietary information protected by copyright, and this Manual and all the accompanying hardware, software, and documentation are copyrighted. No part of this document may be photocopied or reproduced by mechanical, electronic, or other means in any form.

The manufacturer does not warrant that the hardware will work properly in all environments and applications, and makes no warranty or representation, either expressed or implied, with respect to the quality, performance, merchantability, or fitness for a particular purpose of the software or documentation. The manufacturer reserves the right to make changes to the hardware, software, and documentation without obligation to notify any person or organization of the revision or change.

All brand and product names are the trademarks of their respective owners.

© Copyright 2014 Zoom Telephonics, Inc.

All rights reserved.

Safety Issues & Warnings

SAFETY

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

CAUTION:

- Do not put the cable modem in water.
- Do not use the cable modem outdoors.
- Keep the cable modem in an environment that is between 0°C and 40°C (between 32°F and 104°F).
- Do not place any object on top of the cable modem since this may cause overheating.
- Do not place the cable modem in a confined space that may cause overheating.
- Do not restrict the flow of air around the cable modem.
- Zoom Telephonics assumes no liability for damage caused by any improper use of the cable modem.

CONTENTS

CHAPTER 1 GETTING STARTED	6
Package Contents.....	6
CHAPTER 2 INSTALLING THE CABLE MODEM/ROUTER	8
CHAPTER 3 CONNECTING DEVICES TO THE CABLE MODEM/ROUTER..	14
<i>Establishing your Wireless Network</i>	<i>15</i>
<i>Connecting a Wireless-enabled Device (including the iPhone or other cellular phones, iPad or other tablets, the iPod Touch, etc.) to the Cable Modem/Router.....</i>	<i>17</i>
Connecting a Windows 8.1 or Windows 8 Computer with Built-in Wireless Capabilities	18
Connecting a Windows 7 Computer with Built-in Wireless Capabilities.....	19
Connecting a Windows Vista Computer with Built-in Wireless Capabilities	20
Connecting a Windows XP Computer with Built-in Wireless Capabilities.....	21
Connecting a Macintosh OS X Computer with Built-in Wireless Capabilities.....	22
Connecting a Computer with a Wireless adapter to the Cable Modem/Router	23
Using WPS as an alternative way to set up your Wireless Network.....	24
Connecting Additional Computers and/or Other Devices to the Cable Modem/Router's Ethernet/LAN ports	28
CHAPTER 4 CHANGING THE DEFAULT WIRELESS SETTINGS	29
About Wireless Security	29
Changing your Wireless Network Name (SSID) and Pre-Shared Key	30
Setting Up Security Using WEP	32
Disabling Security	33
CHAPTER 5 ONLINE GAMING	34
Gaming	34
DMZ Host.....	35
Port Triggers.....	37
CHAPTER 6 ADVANCED SETTINGS.....	40
Changing Default Settings.....	40
Accessing the Zoom Configuration Manager	41
Understanding the Configuration Manager Interface Screens.....	42
Configuration Manager Interface Menus	43
CHAPTER 7 STATUS PAGE.....	45
Status.....	45
CHAPTER 8 WIRELESS SETTINGS.....	46
Radio.....	46

Primary Network	49
Guest Network.....	53
Advanced	58
WPS	60
Bridging	62
Access Control	63
WMM (Wi-Fi Multimedia)	66
Neighbor APs	68
CHAPTER 9 BASIC MENU OPTIONS	70
Basic LAN Settings	70
DHCP	72
WAN Settings	73
My Network	75
CHAPTER 10 ADVANCED MENU OPTIONS	77
MAC Filtering	77
IP Filtering	79
Port Filtering	81
Port Forwarding	83
Port Triggers	85
DMZ Host	87
DDNS	89
RIP Setup	91
Options	93
CHAPTER 11 FIREWALL MENU OPTIONS	96
Basic	96
Event Log	97
CHAPTER 12 PARENTAL CONTROL MENU OPTIONS	103
Basic	103
User Setup	106
ToD Filter (Time of Day Filter)	109
Event Log	111
CHAPTER 13 VPN (VIRTUAL PRIVATE NETWORK) MENU OPTIONS	112
Basic Setting	112
IPSec	114
L2TP/PPTP	120
Event Log	122
CHAPTER 14 MANAGEMENT MENU OPTIONS	123
Admin Account	123
Remote Management	124
SNMP Event Log	125
Diagnostics	127

Backup/Restore Settings.....	129
CHAPTER 15 CABLE MODEM MENU OPTIONS.....	131
Cable Modem Device Information.....	131
Connection	133
Restart/Restore Factory/Frequency set.....	135
APPENDIX A: TROUBLESHOOTING TIPS.....	136
APPENDIX B: IF YOU NEED HELP	140
APPENDIX C: COMPLIANCE.....	141

1

Getting Started

This User Manual provides instructions for connecting and configuring your Model 5363 Cable Modem/Router and for setting up wireless and wired connections to Model 5363. This manual also includes details about security, firewalls, VPNs (Virtual Private Networks), administrative tasks, and troubleshooting.

Most users should use the Quick Start Flyer to install their cable modem. This User Manual is best used if you need to go beyond the Quick Start Flyer for some reason.

Package Contents

Your package contains the following items:

- Cable Modem/Router
- Power cube
- Ethernet RJ-45 cable
- Quick Start flyer

Before installing your cable modem, please read this.

You need to connect the cable modem to a cable modem service that uses any of the popular DOCSIS standards – 3.0, 2.0, or 1.1. If you need to get cable modem service, please speak with your cable service provider.

Your cable service provider will need to know your modem's **MAC ADDRESS**, which is **printed on a label on the bottom of your modem**. You provide this when you order cable modem service, or by calling the cable company before or after installing your modem, or by entering your CM MAC ADDRESS on an account setup web page that appears when you first connect your cable modem to your provider's network. Normally your cable service provider will tell you when to provide the CM MAC address. You may also be asked for your cable modem's model name and number, which is **ZOOM 5363**. If you need the modem's **serial number**, you can find it near the MAC address on the bottom label. Below is a guide to some of the chapters of this manual.

- If you haven't already set up your Cable Modem/Router using the Quick Start, go to [Chapter 2: Installing the Cable Modem/Router](#).
- If you have already installed your cable modem and want to learn more about how to connect both wired and wireless computers and other devices to your Cable Modem/Router go to: [Chapter 3: Connecting Devices to your Cable Modem/Router](#).
- Your Cable Modem/Router comes from the factory with a default SSID (Wireless Network Name), wireless security enabled and a random Pre-Shared Key (Wireless Password). These default settings for your modem/router are listed on the bottom label of your cable modem/router. Most users can simply use the default settings. You may want to change the wireless settings if you are replacing a wireless router and want to use the same wireless network name and wireless password as the existing router instead of changing all your wireless devices to use the Cable Modem/Router's defaults, or in the unlikely event that one of the wireless devices only supports WEP security. If you want to make changes to the default wireless settings, please refer to [Chapter 4: Changing your Wireless Settings](#).
- If you are using the Cable Modem/Router for online gaming and need to make changes to the router's firewall, please see [Chapter 5: Online Gaming](#).
- If you are like most users, you will **not** need to make changes to the Cable Modem/Router's advanced settings. If your setup requires you to make changes to advanced settings, go to [Chapter 6: Advanced Settings](#).

2

Installing the Cable Modem/Router

This chapter provides basic instructions for setting up your cable modem/router. This chapter is almost identical to the printed Quick Start.

If you are replacing an “old” cable modem, do this:

- 1 Disconnect the coaxial cable from the old cable modem and connect it to your Zoom modem. If the coaxial cable has a screw-on connector, turn the connector clockwise when tightening the cable onto the Zoom cable modem.
- 2 If there’s an Ethernet cable plugged into the old cable modem, unplug the Ethernet cable from the old cable modem and plug it into any of the Zoom cable modem’s LAN jacks.
- 3 Connect the Zoom power cube between the Zoom cable modem and a live power jack. DO NOT use your old cable modem’s power cube on your Zoom cable modem.
- 4 What you do next depends on your cable modem company. Typically you can call your cable modem company’s support department and tell them your cable modem is hooked up. They’ll normally ask for the information mentioned above in [Before installing your cable modem, please read this](#). Some cable companies also let you just open the browser on a computer that’s connected to the Zoom cable modem. A setup page comes up, and you follow the instructions.
- 5 Go to [Now that your cable modem is connected, do this](#) below.

If this is a first-time cable modem installation (that is, you are NOT replacing an “old” cable modem), do this:

- 1 Connect a “live” coaxial cable from your cable service provider to your cable modem. (If you’re not sure a cable is live, you can see whether you get a good

TV signal when that cable is used with a working TV set-top box.) Here are some ways you can get the live cable:



Coaxial Cable



Cable TV Jack

- You have a cable TV cable (“coaxial cable”) with a male connector on the end that isn’t connected to anything. This cable may be coming out of a wall or connected to a cable TV jack.
- There’s a cable TV jack in your wall. You can connect a cable TV “coaxial cable” between that jack and your cable modem. You may have a coaxial cable, possibly one that came with a cable modem starter kit from your cable service provider. If you don’t have a coaxial cable, you can get one at most electronics stores. You want one with a screw-in male F connector at each end, with a length that works for your installation.
- If you don’t have an available cable TV cable or wall jack, use a coaxial “T adapter” or “splitter” available from most electronics retailers.



Make sure you get one designed for cable modems and/or cable TV. These typically have one female IN jack and two female OUT jacks. You can disconnect a live cable from your TV set-top box and screw it into the IN jack of the splitter. Then connect one coaxial cable from an OUT jack to your TV set-top box and another coaxial cable from the other OUT jack to your cable modem. You can see that this approach uses one splitter and 2 additional coaxial cables, each of which has male connectors on each end. Some electronics retailers carry the Zoom

Cable Modem Connection Kit which has an excellent splitter and 2 coaxial cables packaged together at a reasonable price. You can also purchase splitters and coaxial cable separately if you prefer to do that, perhaps because you need a special length of coaxial cable.







- 2 Connect the supplied Ethernet cable between any cable modem LAN jack and a computer's Ethernet jack. We recommend that you do this even if you later plan to disconnect this computer. If connecting the Ethernet cable to a computer is difficult or impossible, you can make a wireless connection as discussed below in [Connecting your Cable Modem/Router wirelessly to some device](#).
- 3 Connect the Zoom power cube between the Zoom cable modem and a live power jack.
- 4 What you do next depends on your cable modem company. Typically you can call your cable modem company's support department and tell them your cable modem is hooked up. They'll normally ask for the information mentioned above in [Before installing your cable modem please read this](#). Some cable companies also let you just open the browser on a computer that's connected to the Zoom cable modem. A setup page comes up automatically, and you follow the instructions.
- 5 Go to [Now that your cable modem is connected, do this](#) below.

Now that your cable modem is connected, do this.

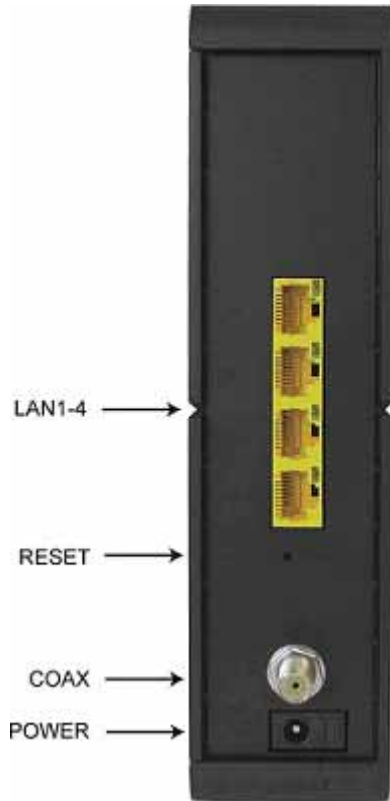
When your cable modem first connects to your cable service provider, allow 5 to 30 minutes for the cable modem to connect to the network. The cable modem uses this time to locate and connect to the appropriate channels for communication. You'll see the DS (downstream), US (upstream), and Online modem lights flashing until the Online light stays steady green to signal success. (Blue US/DS LEDs indicate channel bonding.)

- To check that your cable modem is working, open your browser and go to a familiar Web site. If it works, congratulations! Installation is complete for a single PC. For Internet access using a smartphone, tablet, or other wireless device, first see this chapter's [Connecting your Cable Modem/Router wirelessly to some device](#).
- If you want to connect additional computers or other devices using the modem/router's Ethernet/LAN ports, see this chapter's [Read this only if you are connecting additional computers and/or other devices to your Cable Modem/Router's Ethernet/LAN ports](#).
- If you are using the Cable Modem/Router for online gaming and need to make changes to the router's firewall, please see [Chapter 5: Online Gaming](#).
- If you are like most users, you will **not** need to make changes to the Cable Modem/Router's advanced settings. If your setup requires you to make changes to advanced settings, go to [Chapter 6: Advanced Setup](#).

Front Panel LEDs

LIGHT	COLOR	DESCRIPTION
 Power	Green	ON: Power is supplied to the Cable Modem/Router. OFF: Power is not supplied to the Cable Modem/Router.
 DS Receive Downstream sync	Green or Blue	Blinking: Scanning for downstream channel Green ON: Synchronized on 1 channel only Blue ON: Synchronized with more than 1 channel (Downstream Bond mode)
 US Send Upstream sync	Green or Blue	Blinking: Ranging is in progress. Green: Ranging is complete; operate on 1 channel Blue: Ranging is complete; operate on more than 1 channel (Upstream Bond mode) OFF: Upstream channel is inactive
 Online	Green	Blinking: Cable interface is acquiring IP address, time of day, and configuration ON: Cable Modem/Router is online OFF: Cable Modem/Router is offline
 Wireless or WPS	Green or Orange	ON: Wireless is enabled or Pairing completed successfully OFF: Wireless is not enabled Orange Blinking: WPS is in discovery mode (pairing)
 WPS Button		Pressing the WPS button initiates a WPS connection with other wireless devices.

Back Panel



LAN 1-4 (Gigabit Ethernet 1-4)

Four 10/100/1000 auto-sensing Ethernet ports for computers and other devices that have an Ethernet port.

RESET

Press and hold this recessed button at least 8 seconds in the unlikely event that you want to restore the default factory settings. This button is recessed to prevent accidental resets of your cable modem/router.

COAX

Connect your coaxial cable line to this port.

POWER

Connect the supplied power cube to this port

3

Connecting Devices to the Cable Modem/Router

This chapter explains how to connect devices (computers, phones, tablets, game stations, etc.) to the Cable Modem/Router. These devices can be connected either wirelessly or to one of the Ethernet ports on your Cable Modem/Router.

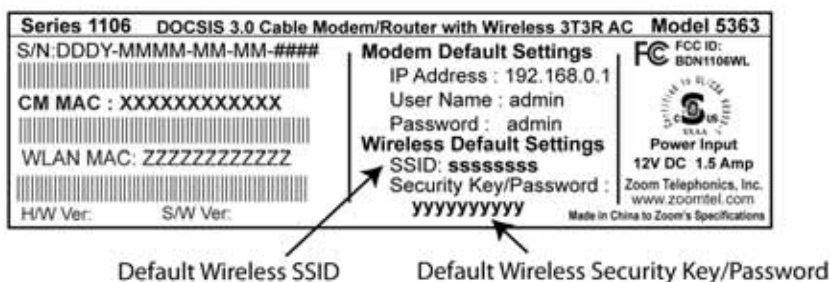
If you are connecting a computer or other device to an Ethernet LAN port of the Cable Modem/Router, please go to [Connecting Additional Computers and/or Other Devices to the Cable Modem/Router's Ethernet/LAN ports](#). If you are connecting one or more Wi-Fi compatible devices wirelessly to the cable modem/router, please continue below.

Connecting Wi-Fi compatible wireless devices to your Cable Modem/Router.

Your Cable Modem/Router comes pre-configured wireless settings as discussed below. Most users should simply use these default settings.

- WPA2-PSK/WPA-PSK security is enabled
- A random Pre-Shared Key (also called a security key or password) is assigned. The Security Key/Password is printed on the bottom label of your Cable Modem/Router.

Cable Modem Bottom Label:



- The default SSID (wireless network name) is assigned as **Zoomxxxx** (where xxxx are the last 4 hexadecimal characters of the cable modem CM MAC address). This SSID is printed on the bottom label of your cable modem/router. The SSID printed on your bottom label is the for the 2.4 GHz network. The SSID for the 5 GHz network is **Zoomxxxx_5G**.

Your Cable Modem/Router is capable of sending and receiving wireless data on both the 2.4GHz frequency band and the 5 GHz frequency band at the same time. Almost all computers, smartphones, tablets, and other client devices support the 2.4 GHz band, and some also support the 5 GHz band. A major advantage of the 5 GHz band is that it's normally much less crowded with other devices trying to use that band. This is especially important in areas with lots of wireless devices, such as some cities. To select Model 5363's 5 GHz network for a client device, pick the network ending in **5G**. You may want to try both SSIDs to see which one gives you better speed and range.

If you want to change these default settings please see [Chapter 4, Changing the Default Wireless Settings](#) before connecting your wireless computers or devices. You must use compatible wireless settings for each computer or device that you want to wirelessly connect to the Cable Modem/Router, as described below.

Establishing your Wireless Network

If all the computers or devices on your network support WPS, you can use WPS to easily set up your network. Windows 8, 8.1 and 7 support WPS. Non Windows devices typically have a button called WPS on them if they support WPS. (Note: Apple iPads, iPhones, and Macintosh computers do not support WPS as of March 2013.) Please see [Using WPS to set up your Wireless network](#) if you want to use WPS for wireless connections to your cable modem/router.

If some of the wireless devices do not support WPS, or if you do not know whether they do support WPS, you can configure each computer or device manually. To do that, select one of the possibilities for that computer or other device below:

- If you have a non-computer **wireless device like an iPhone or other cellular phone, iPad or other tablet, iPod Touch**, etc., see the instructions on page 17 for [Connecting a Wireless-enabled Device to the Cable Modem/Router](#).
- Many newer **Windows 8.1, 8, 7, Vista, and XP computers have built-in wireless networking** capabilities and do not require the installation of a wireless component. If this is the case, you should set up that computer's wireless connection using the Windows 8.1 or 8, 7, Vista, or XP connect utility. See the sections below on connecting [Windows 8.1 or 8](#) (page 18), [Windows 7](#) (page 19), [Vista](#) (page 20), or [XP](#)

(page 21) computers with built-in wireless capabilities.

- If you are using a Macintosh computer see the instructions on page 22 for [Connecting a Macintosh OS X Computer with Built-in Wireless Capabilities](#).
- Some older Windows computers may have **built-in wireless networking** capabilities, but not use the Windows 8, 7, Vista, or XP utility to configure wireless networking. If this is so, set up your computer's wireless connection using the instructions on page 23 for [Connecting a Computer with a wireless adapter to the Cable Modem/Router](#).
- Some **computers** may need a **wireless network adapter installed**. This can be a USB adapter, PC Card adapter, or PCI adapter. When you install the adapter, make sure that it is set to **infrastructure** or **access point** mode (NOT **ad-hoc** or **peer-to-peer** mode). If you need help installing your wireless adapter or setting its mode, refer to the documentation that came with it. After you install the adapter, see the instructions on page 23 for [Connecting a Computer with a wireless adapter to the Cable Modem/ Router](#).

Connecting a Wireless-enabled Device (including the iPhone or other cellular phones, iPad or other tablets, the iPod Touch, etc.) to the Cable Modem/Router

- 1 Select the wireless-enabled computer or device that you want to add to the network. The device should have software that will let it perform a **site search** to scan for available wireless networks in your area. You may have to click on something like **Settings** and then **Wi-Fi**. When the list of available wireless networks appears, click on **Zoomxxxx_5G** to connect to your Cable Modem/Router's 5 GHz network. If you do not see **Zoomxxxx_5G** then most likely your wireless adapter does not support the 5 GHz network, so click on **Zoomxxxx**. In both cases, xxxx are the last 4 characters of the cable modem CM MAC address. You can find **Zoomxxxx** printed on the bottom label of your Cable Modem/Router. In the unlikely event that you changed the SSID from the default, select your new SSID.
- 2 When prompted for the wireless password, enter your Pre-Shared Key (Security Key/Password) and click **Connect** or **Join**. Your Security Key/Password can be found on the bottom label of your Cable Modem/Router.

Tip!

If you need help, refer to the documentation that came with your wireless device.


- 3 Test your wireless connection. Open your device's Web browser (for instance, Internet Explorer, Firefox, or Chrome) and try to connect to a familiar Web address. If you are unable to connect, make sure you followed the instructions. If you did, please see [Appendix A: Troubleshooting Tips](#).

Your device is now connected to your wireless network. If you want to connect additional computers or devices, follow the instructions for your device by starting at the first page of this chapter.

To disconnect from the current network:

- 1 On your wireless device or computer, find the wireless network connection option (similar to the process of adding your device or computer to the network).
- 2 Select or click on **Disconnect**, **Forget**, **Forget this network** or similarly-named button. In doing this, you may need to select your SSID (wireless network name).

Connecting a Windows 8.1 or Windows 8 Computer with Built-in Wireless Capabilities


- 1 On the desktop, click the **Wireless Network Icon**  in your computer's notification area.
- 2 If available, click on **Zoomxxxx_5G** to connect to your Cable Modem/Router's 5 GHz network. If you do not see **Zoomxxxx_5G** than most likely your computer does not support the 5 GHz network, so go ahead and click on **Zoomxxxx**. In both cases, xxxx are the last 4 characters of the cable modem CM MAC address. You can find **Zoomxxxx** printed on the bottom label of your Cable Modem/Router. In the unlikely event that you changed the SSID from the default, select your new SSID.
- 3 Click **Connect**. If you want to connect to this network automatically in the future, check the **Connect Automatically** checkbox.
- 4 When prompted to enter your Network Security Key, enter your Pre-Shared Key (Security Key/Password) and click **Next**. Your Security Key/Password can be found on the bottom label of your Cable Modem/Router.
- 5 When asked "Do you want to turn on sharing between PCs and connect to devices on this network?" Click **Yes** to enable sharing and **No** to disable sharing. Sharing sets up your firewall to allow other users on your network to share files, folders or devices such as printers. Most users should select **Yes**. If you know you don't want to share files or devices, select **No**.
- 6 Test your wireless connection. Open your computer's Web browser and try to connect to a familiar Website. If you are unable to connect, make sure you followed the instructions. If you did, please see [Appendix A: Troubleshooting Tips](#).

Your computer is now connected to your wireless network. If you want to connect additional computers or devices, follow the instructions for your device by starting at the first page of this chapter.

To disconnect from the current wireless network:

- 1 Left-click the wireless network icon in the notification area of the Windows taskbar.
- 2 Left-click your SSID (wireless network name) and select **Disconnect**.

Connecting a Windows 7 Computer with Built-in Wireless Capabilities

- 1 Click the **Wireless Network Configuration** utility icon  in your computer's system tray.
- 2 If available, click on **Zoomxxxx_5G** to connect to your Cable Modem/Router's 5 GHz network. If you do not see **Zoomxxxx_5G** than most likely your wireless adapter does not support the 5 GHz network, so go ahead and click on **Zoomxxxx**. In both cases, xxxx are the last 4 characters of the cable modem CM MAC address. You can find **Zoomxxxx** printed on the bottom label of your Cable Modem/Router. In the unlikely event that you changed the SSID from the default, select your new SSID.
- 3 Click **Connect**. If you want to connect to this network automatically in the future, check the **Connect Automatically** checkbox.
- 4 When prompted to enter your Network Security Key, enter your Pre-Shared Key (Security Key/Password) and click **OK**. Your Security Key/Password can be found on the bottom label of your Cable Modem/Router.
- 5 Test your wireless connection. Open your computer's Web browser and try to connect to a familiar Website. If you are unable to connect, make sure you followed the instructions. If you did, please see [Appendix A: Troubleshooting Tips](#).

Your computer is now connected to your wireless network. If you want to connect additional computers or devices, follow the instructions for your device by starting at the first page of this chapter.

To disconnect from the current network:

- 1 Left-click the wireless network icon in the notification area of the Windows taskbar.
- 2 Left-click your SSID (wireless network name) and select **Disconnect**.

