

Cable Modem/Router with Wireless-N

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 2013 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

GETTING STARTED	5
Package Contents.....	5
System Requirements.....	5
INSTALLING THE CABLE MODEM/ROUTER WITH WIRELESS-N	7
Before Installing Your Cable Modem/Router	7
If your cable service provider provided a cable modem starter kit	7
Hardware Connection.....	11
CONNECTING OTHER DEVICES TO THE CABLE MODEM/ROUTER	13
<i>Establishing your Wireless Network</i>	14
Connecting a Windows 8 Computer with Built-in Wireless Capabilities	15
Connecting a Windows 7 Computer with Built-in Wireless Capabilities.....	16
Connecting a Windows Vista Computer with Built-in Wireless Capabilities	16
Connecting a Windows XP Computer with Built-in Wireless Capabilities.....	18
Connecting a Macintosh OS X Computer with Built-in Wireless Capabilities.....	19
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.....	20
Connecting a Computer with a Wireless adapter to the Cable Modem/Router	21
Using WPS as an alternative way to set up your Wireless Network	22
Connecting Additional Computers and/or Other Devices to the Cable Modem/Router's Ethernet/LAN ports	23
CHANGING THE DEFAULT WIRELESS SETTINGS	25
About Wireless Security	25
Changing your Wireless Network Name(SSID) and Pre-Shared Key	26
Setting Up Security Using WEP	27
Disabling Security	28
ONLINE GAMING	29
Gaming	29
DMZ Host.....	30
Port Triggers.....	31
ADVANCED SETTINGS	34
Changing Default Settings.....	34
Accessing the Zoom Configuration Manager	35
Understanding the Configuration Manager Interface Screens.....	36
Configuration Manager Interface Menus	37
STATUS MENU OPTIONS	39
Software	39
Connection	40
Security.....	41
Diagnostics	43
BASIC MENU OPTIONS	47
Setup	47
DHCP.....	49
DDNS	50
Backup	52

ADVANCED MENU OPTIONS	54
Options	54
IP Filtering	57
MAC Filtering.....	58
Port Filtering.....	60
Forwarding.....	61
Port Triggers.....	63
DMZ Host.....	64
RIP Setup	65
FIREWALL MENU OPTIONS	68
Basic.....	68
Event Log	69
PARENTAL CONTROL MENU OPTIONS	75
Basic.....	75
User Setup	78
ToD Filter (Time of Day Filter)	80
Event Log	81
WIRELESS MENU OPTIONS	83
Radio.....	83
Primary Network	85
Guest Network.....	88
Advanced	92
Access Control	94
WMM (Wi-Fi Multimedia).....	95
Bridging	97
VPN (VIRTUAL PRIVATE NETWORK) MENU OPTIONS	99
Basic Setting	99
IPSec	100
L2TP/PPTP.....	106
Event Log	108
APPENDIX A: TROUBLESHOOTING TIPS	110
APPENDIX B: IF YOU NEED HELP	113
APPENDIX C: COMPLIANCE	114

1

Getting Started

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

Package Contents

Your package contains the following items:

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

System Requirements

- You need to connect the Cable Modem/Router 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.
- To configure your modem, we recommend you use a computer with a built-in Ethernet port if one is available. If one is not available, you can use a wireless device to configure you modem.

You may have already used the Quick Start flyer to set up your Cable Modem/Router, to establish an Internet connection, and perhaps to set up a local area network. If you did, you may not need to read this User Manual. On the other hand, you may choose to read this User Manual for topics not covered in the Quick Start or to make changes to the settings you previously configured.

- If you haven't already set up your Cable Modem/Router using the Quick Start, go to [Chapter 2: Installing the Cable Modem/Router with Wireless-N](#).

- If you have already installed your cable modem and want to learn how to connect both wired and wireless computers and other devices to your Cable Modem/Router go to: [Chapter 3: Connecting Other 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 with Wireless-N

This chapter provides basic instructions for connecting the hardware and configuring the Cable Modem/Router with Wireless-N using the Zoom Configuration Manager. This chapter is almost identical to the printed Quick Start.

Before Installing Your Cable Modem/Router

Your cable service provider needs to know your modem's **CM-MAC ADDRESS (also called MAC address)**, which is printed on a label on the bottom of your modem.

- You can provide the CM-Mac address when you order cable modem service.
- Some cable companies provide setup software that will tell them the CM-MAC Address.
- You can call the cable company BEFORE installing your modem.

You may also be asked for your cable modem's model name and number, which is **ZOOM 5352**. If you need the modem's **serial number**, you can find it near the CM-MAC address on the label.

If your cable service provider provided a cable modem starter kit, please continue below. If you don't have or choose not to use the cable modem starter kit from your service provider, go below to [How to connect to a computer if you don't have or choose not to use a cable modem starter kit](#).

If your cable service provider provided a cable modem starter kit

Some cable service providers supply a cable modem starter kit that can be useful when you install your cable modem. The kit may include a coaxial cable for connecting between a wall jack and your cable modem. (These are also available at most electronics retailers.) The kit will include instructions, and may also include a CD with

software. If you receive a kit like this, we recommend that you read the kit's instructions and use them to install your Zoom Cable Modem/Router. This modem is a DOCSIS 3.0 cable modem/router certified by CableLabs, and connects like a normal cable modem.

You will need to plug in the Cable Modem/Router's power cube, connect to cable modem service using a coaxial cable, and then connect to a computer using either the included Ethernet cable or the wireless feature.

Note: Please refer to the [Hardware Connection](#) section if you would like to see a diagram of the back of the Cable Modem/Router and a description of the connections. You will probably need to take a plastic cap off the RF connector.

After you have installed your cable modem and it has synchronized itself with the cable network, your cable modem can connect your computers, tablets, smartphones and other Wi-Fi compatible or Ethernet-enabled devices to the Internet.

Note: It normally takes 5 to 30 minutes to establish an Internet link the first time a Cable Modem/Router connects to a cable service provider. This allows the cable modem to connect to the appropriate channels for communication. You'll see the DS, US, and/or Online modem lights on your cable modem flashing until the Online light stays steady green to signal success.

Now open the browser of a device connected through a cable or wirelessly to your modem/router. If the browser works, your cable modem is working!

- To learn how to connect both wired and wireless computers and other devices to your Cable Modem/Router go to: [Chapter 3: Connecting Other Devices to your Cable Modem/Router](#).
- Your Cable Modem/Router comes from the factory with a default SSID (Wireless Network Name), **WPA-PSK/WPA2-PSK** wireless security and a random Pre-Shared Key (Security Key/Password). These default settings for your modem/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 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 you may 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 go to [Chapter 6: Advanced Settings](#).

How to connect to a computer if you don't have or choose not to use a cable modem starter kit

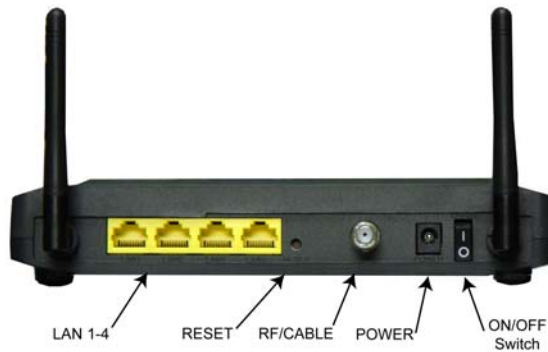
- 1 Be sure your computer is on and the Cable Modem/Router is unplugged.
Note: Please refer to the [Hardware Connection](#) section if you would like to see a diagram of the back of the cable modem and a description of the connections as you read the following steps.
- 2 If there's a plastic cap on the **RF** connector at the back of the cable modem, remove the cap. Connect and securely fasten the coaxial cable onto the round, silver **RF** connector. If the other end of the coaxial cable is loose, connect that end securely to a cable outlet or splitter.
 - You can connect a coaxial cable between an open cable service wall jack and the cable modem. (If no wall jack is available, you can use a coaxial T connector or splitter to share an existing connection with a TV, for example.)
 - Alternatively, there may already be a coaxial cable that is connected to service and that has an open end for connecting to the cable modem.
 - If you are replacing an existing cable modem unscrew the existing coaxial cable from your existing cable modem and then connect it to the **Cable** connector of your Zoom Cable Modem/Router.
- 3 Plug the power cube into the **POWER** connector on the rear panel of the cable modem and into an electrical outlet. Make sure the On/Off switch on the back of the cable modem is on. The Cable Modem/Router should go on with the **Power** LED lit up.

Note: It normally takes 5 to 30 minutes to establish an Internet link the first time a Cable Modem/Router connects to a cable service provider. This allows the cable modem to connect to the appropriate channels for communication. You'll see the DS, US, and/or Online modem lights on your cable modem flashing until the Online light stays steady green to signal success.

- 4 Check to make sure you have Internet access. If you have a computer, connect the modem's Ethernet cable to any Ethernet port (LAN 1, 2, 3, or 4) on the rear panel of the Cable Modem/Router and connect the other end to an Ethernet port on your computer. Now open your browser and go to a familiar Web site to check that the cable modem is working. If it is, your cable modem is ready for use!

- To learn how to connect additional wired and wireless computers and other devices to your Cable Modem/Router go to: [Chapter 3: Connecting Other 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 (Security Key/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](#).

Hardware Connection



Port	Description
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.
RF / Cable	Connect your coaxial cable line to this port.
POWER	Connect the supplied power cube to this port.
ON/OFF SWITCH	Powers the Cable Modem/Router on or off.

Front Panel LEDs

Your Zoom cable modem has several lights on its front panel to help you monitor the Cable Modem/Router's status.

LIGHT	COLOR	DESCRIPTION
WPS	Green	BLINKING: WPS is in discovery mode (LED blinks for up to 2 minutes) ON: LED lit solid for 30 seconds after WPS configuration is successful OFF (after 2 minutes blinking): No Wi-Fi client associated with the Cable Modem/Router via WPS
WLAN	Green	BLINKING: Data is flowing ON: Wi-Fi is enabled OFF: Wi-Fi is not enabled
LINK 1-4 Ethernet LAN ports	Green or Amber	BLINKING: Data is flowing Green: Connected at highest LAN speed, 1 Gbps Amber: Connected at 10 or 100 Mbps OFF: No Ethernet link detected
Online	Green	BLINKING: Cable interface is acquiring IP, Time of Day, and configuration ON: Cable Modem/Router is online OFF: Cable Modem/Router is offline
DS Downstream sync	Green or Blue	BLINKING: Scanning for DS channel GREEN: Synchronized on 1 channel only BLUE: Synchronized with more than 1 channel (DS Bond mode)
US 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 (US Bond mode) OFF: Upstream channel is inactive
DS & US	Blue	Both DS and US blinking together: The Cable Modem/Router is powering up or the cable operator is performing maintenance
Power	Green	ON: power is supplied to the Cable Modem/Router OFF: power is not supplied to the Cable Modem/Router

3

Connecting Other 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 with these wireless 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.
- The default SSID (wireless network name) is assigned as **Zoomxxxx** (where xxxx is 4 random alpha-numeric characters). This SSID is printed on the bottom label of your cable modem/router.

