

# **USER MANUAL**

**Wireless-N Router w 3G + Modem & Voice**

**Series 1098 Model 4530**



## **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 2012

**All rights reserved.**

# Contents

---

<b>Contents .....</b>	<b>3</b>
<b>Getting Started .....</b>	<b>5</b>
Where to Go Next .....	5
<b>Installing the Hardware .....</b>	<b>6</b>
Resetting the Modem/Router to the Factory Configuration .....	7
<b>Using the Modem/Router's Configuration Manager.....</b>	<b>8</b>
Launching the Modem/Router's Configuration Manager .....	8
Launching the Configuration Manager's Setup Wizard .....	10
Step 1. Setup Login.....	10
Step 2. Setup Time Zone.....	11
Step 3. WAN Type Setup .....	11
Selecting the WAN Type.....	12
Step 4. Wireless Settings.....	19
Step 5. Summary .....	22
Step 6. Finish .....	24
<b>Connecting Devices Wirelessly to the Modem/Router.....</b>	<b>26</b>
Establishing your Wireless Network.....	26
Connecting a Windows 7 Computer with Built-in Wireless Capabilities...	27
Connecting a Windows Vista Computer with Built-in Wireless Capabilities .....	28
Connecting a Windows XP Computer with Built-in Wireless Capabilities	29
Connecting a Macintosh OS X Computer with Built-in Wireless Capabilities .....	29
Connecting a Wireless-enabled Computer or Device (including the iPhone or other cellular phones, the iPod Touch, etc.) to the Modem/Router .....	30
Connecting a Computer with a Wireless adapter to the Modem/Router ....	31
Setting up your Network using WPS .....	32
Configuration Methods .....	33
Method One .....	33
Method Two .....	33
Method Three.....	33
<b>Understanding your Modem/Router's Voice Features .....</b>	<b>35</b>
Missed Calls.....	36
Received Calls .....	37
Outgoing Calls .....	38
Telephone Settings .....	39
Call Forwarding .....	40
Call Waiting .....	41
Speed Dial.....	42
<b>Working with Text Messages.....</b>	<b>44</b>
Using your Modem/Router to Send Text Messages.....	44
Working with your Inbox.....	46
The Management Settings Page.....	47

<b>Using the Configuration Manager's Advanced Program.....</b>	<b>49</b>
Changing Default Settings .....	49
Online Help .....	50
Launching the Configuration Manager's Advanced Program.....	50
Configuring Basic Settings .....	51
The Basic Setup Page.....	51
Using your 3G+ modem as a Backup .....	53
The DHCP Server Page.....	54
The Wireless Setting Page .....	54
WPA2/WPA Configuration .....	57
WEP Configuration.....	58
The Change Password Page .....	58
Configuring Forwarding Rules .....	59
The Virtual Server Page .....	60
The Port Triggering Page .....	61
The Miscellaneous Page .....	62
Configuring Security Settings.....	63
Status Page .....	64
Packet Filtering Page .....	65
The Domain Filters Page .....	65
The URL Blocking Page.....	66
The MAC Address Control Page .....	67
The Miscellaneous Page .....	69
Configuring Advanced Settings .....	69
The System Log Page .....	70
The Dynamic DNS Page.....	71
The QoS Page .....	71
The SNMP Page.....	73
The Routing Table Page.....	74
The System Time Page.....	74
The Schedule Rule and Schedule Rule Setting Pages .....	75
Configuring Toolbox Settings.....	78
The System Information Page.....	78
The Firmware Upgrade Page .....	78
The Backup Setting Dialog.....	79
The Reset to Default Dialog .....	79
The Reboot Dialog.....	80
The Miscellaneous Page .....	80
<b>Appendix A: Mobile Broadband Settings .....</b>	<b>81</b>
<b>Appendix B: How to Set Up Tethering on the iPhone .....</b>	<b>85</b>
<b>Appendix C: Registering Your Product and Getting Help.....</b>	<b>87</b>
Limited Warranty .....	88
CE Declaration of Conformity.....	89
RF Exposure Information.....	90

# 1

## Getting Started

---

The Model 4530 package contains the 3G+ Modem/Router, a 12Vdc 1.0A Power Cube, this Quick Start flyer, and a CD that contains additional documentation and warranty information. If anything is missing or damaged, please contact Zoom Customer Support or whoever provided the Modem/Router.