Connecting a Windows Vista Computer with Built-in Wireless Capabilities

- 1 From the **Start** menu select **Connect to**.
- 2 If available, click on **Zoomxxxx_5G** to connect to your Cable Modem/Router's 5 GHz network. If you do not see **Zoomxxxx_5G** than most likely your wireless adapter does not support the 5 GHz network, so go ahead and click on **Zoomxxxx**. In both cases, xxxx are the last 4 characters of the cable modem CM MAC address. You can find **Zoomxxxx** printed on the bottom label of your Cable Modem/Router. In the unlikely event that you changed the SSID from the default, select your new SSID.
- 3 Click **Connect**.
If a message pops up asking you to enter your PIN on the Zoomxxxx page, select "I want to enter the network key or passphrase instead." Then click **Next**.
- 4 When prompted to enter your Network Security Key, enter your Pre-Shared Key (Security Key/Password) and hit **Connect**. Your Security Key/Password can be found on the bottom label of your Cable Modem/Router.
- 5 In the **Successfully connected to [desired network]** dialog box, you have three options. You can:
 - Select **Save the network** and **Start this connection automatically** if you always want to connect to the same network. Then click **Close**. The next time you start your computer, you will automatically connect to the selected network.
 - Select **Save the network** and clear the **Start this connection automatically** check box if you don't want to *automatically* connect to this network every time you start your computer but you will want to *sometimes* connect to this wireless network in the future. Click **Close** to display the **Select a location . . .** dialog box where you choose a location. Windows Vista automatically applies the correct network security settings. If the **User Account Control** dialog box appears, click **Continue**.
 - Click **Close** to complete the connection procedure. Select this option if you are connecting to this network only one time.
- 6 Test your wireless connection. Open your computer's Web browser and try to connect to a familiar Website. If you are unable to connect, make sure you followed the instructions. If you did, please see [Appendix A: Troubleshooting Tips](#).

Your computer is now connected to your wireless network. If you want to connect additional computers or devices, follow the instructions for your device by starting at the first page of this chapter.

To disconnect from the current network:

- 1 From the Windows **Start** menu, select **Connect to**.
- 2 In the **Disconnect or Connect to another network** dialog box, select the current network and click **Disconnect**.
- 3 In the **Are You Sure?** message box, click **Disconnect** again.
- 4 In the next dialog box, you can connect to another network or click **Close** to complete the disconnect procedure.

Connecting a Windows XP Computer with Built-in Wireless Capabilities

- 1 On your Windows desktop, click the **Wireless Network Icon** in the System Tray.
- 2 If available, click on **Zoomxxxx_5G** to connect to your Cable Modem/Router's 5 GHz network. If you do not see **Zoomxxxx_5G** than most likely your wireless adapter does not support the 5 GHz network, so go ahead and click on **Zoomxxxx**. In both cases, xxxx are the last 4 characters of the cable modem CM MAC address. You can find **Zoomxxxx** printed on the bottom label of your Cable Modem/Router. In the unlikely event that you changed the SSID from the default, select your new SSID.
- 3 When prompted to enter your Network Security Key, enter your Pre-Shared Key (Security Key/Password) and click **Connect**. Your Security Key/Password can be found on the bottom label of your Cable Modem/Router.
- 4 Test your wireless connection. Open your computer's Web browser and try to connect to a familiar Website. If you are unable to connect, make sure you followed the instructions. If you did, please see [Appendix A: Troubleshooting Tips](#).

Your computer is now connected to your wireless network. If you want to connect additional computers or devices, follow the instructions for your device by starting at the first page of this chapter.

To disconnect from the current network:

- 1 On your Windows desktop, click the **Wireless Network Icon** in the System Tray.
- 2 Click **View Wireless Networks** button.
- 3 **Select** your SSID (wireless security name) and click **Disconnect**.

Connecting a Macintosh OS X Computer with Built-in Wireless Capabilities

- 1 Click the Wi-Fi icon in the menu bar. If the Wi-Fi icon does not appear on your menu bar, please refer to your built-in Macintosh documentation for how to enable wireless.



Note: On versions prior to OS 10.7 the **Wi-Fi** icon is called **AirPort**.

- 2 If available, click on **Zoomxxxx_5G** to connect to your Cable Modem/Router's 5 GHz network. If you do not see **Zoomxxxx_5G** than most likely your wireless adapter does not support the 5 GHz network, so go ahead and click on **Zoomxxxx**. In both cases, xxxx are the last 4 characters of the cable modem CM MAC address. You can find **Zoomxxxx** printed on the bottom label of your Cable Modem/Router. In the unlikely event that you changed the SSID from the default, select your new SSID.
- 3 When prompted for the password in the next dialog box, enter your Pre-Shared Key (Security Key/Password) and click **Join**. Your Security Key/Password can be found on the bottom label of your Cable Modem/Router.
- 4 Test your wireless connection. Open your computer's Web browser and try to connect to a familiar Website. If you are unable to connect, make sure you followed the instructions. If you did, please see [Appendix A: Troubleshooting Tips](#).

Your computer is now connected to your wireless network. If you want to connect additional computers or devices, follow the instructions for your device by starting at the first page of this chapter.

To disconnect from the current network:

- 1 Click the Wi-Fi icon on the menu bar.
- 2 Select **Turn Wi-Fi Off** (OS 10.7 or later) or **Turn AirPort Off** (OS versions prior to 10.7) to disconnect from the router.

Connecting a Computer with a Wireless adapter to the Cable Modem/Router

- 1 Go to the computer that is set up with a wireless adapter that you want to add to the network. For many wireless adapters, you will use their configuration manager software and click a **Scan** button or select a **Site Scan**, **Scan Networks**, or other similarly named tab to do a site search. When the list of available wireless networks appears, click on **Zoomxxxx_5G** to connect to your Cable Modem/Router's 5 GHz network. If you do not see **Zoomxxxx_5G** than most likely your wireless adapter does not support the 5 GHz network, so go ahead and click on **Zoomxxxx**. In both cases, xxxx are the last 4 characters of the cable modem CM MAC address. You can find **Zoomxxxx** printed on the bottom label of your Cable Modem/Router. In the unlikely event that you changed the SSID from the default, select your new SSID.

If you need help, refer to the documentation that came with your wireless adapter.

Note for Windows 8.1, 8, 7, Vista and XP users: If you installed a wireless adapter on a Windows 8, 7, Vista or XP computer, Windows may try to automatically configure the adapter (rather than let you use the software provided with the wireless adapter). You will know this is happening because you will be prompted with a message about one or more wireless networks being available. You will also be able to click a link to open the **Wireless Network Connection Properties** dialog box. If this happens, click the link, clear the **Use Windows to configure my wireless network settings** check box, and then click **OK**. You can then use the software provided with your wireless adapter without interruption from Windows.

- 2 When prompted for the wireless password, enter your Security Key/Password and hit **Connect**. Your Security Key/Password can be found on the bottom label of your Cable Modem/Router.
- 3 Test your wireless connection. Open your device's Web browser (for instance, Internet Explorer, Firefox, or Chrome) and try to connect to a familiar Web address. If you are unable to connect, make sure you followed the instructions. If you did, please see [Appendix A: Troubleshooting Tips](#).

Your device is now connected to your wireless network. If you want to connect additional computers or devices, follow the instructions for your device by starting at the first page of this chapter.

To disconnect from the current network:

- 1 On your computer that has a wireless adapter, find the wireless network connection option (similar to the process of adding your computer to the network).
- 2 Click or highlight the Cable Modem/Router's SSID.

- 3 Select or click on **Disconnect** or similarly-named button.

Using WPS as an alternative way to set up your Wireless Network

If all the Wi-Fi compatible wireless devices on your network support WPS, you can choose to quickly setup your wireless network by pushing the WPS button on your cable modem/router and on each wireless device connecting to your cable modem/router.

Windows 8 and Windows 7 users should follow the instructions below: Other computers or devices such as tablets should go to [If you are using a non Windows computer or other device that supports WPS.](#)

If you are using a Windows 8.1, 8 or 7, computer:

- 1 On your desktop, open **Connect to a Network** on that computer by left-clicking the network icon in the notification area of the Windows taskbar.
- 2 A list of available networks is displayed.
- 3 Typically you then click **Zoomxxxx_5G** to connect to your Cable Modem/Router's 5 GHz network. If you do not see **Zoomxxxx_5G** than most likely your wireless adapter does not support the 5 GHz network, so go ahead and click on **Zoomxxxx** where xxxx are the last 4 hexadecimal characters of the cable modem CM MAC address. **Zoomxxxx** is the SSID printed on the bottom label of your Cable Modem/Router. In the unlikely event that you changed the SSID from the default, select your new SSID.
- 4 You will see a screen with a text box for the Security key. If WPS configuration is supported, you may see a message such as *You can also connect by pushing the button on the router.* If you see this message, continue at step 5 below.



Windows 7



Windows 8.1 or Windows 8

- 5 Press the Wi-Fi Protected Setup (WPS) button on the router for at least 3 seconds. (You do not need to type a security key or passphrase in the Security key text box on your Windows machine). The Cable Modem/Router will automatically set up the computer to connect to the network and apply the network's security settings.

When asked “**Do you want to turn on sharing between PCs and connect to devices on this network?**” Click **Yes** to enable sharing and **No** to disable sharing. Sharing sets up your firewall to allow other users on your network to share files,

folders or devices such as printers. Most users should select **Yes**. If you know you don't want to share files or devices, select **No**.

Repeat steps 1-5 above for each Windows computer you want to connect to the Cable Modem/Router. If you want to connect a non Windows computer or another device such as a tablet, follow the instructions below.

If you are using a non Windows computer or other device that supports WPS

Please refer to the instructions for your device for more information on using WPS. The directions below should work for most users.

- 1 Press the **WPS** LED pushbutton on the front panel of the router for at least 3 seconds. The WPS LED should blink orange.
- 2 Within 2 minutes (before the WPS LED orange light turns off), press the WPS button on the device that you're linking wirelessly to the modem/router. The button may be a physical pushbutton on the device or a button on a page of the device's wireless network configuration menus.
- 3 Congratulations! You should now have a secure connection between your Cable Modem/Router and a device. Now is a good time to check that your device's Internet connection is working. Open your browser and go to a familiar Web site. If you are able to connect, continue with the next step below.
If you are not able to connect to the Internet, please see [Appendix A: Troubleshooting Tips](#).
- 4 If you have other devices whose WPS security you need to set, repeat steps 1 through 3 for each device. When they are finished, the basic setup for these local wireless devices should be complete.

Connecting Additional Computers and/or Other Devices to the Cable Modem/Router's Ethernet/LAN ports

You can plug up to four computers, game consoles, or other Ethernet-capable devices into the Cable Modem/Router's LAN ports. For information about your specific device, please refer to the documentation that came with that device. Follow the instructions below for each computer or other device.

- 1 If you connected the Cable Modem/Router to a computer using a wired connection when setting up the Cable Modem/Router, unplug the computer now if you don't want that computer to stay connected to the Cable Modem/Router.
- 2 To connect a computer or other Ethernet-capable device, plug one end of an Ethernet cable into an available Ethernet (LAN 1, 2, 3, or 4) port on the Cable Modem/Router and plug the other end of the Ethernet cable into the Ethernet port of the additional device you want to connect to the Cable Modem/Router. (If you are connecting a hub or a switch, this is typically called an Uplink or Expansion port.) **If you are connecting a computer or game station, go to step 5 of this section.**
- 3 If you are connecting a network device such as a switching hub, use the instructions that came with that device. Then reboot any computer that is part of your network. For example, if you connected a switching hub, reboot any computer that will be connected to that switching hub.
- 4 If you are connecting a HomePlug adapter pair with one adapter plugged into the Cable Modem/Router and an AC outlet, and the other adapter plugged into a computer, game station, or other device and an AC outlet, make those connections and then go to step 5.
- 5 Verify that your Internet connection is working. Open a Web browser on each computer that's using your network and try to connect to a familiar Web address.

Congratulations! You have connected an additional device to the Internet. You can connect up to 4 Ethernet-capable devices to the Cable Modem/Router, following the instructions above for each device by starting at step 2 of this section.

4

Changing the Default Wireless Settings

*Your Cable Modem/Router comes from the factory with a default SSID (Wireless Network Name), **WPA-PSK/WPA2-PSK** wireless security and a random Wireless Security Key (Wireless Password). These default settings for your router are listed on the bottom label of your unit. Most users can go ahead and use the default settings.*

You may want to change your wireless settings if the wireless devices on your network are already configured to use an existing wireless network name and password. Instead of having to reconfigure all the devices on your network, you can change the Cable Modem/Router to match the existing settings used by your devices. Read this chapter if you want to use another wireless security mode, or if you want to change either the SSID or Wireless Security Key. If you want to use the default wireless settings, you can skip this chapter.

About Wireless Security

There are two basic wireless security modes, WPA and WEP. There are two versions of WPA: WPA and WPA2. When configured as part of a typical home or small office network, WPA and WPA2 require a Pre-Shared Key, or PSK. These modes are typically called WPA-PSK and WPA2-PSK, respectively, though sometimes they're just called WPA and WPA2. You can enable either WPA-PSK or WPA2-PSK alone, or you can enable both WPA-PSK and WPA2-PSK together. By default, your Cable Modem/Router has both WPA-PSK and WPA2-PSK enabled. You will only need to change the security mode if you know that you have a device you are connecting to your wireless network that only supports WEP go to [Setting up Security using WEP](#). In the unlikely event that you want an unsecured network, this is discussed late in this chapter in [Disabling Security](#).

Note: If you have a Radius Server (very unlikely for a home network), select the WPA/WPA2 options without PSK. All instances of WPA and/or WPA2 that follow refer to WPA-PSK and/or WPA2-PSK unless noted otherwise.

You can check to see if all other clients that you plan to put on the network support WPA or WPA2. You can do this by checking the manual that came with each device or by checking the configuration software for the installed device. Look under **Security** or **Encryption** or **Setup** or **Advanced Features**. Most devices will support one of these modes.

- To change the Wireless Network Name (SSID) or Wireless Security Key (Pre-Shared key) used by your Cable Modem/Router go to [Changing your Wireless Network Name\(SSID\) and Pre-Shared Key](#).
- If any of the devices you want to connect to your wireless network do not support WPA or WPA2, go to [Setting Up Security Using WEP](#).
- If you need to set up an unsecured network, see [Disabling Security](#).

Changing your Wireless Network Name (SSID) and Pre-Shared Key

Most likely your previous wireless network used 802.11n. If you want to change your Cable Modem/Router settings to match your existing network settings follow the steps below. If you have newer devices that support 802.11ac then you should connect to the Cable Modem/Router's 5G network. For instructions on connecting to the 5G network refer to [Chapter 3, Connecting other Devices to the Cable Modem/Router](#).

To check if your device supports 801.11ac, you can scan for available wireless networks on your device. If you see a wireless network named **Zoomxxxx_5G** than your devices supports 802.11ac and you should follow the instructions for connecting that device to the Cable Modem/Router found in Chapter 3. If you only see **Zoomxxxx** then your device does not support 802.11ac. In both cases, xxxx are the last 4 characters of the cable modem CM MAC address. You can find **Zoomxxxx** printed on the bottom label of your Cable Modem/Router.

- 1 Open the Zoom Configuration Manager by typing the following in your Web browser's address bar: **http://192.168.0.1**
- 2 In the **Login** dialog box, type the following User Name and Password in lower case, then click **Login**.

User Name: **admin**
Password: **admin**

- 3 Click **Wireless** on the top menu.
- 4 The Wireless Radio page appears. Under Select 2.4 or 5 GHz option. Select 2.4 GHz if your existing wireless network used 802.11n. If your existing network used 802.11ac or you just want to change the SSID for the 802.11ac network select 5 GHz. Click Apply.
- 5 Then click **Primary Network** on the left-side menu and in the text box labeled **Network Name (SSID)**, type an SSID of your choice. The SSID needs to be at least one character long, and it's probably best to pick a name that you'll recognize as yours.
- 6 To change the wireless security, start by setting all the following drop-down menus to Disable: WPA, WPA-PSK, WPA2, and WPA2-PSK.
- 7 Then select Enable for the mode(s) you choose for setting wireless security.

Note: To use WPA2 /WPA, **all** of the wireless devices on your network must support either encryption method. In this case, enable:

- WPA-PSK and WPA2-PSK (if you want to use a Pre-Shared Key)
- or
- WPA and WPA2 (use this only if your network uses a Radius Server. This is very uncommon for a home network)

If you know that all your devices support the more secure WPA2 you can enable WPA2 only (or WPA2-PSK if you want to use a Pre-Shared Key) instead of WPA and WPA2.

- 8 In the **WPA Pre-Shared Key** text box (only if you selected an option requiring a Pre-Shared Key), enter a passphrase of your choice (a minimum of 8 characters). Write down this passphrase and put it where you can find it – on the bottom of the Cable Modem/Router case, for instance.
- 9 Click **Apply**.
- 10 Now you may need to set up each of your wireless devices with the SSID and passphrase. If your devices were already setup with this SSID and passphrase then your setup should be complete, otherwise, see [Chapter 3. Connecting other Devices to the Cable Modem/Router](#) for help on connecting your wireless computers and devices.

Your security setup configuration is now complete!

Setting Up Security Using WEP

If **any** of your network devices DOES NOT support WPA or WPA2, you can use WEP to configure network security. WEP can be configured two ways: 64-bit and 128-bit. 128-bit WEP provides more security than 64-bit.

- 1 Open the Zoom Configuration Manager by typing the following in your Web browser's address bar: **http://192.168.0.1**
- 2 In the **Login** dialog box, type the following User Name and Password in lower case, then click **Login**.

User Name: admin Password: admin

- 3 Click **Wireless** on the top menu.
- 4 The Wireless Radio page appears. Under Select 2.4 or 5 GHz option. Select 2.4 GHz and click Apply.
- 5 Then click **Primary Network** on the left-side menu.
- 6 To change the wireless security, start by setting the following drop-down menus to Disable: WPA, WPA-PSK, WPA2, and WPA2-PSK
- 7 From the **WEP Encryption** drop-down menu, select **WEP-64 bit (or WEP-128 bit for more security)**.
- 8 For **Network Key 1**, you can either enter your own WEP Key or you can have WEP Keys generated.

If you are entering a network key of your choice, enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

Otherwise, type something into the text box and click on **Generate WEP Keys** and WEP Keys will automatically be generated for you.

Caution! Do not click **Apply** until you have entered WEP Keys.

- 9 Click **Apply**.
- 10 Now you need to set up each of your wireless devices with the SSID and passphrase. See [Chapter 3, Connecting other Devices to the Cable Modem/Router](#) for help on connecting your wireless computers and devices.

Your security setup configuration is now complete!

Disabling Security

If for some reason you need to set up an unsecured network, you will need to disable the default security that is currently set up for your Cable Modem/Router. Follow the instructions below.

- 1 Open the Zoom Configuration Manager by typing the following in your Web browser's address bar: **http://192.168.0.1**
- 2 In the **Login** dialog box, type the following User Name and Password in lower case, then click **Login**.

User Name: admin Password: admin

- 3 Click **Wireless** on the top menu.
- 4 The Wireless Radio page appears. Under Select 2.4 or 5 GHz option, choose 5 GHz and click Apply.
- 5 Then click **Primary Network** on the left-side menu.
- 6 Set all the following drop-down menus to Disable: WPA, WPA-PSK, WPA2, and WPA2-PSK.
- 7 Click **Apply**.
- 8 Click Wireless Radio on the left-side menu. Under Select 2.4 or 5 GHz option, choose 2.4 GHz and click Apply. Repeat steps 5-7 to disable security on the 2.4 GHz band.

That's it! You have now disabled security.

5

Online Gaming

Read this chapter if you are going to use your Cable Modem/Router for online gaming. Some online games require you to make changes to your firewall. This chapter explains the different ways you can modify the firewall to allow your online gaming system access.

Gaming

If you are using your router for gaming, you may need to make changes to the router's firewall setting for the game to work. This is done by setting up a **DMZ** or using **Port Triggering** so that the Cable Modem/Router's firewall won't block the other players from your system during your gaming. The main difference between the methods is the amount of access someone has to your system.

A DMZ allows access on all ports of the computer. Because of this, DMZ's are less secure and should be used with caution with your computer. However DMZ's work well with gaming stations since security is not as much of an issue for gaming stations as it is for computers.

Port triggering works by sensing when data is sent out on a predetermined outgoing port and then automatically opening up the corresponding incoming port(s). It will automatically forward the traffic on the incoming port to the computer that accessed the outgoing port. If your game uses one port to send outgoing data and a different port (or ports) for incoming data, you may want to use port triggering. You do not need to know the IP address of your gaming station to set up port triggering. You will need to know which ports your game requires you to open. This information is usually available with your gaming software or you should be able to find it by searching for it on the web.

- If you want to set up a DMZ for your gaming system, go to [DMZ Host](#).
- If you want to set up Port Triggering for your gaming system, go to [Port Triggering](#).

DMZ Host

The DMZ (De-militarized Zone) Host page allows you to configure a network device (e.g. a PC or gaming system) to be visible directly to the Internet. This may be used if a game doesn't work with port triggers or if you are using a gaming system, where security is less of a concern.

To set up a DMZ for your gaming system, you should first assign your gaming system a static IP address. Normally the Cable Modem/Router handles assigning IP addresses to the different devices on your network using DHCP. However DHCP does not guarantee that your device will always get assigned the same IP address. The DMZ needs to know the IP address of your gaming system to work, if the IP address changes the DMZ will not work. Because your IP address could change over time you need to assign a static IP on your gaming system. To setup a static IP address on your gaming system, please refer to your gaming system's documentation. If you no longer have the documentation that came with your gaming system it usually can be found online.

When assigning a static IP address to your gaming system you should select an address that is outside the IP addresses assigned by the Cable Modem/Router's DHCP server. By default the DHCP Server assigns addresses from 192.168.0.10 to 192.168.0.255. We recommend using 192.168.0.5 as the static IP address for your gaming system.

To setup a **DMZ** for your gaming system:

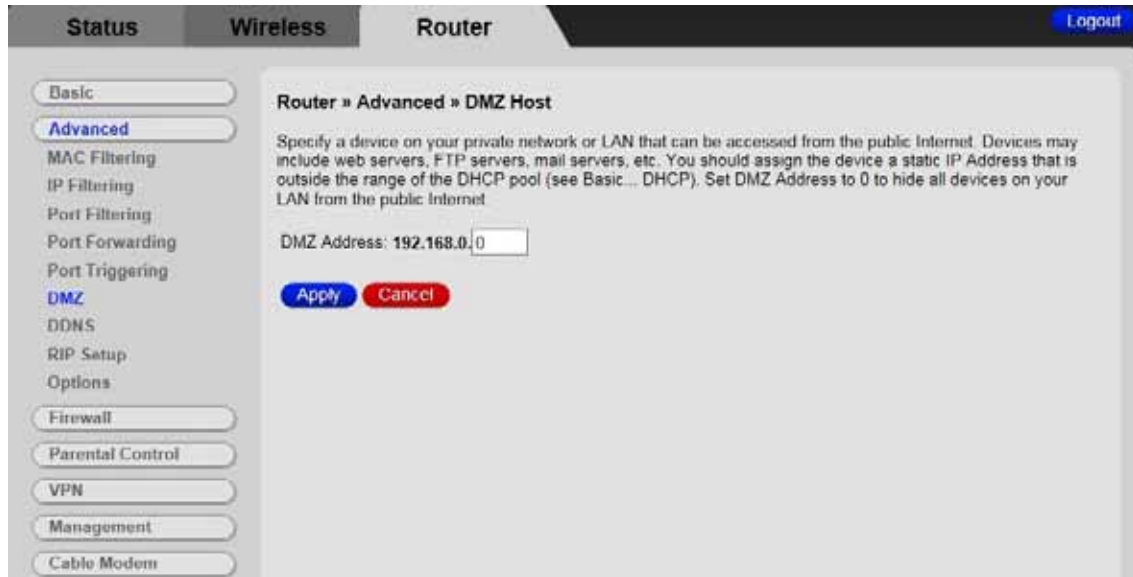
- 1 Follow the instructions for your gaming system to assign a static IP address. We recommend using 192.168.0.5.
- 2 Next access the Cable Modem/Routers configuration menu by launching a Web browser on a computer that is directly connected to one of the router's LAN ports.
- 3 In the browser address bar, type **http://192.168.0.1** and press the **Enter** key.
- 4 In the Login screen, enter:

default username: admin default password: admin
--

Both the username and password are case sensitive. The default username and password are printed on the bottom label of your unit.

- 5 Click the Login button to access the Cable Modem/Router. The **Status** page appears.
- 6 Click **Router** menu tab.

7 Then click the **Advanced / DMZ**. The **DMZ Host** page appears:



8 Enter the last byte of the LAN IP address of the static IP address you assigned to your gaming system. For example if you assigned 192.168.0.5 enter **5**.

9 Click **Apply**.

Your gaming system should now work with all your online games.