Most users should simply use these default settings. 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 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:

- Many newer **Windows 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, 7, Vista, or XP connect utility. See the sections below on connecting [Windows 8](#) (page 15), [Windows 7](#) (page 16), [Vista](#) (page 16), or [XP](#) (page 18) computers with built-in wireless capabilities.
- If you are using a Macintosh computer see the instructions on page 19 for [Connecting a Macintosh OS X Computer with Built-in Wireless Capabilities](#)
- 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 20 for [Connecting a Wireless-enabled Device to the Wireless-N Router](#).
- 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 21 for [Connecting a Computer with a wireless adapter to the Wireless-N 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 21 for [Connecting a Computer with a wireless adapter to the Wireless-N Router](#).

Connecting a Windows 8 Computer with Built-in Wireless Capabilities


- 1 Click the **Wireless Network Configuration** utility icon  in your computer's system tray.
- 2 Typically you then click **Zoomxxxx** where xxxx is 4 random alpha-numeric characters. **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.
- 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 hit **Connect**. 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 Right-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 Typically you then click **Zoomxxxx** where xxxx is 4 random alpha-numeric characters. **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.
- 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 hit **Connect**. 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 Right-click the wireless network icon in the notification area of the Windows taskbar.
- 2 Right-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 In the **Connect to a network** dialog box, typically you then click **Zoomxxxx** where xxxx is 4 random alpha-numeric characters. **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.

- 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 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.
- 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 From the **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 Typically you then click **Zoomxxxx** where xxxx is 4 random alpha-numeric characters. **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.
- 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 hit **Connect**. 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 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 Typically you then click **Zoomxxxx** where xxxx is 4 random alpha-numeric characters. **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.
- 3 When prompted for the password in the next dialog box, 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.
- 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 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, typically you select **Zoomxxxx** where xxxx is 4 random alpha-numeric characters. **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.
- 2 When prompted for the wireless password, 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.

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 Click or highlight your SSID (wireless network name).
- 3 Select or click on **Disconnect** or similarly-named button.

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 appear, you typically select **Zoomxxxx** where xxxx is 4 random alpha-numeric characters. **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.

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

Note for Windows 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 Wireless-N Router's Wireless Security Name.
- 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 a 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 or 7, computer:

- 1 Open **Connect to a Network** on that computer by right-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** where xxxx is 4 random alpha-numeric characters. **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.



a.

b.

- 5 Press the Wi-Fi Protected Setup (WPS) button on the router for at least 7 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. Then click **OK** on the computer's **Connect to a Network** dialog box.

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 7 seconds. The WPS LED should blink green.
- 2 Within 2 minutes (before the WPS LED 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.
- 6 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

- 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 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.
- 5 To change the wireless security, start by setting all the following drop-down menus to Disable: WPA, WPA-PSK, WPA2, and WPA2-PSK.
- 6 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.

- 7 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.
- 8 Click **Apply**.
- 9 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!

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 Then click **Primary Network** on the left-side menu.
- 5 To change the wireless security, start by setting all the following drop-down menus to Disable: WPA, WPA-PSK, WPA2, and WPA2-PSK
- 6 From the **WEP Encryption** drop-down menu, select **WEP-64 bit (or WEP-128 bit for more security)**.
- 7 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.

- 8 Click **Apply**.
- 9 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 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.
- 5 Set all the following drop-down menus to Disable: WPA, WPA-PSK, WPA2, and WPA2-PSK.
- 6 Click **Apply**.
- 7 Now you need to set up each of your wireless devices with the correct SSID. See [Chapter 3, Connecting other Devices to the Cable Modem/Router](#) for help on connecting your wireless computers and devices. Since Security is disabled you do not need to configure security as described in Chapter 3.

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.

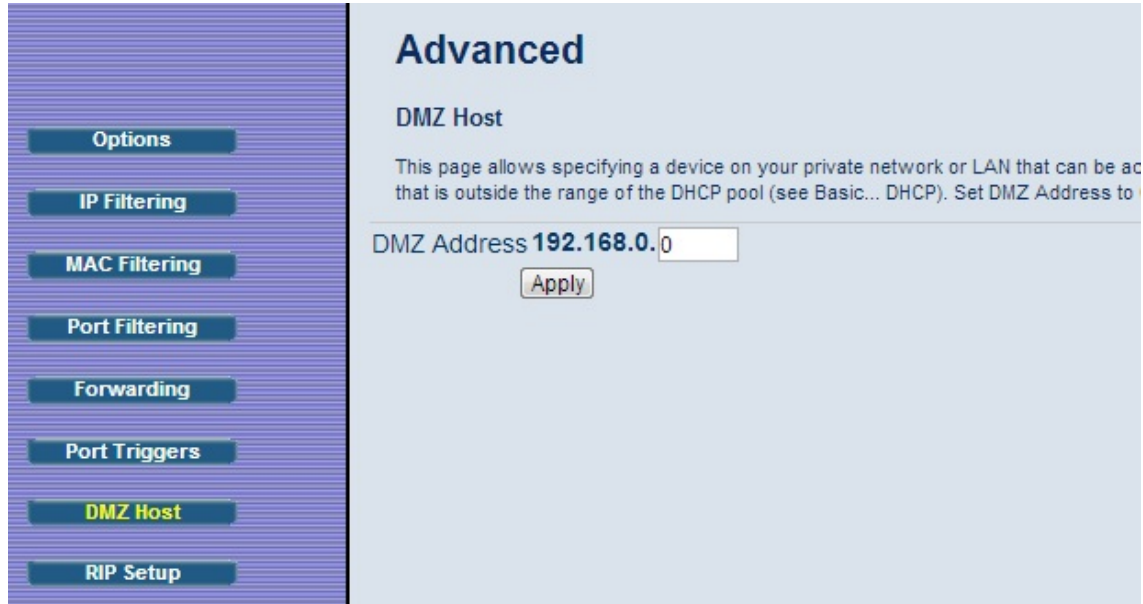
When assigning a static IP address to your gaming system you should select an address that is outside the IP addresses assigned by the Cable Modem/Router's DHCP server. By default the DHCP Server assigns addresses from 192.168.0.10 to 192.168.0.255. We recommend using 192.168.0.5 as the static IP address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

7 Then click the **DMZ Host** submenu. 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 **Advanced** in the menu bar.
- 6 Then click the **Port Triggers** submenu. The **Port Triggers** page appears.

Advanced
Port Triggers

This page allows configuration of dynamic triggers to specific devices on the LAN. This allows for applications with bi-directional traffic voice, gaming, and some messaging program features may require these settings.

Trigger Start Port
Trigger End Port
Target Start Port
Target End Port
Protocol
Description
Enabled

Trigger		Target		Prot	Description	Enabled	<input type="button" value="Remove All"/>
Start Port	End Port	Start Port	End Port				

- 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. Click **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:

Advanced

Port Triggers

This page allows configuration of dynamic triggers to specific devices on the LAN. This allows for applications with bi-directional traffic. Applications such as video conferencing, voice, gaming, and some messaging program features may require these settings.

Create

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

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 Setup 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)

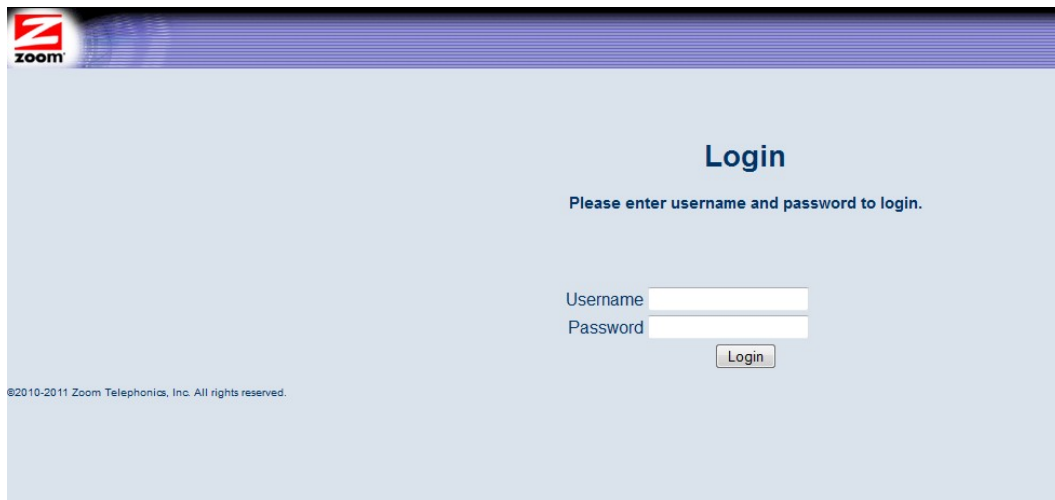


Figure 1. Login Screen

- 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 **Status - Security** page.

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

Understanding the Configuration Manager Interface Screens

The top of the management interface contains a menu bar 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.

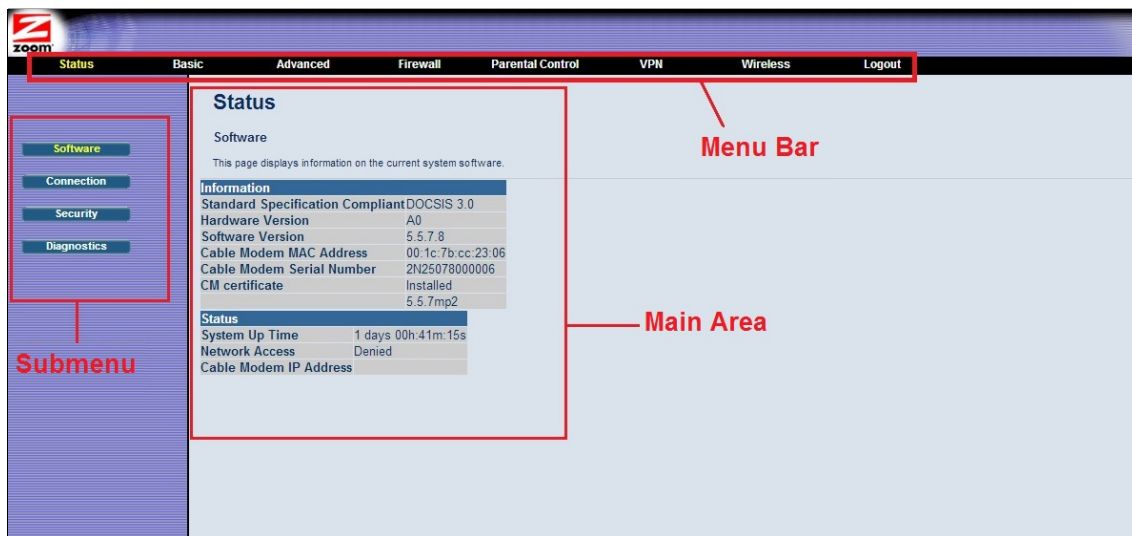


Figure 2. Main Areas on the Configuration Manager Interface

Every menu has submenus associated with it. If you click a menu item, the submenus appear on the left frame of the Configuration Manager. For example, if you click the **Status** menu item, the submenu **Software**, **Connection**, **Security** and **Diagnostics** appear on the left column (see Figure 3).