**Before installing the 3G+ Modem/Router you will need a SIM card for the built-in 3G+ modem.** This SIM card may have been provided to you by your service provider or you may need to purchase one. To use the Modem/Router for both data and voice, you will need a SIM that supports both data and voice. If you just want to use the Modem/Router for Internet access, a SIM that only supports data will work.

### Where to Go Next

---

If you have already followed the steps in the Quick Start to install your Model 4530 3G+ Modem/Router with Phone Port and want to learn how to:

- Add additional wireless devices to your network, go to [Chapter 4: Connecting Devices Wirelessly to the Modem/Router](#).
- Learn about the Modem/Router's voice features including viewing a list of incoming, outgoing or missed calls, or setting up advanced voice features like call forwarding, call waiting, or speed dialing, go to [Chapter 5: Understanding your Modem/Router's Voice Features](#).
- Use Model 4530 for text messaging, go to [Chapter 6: Working with Text Messages](#).
- Use Model 4530's advanced routing features, go to [Chapter 7: Using the Modem/Router's Advanced Features](#). Here you can learn about features such as setting the Modem/Router up for online gaming, changing the default wireless settings including security, backing up your Modem/Router's configuration and setting up scheduling rules to limit when the Modem/Router may be used.

If you have not done the initial setup of your 3G+ Modem/Router with Phone Port, continue on to [Chapter 2: Installing the Hardware](#).

# 2

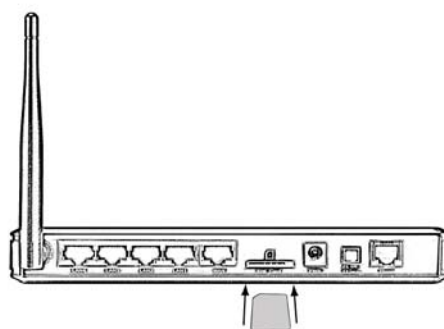
## Installing the Hardware


---

*This chapter explains installing Model 4530 hardware. Before installing the hardware you will need a SIM card to use the Modem/Router's cellular modem. If you want to use the Modem/Router for both voice and data you will need a SIM card that supports voice and data. If you just want to use the Modem/Router for data, then you will need a SIM card that at least supports data.*


To Install Model 4530 follow these steps:

- 1 Place the Modem/Router near a computer to be used for setup. This computer needs an Ethernet (LAN) port.
- 2 Turn off the computer.
- 3 Attach the antenna to the Modem/Router if the antenna isn't already attached. (Remove the antenna from the package. Place the end of the detachable antenna on the open antenna connection port and rotate the antenna clockwise by hand until it no longer turns easily. It may take many turns before the antenna is completely connected). Move the antenna into an upright orientation. The antenna should snap into place.
- 4 Insert the SIM card into the slot on the back of the modem as shown below. You should hear the SIM card click into place.



- 5 Connect one end of the supplied Ethernet cable to any of the computer's Ethernet ports and the other end to any of the Modem/Router's **LAN** ports.
- 6 Plug the supplied power cube into the Modem/Router, Router and then into a power outlet. The Modem/Router has completed powering up when the Status light  starts blinking.