Port Triggers

Port Triggering works by sensing when your game sends data out through a specific port. The outgoing data signals the router to allow the incoming game traffic to be passed through the firewall on the correct port. Since the ports are only open when you are gaming, port triggering is a very secure method for online gaming.

To set up port triggering you need to know what ports your game is using and whether they use TCP, UDP or both on those ports. Typically this should be included with your gaming software. If it is not included, try entering the name of your gaming software followed by "ports used".

Some games use the same ports for both incoming and outgoing traffic, while other games use different ports for incoming and outgoing traffic.

Below is an example of setting up the popular game, World of Warcraft® for port triggering. Looking online, we find that World of Warcraft uses the following ports: 1119-1120, 3724, 4000, 6112-6114, and 6881-6999. We can also find out that these ports are all TCP. In this case the same ports are used for both incoming and outgoing traffic, so we would use the same ports as both the triggering port and the target port as shown below.

To setup **port triggering** for World of Warcraft:

- 1 Launch a Web browser.
- 2 In the browser address bar, type **http://192.168.0.1** and press the **Enter** key.
- 3 In the Login screen, enter:

default username: admin default password: admin
--

Both the username and password are case sensitive. The default username and password are printed on the bottom label of your unit.

- 4 Click the Login button to access the Cable Modem/Router. The **Status** page appears.
- 5 Click the **Router** menu tab.
- 6 Then click **Advanced / Port Triggering**. On the **Port Triggering** page, click on **Create Rule**. The following page appears.



- 7 We will need to setup 5 triggers for World of Warcraft. The first rule would cover ports 1119-1120. Enter 1119 in the **Trigger Start Port** field and 1120 in the **Trigger End Port** field. Since these ports are used to send data both directions enter 1119 in the **Target Start Port** and 1120 in the **Target End Port**.
- 8 Select **TCP** in the **Protocol** drop down menu since these ports use TCP.
- 9 Enter a name for this rule, for example WOW1. Select **ON** to enable, then click **Apply**. Your new rule will appear in the table.
- 10 Repeat steps 7-9 for the next rule. In this case only one port is used, 3724. Enter 3724 in the **Trigger Start/End Port** and **Target Start/End Port** fields.
- 11 Repeat steps 7-9 for the remaining ports that need to be opened. When you are complete the table should look like this:

Status Wireless Router Logout

Basic
Advanced
 MAC Filtering
 IP Filtering
 Port Filtering
 Port Forwarding
Port Triggering
 DMZ
 DDNS
 RIP Setup
 Options

Firewall
 Parental Control
 VPN
 Management
 Cable Modem

Router » Advanced » Port Triggering

Configure dynamic triggers for specific devices on the LAN. This supports applications with bi-directional traffic that require specific port numbers to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these settings. Click Apply to save your configuration.

Create Rule

Trigger		Target		Prot	Description	Enabled	Delete All	
Start Port	End Port	Start Port	End Port				Modify	Delete
1119	1120	1119	1120	TCP	WOW1	Yes	Modify	Delete
3724	3724	3724	3724	TCP	WOW2	Yes	Modify	Delete
4000	4000	4000	4000	TCP	WOW3	Yes	Modify	Delete
6112	6114	6112	6114	TCP	WOW4	Yes	Modify	Delete
6881	6999	6881	6999	TCP	WOW5	Yes	Modify	Delete

If your online game does not work and you are sure that you entered the correct ports on the port triggering page, check to see if you have a firewall running on your computer that is preventing you from playing your online game. This firewall may be either the built-in Windows firewall or may be part of a third party security package you are using on your computer. You will need to allow access through these firewalls to be able to play your online game.

6

Advanced Settings

Advanced Settings is primarily for technically advanced users. For most people, the options that are set by default when the Cable Modem/Router is installed are sufficient.

*However, those who want or need to change the default settings can do so using the advanced setup pages in the **Zoom Configuration Manager**.*

This chapter includes:

- *Suggestions for settings that you might want to change*
- *Instructions for launching the Zoom Configuration Manager program*
- *An overview of the available configuration menus and settings and a guide on what chapter to go to for more information on each settings.*

Changing Default Settings

Here are some reasons why you might want to use the Configuration program to change the router's default settings.

- Your Cable provider instructs you to enable, disable, or change the default settings for your router
- You want to set up a wireless guest network to give users access to the internet but not your internal network.
- You want to change the default firewall settings to block particular IP addresses and intrusive hosts.
- You want to access your corporate network and need to use the built-in VPN function.
- You wish to control the hours that a user on your network can access the Internet.

Accessing the Zoom Configuration Manager

From your Web browser, you will log in to the interface to define system parameters, change password settings, view status windows to monitor network conditions, and control the Cable Modem/Router and its ports.

To access the Zoom Configuration Manager, use the following procedure:

- 1 Launch a Web browser.

Note: Your computer does not have to be online to configure your Cable Modem/Router.

- 2 In the browser address bar, type **http://192.168.0.1** and press the **Enter** key.

For example:



The Login screen appears (see Figure 1).

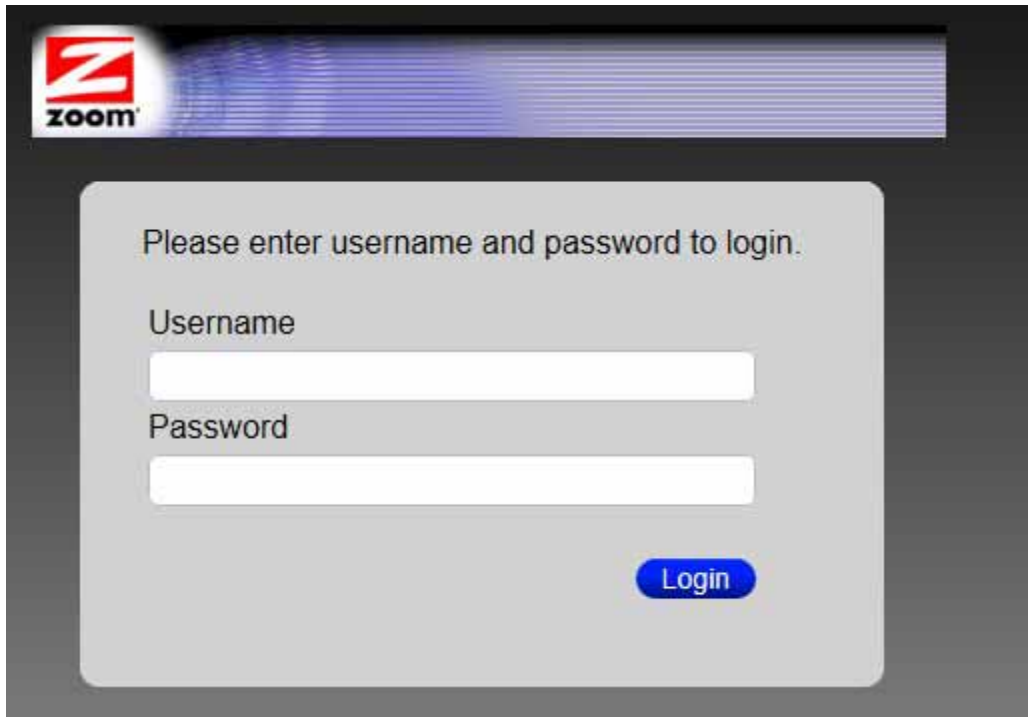


Figure 1. Login Screen

- 3 In the Login screen, enter:

default username: admin default password: admin
--

Both the username and password are case sensitive. The default username and password are printed on the bottom label of your unit. After you log in to the Zoom Configuration Manager interface, you can change the default password on the **Management – Admin Account** page.

- 4 Click the Login button to access the Cable Modem/Router. The **Status** page appears, showing information about your Cable Modem/Router.

Understanding the Configuration Manager Interface Screens

The top of the management interface contains three tabs you use to select menus for configuring the Cable Modem/Router. When you click a menu item, information and any configuration settings associated with the menu appear in the main area of the interface (see Figure 2). If the displayed information exceeds what can be shown in the main area, scroll bars appear to the right of the main area so you can scroll up and down through the information.

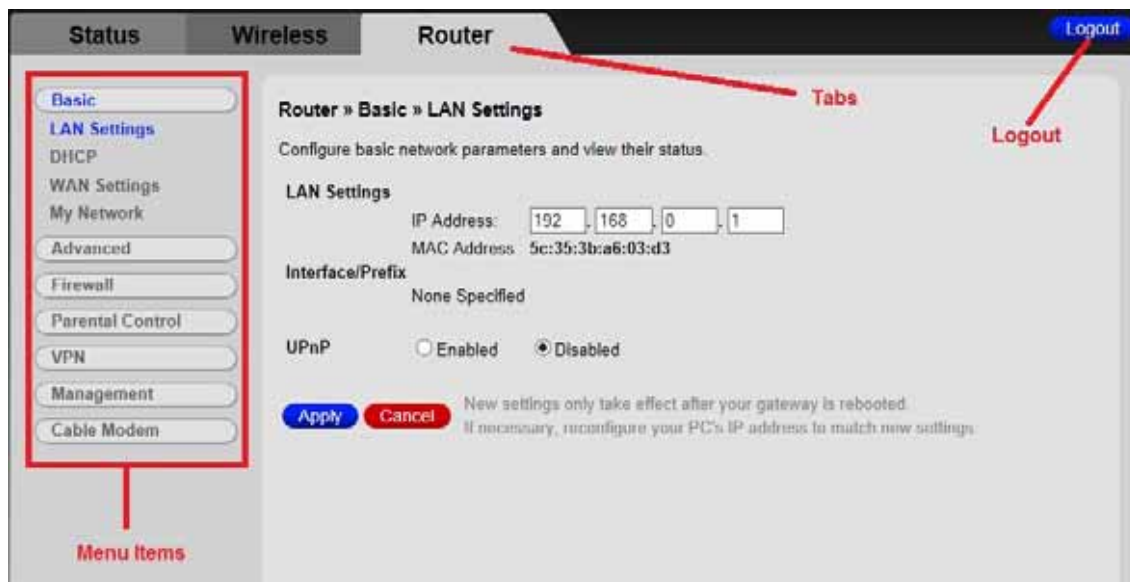


Figure 2. Main Areas on the Configuration Manager Interface

In the upper right hand corner of the page is the logout option. Click it to log out from the Configuration Manager interface.

Configuration Manager Interface Menus

You can skip to specific sections of this User Manual based on your intended use of the Cable Modem/Router. Each of the menu options in your Configuration Manager is covered as a separate chapter in the remaining portions of the User Manual.

- For a description of the Status Tab see [Chapter 7: Status Page](#).
- To configure and use the wireless features supported by the Cable Modem/Router see [Chapter 8: Wireless Settings](#).

The Router tab has several different menus from which you can select. Each menu heading is covered in a separate chapter. Please see Table 1 for a description of each menu heading.

Table 1. Configuration Manager Interface Menus
Menus

Chapter	Menu Options	Go to this section if you want to...	See Page
9	Basic	Make some modifications for more advanced uses	70
10	Advanced	Make use of advanced router features supported by the Cable Modem/Router	77
11	Firewall	Configure the firewall application to protect the private LAN from attacks from the WAN interface	96
12	Parental Control	Configure access policies or rules to specific network devices based on the time of day and Internet contents	103

13	<u>VPN</u>	Enable the VPN protocol and configure IPSec tunnels, L2TP and PPTP server options	112
14	<u>Management</u>	Configure for Admin Account, Remote Management, Backup/Restore Settings and run Diagnostics. View Event Log.	123
15	<u>Cable Modem</u>	View Device Information, and Connection. To Restart and Restore to Factory Defaults	131

7

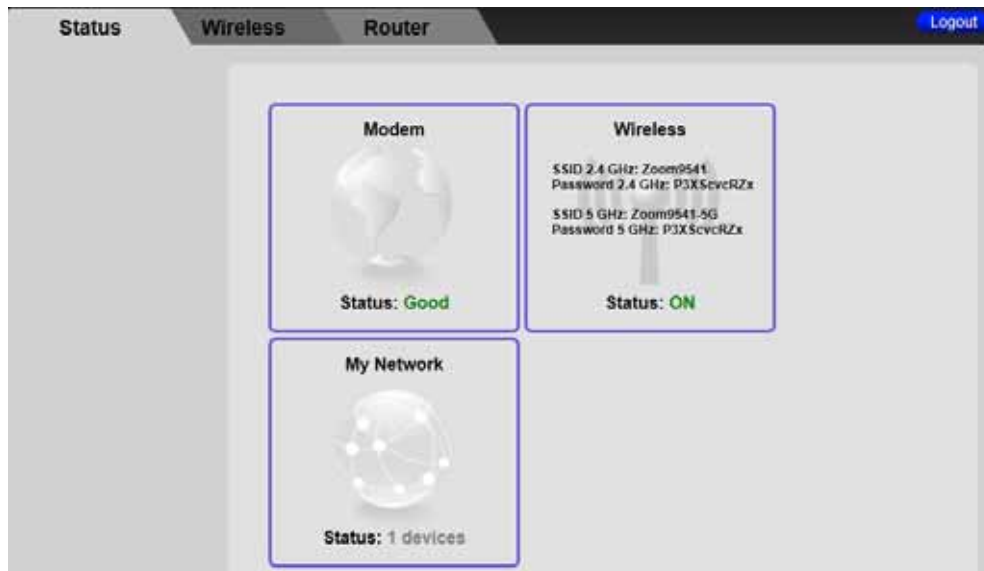
Status Page

The Status Menu lets you

- View the status and connection information of the Cable Modem/Router.
- Click on the Modem box to bring you to the Cable Modem Connection page.
- Click on the Wireless box to bring you to the Wireless page.
- Click on the My Network box to bring you to the My Network page.

Status

The Status page provides a basic overview of your Cable Modem/Router. It displays the connection status, how many wired and wireless devices are connected and information about your wireless networks.



8

Wireless Settings

The Wireless Menu lets you:

- *Configure the Cable Modem/Router to serve as a wireless access point (AP)*
- *Configure essential and advanced settings of a wireless network*
- *Configure a guest network for temporary visitors*
- *Configure WMM QoS*

Note: Your Cable Modem/Router has been preconfigured to support wireless connections without any further configuration. Please see [Chapter 3: Connecting Other Devices to your Cable Modem/Router](#) for details. Most users will not need to read this chapter.

Radio

The Radio page allows you to modify wireless settings.

To access the **Radio** page:

- 1 Click the **Wireless** menu tab.
- 2 The **Radio** submenu page will appear.

Figure 3 shows an example of the menu and Table 2 describes the items you can select.

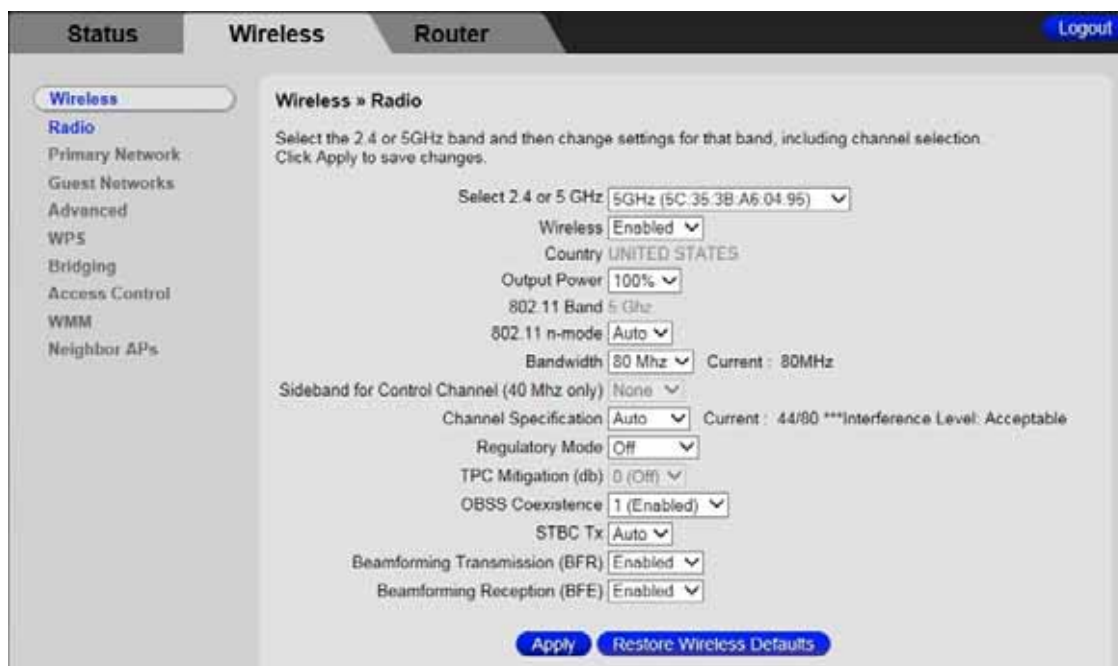


Figure 3 Example Wireless Radio Page

Table 2. Primary Radio Menu Options

Option	Description
Select 2.4 GHz or 5 GHz	Select which frequency band you want to set up. Any setup changes you make will apply to this band only. For example, if you select 5GHz any changes you make on this page will apply to the 5 GHz band only.
Wireless	Select Enable to enable the wireless function.
Country	Your device is configured for operation in the U.S. only.
Output Power	Set the strength of the wireless signal that the Cable Modem/Router transmits. Most users should use the default setting. In some scenarios reducing your output power may help reduce wireless interference. If the Cable Modem/Router is interfering with neighboring Access Points, reducing the power level may reduce this interference, causing the neighboring APs to have fewer retransmissions of their data. This results in less wireless traffic and less congestion. Lowering your power level however will reduce the wireless range of your router.
802.11 Band	This field displays the current band selected.

802.11n-mode	In Auto mode, your Cable Modem/Router will automatically adjust to avoid interference with neighboring devices. Most users should use the default setting of Auto.
Bandwidth	Specify radio frequency bandwidth, either 20 MHz single, or 40MHz (dual channel), that the Cable Modem/Router will use when 802.11n mode is configured as Automatic and the Control Channel is configured as Automatic. Normally 20 MHz is the best choice.

Sideband for Control Channel (40 MHz only)	You may select Sideband and the secondary extension channels if your Cable Modem/Router is operating at 40 MHz bandwidth and the 802.11n-mode is configured as Auto . Most users will not need to change this setting.
Control Channel	Select the channel for AP operation next to the drop-down list box. The current channel number is displayed. The list of detailed control channel and extension channels are shown in the Table below. Most users will not need to change this setting.
Regulatory Mode	By default is Off. Most users will not need to change this setting.
TPC Mitigation (db)	By default is Off. Most users will not need to change this setting.
OBSS Coexistence	By default is set to 1 (Enabled). This allows the wireless bandwidth to fall back from 40Mhz to 20Mhz when the modem/router detects interference in the area. You may select 0 (Disabled) to disable this feature. Disabling OBSS Coexistence can result in poor wireless performance if there is interference in your area. Most users will not need to change these settings.
STBC Tx	By default is set to Auto. Most users will not need to change this setting.
Restore Wireless Defaults	Click on the Restore Wireless Defaults button to restore the Wireless settings.
Beamforming Transmission (BFR)	By default is set to Enable. Most users will not need to change this setting.
Beamforming Reception (BFE)	By default is set to Enable. Most users will not need to change this setting.

Table 3. Country Extension Channel List

Control Channel	Sideband for Control Channel	Extension Channel
US Channel 1-7	Lower	Channel Number + 4
US Channel 5-11	Upper	Channel Number - 4

Example 1: If your control channel is set to 1, the extension channel will be transmitted on channel 5. The total bandwidth of the signals on channel 1 and 5 equals 40 MHz.

Example 2: If your control channel is set to 11, the extension channel will be transmitted on channel 7. The total bandwidth of the signals on channel 11 and 7 equals 40 MHz.

Primary Network

The Primary Network page allows you to configure the primary wireless network and its security settings. Strong security is the best way to prevent unauthorized wireless network access. To access the **Primary Network** page:

- 1 Click the **Wireless** menu tab.
- 2 Then click the **Primary Network** submenu.

Figure 4 shows an example of the menu and Table 4 describes the items you can select

Status **Wireless** **Router** [Logout](#)

Wireless

- Radio
- Primary Network**
- Guest Networks
- Advanced
- WPS
- Bridging
- Access Control
- WMM
- Neighbor APs

Wireless » Primary Network

Configure the wireless Primary Network and its security settings.

Zoom953e-5G (5C:35:3B:A6:04:95)

Primary Network Enabled

Network Name (SSID)

Closed Network Disabled

Mode Required None

AP Isolate Disabled

WPA Disabled

WPA-PSK Enabled

WPA2 Disabled

WPA2-PSK Enabled

WPA/WPA2 Encryption TKIP+AES

WPA Pre-Shared Key Show Key

RADIUS Server

RADIUS Port

RADIUS Key

Group Key Rotation Interval

WPA/WPA2 Re-auth Interval

WEP Encryption Disabled

Shared Key Authentication Optional

802.1x Authentication Disabled

Network Key 1

Network Key 2

Network Key 3

Network Key 4

Current Network Key

PassPhrase

Figure 4. Example Wireless Primary Network page

Table 4. Primary Network Menu Option

Option	Description
Primary Network	Select Enable to enable the primary wireless network.
Network Name (SSID)	Set the Network Name (also known as SSID) of the wireless network. This is a 1-32 Alphanumeric character string.
Closed Network	Select Enable to suppress broadcast of the SSID.
Mode Required	Default set to None. Choice to select None, HT and VHT. Most users will leave this None.
AP Isolate	Prevents wireless clients on your network from communicating with other wireless clients.
WPA	Wi-Fi Protected Access (WPA) offers stronger encryption than WEP. Enable WPA alone if you have a RADIUS server (unlikely for most home users) – otherwise use WPA-PSK or WPA2-PSK.
WPA-PSK	Offers stronger encryption than WEP. When enabled, you must also enter a Pre-Shared Key that will be used by all wireless clients to access the wireless network.
WPA2	Offers state-of-the-art security. Enable WPA2 alone only if you have a RADIUS server (unlikely for most home users) otherwise use WPA2-PSK.
WPA2-PSK	Offers state-of-the-art security. When enabled, you must also enter a Pre-Shared Key below that will be used by all wireless clients to access the wireless network.
WPA/WPA2 Encryption	Select Enable to use WPA/WPA2 encryption. Most users should use the default setting of TKIP+AES.
WPA Pre-Shared Key	Enter a 8-63 Alphanumeric character string if you have enabled WPA-PSK or WPA2-PSK.
RADIUS Server	If you're using a RADIUS server, enter its IP address here. The RADIUS server may be on either public network (WAN) or private network (LAN).

RADIUS Port (Relevant only when the RADIUS server is enabled)	Enter the UDP port number of the RADIUS server. The default port is 1812.
RADIUS Key (Relevant only when the RADIUS server is enabled)	Enter the RADIUS Key.
Group Key Rotation Interval (Relevant only when the RADIUS server is enabled)	When enabled, the Cable Modem/Router generates the best possible random group key and updates all key-management capable clients periodically. Set to zero to disable periodic rekeying.
WPA/WPA2 Re-auth Interval	Interval (in seconds) at which the Cable Modem/Router (if using WPA-PSK key management) or RADIUS server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis.
WEP Encryption	WEP Encryption can be set to WEP 128-bit, 64-bit, or Disable. Both the wireless clients and the Cable Modem/Router must use the same WEP key.
Shared Key Authentication	Select Enable to enable. Shared Key authentication is only available when WEP is enabled.
802.1x Authentication (only available when WEP is enabled)	Select Enable to enable 802.1x authentication. Enable 802.1x Authentication only if you have a RADIUS server. Most users will leave this disabled.
Network Key 1-4	You can pre-define up to 4 keys for 64-bit or 128-bit WEP. 64-bit keys require 10 hexadecimal digits and 128-bit key require 26 hexadecimal digits.
Current Network Key	Select one of the four pre-defined keys as the current network key.
PassPhase	Enter a word or group of printable characters and click Generate WEP keys to generate WEP encryption key. These characters are case sensitive.
Generate WEP Keys	Click to generate 4 WEP keys automatically.

Guest Network

The Guest Network page allows you to configure a guest network. A guest network is a small section of an organization's computer network designed for use by temporary visitors. This guest network often provides full Internet connectivity, but it also strictly limits access to any internal (intranet) Web sites or files.

Traditionally, you needed to use different Wireless Access Points to configure different wireless networks. Your Cable Modem/Router supports Multiple SSIDs, which allows you to use the same access point to provide several wireless networks simultaneously. You can then assign various privileges to different SSIDs and associated networks.