Figure 3. Example of Status Submenu

The right-most item on the menu bar is the logout option. Click it to log out from the Configuration Manager interface.

Configuration Manager Interface Menus

Table 1 describes the menus in the Configuration Manager interface.

You can skip to specific sections of this User Manual based on your intended use of the Cable Modem/Router with Wireless-N. Each of the menu options in your Configuration Manager is covered as a separate chapter in the remaining portion of the User Manual. Refer to the chart on the next page to go to a specific menu option.

Table 1. Configuration Manager Interface Menus

Chapter	Menu Options	Go to this section if you want to...	See Page
7	Status	monitor or troubleshoot problems with the Cable Modem/Router	39
8	Basic	make some modifications for more advanced uses	47
9	Advanced	make use of advanced router features supported by the Cable Modem/Router	54
10	Firewall	configure the firewall application to protect the private LAN from attacks from the WAN interface	68
11	Parental Control	configure access policies or rules to specific network devices based on the time of day and Internet contents	75
12	Wireless	configure and use the wireless features supported by the Cable Modem/Router	83
13	VPN	enable the VPN protocol and configure IPSec tunnels, L2TP and PPTP server options	99

7

Status Menu Options

The Status Menu lets you:

- View the status and connection information of the Cable Modem/Router
- Change the administrator password
- Use diagnostic tools for troubleshooting

Software

The Software page is a read-only screen that shows the Cable Modem/Router's current system software version. This page appears when you first log in to the Configuration Manager interface. You can also display it by clicking **Status** in the menu bar and then click the **Software** submenu. Figure 4 shows an example of the menu and Table 2 describes the items you can select.

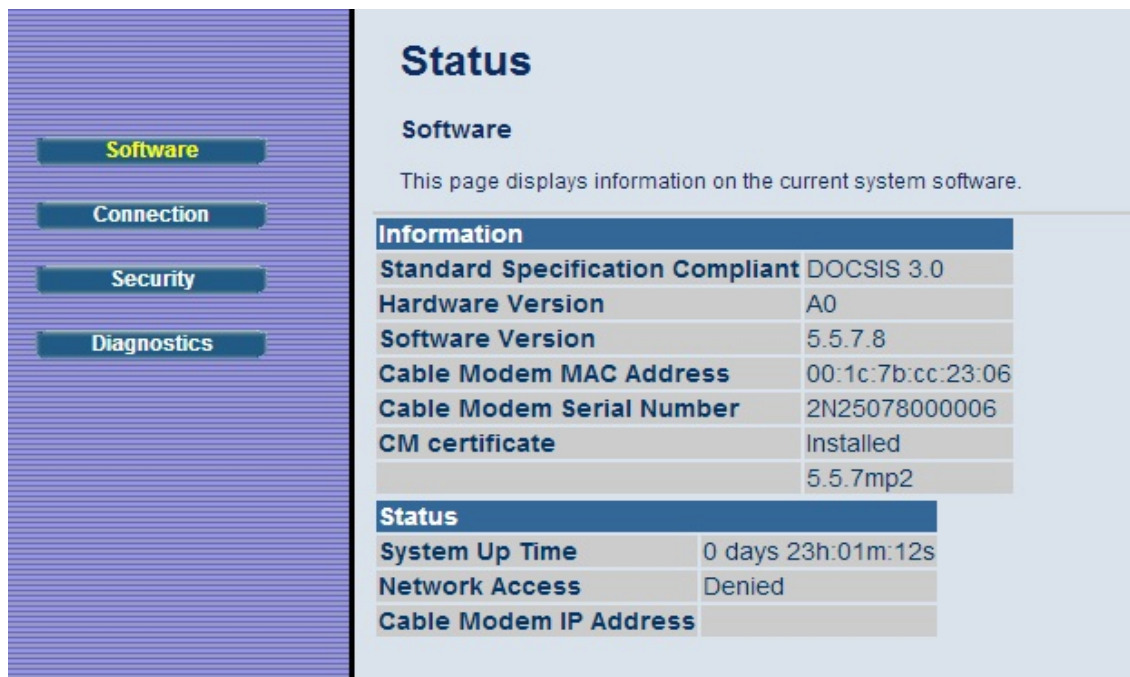


Figure 4. Software Menu

Table 2. Software Menu Option

Option	Description
Information	Shows the information on the current system software.
Status	Shows the system up time, network accessibility, and IP address of the Cable Modem/Router.

Connection

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

To access the Connection page, click **Status** in the menu bar and then click the **Connection** submenu. Figure 5 shows an example of the menu.

Software

Connection

Security

Diagnostics

Status

Connection

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

Startup Procedure		
Procedure	Status	Comment
Acquire Downstream Channel	345000000 Hz	In Progress
Connectivity State	In Progress	Not Synchronized
Boot State		
Configuration File	In Progress	
Security	Disabled	Disabled

Downstream Bonded Channels									
Channel	Lock	Status	Modulation	Channel ID	Frequency	Power	SNR	Correctables	Uncorrectables
1			unknown		345000000 Hz	-15.2 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

CM IP Address	Duration	Expires
	D: -- H: -- M: -- S: -----	

Current System Time: -----

Figure 5. Example of Connection Page

Security

The Security page allows you to configure access privileges and restore the Cable Modem/Router to its factory defaults and allows you to disable routing and use the Cable Modem/Router as a pure bridge modem.

To access the Security page, click **Status** in the menu bar and then click the **Security** submenu. Figure 6 shows an example of the menu and Table 3 describes the items you can select.

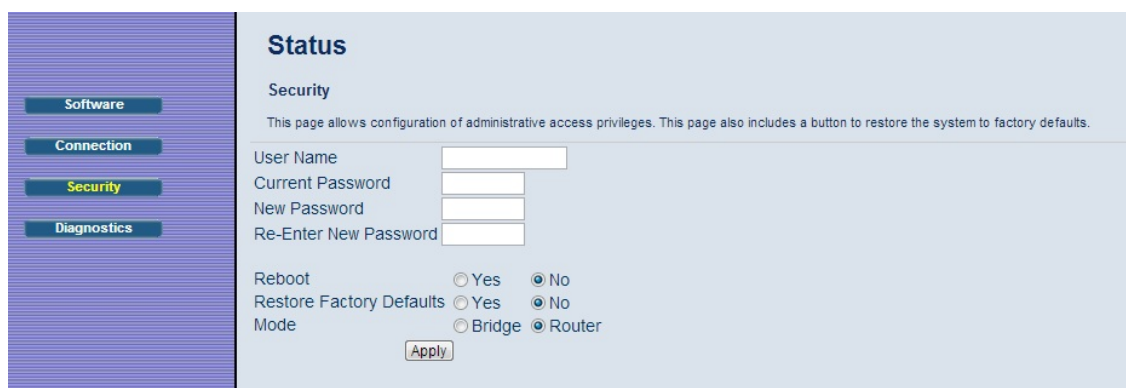


Figure 6. Example of Security Page

To restore the Cable Modem/Router to factory defaults:

- 1 In the Security submenu, select the **Yes** button next to **Restore Factory Defaults**.
- 2 Click **Apply**.
- 3 Click **OK** to reboot the Cable Modem/Router. The reboot is complete when the POWER LED stops blinking.
- 4 If the Login screen doesn't reappear, click the **Refresh** link to log back in to the Configuration Manager.

Table 3. Security Menu Option

Option	Description
User Name	Enter the new User Name for the administrator.
Current 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.
Reboot	Click the Yes button next to reboot, then click Apply to reboot the router.
Mode	Click the Bridge button if you do not wish to use the 5352 as a router. Most users should not change this setting.

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

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 **Status** in the menu bar and then click the **Diagnostics** submenu. Figure 7 and Figure 8 show the examples of the menu and

Table 4 describes the items you can select.

The screenshot shows a web-based interface for network diagnostics. On the left is a vertical navigation menu with four buttons: 'Software', 'Connection', 'Security', and 'Diagnostics' (which is highlighted in yellow). The main content area is titled 'Status' and contains a 'Diagnostics' section. Below this, there is a utility selector set to 'Ping'. The 'Ping Test Parameters' section includes a 'Target' text box, a 'Ping Size' of 64 bytes, a 'No. of Pings' of 3, and a 'Ping Interval' of 1000 ms. At the bottom of this section are three buttons: 'Start Test', 'Abort Test', and 'Clear Results'. Below the parameters is a 'Results' window with a scrollable area containing the text 'Waiting for input...'.

Figure 7. Example of Diagnostics - Ping Page

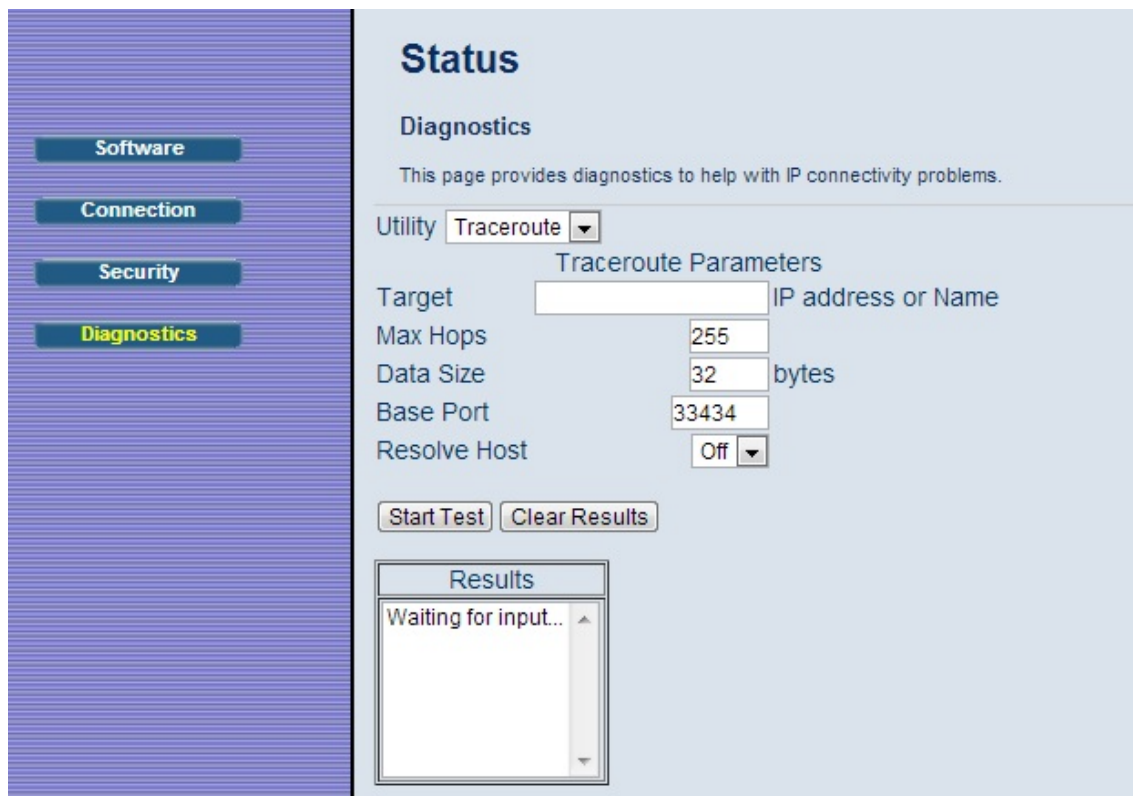


Figure 8. Example of Diagnostics - Traceroute Page

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 4. 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.