**Important:** Use only the power cube shipped with the Modem/Router. Other power cubes may damage the device.

- 7 Check that the Signal Strength light  has changed from red to green or amber. If the light remains red please go to **Troubleshooting your Internet Connection**. A red light means that the Modem/Router can not talk to the mobile broadband network. A green light means you have strong signal, and an amber light means you have a weak signal. If your light is amber, you may try repositioning the antenna or moving the unit to another location.
- 8 Turn on the computer. An Ethernet (LAN) LED on your Modem/Router's front panel should light up sometimes, corresponding to the Ethernet (LAN) port you used. If it doesn't light up, please see the **Troubleshooting Tips** in the User Manual on the CD.

Now continue on to [Chapter 3: Using the Modem/Router's Configuration Manager](#) to configure the Modem/Router.

### **Resetting the Modem/Router to the Factory Configuration**

In the unlikely event that you need to reset the Modem/Router to the factory default configuration, insert the blunt end of a paper clip into the RESET hole on the front panel of the Modem/Router. Hold the clip in place for ten (10) seconds.

# 3

## Using the Modem/Router's Configuration Manager

---

*The Modem/Router includes a built-in Install Wizard that walks you through configuring the Modem/Router's software. For most users running the Install Wizard is all that is needed to configure the Modem/Router. If you are experienced with networking devices and their configuration, you may prefer to use the **Advanced** configuration program to tailor the Modem/Router's configuration to your needs. In that case go to [Using the Configuration Manager's Advanced Program](#) on page 81.*

### Launching the Modem/Router's Configuration Manager

---

To launch the Configuration Manager, please follow these steps:

- 1 If you haven't already done so, plug the supplied Ethernet cable into the Ethernet port on the Modem/Router's back panel and into your computer's Ethernet port.
- 2 Turn on your Modem/Router first, then your computer. Once the computer is on, launch the computer's Web browser.
- 3 In the Web browser address bar, type the Modem/Router's default IP address, **http://192.168.2.1** and then click Enter.

When the **USER'S MAIN MENU** opens for the first time, it displays a System Status page that summarizes the current settings and values for your system.



System Status [ HELP ]		
Item	WAN Status	Sidenote
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0 , 0.0.0.0	
Connection Time	-	Connecting...
Firmware Version	V1.0.0.1-V-4.	

Wireless Modem Information		
Item	Status	Sidenote
Card Info	HSPA USB MODEM	
Link Status	Connecting...	
Signal Strength	N/A	
Bytes Transmitted	0	
Bytes Received	0	
Network Name		

Wireless Status		
Item	WLAN Status	Sidenote
Wireless mode	Enable	(B/G/N Mixed)
SSID	Zoom_2848DD	
Channel	10	
Security	WPA-PSK / WPA2-PSK	(TKIP/AES)
MAC Address	00:50:18:84:EA:52	

Statistics Information		
Statistics of WAN	Inbound	Outbound
Octets	0	0
Unicast packets	0	0
Multicast packets	0	0
WAN MAC Address	00:50:18:84:EA:51	
LAN MAC Address	00:50:18:84:EA:52	

- On the Toolbar, type **admin** (the default password) in the System Password field, then click Login.



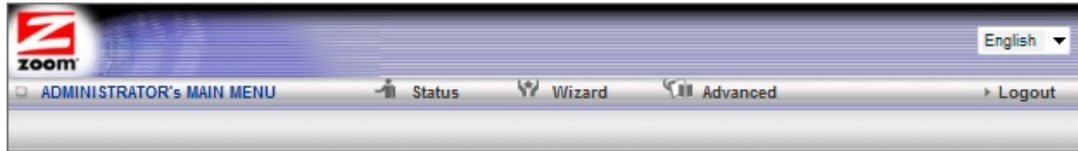
**Note:** Later, if you change the System Password, you will use the new password to log in.

When you log in, the Configuration Manager opens its Main Menu.