- Up to eight wireless networks are allowed on one Cable Modem/Router simultaneously, one for Admin access and seven for Guest Networks.
- If you are using WEP, you must use different WEP keys for different wireless networks.
- You should use different Passwords for different wireless networks if you are using WPA/WPA2.

To access the **Guest Network** page:

- 1 Click **Wireless** in the menu tab.
- 2 Then click the **Guest Network** submenu.

Figure 5 shows an example of the menu and Table 5. Guest Network Menu Option describes the items you can select.

Status **Wireless** **Router** [Logout](#)

Wireless

- Radio
- Primary Network
- Guest Networks**
- Advanced
- WPS
- Bridging
- Access Control
- WMM
- Neighbor APs

Wireless » Guest Network

Configure one or more guest networks.

Guest Network:

Guest WiFi Security Settings		Guest LAN Settings	
Guest Network	<input type="text" value="Disabled"/>	Network	<input type="text" value="LAN"/>
Guest Network Name (SSID)	<input type="text" value="Zoom-guest1-953e-5G"/>	IP Address	<input type="text" value="192.168.1.1"/>
Closed Network	<input type="text" value="Disabled"/>	Subnet Mask	<input type="text" value="255.255.255.0"/>
Mode Required	<input type="text" value="None"/>	Lease Pool Start	<input type="text" value="192.168.1.10"/>
AP Isolate	<input type="text" value="Disabled"/>	Lease Pool End	<input type="text" value="192.168.1.99"/>
WPA	<input type="text" value="Disabled"/>	Lease Time	<input type="text" value="86400"/>
WPA-PSK	<input type="text" value="Disabled"/>	UPnP Enable	<input type="text" value="Enabled"/>
WPA2	<input type="text" value="Disabled"/>	Firewall Enable	<input type="text" value="Disabled"/>
WPA2-PSK	<input type="text" value="Disabled"/>	DHCPv6 Server	<input type="text" value="Enabled"/>
WPA/WPA2 Encryption	<input type="text" value="Disabled"/>	<input type="button" value="Apply"/>	
WPA Pre-Shared Key	<input type="text" value=""/> <input type="checkbox"/> Show Key	<input type="button" value="Restore Guest Network Defaults"/>	
RADIUS Server	<input type="text" value="0.0.0.0"/>		
RADIUS Port	<input type="text" value="1812"/>		
RADIUS Key	<input type="text"/>		
Group Key Rotation Interval	<input type="text" value="0"/>		
WPA/WPA2 Re-auth Interval	<input type="text" value="3600"/>		
WEP Encryption	<input type="text" value="Disabled"/>		
Shared Key Authentication	<input type="text" value="Optional"/>		
802.1x Authentication	<input type="text" value="Disabled"/>		
Network Key 1	<input type="text"/>		
Network Key 2	<input type="text"/>		
Network Key 3	<input type="text"/>		
Network Key 4	<input type="text"/>		
Current Network Key	<input type="text" value="1"/>		
PassPhrase	<input type="text"/>		
<input type="button" value="Generate WEP Keys"/>			
<input type="button" value="Apply"/>			

Figure 5. Example of Guest Network Page

Table 5. Guest Network Menu Option

Option	Description
Guest Network Selection	Select which Guest Network to setup.
Guest Network	Select Enable to enable guest network.
Guest Network Name (SSID)	Enter a name for the guest network.
Closed Network	Select Enable to suppress broadcast of the SSID.
Mode Required	Default set to None. Choice to select None, HT and VHT. Most users will leave this None.
AP Isolate	Prevents wireless clients on your network from communicating with other wireless clients.
WPA	Wi-Fi Protected Access (WPA) offers stronger encryption than WEP. Enable WPA alone if you have a RADIUS server (unlikely for most home users) – otherwise WPA-PSK or WPA2-PSK
WPA-PSK	Offers stronger encryption than WEP. When enabled, you must also enter a Pre-Shared Key that will be used by all wireless clients to access the wireless network.
WPA2	Offers state-of-the-art security. Enable WPA2 alone only if you have a RADIUS server (unlikely for most home users); otherwise use WPA2-PSK.
WPA2-PSK	Offers state-of-the-art security. When enabled, you must also enter a Pre-Shared Key that will be used by all wireless clients to access the wireless network.
WPA/WPA2 Encryption	Select Enable to use WPA/WPA2 encryption. Most users should leave the default settings of TKIP+AES.
WPA Pre-Shared Key	Enter a 8-63 Alphanumeric character string if you have enabled WPA-PSK or WPA2-PSK.
RADIUS Server	If you're using a RADIUS server, enter its IP address here. The RADIUS server may be on either public network (WAN) or private network (LAN).

RADIUS Port (Relevant only when the RADIUS server is enabled)	Enter the UDP port number of the RADIUS server. The default port is 1812.
RADIUS Key (Relevant only when the RADIUS server is enabled)	Enter the RADIUS Key.
Group Key Rotation Interval (Relevant only when the RADIUS server is enabled)	When enabled, the Cable Modem/Router generates the best possible random group key and updates all key-management capable clients periodically. Set to zero to disable periodic rekeying.
WPA/WPA2 Re-auth Interval	Interval (in seconds) at which the Cable Modem/Router (if using WPA-PSK key management) or RADIUS server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis.
WEP Encryption	WEP Encryption can be set to WEP 128-bit, 64-bit, or Disable. Both the wireless clients and the Cable Modem/Router must use the same WEP key.
Shared Key Authentication	Select Enable to enable. Shared Key authentication is only available when WEP is enabled.
802.1x Authentication (only available when WEP is enabled)	Select Enable to enable 802.1x authentication. Enable 802.1x Authentication only if you have a RADIUS server. Most users will leave this as disabled.
Network Key 1-4	You can pre-define up to 4 keys for 64-bit or 128-bit WEP. 64-bit keys require 10 hexadecimal digits and 128-bit key require 26 hexadecimal digits.
Current Network Key	Select one of the four pre-defined keys as the current network key.
PassPhase	Enter a word or group of printable characters and click Generate WEP keys to generate WEP encryption key. These characters are case sensitive.
Generate WEP Keys	Click to generate 4 WEP keys automatically.
Guest LAN Settings	Select LAN for existing LAN - same as Primary Network -

	or GUEST to create a Virtual LAN.
IP Address	Enter the IP address to be the default Cable Modem/Router address for clients connected this guest network.
Subnet Mask	Enter the subnet mask for this guest network.
Lease Pool Start	Enter the starting IP address of this DHCP address pool.
Lease Pool End	Enter the ending IP address of this DHCP address pool.
Lease Time	Enter the lease time for DHCP clients. DHCP clients will resend DHCP request before expiration. Maximum value is 86400 seconds.
UPnP Enable	Select Enabled to enable UPnP on your guest network
Firewall Enable	Enables or Disables the Firewall on your guest network.
DHCPv6 Server	Selecting Enabled allows the DHCP server to assign IPv6 addresses.
Restore Guest Network Defaults	Click the Restore Guest Network Defaults button to restore the Guest Network factory settings.

Advanced

The Advanced page allows you to configure advanced wireless settings. Most users will have no need to change these settings.

To access the **Advanced** page:

- 1 Click the **Wireless** menu tab.
- 2 Then click the **Advanced** submenu.

Figure 6 shows an example of the menu and Table 6 describes the items you can select.

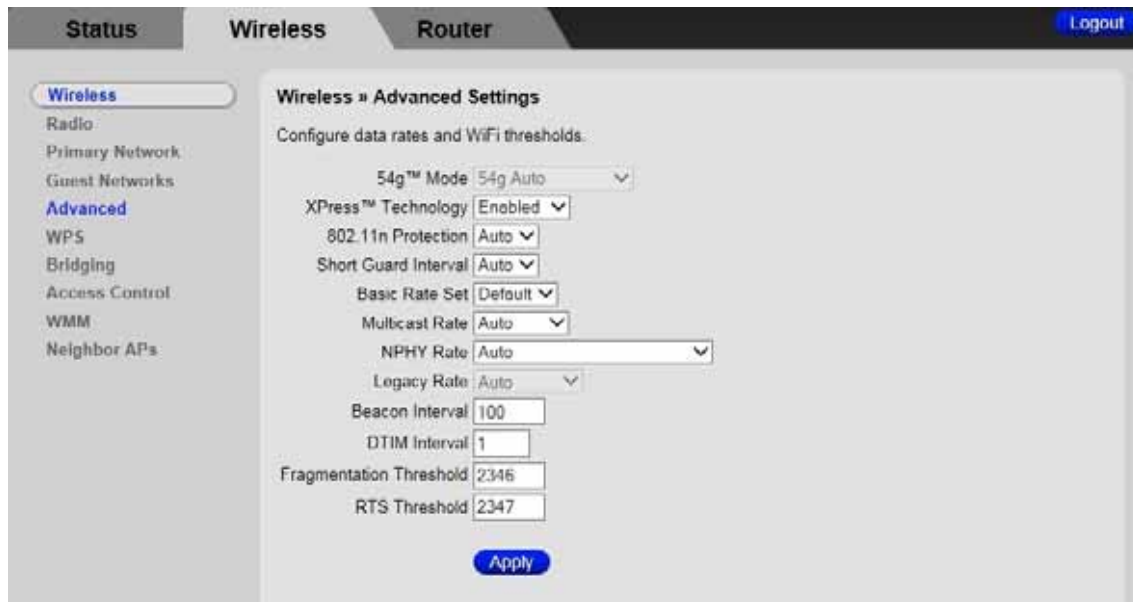


Figure 6. Example of Advanced Page

Table 6. Advanced Menu Option

Option	Description
54g™ Mode	Auto by default.
XPress™ Technology	When Xpress is turned on, aggregate throughput can improve significantly.
802.11n Protection	The 802.11g standards provide a protection method so 802.11g and 802.11b devices can co-exist in the same network without “speaking” at the same time. Do not disable 802.11n protection if there is a possibility that 802.11b or 802.11g devices will use your wireless network. In Auto mode, the wireless devices use RTS/CTS to improve 802.11n performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11n throughput under most conditions.
Short Guard Interval	Provides compatibility with certain devices that do not meet 802.11 specifications.
Basic Rate Set	Select the wireless transmission rate to a particular speed or leave it as default (Auto) to allow the AP adjusts speed automatically.
Multicast Rate	Specify the rate at which multicast packets are transmitted and received on your wireless network. Multicast packets are used to send a single message to a set of recipients in a defined group. Teleconferencing, videoconferencing and group email are some examples of multicast applications. Specifying a high multicast rate may improve performance of multicast features. The rates are in Mbps. You can select Automatic, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 and 54 .
NPHY Rate	Set the Physical Layer (NPHY) rate. These rates are only applicable when the 802.11n mode is configured as Automatic .
Legacy Rate	Auto by default.

Beacon Interval	A beacon is a packet broadcast by the router to synchronize the wireless network. The default interval is 100 ms.
DTIM Interval	Interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast message. The default value is 1.
Fragmentation Threshold	This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the fragmentation threshold. Setting the fragmentation threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of 2346.
RTS Threshold	Using this setting can regulate your wireless network if you experience any inconsistent data flow. Make only minor adjustments to the default value of 2347.

WPS

The WPS page allows you to configure settings for WPS. Most users will have no need to change these settings.

To access the **WPS** page:

- 1 Click the **Wireless** menu tab.
- 2 Then click the **WPS** submenu.

Figure 7 Example WPS pageshows an example of the menu and Table 7 describes the items you can select.

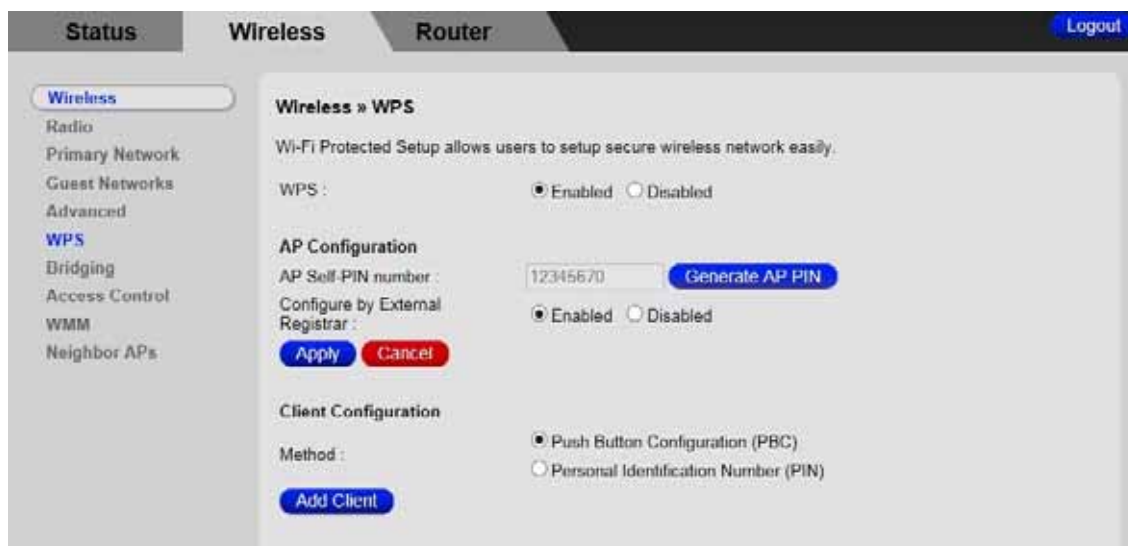


Figure 7 Example WPS page

Table 7 WPS Menu Options

Option	Description
WPS	Disable or enable WPS. WPS does not work with WEP.
AP Self-PIN number:	Click the Generate AP PIN button to generate new PIN number.
Configure by External Registrar	Default is enabled.
Push-Button Configuration (PBC)	Select this option and press the Add Client button is equivalent to pushing the WPS button on your Cable Modem/Router. After clicking the Add Client button, within 2 minutes, activate WPS on your client device(s).
Personal Identification Number (PIN)	Select this option and press the Add Client button to allow Client PIN number field appear. For devices that require a PIN, enter the PIN in the Client PIN's number field, and then click Add Client button.

Bridging

The Bridging page allows you to configure WDS (Wireless Distribution System) feature.

Only those bridges listed in the Remote Bridges table will be granted access. APs must operate in the same channel to be bridged together.

To access the **Bridging** page:

- 1 Click the **Wireless** menu tab.
- 2 Then click the **Bridging** submenu.

Figure 8. Example of Bridging Page shows an example of the menu and Table 8 describes the items you can select.

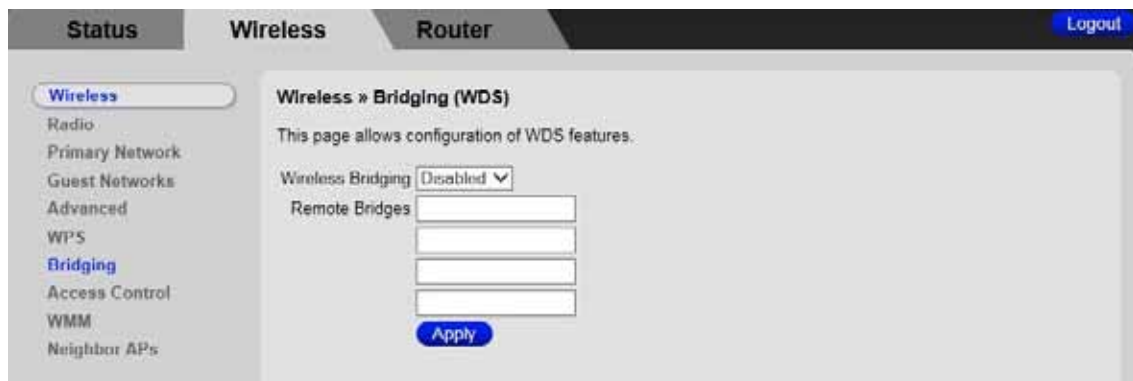


Figure 8. Example of Bridging Page

Table 8. Bridging Menu Option

Option	Description
Wireless Bridging	Select to enable or disable wireless bridging.
Remote Bridges	Table of remote bridge MAC addresses authorized to establish a wireless bridge. Up to 4 remote bridges may be connected. Typically, you will also have to enter your AP's MAC address on the remote bridge. The Cable Modem/Router's wireless MAC address can be found on the Wireless Interfaces page.

Access Control

This page allows you to control which wireless clients can access your wireless network. It also provides information about wireless clients connected to your access point.

To access the **Access Control** page:

- 1 Click the **Wireless** menu tab.
- 2 Then click the **Access Control** submenu.

Figure 9. Example of Access Control Page shows an example of the menu and Table 9 describes the items you can select.

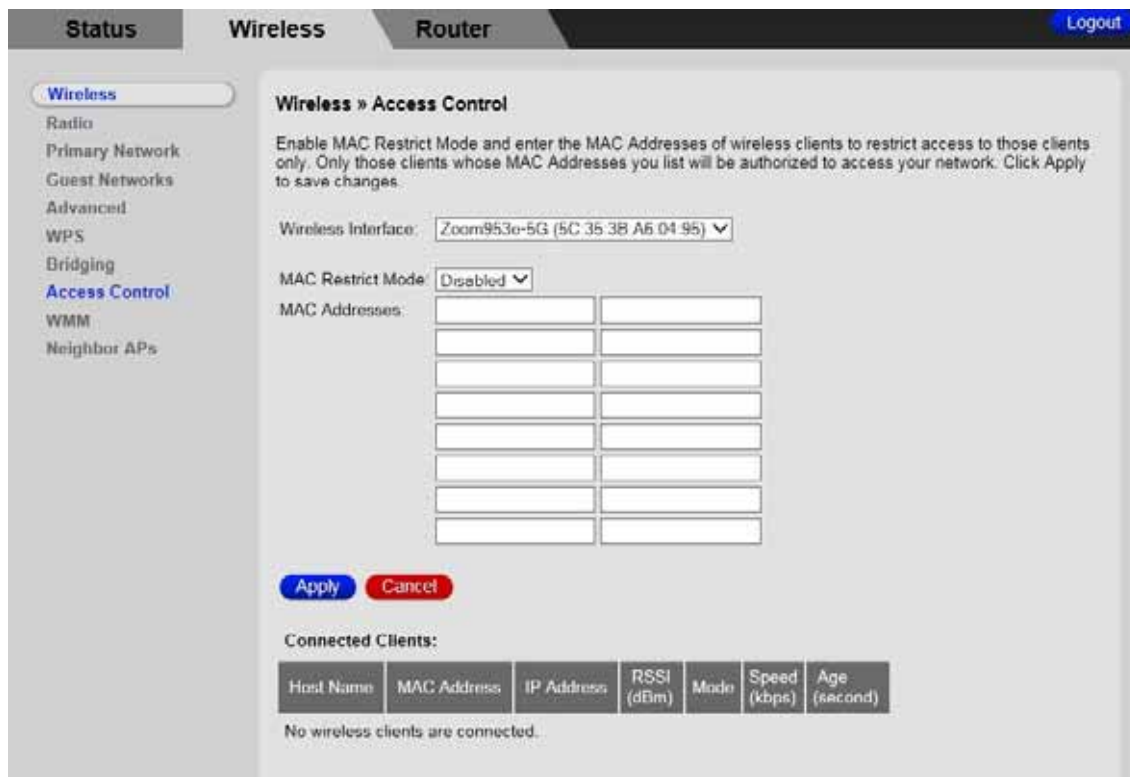


Figure 9. Example of Access Control Page

Table 9. Access Control Menu Option

Option	Description
Wireless Interface	Select the wireless interface to configure the access control list.
MAC Restrict Mode	Select whether wireless clients with the specified MAC address are allowed or denied wireless access. To allow all clients, select Disabled.
MAC Addresses	Shows the list of wireless client MAC addresses to allow or deny based on the Restrict Mode setting. Valid MAC address formats are XX:XX:XX:XX:XX:XX
Connected Clients	Shows the list of connected wireless clients. When a client connects (associates) to the network, it is added to the list; when a client leaves (disassociates) from the network, it is removed from the list. For each client, the age (in seconds), estimated average receive signal strength (in dBm), IP address, and host name are presented. The age is the amount of time elapsed since data was transmitted to or received from the client.

WMM (Wi-Fi Multimedia)

The WMM page allows you to configure WMM (Wi-Fi Multimedia) feature. WMM is a subset of the 802.11e wireless LAN (WLAN) specification that enhances quality of service (QoS) on a network by prioritizing data packets according to their categories. WMM enhances QoS at the wireless driver level. It provides a mechanism to prioritize wireless data traffic to and from the associated (WMM capable) stations.

If you enable the WMM feature, you may need to decide whether or not to broadcast Cable Modem/Router's network name. Broadcasting allows you to easily recognize your wireless network in the list of available networks. Once you have configured your wireless clients, it is recommended that you disable the broadcasting feature.

To access the **WMM** page:

- 1 Click the **Wireless** menu tab.
- 2 Then click the **WMM** submenu.

Figure 10 shows an example of the menu and Table 10 describes the items you can select.

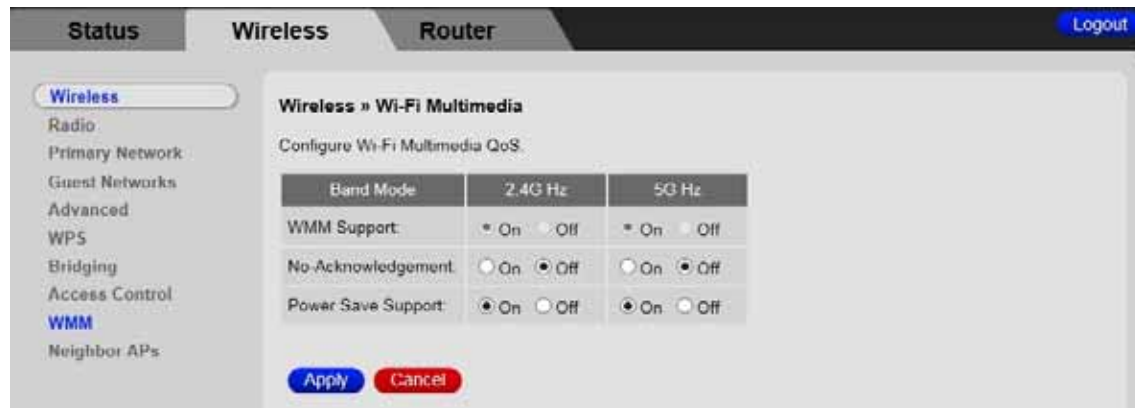


Figure 10. Example of WMM Page

Table 10. WMM Menu Option

Option	Description
WMM Support	Select On to include the WME Information Element in the beacon frame.
No-Acknowledgement	Select On to not transmit acknowledgments for data.
Power Save Support	Select On to allow the AP (Cable Modem/Router) queuing packets for stations/clients in power-save mode. Queued packets are transmitted when the station/client notifies AP that it has left power-save mode.

Neighbor APs

This page allows you to view Nearby Wireless Access Points.

To access the **Neighbor APs** page:

- 1 Click the **Wireless** menu tab.
- 2 Then click the **Neighbor APs** submenu.

Figure 11 shows an example of the menu and Table 11 describes the items you can select.



The screenshot displays the 'Neighbor APs' page within a network management interface. The page title is 'Wireless » Neighbor APs'. Below the title, it states 'This page shows the nearby APs.' and includes a 'Refresh' button. A table titled 'Nearby Wireless Access Points' lists the following data:

Network Name	Security Mode	Mode	PHY Mode	RSSI	Channel	BSSID
CRD2	WPA2-PSK AES-CCMP	Managed	802.11n	-88 dBm	42	88:1f:a1:34:10:95
Greys	WPA2-PSK AES-CCMP	Managed	802.11n	-73 dBm	36	ac:67:06:33:b5:2c
Greys-guest	WPA2-PSK AES-CCMP	Managed	802.11n	-72 dBm	36	ac:67:06:73:b5:2c
MI_WIFI	WPA2-PSK AES-CCMP	Managed	802.11a	-91 dBm	36	00:3a:98:16:2d:40
PhoostoneAP	WPA2-PSK AES-CCMP TKIP	Managed	802.11n	-76 dBm	40	14:d6:4d:3a:c5:fa
Zoom951e-5G	WPA2-PSK AES-CCMP TKIP	Managed	802.11n	-52 dBm	42	5c:35:3b:a6:03:d5

Figure 11 Neighbor APs page

Table 11. Neighbor APs Options

Option	Description
Network Name	Shows the list of Wireless Access Points.
Security Mode	Shows the Wireless Security mode associated to the AP.
Mode	Shows the status of the AP.
PHY Mode	Shows the Physical layer mode as 802.11ac, 802.11n, 802.11g, or 802.11b.
RSSI	Shows the Wireless signal strength.
Channel	Shows the channel being broadcast.
BSSID	Shows the APs MAC being broadcast.