8

Basic Menu Options

The Basic Menu lets you:

- Configure the basic settings of your Cable Modem/Router
- Configure DHCP server for the LAN
- Configure DDNS service
- Backup and restore of configuration settings

Setup

The Setup page allows you to configure the basic features of the Cable Modem/Router related to your ISP's connection.

To access the Setup page, click **Basic** in the menu bar and then click the **Setup** submenu. Figure 9 shows an example of the menu and Table 5 describes the items you can select.

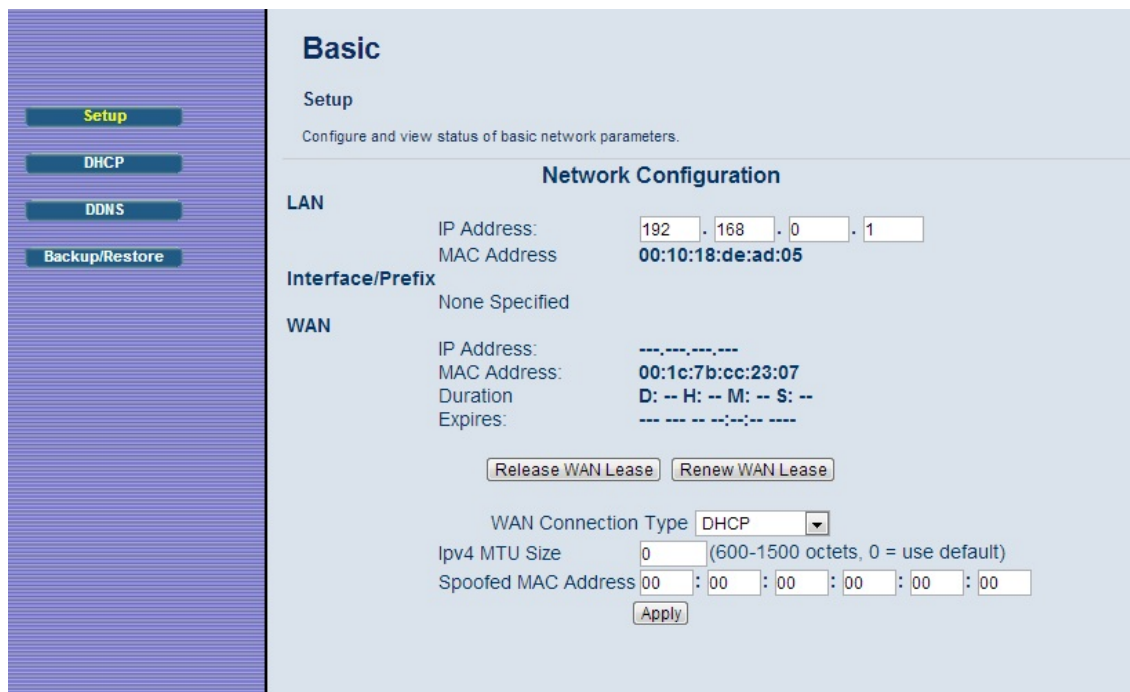


Figure 9. Example of Setup Page

Table 5. Setup 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.
WAN Connection Type	Select how your Cable Modem/Router obtains an IP address. The options are via DHCP or manual configuration of a static IP address. Unless you have arranged for a static IP address from your service provider, you should leave this setting at its default, DHCP.

DHCP

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

To access the **DHCP** page:

- 1 Click **Basic** in the menu bar.
- 2 Then click the **DHCP** submenu.

Figure 10 shows an example of the menu and Table 6 describes the items you can select.

Basic

DHCP

This page allows configuring the internal DHCP server for the LAN and viewing its status.

DHCP Server Yes No

Starting Local Address

Number of CPEs

Lease Time seconds

DHCP Clients

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
00262d61846a	192.168.000.014	255.255.255.000	D:01 H:00 M:00 S:00	---	<input type="radio"/>

Current System Time: -----

Figure 10. 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 6. DHCP Menu Options

Option	Description
DHCP Server	Select Yes to use 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.

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 **Basic** in the menu bar.
- 2 Then click the **DDNS** submenu.

Figure 11 shows an example of the menu and Table 7 describes the items you can select.

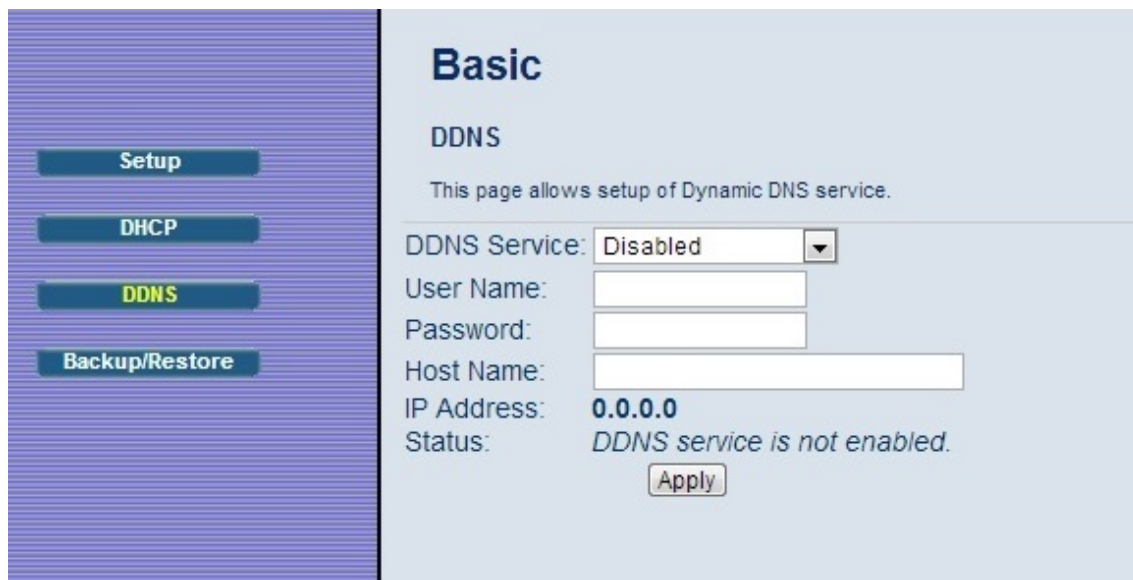


Figure 11. Example of DDNS Page

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 Basic / Setup web page.)
- 4 Enter your account information on the Basic / 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 7. 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.

Backup

Note: Some software versions may not support this feature.

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** page:

- 1 Click **Basic** in the menu bar.
- 2 Then click the **Backup/Restore** submenu.

Figure 12 shows an example of the menu.

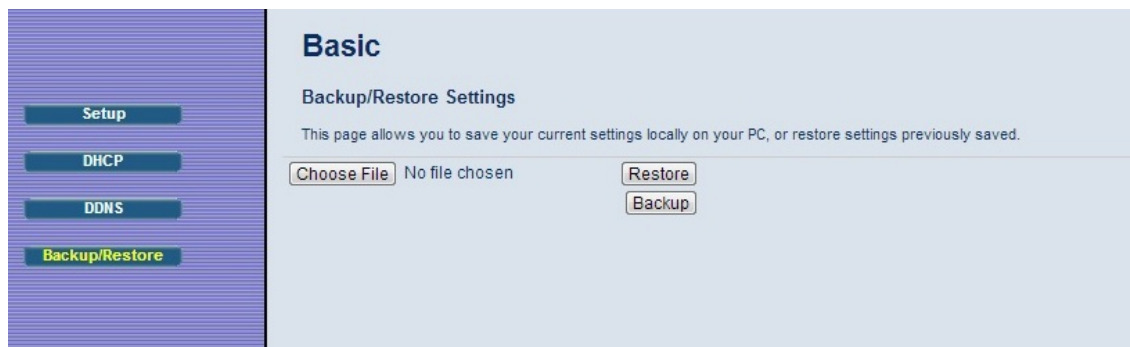


Figure 12. Example of Backup Page

9

Advanced Menu Options

The Advanced Menu lets you:

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

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 **Advanced** in the menu bar.
- 2 Then click the **Options** submenu.

Figure 13 shows an example of the menu and Table 8 describes the items you can select.

Options

IP Filtering

MAC Filtering

Port Filtering

Forwarding

Port Triggers

DMZ Host

RIP Setup

Advanced

Options

This page allows configuration of advanced features of the cable modem's router.

WAN Blocking	<input checked="" type="checkbox"/> <i>Enable</i>
IPSEC PassThrough	<input checked="" type="checkbox"/> <i>Enable</i>
PPTP PassThrough	<input checked="" type="checkbox"/> <i>Enable</i>
Remote Config Management	<input type="checkbox"/> <i>Enable</i>
Multicast Enable	<input type="checkbox"/> <i>Enable</i>
UPnP Enable	<input type="checkbox"/> <i>Enable</i>
Primary Network Bridged	<input type="checkbox"/> <i>Enable</i>

PassThrough Mac Addresses (example: 01:23:45:67:89:AB)

Add Mac Address

Addresses entered: 0/32

Remove Mac Address
Clear All

NAT ALG Status

RSVP	<input checked="" type="checkbox"/> <i>Enable</i>
FTP	<input checked="" type="checkbox"/> <i>Enable</i>
TFTP	<input checked="" type="checkbox"/> <i>Enable</i>
Kerb88	<input checked="" type="checkbox"/> <i>Enable</i>
NetBios	<input checked="" type="checkbox"/> <i>Enable</i>
IKE	<input checked="" type="checkbox"/> <i>Enable</i>
RTSP	<input checked="" type="checkbox"/> <i>Enable</i>
Kerb1293	<input checked="" type="checkbox"/> <i>Enable</i>
H225	<input checked="" type="checkbox"/> <i>Enable</i>
PPTP	<input checked="" type="checkbox"/> <i>Enable</i>
MSN	<input checked="" type="checkbox"/> <i>Enable</i>
SIP	<input checked="" type="checkbox"/> <i>Enable</i>
ICQ	<input checked="" type="checkbox"/> <i>Enable</i>
IRC666x	<input checked="" type="checkbox"/> <i>Enable</i>
ICQTalk	<input checked="" type="checkbox"/> <i>Enable</i>
Net2Phone	<input checked="" type="checkbox"/> <i>Enable</i>
IRC7000	<input checked="" type="checkbox"/> <i>Enable</i>
IRC8000	<input checked="" type="checkbox"/> <i>Enable</i>

Apply

Figure 13. 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 8. 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.
Remote Configuration Management	Allows the Cable Modem/Router to be remotely administered at port 8080. When enabled, navigate to http://CMIPAddress:8080/ to administer the Cable Modem/Router remotely). You can find your CM: WAN IP address on the Basic Setup page.
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.
UPnP Enable	Select Enable to enable the UPnP agent in the Cable Modem/Router. If you are running an application that requires UPnP, check this box.
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.