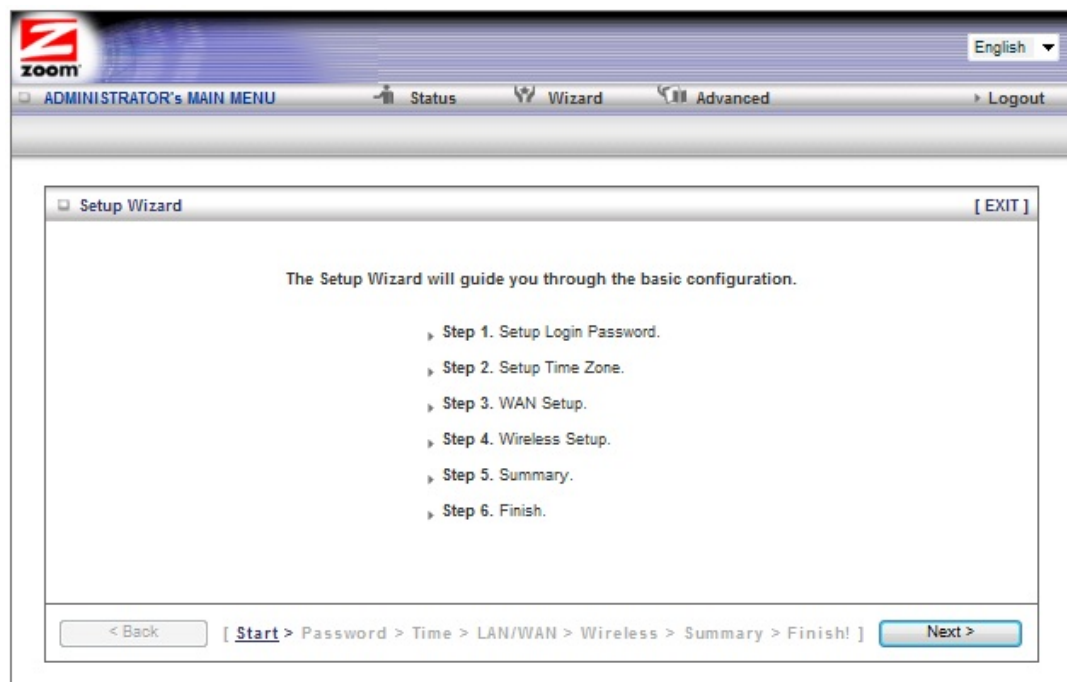
## Launching the Configuration Manager's Setup Wizard

When you start the Configuration Manager (<http://192.168.2.1> on your Web browser) and log in, the ADMINISTRATOR'S MAIN MENU opens.

Click Wizard on the Toolbar to launch the Setup Wizard, which will guide you through the configuration process.



The Setup Wizard page opens.



Each of the six Steps guides you in configuring a specific setting or group of settings. When you click Next or Back, you move from one step to another. If there is a setting that you don't want to change, simply click **Next** to go to the next setting.

### Step 1. Setup Login

To view or change configuration settings, you must enter a password. Your Modem/Router has a default password (admin) that was set by the factory and that you used to access the Configuration Manager initially. If you want to keep the default password, click Next to skip this step. Otherwise, to safeguard your configuration, we **strongly** recommend that you change the login password.