9

Basic Menu Options

The Basic Menu lets you:

- Configure LAN Settings
- Configure the DHCP server for the LAN and UPnP
- Configure WAN Settings
- View the list of wireless or wired connected devices

Basic LAN Settings

The LAN Settings page allows you to configure the LAN Settings and UPnP.

To access the LAN Settings page,

- 1 Click the **Router** menu tab.
- 2 Then click the **Basic** submenu.

Figure 12 shows an example of the menu and Table 12 describes the items you can select.

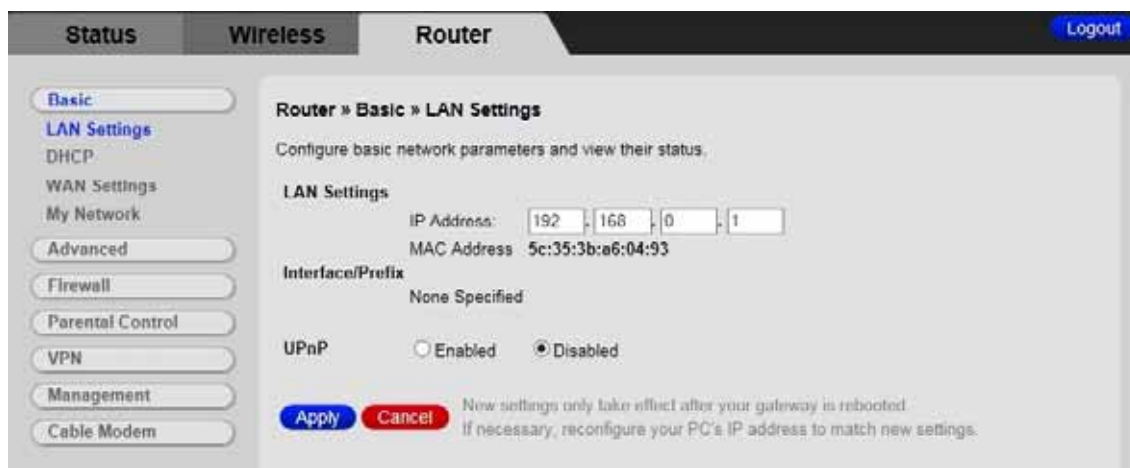


Figure 12. Example of Setup Page

Table 12. LAN Settings Menu Option

Option	Description
LAN IP Address	Set the base LAN IP for your private network. By default this is 192.168.0.1 There is normally no need to change this.
UPnP	Select Enable to enable the UPnP agent in the Cable Modem/Router. If you are running an application that requires UPnP, check this box.

DHCP

The DHCP page allows you to configure your Cable Modem/Router's DHCP server.

To access the **DHCP** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **DHCP** submenu.

Figure 13 shows an example of the menu and Table 13 describes the items you can select.

MAC Address (e.g. 11-22:33-aa-bb:cc)	IP Address	Action
<input type="text"/>	192.168.0. <input type="text"/>	<input type="button" value="Add"/>

Figure 13. Example of DHCP Page

In the unusual event that you have a separate DHCP server on your LAN, you can disable the Cable Modem/Router's DHCP server by selecting the No radio button. If you do this, make sure the IP address assigned to the Cable Modem/Router is on the same subnet as that of the external DHCP server, or you won't be able to access the Cable Modem/Router from the LAN. The base LAN IP address of the Cable Modem/Router can be set from the Basic Setup page.

Note that the Cable Modem/Router will only operate on a class C subnet, with subnet mask 255.255.255.0

You may also want to disable the DHCP server if you have assigned static IP addresses to all devices on your network.

Table 13. DHCP Menu Options

Option	Description
DHCP Server	Select Yes to use the internal DHCP server of the Cable Modem/Router, or select No to disable it.
Starting Local Address	Configure the starting IP address for IP leases available to devices on the LAN.
Number of CPEs	Configure the number of PCs supported on the LAN.
Lease Time	Configure the time a lease will last before it must be renewed. Default is 86400 seconds, or 1 day.
Reserved IP Addresses	Configure the MAC Address and IP Address to allow fixed IP address.

WAN Settings

The WAN Settings page allows you to configure your Cable Modem/Router's in Bridging (NAT off) or Routing (NAT on) operation mode.

To access the **WAN Settings** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **WAN Settings** submenu.

Figure 14 shows an example of the menu and Figure 14 Wan Settings page

Table 14 describes the items you can select.

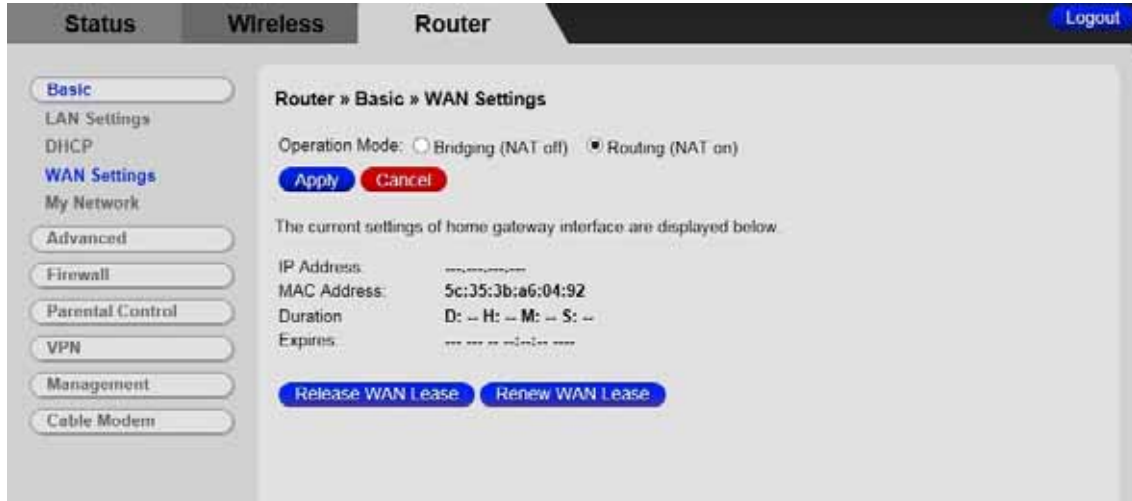


Figure 14 Wan Settings page

Table 14. WAN Settings Menu Options

Option	Description
Operation Mode	Click the Bridge button if you do not wish to use the 5363 as a router. Most users should not change this setting.
Release WAN Lease	Click to release the WAN IP address.
Renew WAN Lease	Click to renew the WAN IP address.

My Network

The My Network page allows you to view all users wired or wireless connected to the device.

To access the **My Network** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **My Network** submenu.

Figure 15 shows an example of the menu and Table 6 describes the items you can select.

Router » Basic » My Network

All users connected to this device are listed below.

MAC Address	IP Address	Subnet Mask	Lease Time	Speed (kbps)	Connected to
00:e0:4c:77:47:9b	192.168.0.4	255.255.255.0	60	1000000	Ethernet

Figure 15. My Network Page

Table 15. My Network Menu Options

Option	Description
Mac Address	View status of the connected client's MAC address.
IP Address	View status of connected client's IP address.
Subnet Mask	View status of the connected client's Subnet Mask.
Lease Time	View status of the connected client's Lease Time.
Speed (kbps)	View status of the connected client's Speed.
Connected to	View whether the connected client is Ethernet or Wireless.

10

Advanced Menu Options

The Advanced Menu lets you:

- *Enable advanced features of the Cable Modem/Router*
- *Configure the LAN IP address, MAC address, and port number filtering*
- *Configure WAN to LAN port forwarding and triggers*
- *Configure DMZ hosting*
- *Configure DDNS*
- *Configure RIP parameters*
- *Configure Options*

MAC Filtering

The MAC Filtering page allows you to configure MAC address filters in order to block Internet traffic to specific network devices on your LAN.

To access the **MAC Filtering** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Advanced/MAC Filtering** submenu.

Figure 16 shows an example of the menu and Table 16 describes the items you can select.

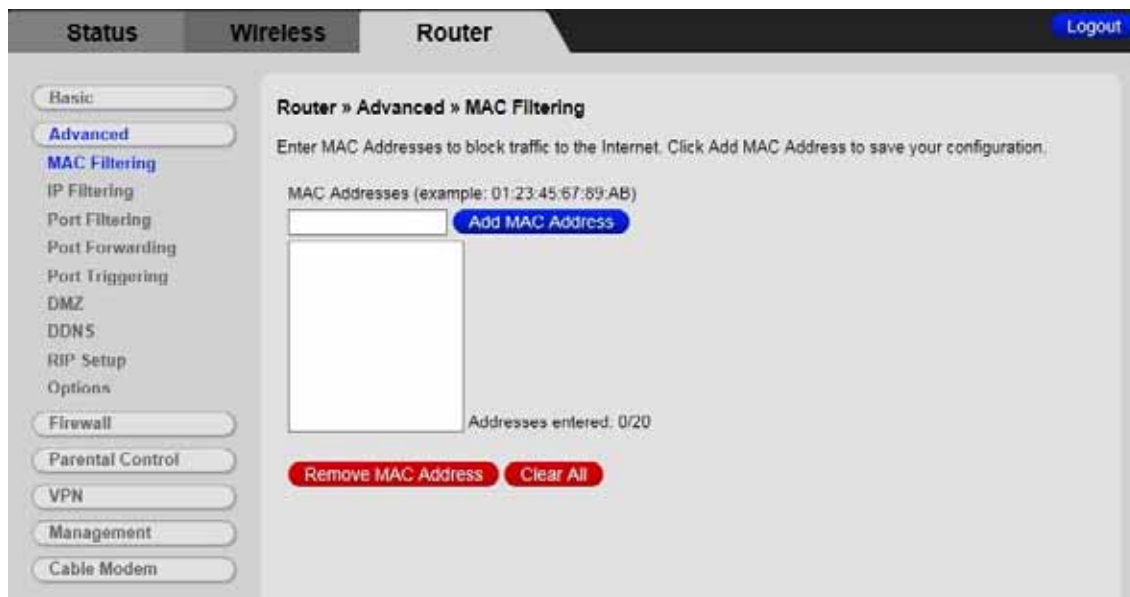


Figure 16. Example of MAC Filtering Page

Table 16. MAC Filtering Menu Option

Option	Description
MAC Address	<p>PCs and other devices can be added to the MAC filter table by entering their MAC addresses into the Add MAC Address box, and clicking the Add MAC Address button. Internet traffic to and from each listed Address will be blocked.</p> <p>The Mac Addresses of the computers attached to your network can be found in the My Network table. To access the DHCP Clients table click on Router on the menu tab then Basic/My Network submenu.</p>

IP Filtering

The IP Filtering page allows you to configure IP address filters in order to block specific network devices on your LAN from accessing the Internet. By entering starting and ending IP address ranges, you can configure which local PCs are denied access to the WAN.

We recommend assigning a static IP address to your computer when using IP Filtering. By default, the Cable Modem/Router uses DHCP to assign IP addresses. DHCP does not guarantee that your computer will be assigned the same IP address. When assigning a static IP address to your computer you should select an address that is outside the IP addresses assigned by the Cable Modem/Router's DHCP server. By default the DHCP Server assigns addresses from 192.168.0.10 to 192.168.0.255. We recommend using 192.168.0.6 as the static IP address for your computer.

To access the **IP Filtering** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Advanced/IP Filtering** submenu.

Figure 17 shows an example of the menu and Table 17 describes the items you can select.

Status Wireless Router Logout

Basic
Advanced
 MAC Filtering
IP Filtering
 Port Filtering
 Port Forwarding
 Port Triggering
 DMZ
 DDNS
 RIP Setup
 Options
 Firewall
 Parental Control
 VPN
 Management
 Cable Modem

Router » Advanced » IP Filtering

Enter LAN IP Addresses to block traffic to the Internet. Enter the same IP Address as both Start and End Address to block a single Address, or enter two IP Addresses to block the range of Addresses that they define. Click the Enable checkbox and click Apply to save your configuration.

IP Filtering		
Start Address	End Address	Enabled
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>

Apply Cancel

Figure 17. Example of IP Filtering Page

To activate the IP address filter:

- 1 Enter the last byte (the numbers after the last period) of the IP address in **Start Address** and **End Address**.
- 2 Check the **Enable** box to the right of the entry to store settings.
- 3 Click the **Apply** button to activate the filter rules.

Table 17. IP Filtering Menu Option

Option	Description
Start/End Address	Enter the last byte of the IP address. The upper bytes of the IP address are set automatically from the Cable Modem/Router IP address.
Enable	To activate the IP address filter, you must also check the Enable box and click Apply . You can disable this filter while retaining the addresses you entered for later use.

Port Filtering

The Port Filtering page allows you to configure port filters in order to block Internet traffic to specific ports on all devices on your LAN.

Similarly, you can prevent PCs from sending outgoing TCP/UDP traffic to the Internet from specific IP port numbers. This can be configured using the Port Filtering page.

To access the **Port Filtering** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Advanced/Port Filtering** submenu.

Figure 18 shows an example of the menu and

Table 18 describes the items you can select.

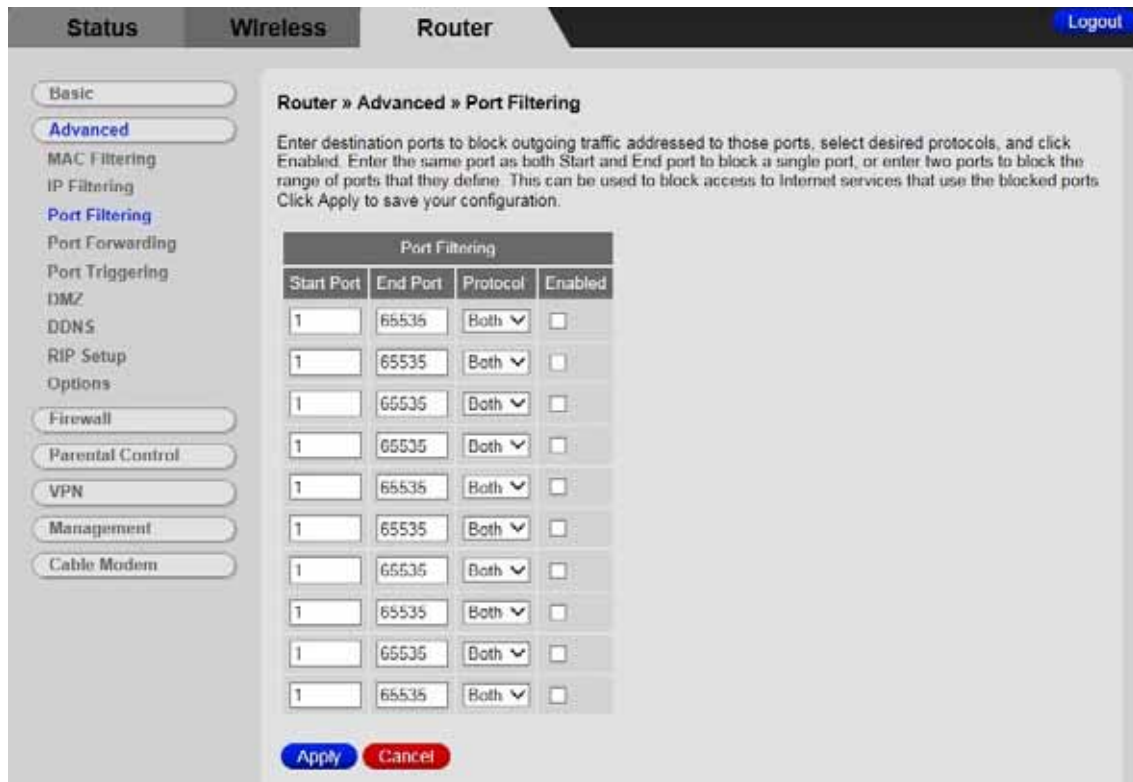


Figure 18. Example of Port Filtering Page

For example, if you would like to block all PCs on the private LAN from accessing HTTP sites (or “web surfing”):

- 1 Set the Start Port to **80**, the End Port to **80**.
- 2 Set the protocol to **TCP**.
- 3 Check the **Enable** box to the right of the entry to store settings.
- 4 Click **Apply** button to activate the filter rules.

Table 18. Port Filtering Menu Option

Option	Description
Start/End Port	Enters the start and end port of the port filter range
Protocol	Filter either both TCP and UDP traffic or just UDP or just TCP.

Port Forwarding

The Port Forwarding page allows you to run a publicly accessible server from your LAN by specifying the mapping of TCP/UDP ports to a local PC. It allows incoming requests to specific port numbers to reach a web server, FTP server, mail server, etc.

To access the **Port Forwarding** page,

- 1 Click the **Router** menu tab.
- 2 Then click the **Advanced/Forwarding** submenu.
- 3 To add a new rule, click on the **Create IPv4 Rule** button.

Figure 19 shows an example of the menu and

Table 19 describes the items you can select.

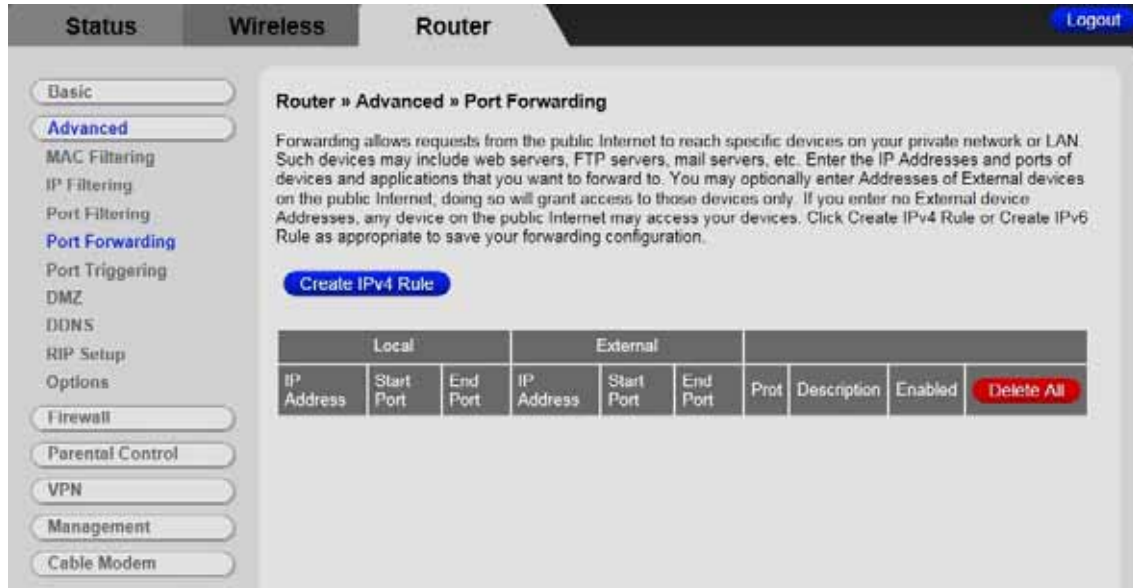


Figure 19. Example of the Port Forwarding Page

To activate the port forwarding:

- 1 Enter the port range of the Internet traffic that you want to forward, and the IP address of the server to which you want to forward that traffic. If you enter no External device on the public internet; doing so will grant access to those devices only.
- 2 Select the protocol(s) to be forwarded.
- 3 Enter the Description name.
- 4 Select ON for the **Enable** box to enable Port Forwarding rule.
- 5 Click the **Apply** button to activate the forwarding rules.

Table 19. Forwarding Menu Option

Option	Description
Local IP Address	Enter the IP address to which forwarded traffic should be sent.
Start/End Port	Enter the range of port numbers (start and end port) to forward. If only a single port is desired, enter the same port number in the Start and End locations.
External IP	You may optionally enter Addresses of External devices on the public internet; doing so will grant access to those devices only. If you enter no External device Addresses, any device on the public Internet may access your devices.
External Start/End Port	Enter the range of port numbers (start and end port). If only a single port is desired, enter the same port number in the Start and End locations.
Protocol	Select the protocol(s) to be forwarded.
Description	Enter the Description name here.
Enable	Select ON or OFF to enable Port Forwarding rule.

Note: You may need to assign static IP addresses to devices on your LAN to insure that the port forwarding you have set up will always apply to them.

Port Triggers

The Port Triggers page allows you to configure dynamic triggers to specific devices on the LAN. This allows for special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special settings.

Port Triggers are similar to Port Forwarding except that they are not static ports held open all the time. With the port triggering function, the Cable Modem/Router detects outgoing data on a specific IP port number and opens corresponding target ports for incoming data. If no outgoing traffic is detected on the Trigger Range ports for 10 minutes, the Target Range ports will close.

To access the **Port Triggers** page:

- 1 Click **Router** in the menu tab.
- 2 Then click the **Advanced/Port Triggers** submenu.
- 3 To add a new rule, click on the **Create Rule** button.

Figure 20 shows an example of the menu and Table 20 describes the items you can select.

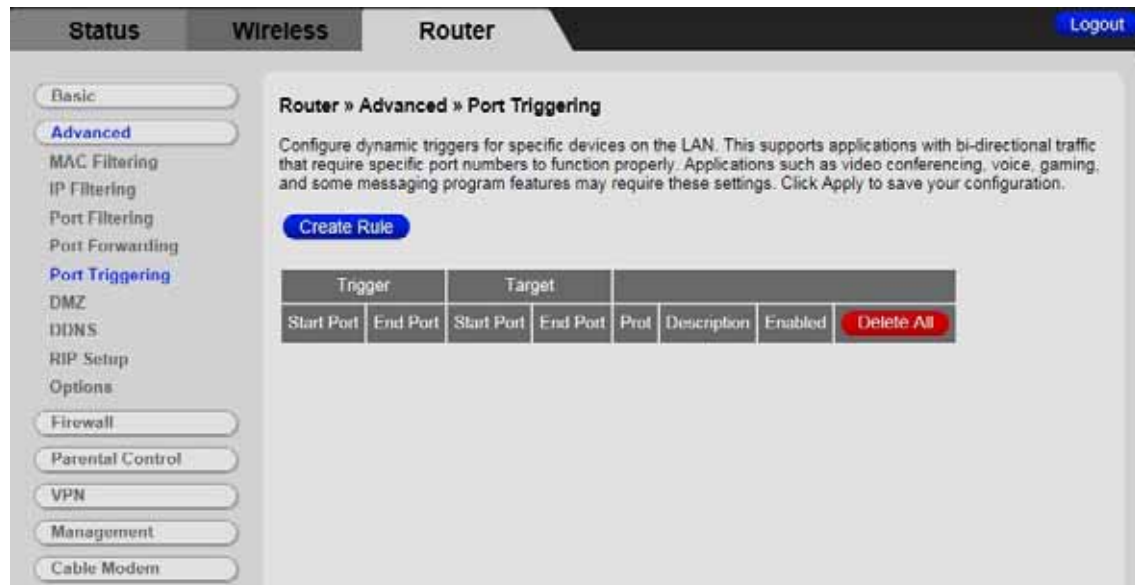


Figure 20. Example of port Triggers Page

To activate a port trigger

- 1 Enter the trigger and target ports range for the Internet traffic to forward to.
- 2 Select the forwarding protocol(s).
- 3 Enter a name for your port triggering rule.
- 4 Select ON for the **Enable** box to enable Port Triggering.
- 5 Click the **Apply** button to activate the forwarding rules.

Table 20. Port Triggers Menu Option

Option	Description
Trigger Range (Start / End Port)	Enter the trigger range (starting and ending ports) of the application for which you want to enable port triggering. The application will send data from these ports.
Target Range (Start / End Port)	Enter the target range (starting and ending ports) to open for the same application. The application will receive data on these ports.
Protocol	Select the protocol for this rule.
Description	Enter the Description name here.
Enable	Select ON or OFF to enable Port Triggering rule.

DMZ Host

The DMZ (De-militarized Zone) Host page allows you to configure a network device (e.g. a PC) to be exposed or visible directly to the Internet. This may be used if an application doesn't work with port triggers. If you have an application that won't run properly behind the NAT firewall, you can configure it for unrestricted two-way Internet access by defining it as a virtual DMZ host. Adding a client to the DMZ may expose your local network to various security risks because the client is not protected, so use this option as a last resort.

To access the **DMZ Host** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Advanced/DMZ Host** submenu.

Figure 21 shows an example of the menu.