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 **Advanced** in the menu bar.
- 2 Then click the **IP Filtering** submenu.

Figure 14 shows an example of the menu and Table 9 describes the items you can select.

Advanced

IP Filtering

Enter LAN IP Addresses to block traffic that comes from those LAN Addresses from reaching the Internet.

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"/>

Apply

Figure 14. 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 9. 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.

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 **Advanced** in the menu bar.
- 2 Then click the **MAC Filtering** submenu.

Figure 15 shows an example of the menu and Table 10 describes the items you can select.

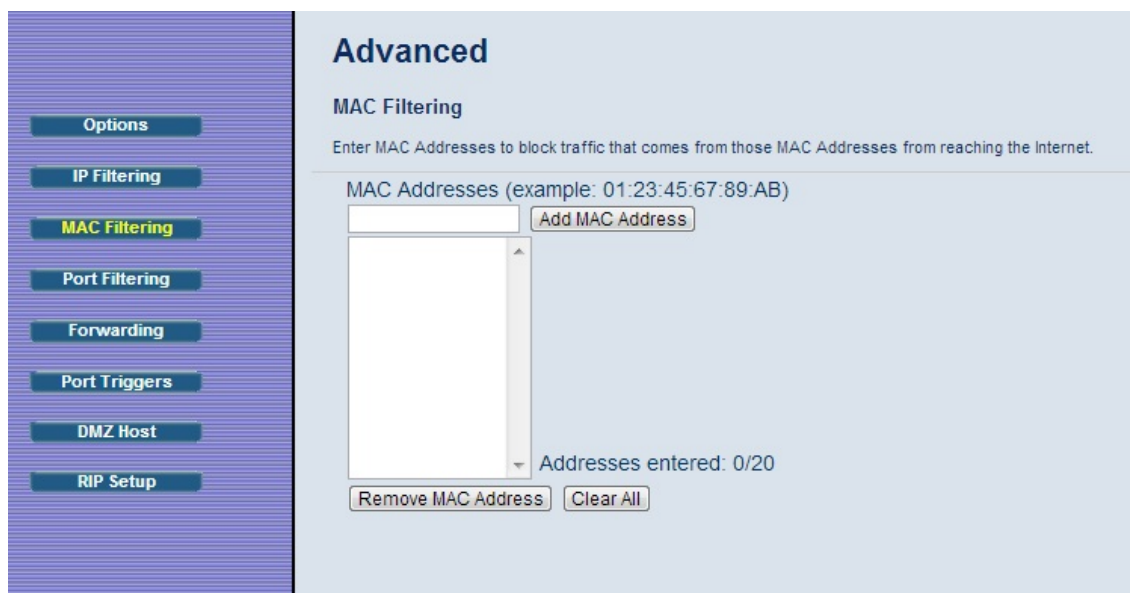


Figure 15. Example of MAC Filtering Page

Table 10. 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 DHCP Clients table. To access the DHCP Clients table click on Basic on the menu bar then DHCP.</p>

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 **Advanced** in the menu bar.
- 2 Then click the **Port Filtering** submenu.

Figure 16 shows an example of the menu and Table 11 describes the items you can select.

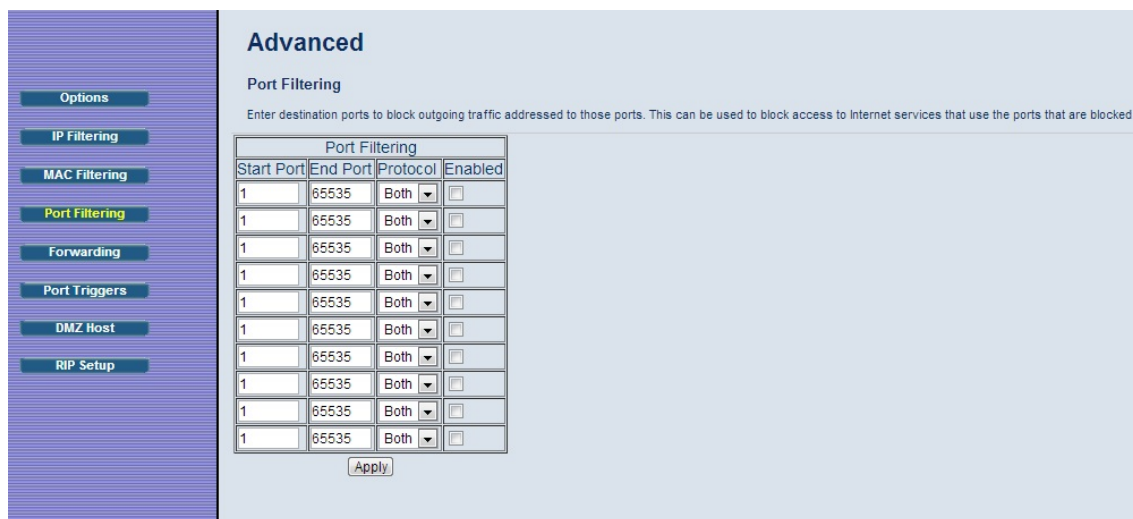


Figure 16. Example of Port Filtering Page

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 11. 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.

Forwarding

The 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 **Forwarding** page,

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

Figure 17 shows an example of the menu and Table 12 describes the items you can select.

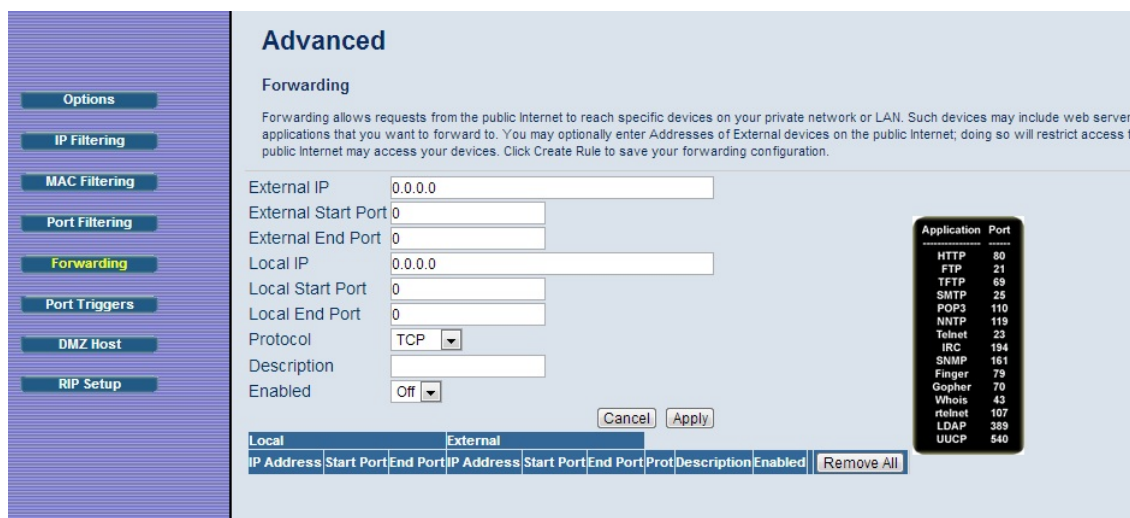


Figure 17. Example of Forwarding Page

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.
- 2 Select the protocol(s) to be forwarded.
- 3 Check the **Enable** box to the right of the entry to store settings.
- 4 Click the **Apply** button to activate the forwarding rules.

Table 12. 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.
Protocol	Select the protocol(s) to be forwarded.

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 **Advanced** in the menu bar.
- 2 Then click the **Port Triggers** submenu.

Figure 18 shows an example of the menu and Table 13 describes the items you can select.

Trigger		Target						
Start Port	End Port	Start Port	End Port	Prot	Description	Enabled		Remove All

Figure 18. 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 Check the **Enable** box to the right of the entry to store settings.
- 5 Click the **Apply** button to activate the forwarding rules.

Table 13. 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.

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 **Advanced** in the menu bar.
- 2 Then click the **DMZ Host** submenu.

Figure 19 shows an example of the menu.



Figure 19. 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.

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 **Advanced** in the menu bar.
- 2 Then click the **RIP Setup** submenu.

Figure 20 shows an example of the menu and Table 14 describes the items you can select.

The screenshot shows a web interface for configuring RIP. On the left is a vertical menu with buttons for 'Options', 'IP Filtering', 'MAC Filtering', 'Port Filtering', 'Forwarding', 'Port Triggers', 'DMZ Host', and 'RIP Setup'. The 'RIP Setup' button is highlighted in yellow. The main content area is titled 'Advanced' and 'Routing Information Protocol Setup'. It includes a descriptive paragraph: 'This page allows configuration of RIP parameters related to authentication, destination IP Address, subnet mask, Address.' Below this are several configuration fields: 'RIP Enable' with an unchecked 'Enable' checkbox; 'RIP Authentication' with a checked 'Enable' checkbox; 'RIP Authentication Key' with an empty text input; 'RIP Authentication Key ID' with a text input containing '0'; 'RIP Reporting Interval' with a text input containing '30' and the unit 'seconds'; 'RIP Destination IP Address' with four text inputs containing '0', '0', '0', and '0'; and 'RIP Destination IP Subnet Mask' with four text inputs containing '255', '255', '255', and '0'. An 'Apply' button is located at the bottom of the form.

Figure 20. Example of RIP Setup Page

Note: RIP messages will only be sent when the Cable Modem/Router is configured for Static IP Addressing (see the [Basic – Setup](#) page).

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 14. RIP Setup Menu Option

Option	Description
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.

10

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 **Firewall** in the menu bar.
- 2 Then click the **Basic** submenu.

Figure 21 shows an example of the menu and Table 15 describes the items you can select.