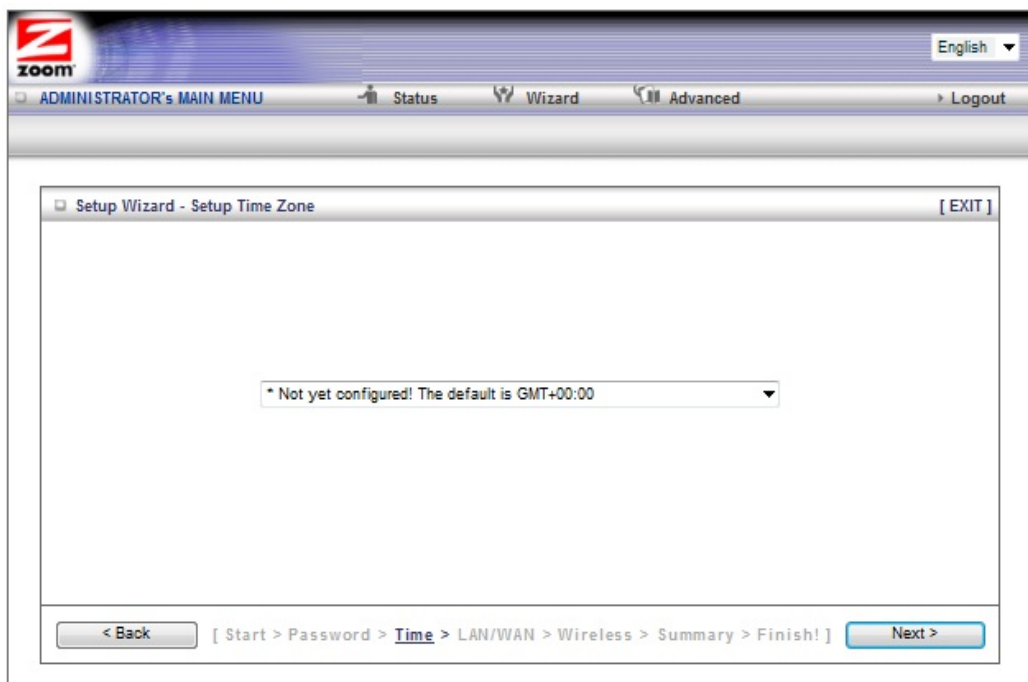
- 1 On the Setup Login Password page, type the old password in the Old Password field.
- 2 Type the new password in the New Password field.

3 Type the new password in the Retype Password field, then click Next.

**Note:** If you forget the new password, you won't have access to the Configuration Manager and will need to restore the device to its factory settings, thus losing any changes you made to your Modem/Router's configuration. To avoid this problem, we recommend that you write the new password here and on the bottom of your Modem/Router, and also save it elsewhere such as a settings document.  
PASSWORD: \_\_\_\_\_  
Please refer to [Resetting the Modem/Router to the Default Configuration](#) on page 7 or [The Reset to Default Dialog](#) on page 79 for more information in the unlikely event that you need to restore the Modem/Router's default settings.

## Step 2. Setup Time Zone

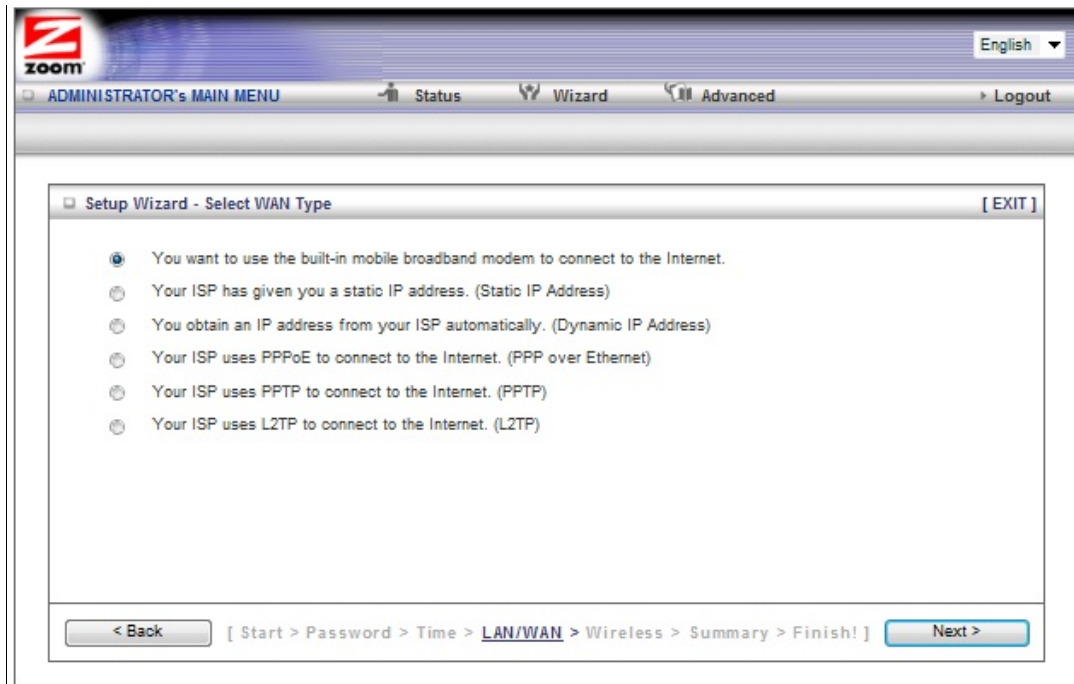
The Time Zone setting is used to track your incoming, outgoing, and missed calls, and for fairly sophisticated functions, such as changing Modem/Router access rules depending on the time of day. We recommend that you set your time zone now.