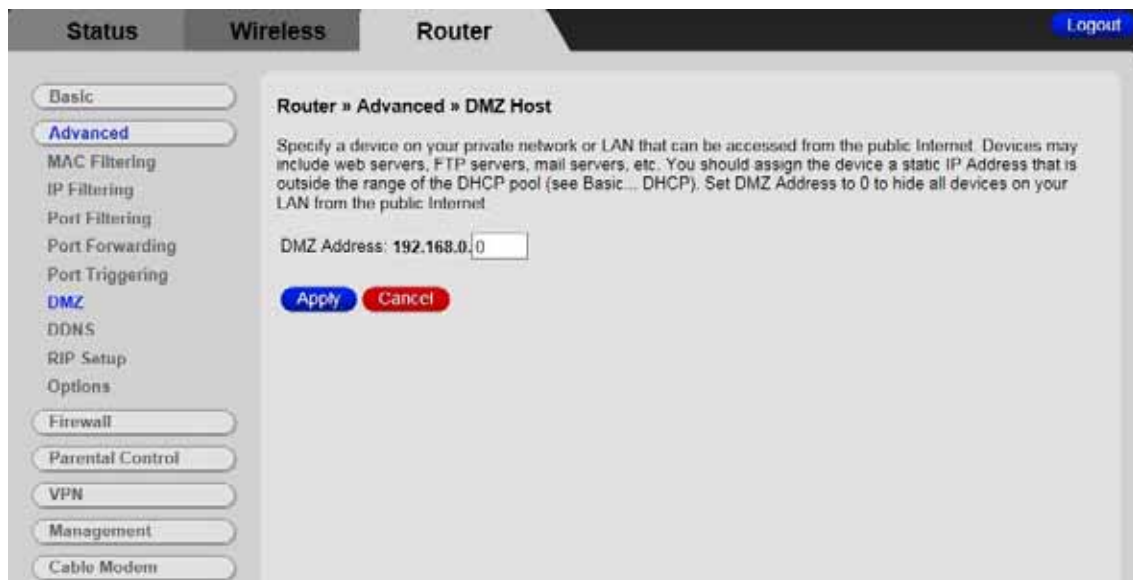


Figure 21. Example of DMZ Host Page

To configure DMZ settings:

- 1 Enter the last byte of the LAN IP address of the PC or other device on your network that you want to configure as a DMZ host.
- 2 Click **Apply**.

Note: If a specific PC is set as a DMZ Host, remember to set this back to “0” when finished with the needed application, since this PC will be effectively exposed to the public Internet.

Note: You may need to assign your DMZ host a static IP address on your LAN to insure that it will always be at that address.

DDNS

The DDNS page allows you to make use of a DDNS server. Dynamic DNS (DDNS) allows a dynamic IP address to be aliased to a static, pre-defined host name so that the host can be easily contacted by other hosts on the internet even if its IP address changes. This means you can host a server on your LAN that can be accessed from anywhere on the Internet.


Caution: Some service providers may consider connection of such a server to be a breach of your service agreement.

The Cable Modem/Router supports a dynamic DNS client compatible with the Dynamic DNS service (<http://www.dyndns.com/>). You must sign up with this service if you want to use it.

To access the **DDNS** page:

- 1 Click **Router** in the menu tab.
- 2 Then click the **Advanced/DDNS** submenu.

Figure 22 shows an example of the menu and Table 21 describes the items you can select.



The screenshot shows a web interface for a router with three main tabs: **Status**, **Wireless**, and **Router**. The **Router** tab is selected. On the left side, there is a vertical menu with buttons for **Basic**, **Advanced** (highlighted in blue), **MAC Filtering**, **IP Filtering**, **Port Filtering**, **Port Forwarding**, **Port Triggering**, **DMZ**, **DDNS** (highlighted in blue), **RIP Setup**, **Options**, **Firewall**, **Parental Control**, **VPN**, **Management**, and **Cable Modem**. The main content area is titled **Router » Advanced » DDNS**. It contains a paragraph of text: "This page allows you to provide Internet users with a 'friendly' name (instead of an IP Address) to access servers on your LAN. This device supports dynamic DNS service provided by 'http://www.dyndns.org'. You must first register your friendly name with 'http://www.dyndns.org' before you can activate this service." Below this text are several input fields: **DDNS Service** (a dropdown menu set to "Disabled"), **User Name** (a text box), **Password** (a text box), **Host Name** (a text box), **IP Address** (set to "0.0.0.0"), and **Status** (set to "DDNS service is not enabled."). At the bottom of the form are two buttons: **Apply** (blue) and **Cancel** (red). A **Logout** button is visible in the top right corner of the interface.

Figure 22. Example of DDNS Page

To activate the DDNS client:

- 1 Go to the DynDNS website and create an account for the **Dynamic DNS** service.
- 2 You will create a **username** and **password**, and be asked to choose a **host name** for your server, and the dynamic DNS domain to which your host will be assigned.
- 3 You will also be asked for your host's current **IP address**. This is the WAN IP address that has been assigned to your Cable Modem/Router during provisioning. (See WAN IP Address on the Router tab, Basic/My Network page)
- 4 Enter your account information on the Advanced / DDNS web page, enable the service by selecting www.DynDNS.org from the **DDNS Service** drop-down list, and click **Apply**.
- 5 The DDNS client will notify the DDNS service whenever the WAN IP address changes so that your chosen host name will be resolved properly by inquiring hosts. The current status of the service is shown at the bottom of the DDNS web page.

Table 21. DDNS Menu Option

Option	Description
DDNS Service	Select the type of service that you are registered for from your DDNS service provider.
User Name	Enter your DDNS account username subscribed to the service provider.
Password	Enter the password of the account.
Host Name	Enter the host name of your service host.
IP Address	Shows the current WAN side public IP address.
Status	Shows the status of DDNS service.

RIP Setup

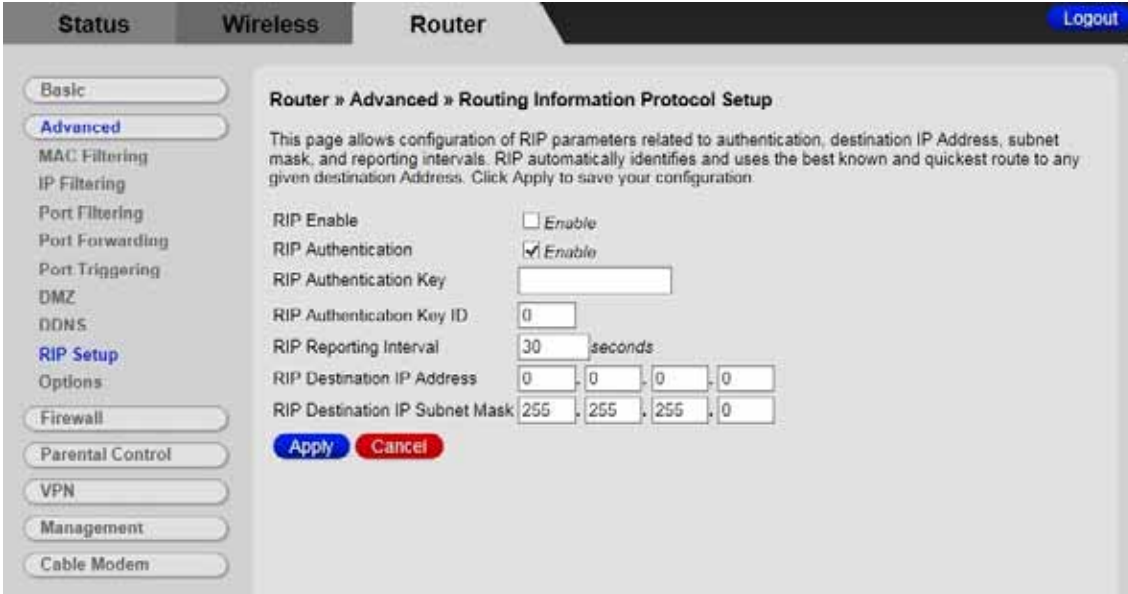
The RIP Setup page allows you to configure RIP (Router Information Protocol) parameters. RIP automatically identifies and uses the best known and quickest route to any given destination address to help reduce network congestion and delays.

RIP is a protocol that requires negotiation from both sides of the network (e.g. both the Cable Modem/Router and your service provider's CMTS (Cable Modem Termination System)). Your service provider will normally set this up based on their knowledge of their CMTS settings.

To access the **RIP Setup** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Advanced/RIP Setup** submenu.

Figure 23 shows an example of the menu and Table 22 describes the items you can select.



The screenshot shows a web interface for a router. At the top, there are tabs for 'Status', 'Wireless', and 'Router', with 'Router' selected. A 'Logout' button is in the top right. On the left, a sidebar contains menu items: 'Basic', 'Advanced' (selected), 'MAC Filtering', 'IP Filtering', 'Port Filtering', 'Port Forwarding', 'Port Triggering', 'DMZ', 'DDNS', 'RIP Setup' (highlighted in blue), 'Options', 'Firewall', 'Parental Control', 'VPN', 'Management', and 'Cable Modem'. The main content area is titled 'Router » Advanced » Routing Information Protocol Setup'. It contains a descriptive paragraph and several configuration fields: 'RIP Enable' (checkbox, 'Enable'), 'RIP Authentication' (checkbox, 'Enable'), 'RIP Authentication Key' (text input), 'RIP Authentication Key ID' (text input, '0'), 'RIP Reporting Interval' (text input, '30', followed by 'seconds'), 'RIP Destination IP Address' (four text inputs, '0', '0', '0', '0'), and 'RIP Destination IP Subnet Mask' (four text inputs, '255', '255', '255', '0'). At the bottom of the form are 'Apply' and 'Cancel' buttons.

Figure 23. Example of RIP Setup Page

Note: RIP messages will only be sent when the Cable Modem/Router is configured for Static IP Addressing.

It is unlikely that your cable Internet service supports this mode. If they do, and you want to enable RIP, you will need to ask for the CMTS's key name and number. You may need additional information.

To enable the Cable Modem/Router to perform RIP, do the following (this example uses BRCMV2 as the RIP Authentication Key and 1 as the Key ID):

- To turn on RIP MD5 Authentication, and check the **Enable** box.
- To specify a RIP MD5 Authentication Key String, type **BRCMV2** for this example.
key name = a string value to match CMTS key name value
- To specify a RIP MD5 Auth Key ID, type **1**.
key number = a number to match the CMTS key number value
- To change the RIP announcement interval, enter a number in seconds.
reporting interval by default = 30 seconds
- To specify a RIP unicast destination IP address, enter the IP address and subnet mask.

Table 22. RIP Setup Menu Option

Option	Description
RIP Enable	Check this box to enable RIP.
RIP Authentication	Check this box to enable RIP authentication for routing protocols.
RIP Authentication Key	Enter the set of keys for your interface.
RIP Authentication Key ID	Enter the ID to identify the key used to create the authentication data.
RIP Reporting Interval	Enter the interval at which to update routing table.
RIP Destination IP Address	Enter the destination IP address for RIP.
RIP Destination IP Subnet Mask	Enter the subnet mask for the destination IP address.

Options

The Options page allows you to configure the Cable Modem/Router to operate in different modes that adjust how the device routes IP traffic.

To access the **Options** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Advanced/Options** submenu.

Figure 24 shows an example of the menu and Table 23 describes the items you can select.

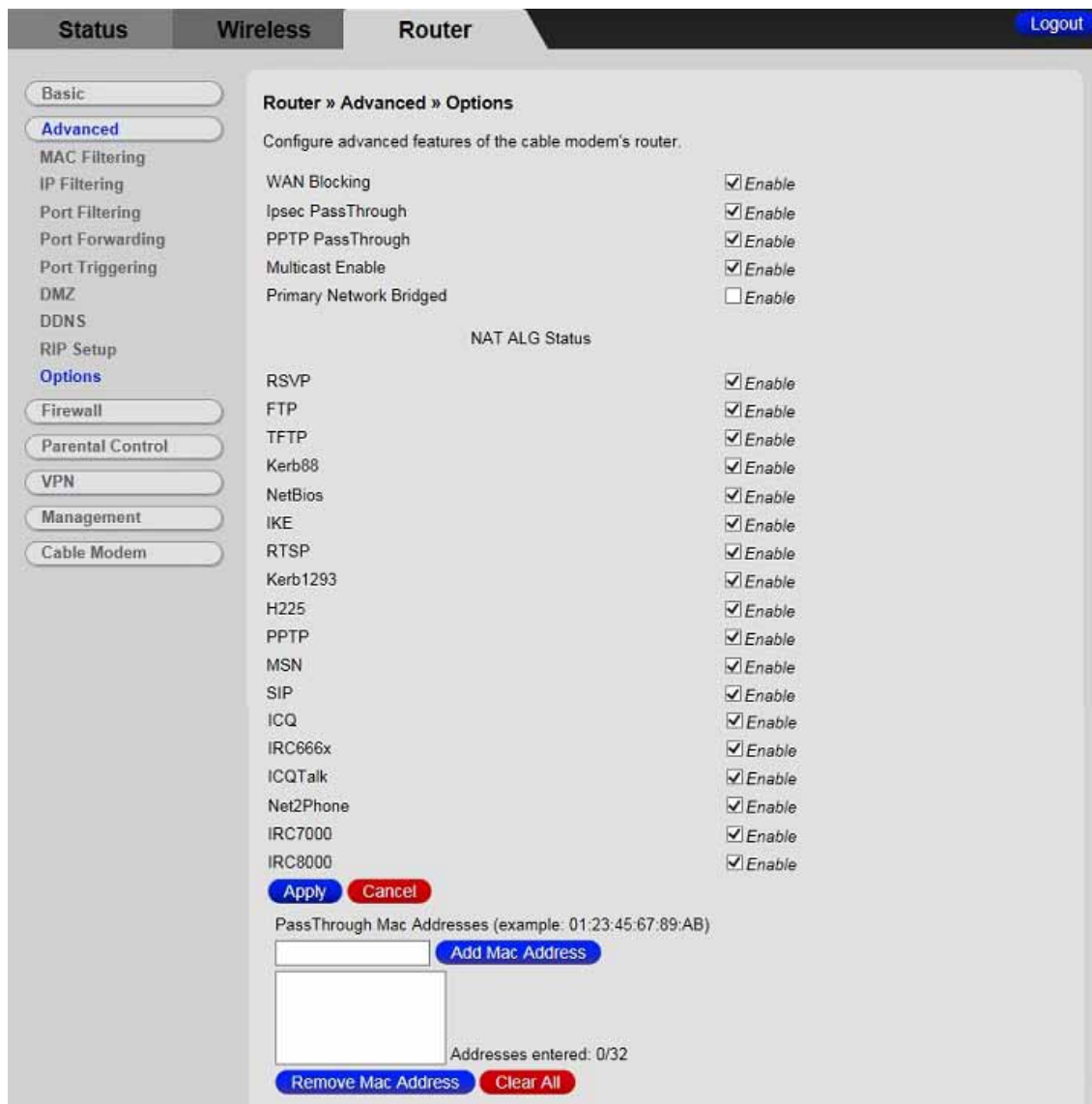


Figure 24. Example of Options Page

To enable a feature:

- 1 Click the appropriate check box (a check mark will appear).

- 2 When you are done with your selections, click on the **Apply** button.

Table 23. Options Menu Option

Option	Description
WAN Blocking	Prevents the Cable Modem/Router or the PCs from responding to pings to the Cable Modem/Router's WAN IP address or to the devices behind it. This makes it more difficult for hackers to attack your PCs and other devices on your network.
IPSec/PPTP PassThrough	Enable to support VPN devices or software on your network.
Multicast Enable	Allows multicast specific traffic (denoted by a multicast specific address) to be passed to and from the PCs on the private network behind the Cable Modem/Router.
Primary Network Bridged	Allows all LAN hosts to bypass NAT and the Cable Modem/Router's LAN DHCP Server. Adding MAC addresses into the table is not required. If MAC addresses are added to the table then only those MAC addresses in the list will bypass NAT and the LAN DHCP. All other LAN hosts NOT in the list will use the NAT and LAN DHCP Server as normal.
NAT ALG Status	The NAT ALG section shows which ALGs (Application Layer Gateway) are allowed to pass through the NAT Firewall. Most users will not need to change these settings.
PassThrough Mac Addresses	Enter the MAC Address that you want to passthrough and click the Add Mac Address button.

11

Firewall Menu Options

The Firewall Menu lets you:

- Configure the level of protection your firewall provides
- View the firewall logs

Basic

The Basic page allows you to configure the level of protection your firewall offers and also what type of attacks it should detect..

To access the **Basic** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Firewall/Basic** submenu.

Figure 25 shows an example of the menu and Table 24 describes the items you can select.

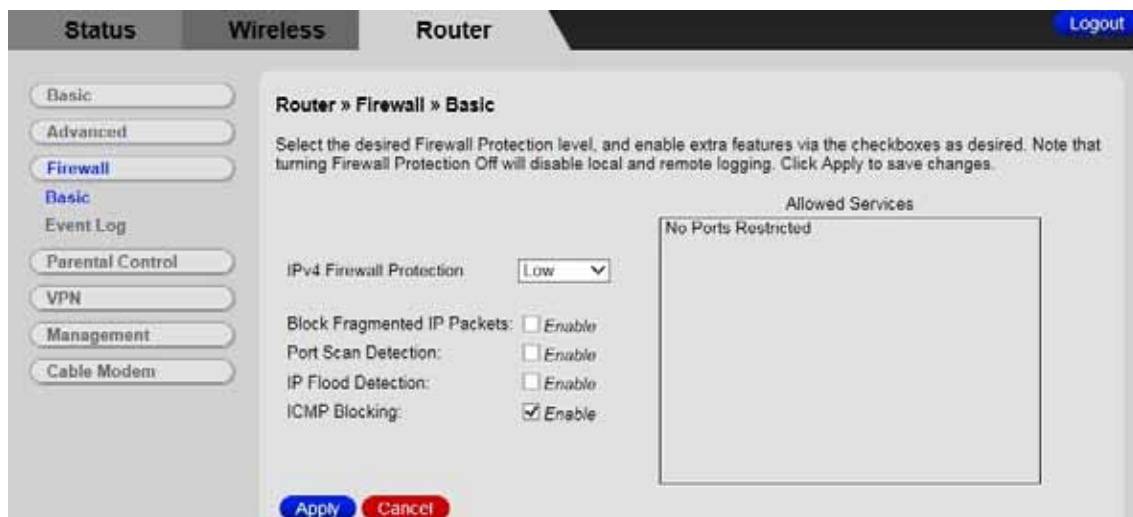


Figure 25. Example of Basic Page

Table 24. Basic Menu Option

Option	Description
IPv4 Firewall Protection	By increasing the level from low to medium or high you can restrict traffic to only certain predefined ports.
Block Fragmented IP packets	Prevents all fragmented IP packets from passing through the firewall.
Port Scan Detection	Detects and blocks port scan activity originating on both the LAN and WAN.
IP Flood Detection	Detects and blocks packet floods originating on both the LAN and WAN.
ICMP Blocking	Prevents the Cable Modem/Router or the PCs from responding to pings to the Cable Modem/Router's WAN IP address or to the devices behind it. This makes it more difficult for hackers to attack your PCs and other devices on your network.

Event Log

The Event Log page allows you to send firewall event log reporting to a standard SysLog server or via email. Individual attack or configuration items can be selected that will be sent to the SysLog server or emailed so that only the items of interest can be monitored. Permitted connections, blocked connections, known Internet attack types, and Cable Modem/Router configuration events can also be logged. The SysLog server must be on the same subnet as the Private LAN behind the Cable Modem/Router (typically 192.168.0.x).

To access the **Event Log** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Firewall/Event Log** submenu.

Figure 23 shows an example of the menu and Table 25 describes the items you can select.

To enable the automatic email alerts:

- 1 Configure the email address you want to send alerts to. You also need to configure the email account you will send from (this may be the same account). This includes the SMTP (outgoing)/ mail server address, together with username and password. You may need to contact your service provider to find the information.
- 2 Check the **Enable** box and click the Apply button.



Figure 26. Example of Event Log Page

Table 25. Local Log Menu Option

Option	Description
Permitted Connections	Enabling this feature causes the Cable Modem/Router to report all permitted connection attempts.
Blocked Connections	Enabling this feature causes the Cable Modem/Router to report all blocked connection attempts.
Known Internet Attacks	Enabling this feature causes the Cable Modem/Router to report any known Internet attacks.
Product Configuration Events	Enabling this feature causes the Cable Modem/Router to report all configuration changes.
SysLog server at 192.168.0.x	Enter the address of your local SysLog server, if you have one.
Contact Email Address	Enter the email address where you want to receive the alert email.
SMTP Server Name	Enter the SMTP (Outgoing) mail server address of the email account you will send from.
SMTP Username	Enter the username of the email account you will send from.
SMTP Password	Enter the password of the email account you will send from.
E-mail Alerts	Check to enable sending alert email, when an attack is detected.

Below is a complete list of the capable SysLog server attack/notification types and their format. The generic format of sysLog messages for traffic or administration-related events is:

```
MMM DD HH:MM:SS YYYY SYSLOG[0]: [Host HostIP] Protocol SourceIP,SourcePort
--> DestIP,DestPort EventText
```

Table 26. SysLog Server Event Format

Parameter	Description
MMM	The three-letter abbreviation for the month (e.g., JUN, JUL AUG, etc.)
DD	The two-digit day of the month (e.g., 01, 02, 03, etc.)
HH:MM:SS	The time displayed as two-digit values for the hour, minute, and second, respectively.
YYYY	The four-digit year.
HostIP	The IP address of Cable Modem/Router sending the SysLog event. This is the LAN IP Address on the Basic - Setup page.
Protocol	Can be one of the following: "TCP", "UDP", "ICMP", "IGMP" or "OTHER". In the case of "OTHER" the protocol type is displayed in parentheses (). For ICMP packets, the ICMP type is displayed in parentheses.
SourceIP	The IP address of the originator of the session/packet.
SourcePort	The source port at the originator.
DestIP	The IP address of the recipient of the session/packet.
DestPort	The destination port at the recipient.
EventText	A textual description of the event.

The format of SysLog messages for informational events is simplified:

MMM DD HH:MM:SS YYYY SYSLOG[0]: [Host HostIP] EventText

The table below lists all events that can be sent to the SysLog server.

Table 27. SysLog Server Event and Meaning

Event Text	Meaning
ALLOW: Inbound access request	An inbound request was made, and accepted, from a public network client to use a service hosted on the firewall or a client behind the firewall.
ALLOW: Outbound access request	An outbound request was made, and accepted, from a public client to use a service hosted on a public network server.
DENY: Inbound or outbound access request	A request to traverse the firewall by a public or private client violated the security policy, and was blocked.
DENY: Firewall interface access request	A request was made to the public or private firewall interface by a public or private client that violated the security policy, and was blocked.
FAILURE: User interface login [Invalid username or password]	An attempt was made to login to the user interface, and access was denied because the username and/or password was incorrect.
SUCCESS: User interface login	An attempt was made to login to the user interface, and access was allowed.
ALLOW: User interface access [request]	An HTTP GET or POST request was made by an authenticated user to the user interface.
DENY: Inbound or outbound [internet attack name] attack	A known internet attack was detected attempting to traverse the firewall, and was blocked. Examples of known internet attacks are Ping Of Death, Teardrop, WinNuke, XmasTree, SYN Flood, etc.
DENY: Firewall interface [internet attack name] attack	A known internet attack directed at the firewall itself was detected and blocked. Examples of known internet attacks are Ping Of Death, Teardrop, WinNuke, XmasTree, SYN Flood, etc.
Firewall Up	The public interface (WAN) connection is up, and the

	firewall has begun to police traffic, or the firewall was previously disabled, and the user has enabled it through the user interface.
Remote config management enabled [port#]	Remote configuration management (via HTTP through the specified port # on the public interface) has been enabled via the user interface.
Remote config management disabled	Remote configuration management has been disabled via the user interface.
Time Of Day established	The system established the current system time via the DOCSIS cable modem registration process. The system time is used by the firewall to timestamp events.
Public Network Interface up (IP address x.x.x.x)	The firewall successfully obtained an IP address for the public network (WAN) interface via DHCP. This process takes place after the cable modem registration process successfully completes.

12

Parental Control Menu Options

The Parental Control Menu lets you:

- *Configure the rules for Internet access based on user or time period*
- *Configure the rules to block certain Internet contents and certain web sites*
- *View the event logs related to parental control*

To set up Parental Control, you first set up Policies in the [Basic Setup](#) submenu. Next, you assign a user name and password for each user on your network. Finally you apply the Policies to individual users in the [User Setup](#) Menu. When you enable Parental Control, each user must log on to view Internet content. The content a user may access will be defined by the policy that you assigned to that user. A user profile may optionally be applied to a specific computer, so that no login is required for users of that computer.