Figure 21. Example of Basic Page

Table 15. 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.
Port Scan Detection	Detects and blocks port scan activity originating on both the LAN and WAN.
Block Fragmented IP packets	Prevents all fragmented IP packets from passing through the firewall.
IP Flood Detection	Detects and blocks packet floods originating on both the LAN and WAN.

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 **Firewall** in the menu bar.
- 2 Then click the **Event Log** submenu.

Figure 23 shows an example of the menu and Table 16 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.

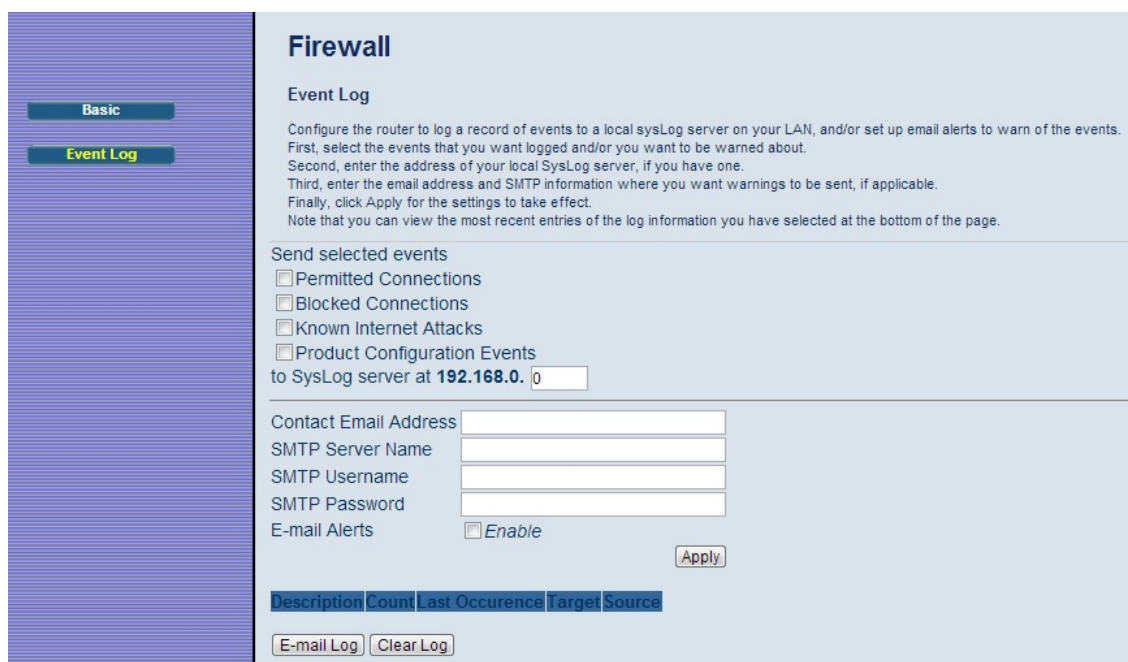


Figure 22. Example of Event Log Page

Table 16. 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.
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 17. 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 18. 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	Remote configuration management (via HTTP through the

management enabled [port#]	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.

11

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](#) Menu. 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 **Parental Control** in the menu bar.
- 2 Then click the **Basic** submenu.

Figure 23 shows an example of the menu and Table 19 describes the items you can select.

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

Basic

User Setup

ToD Filter

Event Log

Parental Control

Basic Setup

Make rules to block access to certain web sites, and allow access to others. Do this by defining one or more Policies. Click the Apply, Add Refresh button to see the currently active settings.

Parental Control Activation
 This box must be checked to turn on Parental Control
 Enable Parental Control

Content Policy Configuration

Content Policy List
 1. Default

Keyword List	Blocked Domain List	Allowed Domain List
<input type="text" value="anonymizer"/> <input type="button" value="Add Keyword"/> <input type="button" value="Remove Keyword"/>	<input type="text" value="anonymizer.com"/> <input type="button" value="Add Domain"/> <input type="button" value="Remove Domain"/>	<input type="text"/> <input type="button" value="Add Allowed Domain"/> <input type="button" value="Remove Allowed Domain"/>

Override Password
 If you encounter a blocked website, you can override the block by entering the following password

Password	*****
Re-Enter Password	*****
Access Duration(minutes)	30
<input type="button" value="Apply"/>	

Figure 23. Example of Basic Page

Table 19. 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 .
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.
Content Policy List	Pull-down list that shows Policy Names that you have created. Select the policy you want to define or edit.
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 T 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 **Parental Control** in the menu bar.
- 2 Then click the **User Setup** submenu.

Figure 24 shows an example of the menu and Table 20 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.

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 the him or her. Click the Add User and Remove User buttons as appropriate to save changes.

User Configuration

Add User

User Settings

1. Default Enable Remove User

Password

Re-Enter Password

Trusted User Enable

Content Rule White List Access Only 1. Default

Time Access Rule

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. Enter a maximum of 3 MAC addresses

00 : 00 : 00 : 00 : 00 : 00 Add

No Trusted Computers

Remove

Figure 24. Example of User Setup Page

Table 20. 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 Basic on the menu bar then DHCP.</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 **Parental Control** in the menu bar.
- 2 Then click the **ToD Filter** submenu.

Figure 25 shows an example of the menu and Table 21 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 the 'Parental Control' interface. On the left is a vertical menu with buttons for 'Basic', 'User Setup', 'ToD Filter' (highlighted in yellow), and 'Event Log'. The main content area is titled 'Parental Control' and 'Time of Day Access Policy'. Below this is a sub-header 'Time Access Policy Configuration' with a text input field and an 'Add New Policy' button. A section titled 'Time Access Policy List' contains a dropdown menu showing 'No filters entered.', an 'Enabled' checkbox, and a 'Remove' button. Under 'Days to Block', there are checkboxes for 'Everyday', 'Sunday', 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday', and 'Saturday'. The 'Time to Block' section has an 'All day' checkbox, and 'Start' and 'End' time pickers (hour, minute, AM/PM). 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 at the bottom.

Figure 25. Example of ToD Filter Page

Table 21. 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 **Parental Control** in the menu bar.
- 2 Then click the **Event Log** submenu.

Figure 26 shows an example of the menu.



Figure 26. Example of Event Log Page

12

Wireless Menu Options

The Wireless Menu lets you:

- Configure Cable Modem/Router to serve as a wireless access point (AP)
- Configure essential and advanced settings of wireless network
- Configure 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 **Wireless** in the menu bar.
- 2 Then click the **Radio** submenu.

Figure 27 shows an example of the menu and Table 22 describes the items you can select.

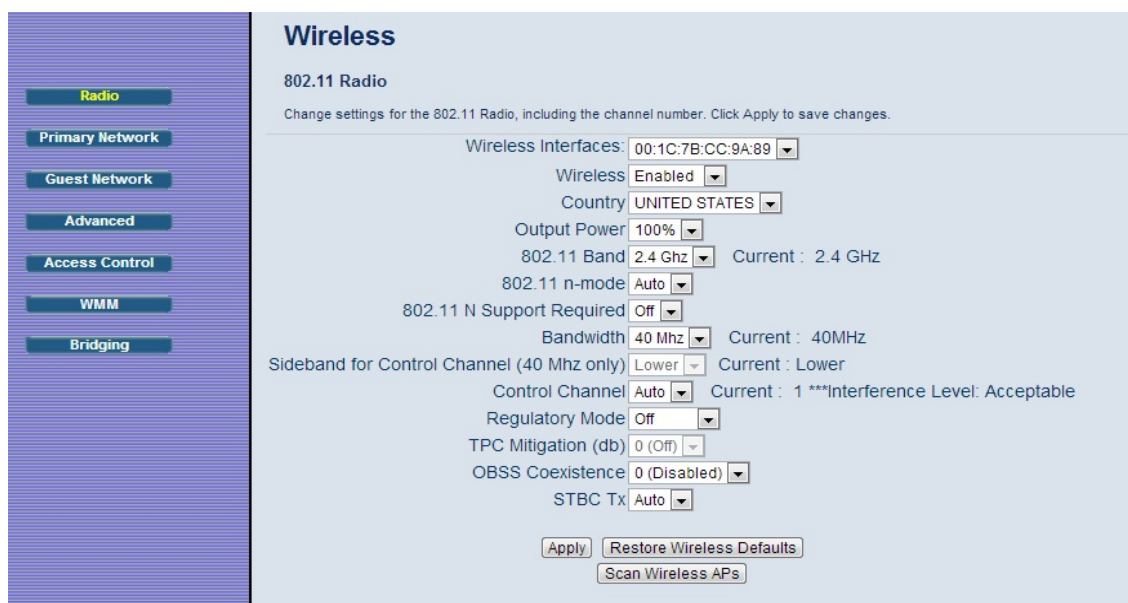


Figure 27. Example of Radio Page

Table 22. Radio Menu Option

Option	Description
Wireless Interface	This is the MAC address of the wireless interface.
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.
802.11 Band	Your device supports 2.4 GHz only.
802.11n-mode	In Auto mode, your Cable Modem/Router will automatically adjust to avoid interference with neighboring devices.
Bandwidth	Specify radio frequency bandwidth, either 20MHz single, or 40MHz (dual channel), that the Cable Modem/Router will use if 802.11n mode is configured as Automatic and the Control Channel is configured as Automatic.
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 .
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.

Table 23. 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 **Wireless** in the menu bar.
- 2 Then click the **Primary Network** submenu.

Figure 28 shows an example of the menu and Table 24 describes the items you can select.