To set the time zone, select the time zone that applies to your location from the dropdown menu, and then click Next.

## Step 3. WAN Type Setup

The WAN Type refers to the protocol used by your Internet Service Provider in establishing your Internet connection. By default, WAN Type is set to use the built-in cellular modem. If that is what you want, you can select **Next** to skip this section.



## Selecting the WAN Type

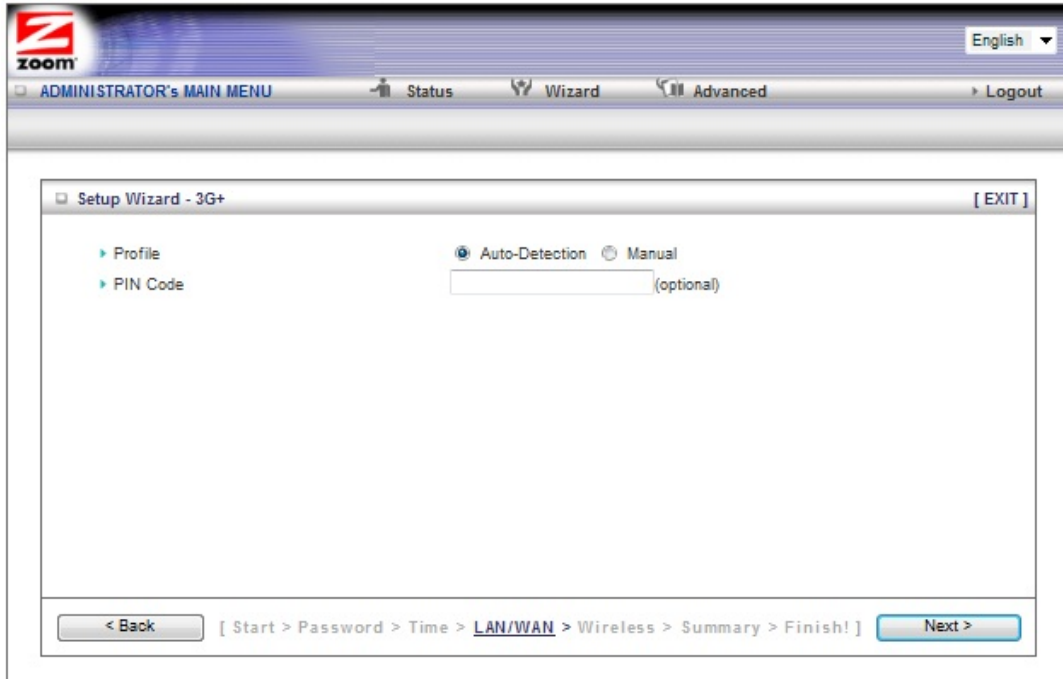
Please check with your service provider if you read the discussion below and are still unsure which WAN Type to choose.