Basic

This Basic Setup page allows you to configure rules which block certain Internet content and certain Web sites. An override password and access duration timer allows user override of the content filter settings. When entered, these allow a user Internet access without the constraint of the rules entered until the timer expires.

To access the Basic page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Parental Control /Basic Setup** submenu.

Figure 27 shows an example of the menu and Table 28 describes the items you can select.

Note: Always remember to click the **Apply** button to complete changes on this page.



Figure 27. Example of Basic Setup Page

Table 28. Basic Setup Menu Option

Option	Description
Enable Parental Control	Check the box to enable Parental Control.
Content Policy Configuration	Enter a name for a content policy, and click Add New Policy .
Content Policy List	Pull-down list that shows Policy Names that you have created. Select the policy you want to define or edit.
Keyword List	Enter a keyword in the field at the bottom of the keyword list, and click Add Keyword . The keyword is associated with the respective entries in the Blocked and Allowed Domain Lists . See the User Setup page for more details.
Blocked Domain List	Type the domain name and add this domain to be blocked item and tied to a particular rule name. Blocked Domain feature can be time constrained to certain parts of the day or night via the settings from the Parental Control - ToD Filter page.
Allowed Domain List	Type the domain name and add this domain to be exclusively passed item and tied to a particular rule name. Allowed Domain feature can be time constrained to certain parts of the day or night via the settings from the Parental Control - ToD Filter page.
Override Password	Enter the password and access duration timer for user override of the content filter settings.

User Setup

The User Setup page is the master page to which each individual “user” is linked to a specified time access rule, content filtering rule, and login password.

To access the **User Setup** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Parental Control /User Setup** submenu.

Figure 28 shows an example of the menu and Table 29 describes the items you can select.

Note: Always remember to click on the appropriate **Apply**, **Add** or **Remove** button to store and activate the settings.

Status **Wireless** **Router** [Logout](#)

Basic
Advanced
Firewall
Parental Control
Basic Setup
User Setup
ToD Access Policy
Event Log
VPN
Management
Cable Modem

Router » Parental Control » User Setup

Add users who will be affected by Parental Control, and assign Policies to these users.(See Basic page).The White List Only feature limits the user to those sites specified in the Allowed Domain List of the Policy you have assigned to him or her. Click the Add User and Remove User buttons as appropriate to save changes.

User Configuration	
<input type="text"/>	Add User
User Settings	
1. Default	<input type="checkbox"/> Enable Remove User
Password	<input type="password"/>
Re-Enter Password	<input type="password"/>
Trusted User	<input type="checkbox"/> Enable
Content Rule	<input type="checkbox"/> White List Access Only 1. Default
Time Access Rule	No rule set
Session Duration	0 min
Inactivity time	0 min
Apply	

Trusted Computers
Optionally, the user profile displayed above can be assigned to a computer to bypass the Parental Control login on that computer.
(Maximum of 10 MAC addresses)

00 : 00 : 00 : 00 : 00 : 00 [Add](#)

No Trusted Computers

Figure 28. Example of User Setup Page

Table 29. User Setup Menu Option

Option	Description
User Configuration	Enter a user name (e.g. Mom, Dad, Bro, Sis) and click Add User .
Users Settings	Select a user from the drop-down list. Click the checkbox to enable parental control for this user.
Password	Enter the password for this user.
Re-Enter Password	Re-enter (confirm) the password for this user.
Trusted User	Select Enable to grant this user access to all Internet content regardless of any policy or time settings.
Content Rule	Select the content policy for this. The content policy is defined in the Parental Control - Basic page.
White List Only	Click this checkbox to limit the user to visit only the sites specified in the Allowed Domain List (see Parental Control - Basic page) of his/her content policy.
Time Access Rule	Select the access time rule for this user. The content policy is defined in Parental Control - ToD Filter page.
Session Duration	Enter the session duration time to limit this user's Internet access time.
Inactivity Time	Configure the inactivity timeout for this user to re-login. If there is no Internet activity for the specified amount of time (in minutes), the user must login again to continue using the Internet.

When all above information has been entered, click the **Apply** button to activate these settings. Repeat for each user.

Trusted Computers	<p>Enter the MAC address of a computer or other device to bypass the login requirement. This computer or device will always have access as defined by the User profile above.</p> <p>The Mac Addresses of the computers attached to your network can be found in the DHCP Clients table. To access the DHCP Clients table click on Router Menu tab, then Basic/My Network submenu.</p>
--------------------------	---

When the above information has been entered, click the **Apply** button to activate these settings. Repeat for each user.

ToD Filter (Time of Day Filter)

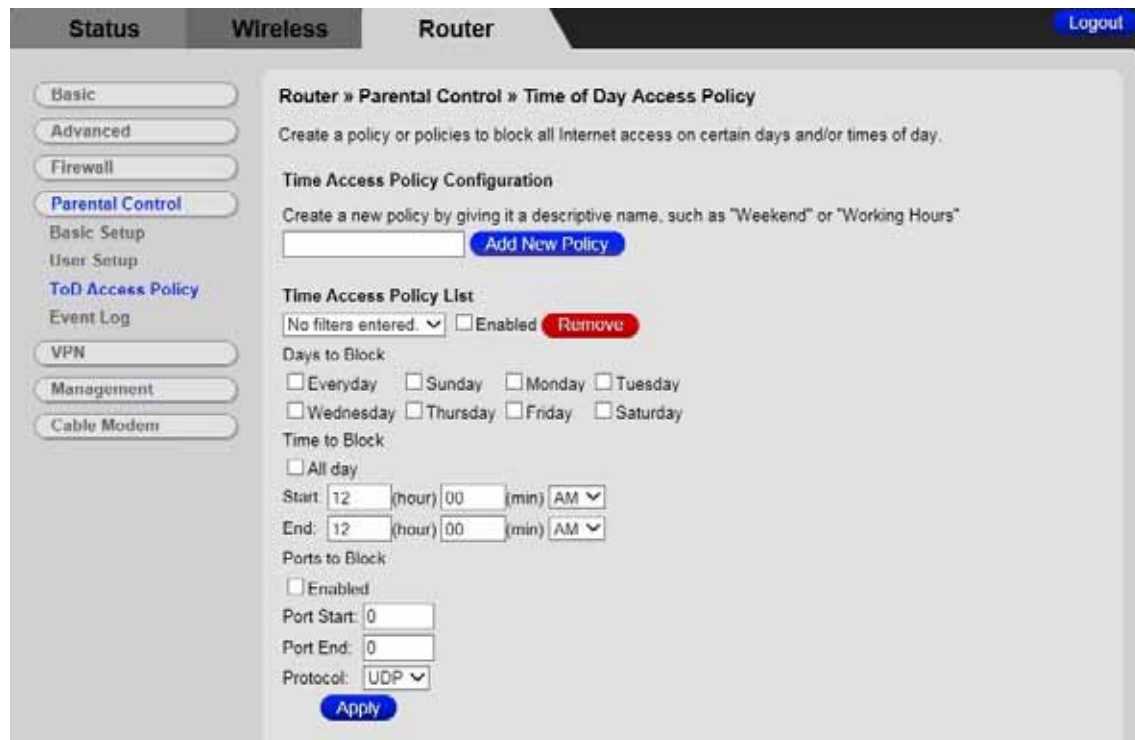
The ToD page allows you to configure the Internet access policies according the time of day settings. This page is tied to the **Parental Control - User Setup** page. You can define up to 30 time access policies. You can define policies that block all public Internet traffic for entire days or for specific time periods within each day. You can combine these policies in any way you want.

To access the **ToD Filter** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Parental Control /ToD Filter** submenu.

Figure 29 shows an example of the menu and Table 30 describes the items you can select.

Note: Always remember to click on the appropriate **Apply**, **Add** or **Remote** button to store and activate the settings.



The screenshot shows a web interface for configuring a Time of Day (ToD) filter. The interface is divided into a left sidebar and a main content area. The sidebar contains a navigation menu with the following items: Basic, Advanced, Firewall, Parental Control (highlighted), Basic Setup, User Setup, ToD Access Policy (highlighted), Event Log, VPN, Management, and Cable Modem. The main content area is titled "Router » Parental Control » Time of Day Access Policy" and includes a "Logout" button in the top right corner. Below the title, there is a description: "Create a policy or policies to block all Internet access on certain days and/or times of day." The "Time Access Policy Configuration" section contains a text input field for a policy name and an "Add New Policy" button. The "Time Access Policy List" section shows "No filters entered" and an "Enabled" checkbox. Below this, there are sections for "Days to Block" (with checkboxes for Everyday, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday) and "Time to Block" (with an "All day" checkbox and time selection fields for Start and End). The "Ports to Block" section includes an "Enabled" checkbox, "Port Start" and "Port End" input fields, and a "Protocol" dropdown menu set to "UDP". An "Apply" button is located at the bottom of the configuration area.

Figure 29. Example of ToD Filter Page

Table 30. ToD Filter Menu Option

Option	Description
Time Access Policy Configuration	Enter a name for the time access policy and click Add New Policy .
Time Access Policy List	Select a policy from the drop-down list. Click the Enable checkbox to enable this rule.
Days to Block	Click the checkboxes of the days that this rule applies to.
Time to Block	Click the checkbox All Day to define this policy to block Internet access for the entire day of each day selected – or enter the start and stop times of the periods you want to block access. Note: If you want to allow access for only a part of the day, you may need to create and apply two time policies. See example below.
Ports to Block	Click enable if you want to block specific ports
Port Start	This is first port you want to block.
Port End	This is the end of the range of ports you want to block. If you only want to block one port enter the port number in both the start and end fields.

Example of Time to Block – create and apply two time policies to allow access Mon – Fri 7:00pm – 9:00pm:

Time Policy Name	Days to Block	Time to Block
Weekday I	Mon – Fri	12:00am – 7:00pm
Weekday II	Mon – Fri	9:00pm – 12:00am

Select both Weekday I and Weekday II at User/Time Access Rule.

Event Log

The Event Log page shows you the events related to the settings of Parental Control. This table is a running list of the last 30 Parental Control access violations that include the following items on Internet traffic:

- If the user's internet access is blocked. (time filter)
- If a blocked keyword is detected in the URL.
- If a blocked domain is detected in the URL.
- If the online lookup service detects that the URL falls in a category that is blocked.

To access the **Event Log** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Parental Control /Event Log** submenu.

Figure 30 shows an example of the menu.

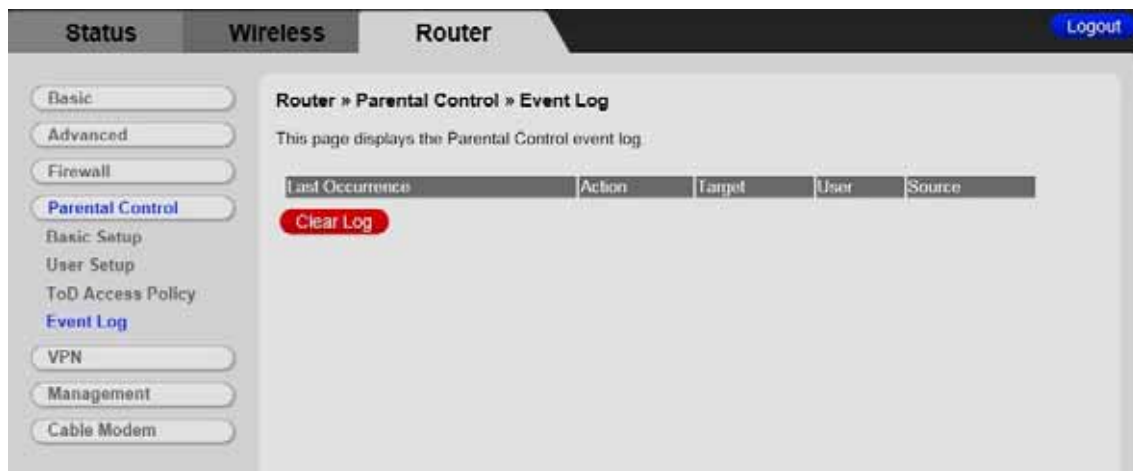


Figure 30. Example of Event Log Page

13

VPN (Virtual Private Network) Menu Options

The **VPN Menu** lets you:

- Configure a VPN tunnel
- View VPN event logs

Basic Setting

This page allows you to enable VPN protocols and manage VPN tunnels. A virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits within some larger network (e.g., the Internet) as opposed to by physical wires, as in a traditional private network. A VPN can be used to separate the traffic of different user communities over an underlying network with strong security features.

To access the **Basic** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **VPN/Basic** submenu.

Figure 31 shows an example of the menu and Table 30 describes the items you can select.

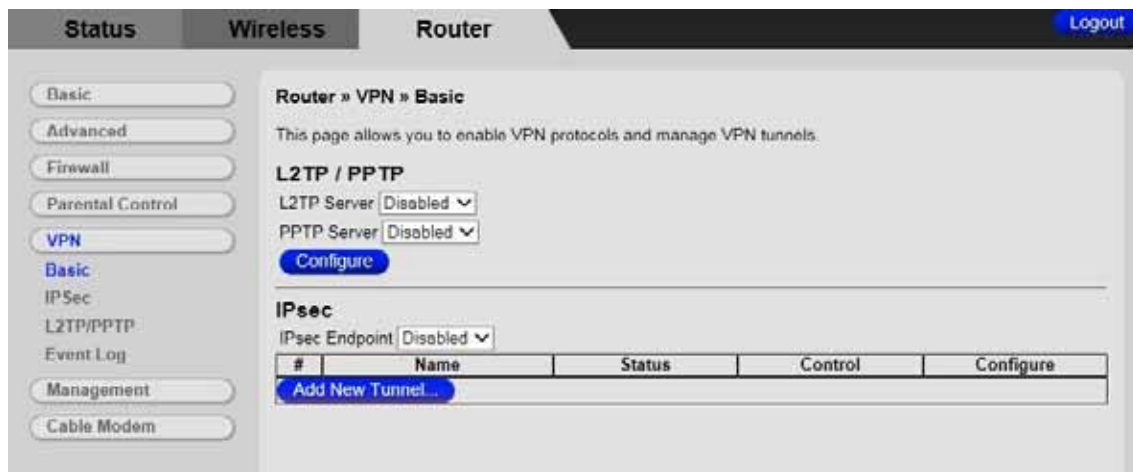


Figure 31. Example of Basic Page

Table 31. Basic Menu Option

Option	Description
L2TP Server	Select Enable to enable L2TP (Layer 2 Tunneling Protocol) server.
PPTP Server	Select Enable to enable PPTP (Point-to-Point Tunneling Protocol) server.
Configure	Select Configure to set up L2TP or PPTP.
IPSec Endpoint	Select Enable to enable IPSec endpoint.

IPSec

The IPSec page allows you to configure IPSec tunnel and endpoint settings. A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters Cable Modem/Router and the remote IPSec Cable Modem/Router will use.

- The **first phase** establishes an Internet Key Exchange (IKE) SA between the Cable Modem/Router and the remote IPSec Cable Modem/Router.
- The **second phase** uses the IKE SA to securely establish an IPSec SA through which the Cable Modem/Router and remote IPSec Cable Modem/Router can send data between computers on the local network and remote network.

Before IPSec VPN configuration, try to familiarize yourself with terms like IPSec Algorithms, Authentication Header and ESP protocol.

IPSec Algorithms

The ESP and AH protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the AH and ESP protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

AH (Authentication Header) Protocol

The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an AH can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

ESP (Encapsulating Security Payload) Protocol

The ESP protocol (RFC 2406) provides encryption as well as the services offered by AH. ESP authenticating properties are limited compared to the AH due to the non-inclusion of the IP header information during the authentication process. However, ESP is sufficient if only the upper layer protocols need to be authenticated. An added feature of the ESP is payload padding, which further protects communications by concealing the size of the packet being transmitted.

To access the **IPSec** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **VPN /IPSec** submenu.

Figure 32 shows an example of the menu and Table 32 describes the items you can select.

The screenshot displays the configuration interface for an IPSec tunnel. The breadcrumb trail is 'Router » VPN » IPSec'. The page title is 'Router » VPN » IPSec'. Below the title, it states 'This page allows configuration of IPSec tunnels.' The interface is divided into several sections:

- Tunnel List:** Shows 'Tunnel list is EMPTY.' with a dropdown arrow. To the right are buttons for 'Delete Tunnel' (red), 'Add New Tunnel' (blue), and 'Apply' (blue).
- Local endpoint settings:**
 - Address group type: IP subnet (dropdown)
 - Subnet: 192 . 168 . 0 . 0
 - Mask: 255 . 255 . 255 . 0
 - Identity type: IP address (dropdown)
 - Identity: (null)
- Remote endpoint settings:**
 - Address group type: IP subnet (dropdown)
 - Subnet: 0 . 0 . 0 . 0
 - Mask: 0 . 0 . 0 . 0
 - Identity type: IP address (dropdown)
 - Identity: (null)
 - Network address type: IP address (dropdown)
 - Remote Address: 0.0.0.0
- IPsec settings:**
 - Pre-shared key: (null)
 - Phase 1 DH group: Group 1 (168 bits) (dropdown)
 - Phase 1 encryption: DES (dropdown)
 - Phase 1 authentication: MD5 (dropdown)
 - Phase 1 SA lifetime: 0 seconds
 - Phase 2 encryption: DES (dropdown)
 - Phase 2 authentication: MD5 (dropdown)
 - Phase 2 SA lifetime: 0 seconds

At the bottom of the configuration area, there are buttons for 'Show Advanced Settings' (blue) and 'Apply' (blue).

Figure 32. Example of IPSec Page

Table 32. IPsec Menu Option

Option	Description
Tunnel	This is a pull-down list of VPN Names defined below. Select the specific VPN tunnel to configure.
Name	Enter a VPN name and click Add New Tunnel .
Local Endpoint Settings	Configure the local network located at your Cable Modem/Router's LAN side.
Address Group Type	Define the local address type. Select IP Subnet to protect the whole subnet; select Single IP address to protect a single PC or device; select IP address range to protect several PCs, or devices.
Subnet	Enter the subnet scale for address group.
Mask	Enter the subnet mask for address group.
Identity Type	Select the type to identify the Cable Modem/Router. The choices are: WAN IP address, LAN IP address, FQDN (Fully Qualified Domain Name) or Email address.
Identity	Enter the value corresponding to the selected identity type.
Remote Endpoint Settings	Record the parameters of the network on which the peer VPN is located.
Address Group Type	Define the local address type. Select IP Subnet to protect the whole subnet; select Single IP address to protect a single PC; select IP address range to protect several PCs.
Subnet	Enter the subnet for address group.
Mask	Enter the subnet mask for address group.
Identity Type	Select the type to identify the Cable Modem/Router. The choices are WAN IP address, IP address, FQDN or Email address.
Identity	Enter the value corresponding to the selected identity type.
Network Address Type	Enter the IP address or domain name of the peer VPN Cable Modem/Router. You can select IP address, which is typically suitable for static public IP addresses or FQDN, which is typically suitable for dynamic public IP address.

Remote Address	Enter IP address according to the Network Address Type .
IPSec Settings	Configure the IPSec protocol related parameters.
Pre-Shared Key	Enter a key (Pre-Shared key) for authentication.
Phase 1 DH Group	Select the Diffie-Hellman key group (DHx) you want to use for encryption keys. DH1: uses a 768-bit random number DH2: uses a 1024-bit random number DH5: uses a 1536-bit random number.
Phase 1 Encryption	Select the key size and encryption algorithm to use for data communications. DES: a 56-bit key with the DES encryption algorithm 3DES: a 168-bit key with the DES encryption algorithm. Both the Cable Modem/Router and the remote IPSec router must use the same algorithms and key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. Longer keys require more processing power, resulting in increased latency and decreased throughput. AES: AES (Advanced Encryption Standard) is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES. Here you have the choice of AES-128, AES-192 and AES-256.
Phase 1 Authentication	Select the hash algorithm used to authenticate packet data in the IKE SA. SHA1: generally considered stronger than MD5, but it is also slower. MD5 (Message Digest 5): produces a 128-bit digest to authenticate packet data. SHA1 (Secure Hash Algorithm): produces a 160-bit digest to authenticate packet data.
Phase 1 SA Lifetime	In this field define the length of time before an IKE SA automatically renegotiates. This value may range from 120 to 86400 seconds. A short SA lifetime increases security by forcing the two VPN Cable Modem/Router's to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources

	are temporarily disconnected.
Phase 2 Encryption	<p>Select the key size and encryption algorithm to use for data communications.</p> <p>Null: No data encryption in IPsec SA. Not recommended.</p> <p>DES: a 56-bit key with the DES encryption algorithm</p> <p>3DES: a 168-bit key with the DES encryption algorithm. Both the Cable Modem/Router and the remote IPsec router must use the same algorithms and key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. Longer keys require more processing power, resulting in increased latency and decreased throughput.</p> <p>AES: Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES. Here you have the choice of AES-128, AES-192 and AES-256.</p>
Phase 2 Authentication	Select the hash algorithm used to authenticate packet data in the IKE SA. SHA1 is generally considered stronger than MD5, but it is also slower.
Phase 2 SA Lifetime	In this field define the length of time before an IPsec SA automatically renegotiates. This value may range from 120 to 86400 seconds.
Key Management	Select to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.
IKE Negotiation Mode	<p>Select how Security Association (SA) will be established for each connection through IKE negotiations.</p> <p>Main Mode: ensures the highest level of security when the communicating parties are negotiating authentication (phase 1).</p> <p>Aggressive Mode: quicker than Main Mode because it eliminates several steps when the communicating parties are negotiating authentication (phase 1).</p>
Perfect Forward Secrecy (PFS)	Perfect Forward Secret (PFS) is disabled by default in phase 2 IPsec SA setup. This allows faster IPsec setup, but is not as secure. You can select DH1, DH2 or DH5 to enable PFS.
Phase 2 DH Group	Select DHx after enabling PFS.

Replay Detection	Select Enable to enable replay detection. As VPN setup is processing intensive, the system is vulnerable to Denial of Service (DOS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks.
NetBIOS Broadcast Forwarding	Select Enable to send NetBIOS (Network Basic Input/Output System) packets through the VPN connection. NetBIOS packets are TCP or UDP packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.
Dead Peer Detection	Select Enable to force the Cable Modem/Router to periodically detect if the remote IPSec Cable Modem/Router is available or not.
Manual Encryption Key	If Manual mode is selected in the Key Management field, enter a 16 hexadecimal digits manual encryption key for encryption.
Manual Authentication Key	Enter a 32 hexadecimal digit unique authentication key to be used by IPSec.
Inbound SPI	Enter a unique SPI (Security Parameter Index) for inbound SPI.
Outbound SPI	Enter a unique SPI (Security Parameter Index) for outbound SPI.

L2TP/PPTP

The L2TP/PPTP page allows you to configure server and security settings. The L2TP (Layer 2 Tunneling Protocol) and PPTP (Point-to-Point Tunneling Protocol) both allow PPP frames to be tunneled through the network. PPTP is a Microsoft proprietary protocol, which is very similar to L2TP.

To access the **L2TP/PPTP** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **VPN /L2TP/PPTP** submenu.

Figure 33 shows an example of the menu and Table 33 describes the items you can select.

The screenshot shows a web interface for configuring L2TP/PPTP. The top navigation bar includes 'Status', 'Wireless', 'Router', and 'Logout'. A left sidebar contains menu items: 'Basic', 'Advanced', 'Firewall', 'Parental Control', 'VPN', 'Basic', 'IPSec', 'L2TP/PPTP', 'Event Log', 'Management', and 'Cable Modem'. The main content area is titled 'Router » VPN » L2TP/PPTP' and contains the following configuration options:

- PPP Address Range:** Start (10.0.0.1) and End (10.0.0.254).
- PPP Security:** MPPE Encryption (Enabled) with an 'Apply' button.
- Users:** Username, Password, and Confirm Password fields with an 'Add' button.
- User List:** A message stating 'User list is empty.'
- L2TP Server:** Preshared Phrase field with an 'Apply' button.