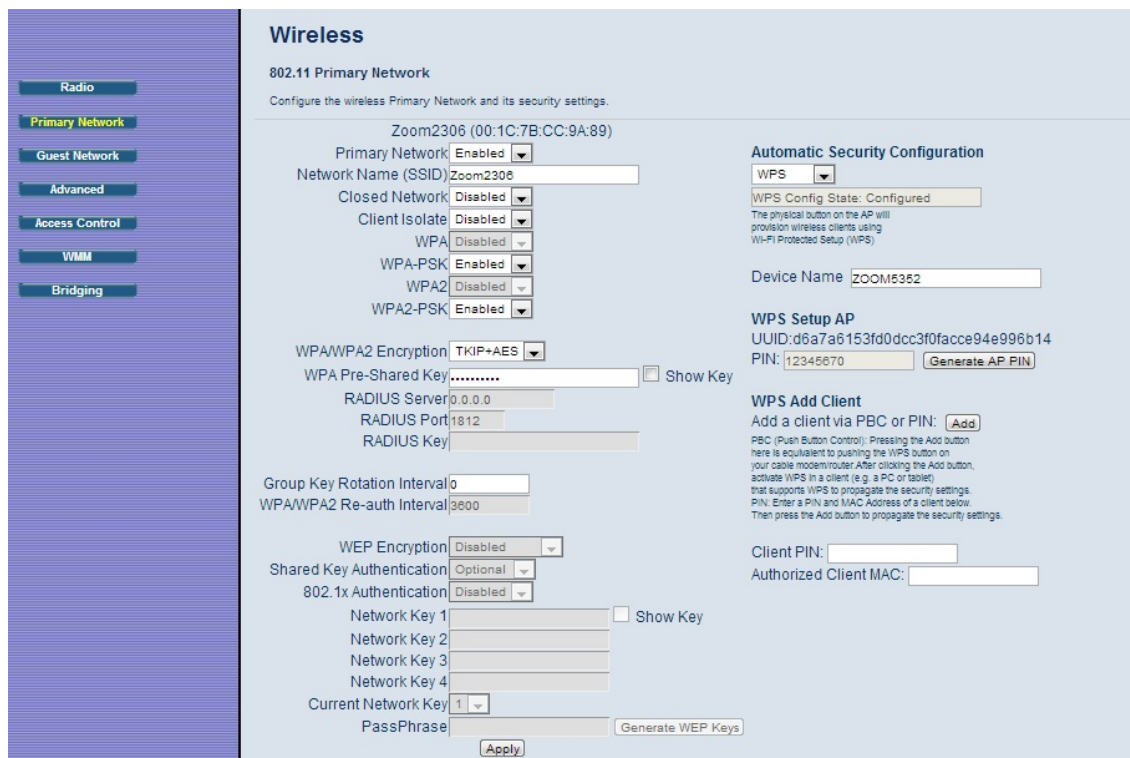


Figure 28. Example of Primary Network Page

Table 24. Primary Network Menu Option

Option	Description
Primary Network	Select Enable to enable primary wireless network.
Network Name (SSID)	Set the Network Name (also known as SSID) of the wireless network. This is a 1-32 ASCII character string.
Closed Network	Select Enable to suppress broadcast of the SSID.
Client 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.
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 ASCII 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.
Automatic Security Configuration	Disable or enable WPS. WPS does not work with WEP.
Device Name	Enter a name to identify this Cable Modem/Router in WPS network.
WPS Setup AP PIN	PIN (Personal Identification Number) is the WDS ID number of your PC or game machine. When a WPS-supported device tries to connect to this Cable Modem/Router, you have to enter its PIN into the WPS Setup AP's PIN field, then click Configure .
WPS Add Client	Select WPS mode to be deployed.
Push-Button	In Push-Button mode, then user only needs to push the WPS button on the Cable Modem/Router. Then, within 2 minutes, activate WPS on your client device(s).
PIN	For devices that require a PIN, enter the PIN in the WPS Add Client PIN's field, and then click Add .

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 APs to configure different Basic Service Sets (BSSs). Your Cable Modem/Router supports Multiple SSIDs which allows you to use the same access point to provide several BSSs simultaneously. You can then assign various privileges to different SSIDs and associated networks.

- Up to five BSSs are allowed on one Cable Modem/Router simultaneously, one for Admin access and four for Guest Networks.
- If you are using WEP, you must use different WEP keys for different BSSs.
- You should use different PSKs for different BSSs if you are using WPA/WPA2.

To access the **Guest Network** page:

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

Figure 36 shows an example of the menu and Table 25 describes the items you can select.

Wireless

802.11 Guest Network

This page allows configuration of one or more guest networks.

Guest Network: **ZOOM_G0 (02:1C:7B:CC:8A:8A)**

Guest WiFi Security Settings

Guest Network: Disabled

Guest Network Name (SSID): ZOOM_G0

Closed Network: Disabled

Client Isolate: Disabled

WPA: Disabled

WPA-PSK: Disabled

WPA2: Disabled

WPA2-PSK: Disabled

WPA/WPA2 Encryption: Disabled

WPA Pre-Shared Key: Show Key

RADIUS Server: 0.0.0.0

RADIUS Port: 1812

RADIUS Key:

Group Key Rotation Interval: 0

WPA/WPA2 Re-auth Interval: 3600

WEP Encryption: Disabled

Shared Key Authentication: Optional

802.1x Authentication: Disabled

Network Key 1: Show Key

Network Key 2:

Network Key 3:

Network Key 4:

Current Network Key: 1

PassPhrase:

Guest LAN Settings

Network: LAN

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Lease Pool Start: 192.168.1.10

Lease Pool End: 192.168.1.99

Lease Time: 86400

UPnP Enable: Enabled

Firewall Enable: Disabled

DHCPv6 Server: Enabled

Figure 29. Example of Guest Network Page

Table 25. Guest Network Menu Option

Option	Description
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.
Client 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.
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 ASCII 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 start IP address of this DHCP address pool.
Lease Pool End	Enter the end IP address of this DHCP address pool.
Lease Time	Enter the leased 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.

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 **Wireless** in the menu bar.
- 2 Then click the **Advanced** submenu.

Figure 30 shows an example of the menu and Table 26 describes the items you can select.

Wireless

802.11 Advanced

This page allows configuration of data rates and WiFi thresholds.

54g™ Mode	54g Auto
XPress™ Technology	Enabled
802.11n Protection	Auto
Short Guard Interval	Auto
Basic Rate Set	Default
Multicast Rate	Auto
NPHY Rate	Auto
Legacy Rate	Auto
Beacon Interval	100
DTIM Interval	1
Fragmentation Threshold	2346
RTS Threshold	2347

Apply

Figure 30. Example of Advanced Page

Table 26. 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 .
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.

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 **Wireless** in the menu bar.
- 2 Then click the **Access Control** submenu.

Figure 31 shows an example of the menu and Table 27 describes the items you can select.

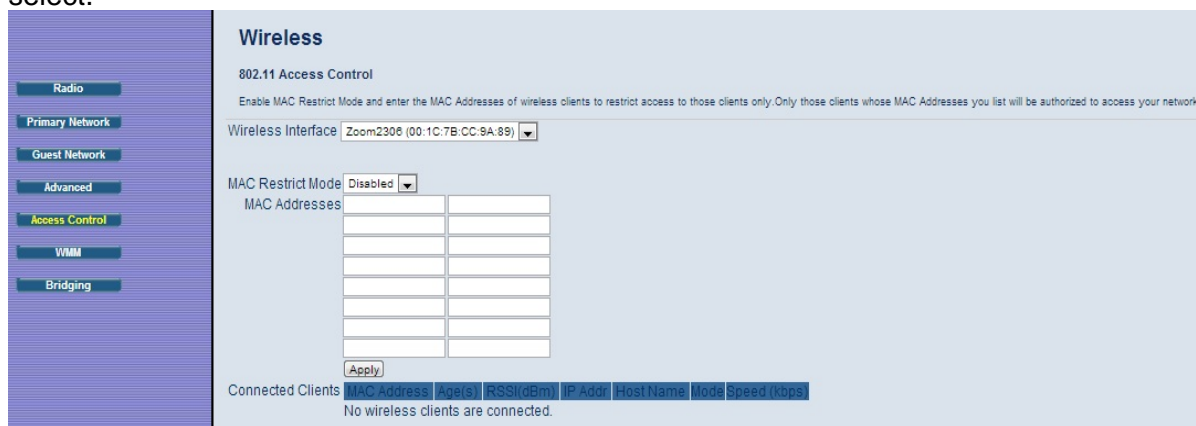


Figure 31. Example of Access Control Page

Table 27. 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 and 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 **Wireless** in the menu bar.
- 2 Then click the **WMM** submenu.

Figure 32 shows an example of the menu and Table 28 describes the items you can select.

Wireless

802.11 Wi-Fi Multimedia

This page allows configuration of Wi-Fi Multimedia QoS.

WMM Support
 No-Acknowledgement
 Power Save Support

EDCA AP Parameters	CWmin	CWmax	AIFSN	TXOP(b) Limit (usec)	TXOP(a/g) Limit (usec)	Discard Oldest First
AC_BE	15	63	3	0	0	Off <input type="button" value="v"/>
AC_BK	15	1023	7	0	0	Off <input type="button" value="v"/>
AC_VI	7	15	1	6016	3008	Off <input type="button" value="v"/>
AC_VO	3	7	1	3264	1504	Off <input type="button" value="v"/>
EDCA STA Parameters						
AC_BE	15	1023	3	0	0	
AC_BK	15	1023	7	0	0	
AC_VI	7	15	2	6016	3008	
AC_VO	3	7	2	3264	1504	
WMM TXOP Parameters						
	Short Retry Limit	Short Failok Limit	Long Retry Limit	Long Failok Limit	Max Rate in 500kbps	
AC_BE	7	3	4	2	0	
AC_BK	7	3	4	2	0	
AC_VI	7	3	4	2	0	
AC_VO	7	3	4	2	0	

Figure 32. Example of WMM Page

Table 28. WMM Menu Option

Option	Description
WMM Support	Select On to include the WME Information Element in 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.
EDCA AP Parameters	<p>Enter the transmit parameters for traffic transmitted from the AP to the STA (station) for the four Access Categories (AC): Best Effort (AC_BE), Background (AC_BK), Video (AC_VI) and Voice (AC_VO). Transmit parameters include Contention Window (CWmin and CWmax), Arbitration Inter Frame Spacing Number (AIFSN), and Transmit Opportunity Limit (TXOP Limit).</p> <p>There are also two AP-specific settings:</p> <ul style="list-style-type: none"> • Admission Control: Specify if admission control is enforced for the Access Categories. • Discard Oldest First. Specify the discard policy for the queues. On discards the oldest first and Off discards the newest first.
EDCA STA Parameters	Specifies the transmit parameters for traffic transmitted from the STA (station) to the AP for the four Access Categories (AC): Best Effort (AC_BE), Background (AC_BK), Video (AC_VI), and Voice (AC_VO). Transmit parameters include Contention Window (CWmin and CWmax), Arbitration Inter Frame Spacing Number (AIFSN) and Transmit Opportunity Limit (TXOP Limit).

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 **Wireless** in the menu bar.
- 2 Then click the **Bridging** submenu.

Figure 33 shows an example of the menu and Table 29 describes the items you can

select.

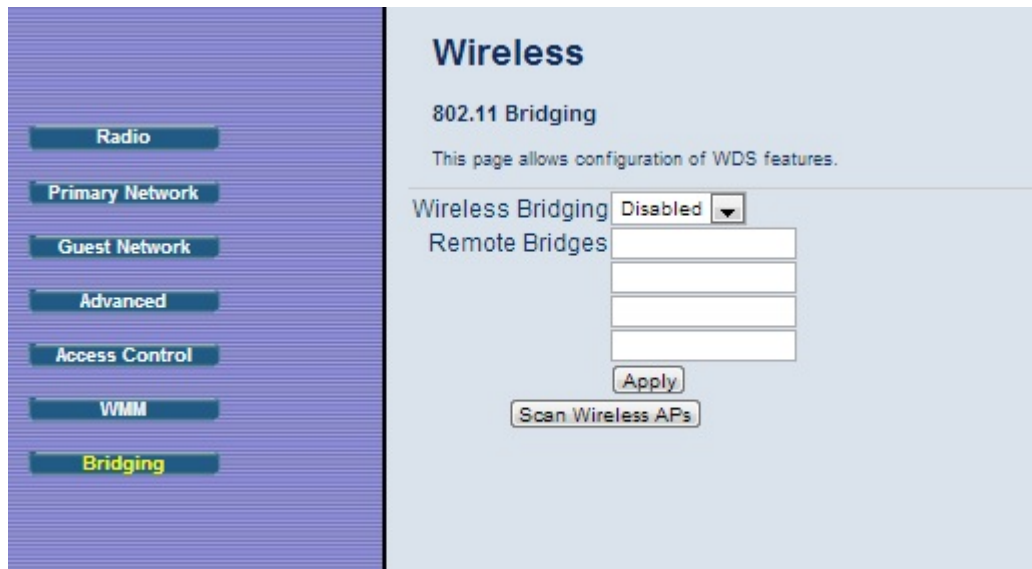


Figure 33. Example of Bridging Page

Table 29. 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.

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 **VPN** in the menu bar.
- 2 Then click the **Basic** submenu.

Figure 34 shows an example of the menu and Table 30 describes the items you can select.

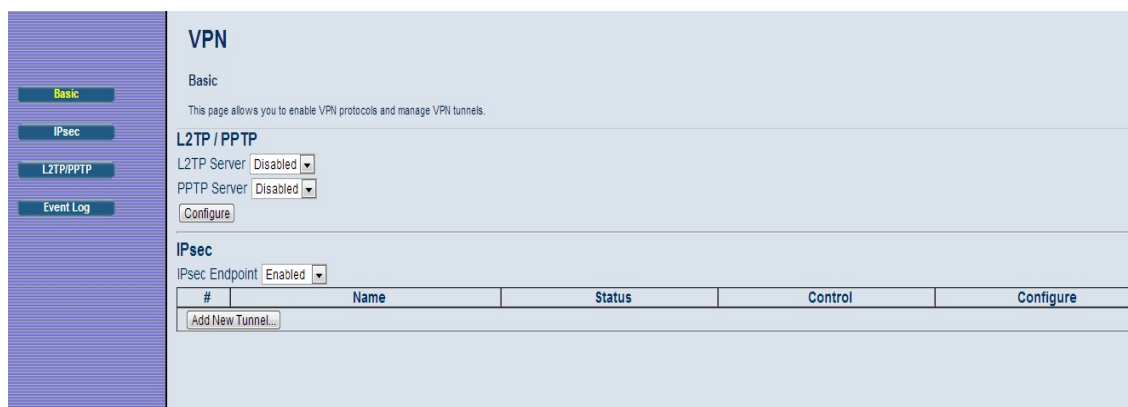


Figure 34. Example of Basic Page

Table 30. 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 **VPN** in the menu bar.
- 2 Then click the **IPSec** submenu.

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

VPN

IPsec

This page allows configuration of IPsec tunnels.

Tunnel	Tunnel list is EMPTY. ▼	Delete Tunnel
Name	(null)	Add New Tunnel
	Disabled ▼	Apply

Local endpoint settings

Address group type: IP subnet ▼

Subnet: 192 . 168 . 0 . 0

Mask: 255 . 255 . 255 . 0

Identity type: IP address ▼

Identity: (null)

Remote endpoint settings

Address group type: IP subnet ▼

Subnet: 0 . 0 . 0 . 0

Mask: 0 . 0 . 0 . 0

Identity type: IP address ▼

Identity: (null)

Network address type: IP address ▼

Remote Address: 0.0.0.0

IPsec settings

Pre-shared key: (null)

Phase 1 DH group: Group 1 (768 bits) ▼

Phase 1 encryption: DES ▼

Phase 1 authentication: MD5 ▼

Phase 1 SA lifetime: 0 seconds

Phase 2 encryption: DES ▼

Phase 2 authentication: MD5 ▼

Phase 2 SA lifetime: 0 seconds

Show Advanced Settings

Apply

Figure 35. Example of IPsec Page

Table 31. 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 AN 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	<p>Select the Diffie-Hellman key group (DHx) you want to use for encryption keys.</p> <p>DH1: uses a 768-bit random number DH2: uses a 1024-bit random number DH5: uses a 1536-bit random number.</p>
Phase 1 Encryption	<p>Select the key size and encryption algorithm to use for data communications.</p> <p>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.</p> <p>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.</p>
Phase 1 Authentication	<p>Select the hash algorithm used to authenticate packet data in the IKE SA.</p> <p>SHA1: generally considered stronger than MD5, but it is also slower.</p> <p>MD5 (Message Digest 5): produces a 128-bit digest to authenticate packet data.</p> <p>SHA1 (Secure Hash Algorithm): produces a 160-bit digest to authenticate packet data.</p>
Phase 1 SA Lifetime	<p>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</p>

	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 **VPN** in the menu bar.
- 2 Then click the **L2TP/PPTP** submenu.

Figure 36 shows an example of the menu and Table 32 describes the items you can select.

VPN

Basic

This page allows configuration of L2TP and PPTP server options.

PPP Address Range

Start	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
End	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="254"/>

PPP Security

MPPE Encryption

Users

Username

Password

Confirm Password

User List

User list is empty.

L2TP Server

Preshared Phrase

Figure 36. Example of L2TP/PPTP Page

Table 32. L2TP/PPTP Menu Option

Option	Description
PPP Address Range (Start/End)	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).
PPP Security (MPPE Encryption)	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.
Username	Enter the user name for the L2TP or PPTP tunneling.
Password	Enter the password for the L2TP or PPTP tunneling.
Confirm Password	Re-enter to confirm the password.
User List	Show the existing user list.
L2TP Server (Preshared Phrase)	Enter a key (Pre-Shared key) for authentication. This key is used by IPSec to validate the computer as a trusted machine.

Event Log

The Event Log page shows the VPN event log.

To access the **Event Log** page:

- 1 Click **VPN** in the menu bar.
- 2 Then click the **Event Log** submenu.

Figure 37 shows an example of the menu and Table 33 describes the items you can select.

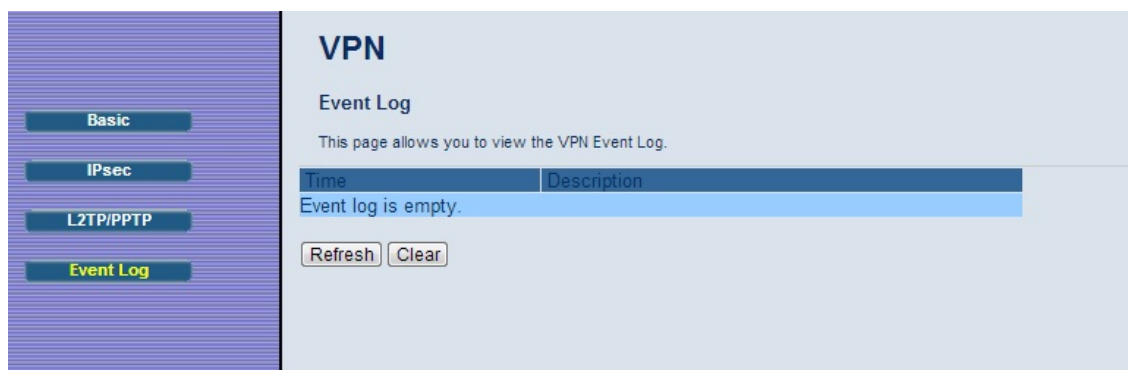


Figure 37. Example of Event Log Page

Table 33. 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.

Appendix A: Troubleshooting Tips

Problem

I cannot access my Internet service or send or receive email.

Solution

The following front panel lights on the Cable Modem/Router – **ONLINE**, **US** (upstream), **DS** (downstream), and **POWER** – must be solidly lit before your modem will let you connect to the Internet. If they are not:

- Check all modem connections (power, Ethernet, and cable modem line).
- Unplug your Cable Modem/Router and then plug it back in.
- Restart your computer.
- Check to see that your cable TV is working.
- If you have any splitters between the cable modem and the wall, remove the splitter and connect the cable modem 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.
- Check with your cable service provider to make sure that high speed access is available and running.
- In rare instances, the cable signal may be weak or noisy. If this is the case, call your cable service provider.
- If you are using your PC's Ethernet port, check that this port is functioning correctly. If you are using wireless, check that your wireless connection is functioning correctly. Refer to its documentation if necessary.
- Check that your Web browser is configured correctly. It should be set to use a network connection; this might be called a LAN (Local Area Network) or broadband connection.
- Check that your computer's network settings are configured correctly. A Windows computer should have a local area connection that should normally be Internet Protocol version 4, Internet Protocol version 6, or TCP/IP; not AOL, Dial-up, or Adapter. A Macintosh computer should be configured for Built-in Ethernet, and TCP/IP should be set to Using DHCP.
- You may need to register your modem's MAC address with your cable provider. When your provider asks for your MAC address tell them the **CM MAC** address on your Cable Modem/Router's bottom label.

Problem

I cannot access my Internet service or send or receive email and my **ONLINE**, **US**(upstream), **DS** (downstream), and **POWER** lights are correct on the front panel

Solution

- You may need to register your modem's MAC address with your cable provider. When your provider asks for your MAC address tell them the **CM MAC** address on your Cable Modem/Router's bottom label.
- 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

My computer/devices are not connecting wirelessly to the Cable Modem/Router.

Solution

Try the following:

- Check the wireless security settings on the device not connecting to the router 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. These settings must match the settings on your device.
- 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 the following:
 - Reorient the antennas on the Cable Modem/Router.
 - If possible, move the Cable Modem/Router to another area.
 - Move the device trying to access the Cable Modem/Router to a different location, ideally closer to the Cable Modem/Router.
- Change the wireless channel. You may experience performance issues with your wireless network, you may want to change the wireless channel your device is using. 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, then click **Login**.
User Name: **admin**
Password: **admin**
 - 3 Click **Wireless** on the menu bar to open the **Wireless** page.
 - 4 On the Radio page, 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.

- 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. 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, then click **Login**.
User Name: **admin**
Password: **admin**
 - 3 Click **Wireless** on the menu bar to open the **Wireless** page. On the Radio page, from the **Bandwidth** drop-down menu, select 20 Mhz
 - 4 Click Apply.

Problem

I followed the instructions for connecting the Modem/Router and entered **http://192.168.0.1** in my web browser's address bar, but I cannot access the Modem/Router. (The **Logon** page does not appear).

Solution

- Verify that power is on to the Modem/Router and that the Ethernet cable is plugged between your Modem/Router and your computer's Ethernet (LAN) port.
- 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.
- The computer connected to the Modem/Router must have it's TCP/IP parameters setup to use DHCP (also called Dynamic IP). Check that your computer is setup to use DHCP.

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.