Figure 33. Example of L2TP/PPTP Page

Table 33. L2TP/PPTP Menu Option

Option	Description
PPP Address Range (Start/End)	<p>Configure the dedicated IP address pool for L2TP/PPTP. The LAN IP subnet at one end of the VPN tunnel must be different from the LAN IP subnet at the other end of the VPN tunnel. For example, if one side's LAN subnet is 192.168.0.x, then the other side should be 192.168.1.x (where the subnet mask in this example is 255.255.255.0).</p>
PPP Security (MPPE Encryption)	<p>Select Enable to enable MPPE (Microsoft Point-to-Point Encryption). MPPE is used to enhance the confidentiality of PPP-encapsulated packets. It uses the RSA RC4 encryption algorithm.</p>
Username	<p>Enter the user name for the L2TP or PPTP tunneling.</p>
Password	<p>Enter the password for the L2TP or PPTP tunneling.</p>
Confirm Password	<p>Re-enter to confirm the password.</p>
User List	<p>Show the existing user list.</p>
L2TP Server (Preshared Phrase)	<p>Enter a key (Pre-Shared key) for authentication. This key is used by IPSec to validate the computer as a trusted machine.</p>

Event Log

The Event Log page shows the VPN event log.

To access the **Event Log** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **VPN /Event Log** submenu.

Figure 34 shows an example of the menu and Table 34 describes the items you can select.



Figure 34. Example of Event Log Page

Table 34. Event Log Menu Option

Option	Description
Time	Shows the local time mapping to a certain log event.
Description	Shows detailed information of a VPN event log.

14

Management Menu Options

The Management Menu lets you:

- *Configure Admin Account*
- *Configure Remote Management*
- *View Event Log*
- *Run Diagnostics*
- *Configure Backup and Restore Settings*

Admin Account

This page allows you to configure access privileges.

To access the **VPN /Event Log**:

- 1 Click the **Router** menu tab.
- 2 Then click the Management/Admin Account submenu

Figure 31 shows an example of the menu and Table 35 describes the items you can select.



Figure 35. Example of Admin Account Page

Table 35. Admin account Menu Option

Option	Description
Old Password	Enter the existing security password. The password can be found on the bottom label of the unit.
New Password	Enter the new security password.
Re-Enter New password	Re-enter (confirm) the new security password.

Note: DO NOT restore factory defaults to any changes on this page.

Remote Management

This page allows you to configure remote access to this device via web browser.

To access the **Remote Management** page

- 1 Click the **Router** menu tab.

- 2 Then click the Management/Remote Management submenu

Figure 31 shows an example of the menu and Table 36 describes the items you can select.



Figure 36. Example of the Remote Management page

Table 36. Remote Management Menu Option

Option	Description
Remote Management	Select Enable to allow remote access to this device via web browser.

SNMP Event Log

The SNMP Event Log page shows the content of SNMP event log.

To access the **SNMP Event Log** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Management/Event Log** submenu.

Figure 37 below shows an example of the menu and Table 37 describes the items you can select.

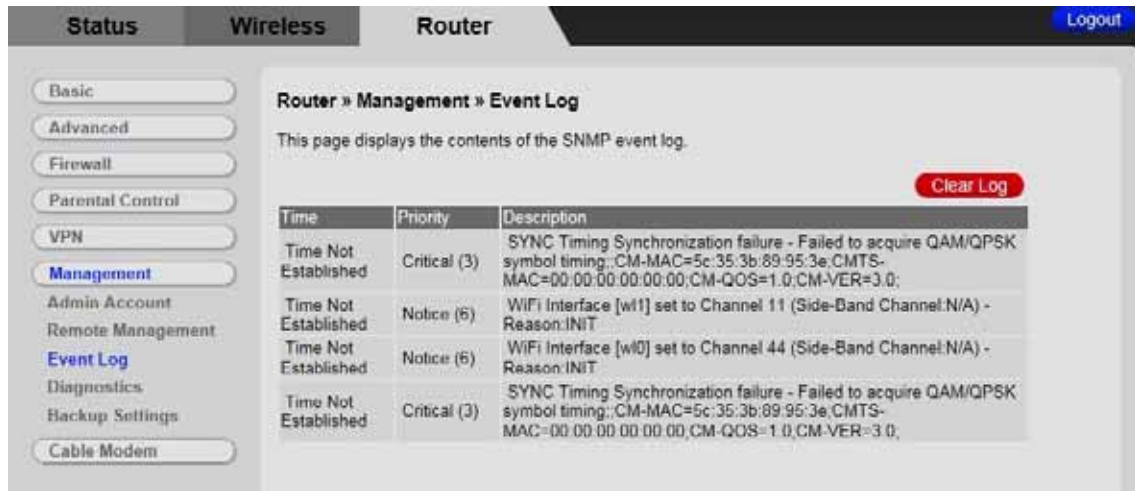


Figure 37 Example of Event Log Page

Table 37 Event Log Menu Option

Option	Description
Time	Shows the local time mapping to a certain log event.
Priority	Shows the priority of the log event issue.
Description	Shows detailed information of a event log.

Diagnostics

Note: Some software versions may not support this feature.

The Diagnostics page allows you to troubleshoot connectivity problems. Two utilities are provided for troubleshooting network connectivity: Ping and Traceroute.

Ping allows you to check connectivity between the Cable Modem/Router and devices on the LAN while Traceroute allows you to map the network path from the Cable Modem/Router to a public host.

Selecting Traceroute from the drop-down Utility list will present alternate controls for the Traceroute utility.

To access the Diagnostics page, click the **Router** menu tab and then click the **Diagnostics** submenu.

Figure 38 and Figure 39 show the examples of the menu and Table 38 describes the items you can select.

The screenshot displays the Router's Diagnostics interface. At the top, there are tabs for 'Status', 'Wireless', and 'Router', with 'Router' being the active tab. A 'Logout' link is visible in the top right corner. On the left side, a vertical menu lists various settings: 'Basic', 'Advanced', 'Firewall', 'Parental Control', 'VPN', 'Management' (highlighted in blue), 'Admin Account', 'Remote Management', 'Event Log', 'Diagnostics' (highlighted in blue), 'Backup Settings', and 'Cable Modem'. The main content area is titled 'Router » Management » Diagnostics'. It includes a sub-header 'Router » Management » Diagnostics' and a descriptive text: 'This page provides diagnostics to help with IP connectivity problems.' Below this, there is a 'Test Utility' dropdown menu currently set to 'Ping'. Underneath, the 'Ping Test Parameters' section contains several input fields: 'Target' with the value '192.168.0.2', 'Ping Size' set to '64' Bytes, 'No. of Pings' set to '3', and 'Ping Interval' set to '1000' ms. Three buttons are located below the parameters: 'Start Test' (blue), 'Abort Test' (blue), and 'Clear Results' (red). At the bottom, a 'Results' section is visible, containing the text 'Waiting for input...'.

Figure 38. Example of Diagnostics - Ping Page

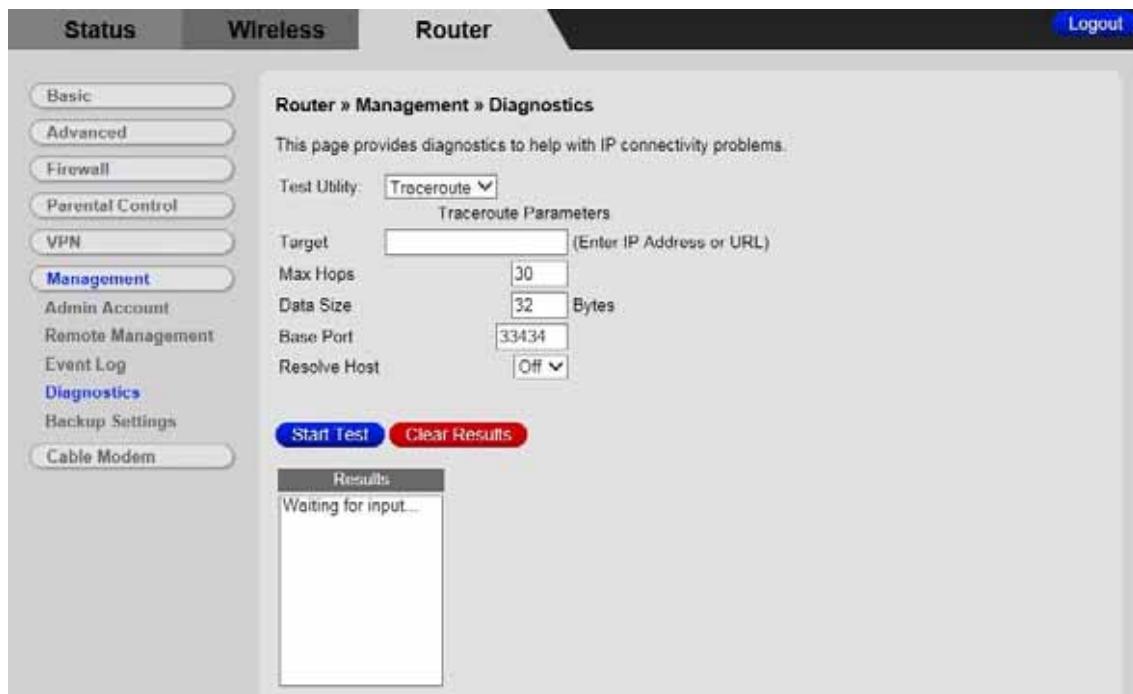


Figure 39. Example of Diagnostics - Traceroute Page

To run either utility:

- 1 Select the utility from the Utility drop-down list.
- 2 Make any changes to the default parameters.
- 3 Select **Start Test** to begin. The window will automatically be refreshed as the results are displayed in the Results table.

Table 38. Diagnostics Menu Option

Option	Description
Utility	Select the utility for troubleshooting.
Parameters	Enter the required parameters to perform diagnostics.
Start Test	Click this button to begin diagnostic after making any changes to the default parameters.
Abort Test	Click this button to abort Ping diagnostics.
Clear Results	Click this button to clear the results table.

Backup/Restore Settings

The Backup page allows you to save the current Cable Modem/Router configuration settings to a local PC. You can then later restore these settings if you need restore a particular configuration, or to recover from changes you may have made that have had an undesirable effect.

To backup the current configuration:

- Click **Backup** and follow the prompts.

To restore a previous configuration:

- Click **Browse** and use the navigation window to locate the file. (Usually GatewaySettings.bin, unless you rename it before saving.) Once the file has been located, click **Restore** to restore the settings.
- **Note:** Once the settings are restored, the device will reboot.

To access the **Backup/Restore Settings** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Management/Backup Settings** submenu.

Figure 40 shows an example of the menu and Table 39 describes the items you can select.



Figure 40 Example of Backup/Settings Page

Table 39 Backup/Restore Settings Menu Option

Option	Description
Backup	Click the Backup button to save your Cable Modem/Router's current settings locally on your PC.
Restore	Browse the restore file and Click the Restore button to restore settings previously saved.

15

Cable Modem Menu Options

The Cable Modem Menu lets you:

- *View Device Information*
- *View information about your current Connection.*
- *Restore Factory Defaults or Reboot your Cable Modem/Router.*
- *Set the Frequency band your Cable Modem/Router uses.*

Cable Modem Device Information

The Device Information page is a read-only screen that shows the Cable Modem/Router's current system software version, cable modem MAC address, serial number, system up time, network access, cable modem IP address, MDD IP Provisioning mode and IP Provisioning mode override.

To access the **Cable Modem Device Information** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Cable Modem/Device Information** submenu

Figure 41 The Device Information page. shows an example of the page and Table 40 describes the information on the page.

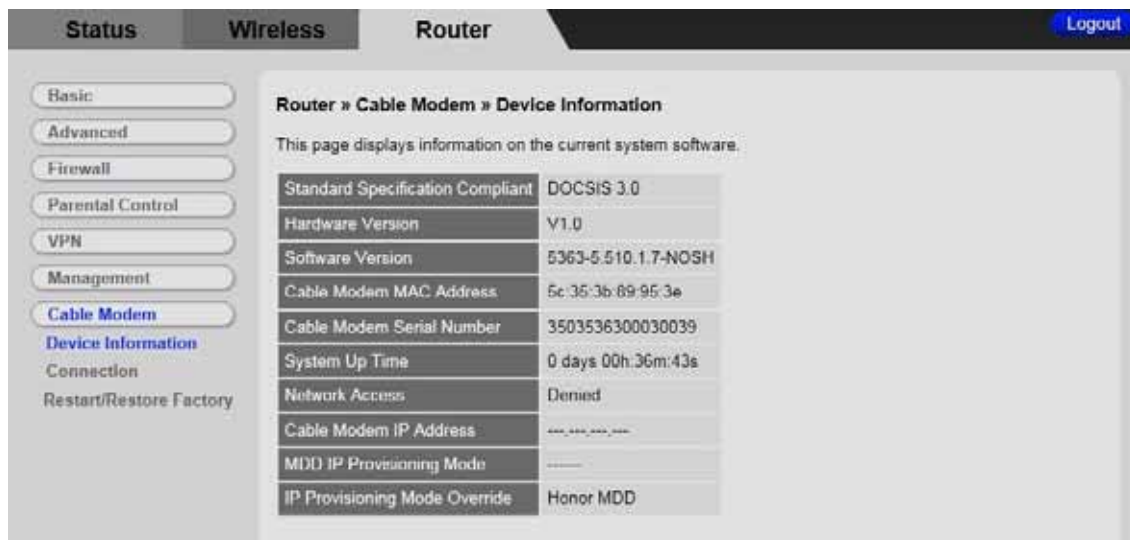


Figure 41 The Device Information page.

Table 40. Device Information Menu Option

Option	Description
Software Version	Shows the information on the current system software.
Information	Shows the Standard Specification Compliant, Hardware Version, Cable Modem Mac Address, Cable Modem Serial Number, System Up Time, Network Access, Cable Modem IP Address, MDD IP Provisioning Mode and IP Provisioning Mode Override.

Connection

The Connection page is a read-only screen that shows the status of the steps in your Cable Modem/Router registration process. It also shows your Cable Modem/Router's upstream and downstream channel status.

To access the **Cable Modem Connection** page:

- 1 Click the **Router** menu tab.
- 2 Then click the **Connection** submenu.

Figure 42. Example of the Connection Page shows an example of the page and Table 40 describes the information on the page.

Status **Wireless** Router Logout

Basic
Advanced
Firewall
Parental Control
VPN
Management
Cable Modem
Device Information
Connection
Restart/Restore Factory

Router » Cable Modem » Connection

This page displays information about the connection to the cable network.

Startup Procedure		
Procedure	Status	Comment
Acquire Downstream Channel	993000000 Hz	In Progress
Connectivity State	In Progress	Not Synchronized
Configuration File	In Progress	

Downstream Bonded Channels								
Channel	Lock Status	Modulation	Channel ID	Frequency	Power	SNR	Correctables	Uncorrectables
1	Not Locked	Unknown		993000000 Hz	0.0 dBmV	0.0 dB	0	0
2		Unknown		0 Hz	0.0 dBmV	0.0 dB	0	0
3		Unknown		0 Hz	0.0 dBmV	0.0 dB	0	0
4		Unknown		0 Hz	0.0 dBmV	0.0 dB	0	0
5		Unknown		0 Hz	0.0 dBmV	0.0 dB	0	0
6		Unknown		0 Hz	0.0 dBmV	0.0 dB	0	0
7		Unknown		0 Hz	0.0 dBmV	0.0 dB	0	0
8		Unknown		0 Hz	0.0 dBmV	0.0 dB	0	0

Total Correctables	Total Uncorrectables
0	0

Upstream Bonded Channels						
Channel	Lock Status	US Channel Type	Channel ID	Symbol Rate	Frequency	Power
1		Unknown		0 Ksym/sec	0 Hz	0.0 dBmV
2		Unknown		0 Ksym/sec	0 Hz	0.0 dBmV
3		Unknown		0 Ksym/sec	0 Hz	0.0 dBmV
4		Unknown		0 Ksym/sec	0 Hz	0.0 dBmV

Current System Time: ---:--:--

Figure 42. Example of the Connection Page

Restart/Restore Factory/Frequency set

The Restart/RestoreFactory page allows you to configure restart and restore the Cable Modem/Router to its factory defaults.

To access the Restart/Restore Factory page, click the **Router** menu tab and then click the Cable Modem/Restart/Restore Factory submenu.

Figure 43 shows an example of the page.

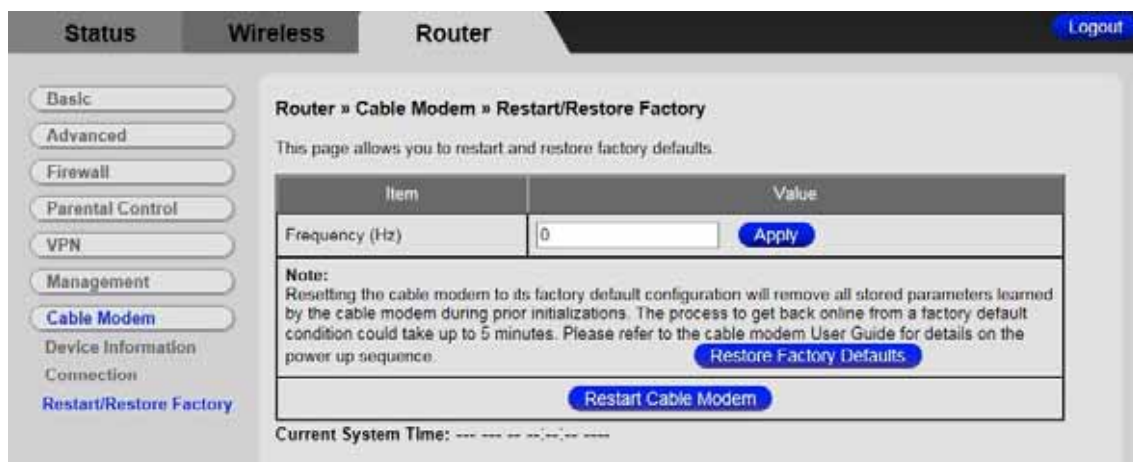


Figure 43. Example of Restart/Restore Factory Page

To restore the Cable Modem/Router to factory defaults:

- 1 In the Restart/Restore Factory submenu, click the **Restore Factory Defaults** button.
- 2 Please wait 2 to 3 minutes then log back in to the Configuration Manager.

To restart the Cable Modem/Router to factory defaults:

- 1 In the Restart/Restore Factory submenu, click the **Restart Cable Modem** button.
- 2 Please wait 2 to 3 minutes then log back in to the Configuration Manager.

Appendix A: Troubleshooting Tips

Problem: I cannot access the Internet. What should I do first?

Solution:

- Make sure that your Cable Modem/Router's MAC address is registered with your cable provider. When your provider's representative or setup software asks for your MAC address, you can find the **CM MAC** address on your modem/router's bottom label. If you are having a problem, you may need to check with your cable service provider to make sure the service provider set up its system properly for your cable modem.
- Check your Cable Modem/Router's Ethernet and coaxial cable connections. Make sure the coaxial cable is tightly connected. If a computer is plugged into an Ethernet port, make sure that the cable is plugged in all the way on both ends.
- If you are using wireless, check that your wireless connection is functioning correctly. Check the section below, "I am having trouble connecting my computer or other device wirelessly to the Cable Modem/Router."
- Power off your modem/router for at least 10 seconds and then power it back on.
- Restart your computer or other devices connected to the Cable Modem/Router. This ensures that they receive a correct IP address from the router.

Problem: I cannot access the Internet. My Power light is on, my Downstream and Upstream lights are on or blinking, and my Online light is on.

Solution:

- If you are using your computer's Ethernet port, check that there is a good connection between your computer and the modem/router's Ethernet port. Check that the light for that port is on or flashing.
- If you are using wireless, check that your wireless connection is functioning correctly. Check the section below, "I am having trouble connecting my computer or other device wirelessly to the Cable Modem/Router."

Problem: I cannot access the Internet. My Power light is on, and my Downstream and Upstream lights are on or blinking. My Online light won't stay on.

Solution:

- Check to see that your cable TV is working. If it isn't, contact your cable service provider. There may be a bad connection to the cable to your home or location.
- Check with your cable service provider to make sure that your cable data service is available and running.
- In some cases, the cable signal may be weak or noisy. If possible, see if the cable modem/router works better when it's connected as near as possible to where the coaxial cable comes into your home.
- If you have a splitter between the cable modem/router and the wall, remove the splitter and connect the cable modem/router directly to the wall. A splitter is a small device that has a single coax cable on one side and 2 coax cables on the other side. If this fixes the problem, you may need to get a better splitter.
- If the problem persists, you may need to ask your cable service provider to check the signal quality on your cable connection.

Problem: I am having trouble connecting my computer or other device wirelessly to the Cable Modem/Router.

Solution: Try the following:

- Verify that you can access the Internet with a computer or other device connected through an Ethernet cable to one of the LAN ports of your cable modem/router.

If you cannot, try the steps outlined in the previous troubleshooting tips.

If the wired computer can access the Internet, reboot the wireless device (this will allow the device to release and renew their IP addresses) and try to access the Internet again.

If you still cannot connect to the Internet wirelessly, continue below.

- Check the wireless security settings on the wireless device and verify that your device is using the same wireless security and password as the Cable Modem/Router. The default wireless settings can be found on the bottom label of your router. The settings on your computer, phone, or other device must match the modem/router settings – either the default settings or some new settings you made.
- Check the signal strength of your wireless connection. Most wireless adapters have some type of signal strength meter that shows how strong your wireless signal is. **Windows users**, click the **Wireless** icon in your system tray to check signal strength. If your signal strength is not strong enough, try reorienting the antennas on the Cable Modem/Router.
- Change the wireless channel. To do that, follow these steps:
 - 1 Open the Zoom Configuration Manager by entering the following in your Web browser's address bar: <http://192.168.0.1>
 - 2 In the **Login** dialog box, type the following User Name and Password in lower case, and then click **Login**.

User Name: admin Password: admin

- 3 Click **Wireless** on the menu tab to open the **Wireless** page.
 - 4 On the Radio page, Under Select 2.4 or 5 GHz option. If you chose to use 2.4 GHz, then go from the **Control Channel** drop-down menu, select a channel that is 5 channels away from the current channel you are using. You may need to switch the **Sideband for Control Channel** setting from lower to upper to access the higher channels. If you chose to use 5 GHz, then go from the Channel Specification drop-down menu, select a different channel.
 - 5 Be sure to click **Apply** after you change the channel. All devices connecting wirelessly will automatically switch to the new channel.
- If changing the wireless channel did not help, you should reduce the amount of bandwidth your wireless connection is using from 40 Mhz to 20 Mhz on the same **wireless** page.
 - Move the device trying to access the Cable Modem/Router to a different location, ideally closer to the Cable Modem/Router.
 - If possible, move the Cable Modem/Router to a new location, ideally closer to the wireless device.

- For some computers and some tablets, try deleting the old network settings including the SSID and password/pre-shared key. After you do that, use the new settings. Normally the new settings should be the modem/router's default settings as discussed above.
- Refer to your computer's or other device's documentation if necessary.

Problem: I changed the subnet mask of my LAN (most people don't). I can't access the Cable Modem/Router's Configuration Manager.

Solution:

- Manually reset the modem/router. Insert a paper clip into the RESET opening on the front panel, then press and hold down for 10 seconds. Then power off your computer and power it back on. After you've done that, re-enter **http://192.168.0.1** in your web browser's address bar.

Problem: I don't know my Cable Modem/Router's SSID or Password.

Solution:

The default values are printed on the bottom label of the modem/router.

If you have **changed** these values, connect a computer to any Ethernet port of the modem, open the computer's Web browser, enter <http://192.168.0.1> into the browser's address bar, and press ENTER to go to that address. When the modem/router's user interface comes up, enter **admin** for both the username and password. Under the Status page you will find the Wireless SSID and password (also called Pre-shared Key or Passphrase).

Problem: What if I'm told that Model 5363 Cable Modem/Router isn't approved for my cable modem service?

Solution: This product has been certified by CableLabs®, the cable service provider's primary test lab. However, some cable service providers have their own certification process. To see whether model 5363 is certified by your cable service provider, you should be able to check your service provider's Web site or to speak with someone from your service provider.

Appendix B: If You Need Help

We encourage you to register your product and to notice the many support options available from Zoom. Please go to www.zoomtel.com/techsupport. From here you can **register your router** and/or **contact our technical support experts** and/or use our intelligent database **SmartFacts™** and/or get **warranty** information.

US: (617) 753-0963

UK - London: +44 2033180660

UK - Manchester: +44 1618840074

Appendix C: Compliance

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device is going to be operated in 5.15~5.25GHz frequency range, it is restricted in indoor environment only.

IMPORTANT NOTE:

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Note to CATV System Installer - This reminder is provided to call the CATV systems installer's attention to Section 820-93 of the National Electric Code which provide guideline for proper grounding and, in particular, specify that the Coaxial cable shield shall be connected to the grounding system of the building, as close to the point of cable entry as practical.