- [Mobile Broadband Modem](#) - Select this if you want to use the Modem/Router's built-in 3G+ modem for voice and data.. (If you want to use the 3G+ modem as the backup to a DSL or Cable modem, you'll need to use the Configuration Manager's Advanced program to configure this setup. Please refer to 3G Failover on [The Basic Setup Page](#) on page 51.) You should select your primary connection type using the Setup Wizard. (To access the Setup Wizard, refer to page 10 for instructions.)
- [Configuring the Dynamic IP Address](#) – This is only used by Cable modem users and by DSL modem users who are not using PPPoE. (A DSL service providers will typically tell you whether you are using PPPoE, which requires you to enter an PPPoE-related password into the Modem/Router. If you are using DSL with 1483 routed, bridged, or PPPoA modes, you are not using PPPoE.)
- [Static IP Address](#) - Typically you have to request and pay extra for a static IP address, so this is not typically used.
- [PPPoE](#) – Only use this if you are plugging an ADSL modem into the Modem/Router, and if your ADSL service provider uses PPPoE.
- [PPTP](#) - The Point to Point Tunneling Protocol is more common in corporate environments and most users will not use this setting.
- [L2TP](#) - The Layer 2 Tunneling Protocol is more common in corporate environments and most users will not use this setting.

The relevant section immediately below depends on the WAN Type you selected.

### **Configuring the Built-in 3G+ Modem**

The page shown below only appears if you select the Cellular modem button on the Select WAN Type menu. Otherwise skip this section.



On the **Setup 3G+** page, **Auto-Detection** is enabled by default to automatically detect your SIM card provider. A message will show whether auto-detection was successful or not. If auto-detection was successful click **Next**. If auto-detection failed to detect your SIM card provider, click **OK** to close the message box and then select **Manual Setup**. On the **Manual Setup** page select your **Country**, and then select the name of your **Service Provider** from the drop down list. The rest of the fields on the page are automatically filled in. If a field is left empty, don't worry since that field is not used for your provider. Click **Next**.

**Note:** If your country or service provider does not appear in the dropdown list you must manually enter your service providers settings on the **Basic Setup** page. Please see [Chapter 7, Using the Configuration Manager's Advanced Program](#) for how to do this

Go to [Step 4. Wireless Settings](#).

### **Configuring the Static IP Address**

The page shown below will only appear in the unlikely event that you select the Static IP Address button on the Select WAN Type menu. Otherwise skip this section.

- **Static IP Address**  
This is the IP address that is given to you by your service provider when you sign up for a Static IP address. This address identifies your Modem/Router with Wireless-N when seen from the Internet.
- **Static Subnet Mask**  
This is the Modem/Router's subnet mask. Your service provider supplies this address.
- **Static Gateway**  
This is the IP address of the ISP server. Your service provider supplies this address.
- **Static Primary DNS**  
This is the Domain Name System (DNS) server's IP address. Your service provider supplies this address.
- **Static Secondary DNS**  
This is the IP address of an alternate Domain Name System (DNS) server. Your service provider supplies this address.

Go to [Step 4. Wireless Settings](#) on page 19.

### **Configuring the Dynamic IP Address**

The page shown below only appears if you select the Dynamic IP Address button on the Select WAN Type menu. Otherwise skip this section.

The screenshot shows the Zoom configuration wizard interface. At the top, there is a navigation bar with the Zoom logo, a language dropdown set to 'English', and links for 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area is titled 'Setup Wizard - Dynamic IP Address' and contains two input fields: 'Host Name' (optional) and 'ISP registered MAC Address'. A 'Clone' button is positioned next to the MAC address field. At the bottom, there is a progress bar with a '< Back' button, a breadcrumb trail '[ Start > Password > Time > LAN/WAN > Wireless > Summary > Finish! ]', and a 'Next >' button.

- Host Name  
This is the name that identifies your 3G+ Modem/Router with Phone Port. Some service providers require a host name. Your service provider supplies this name, if needed.
- ISP registered MAC Address  
This is the 12-digit **Media Access Control (MAC)** address of your Modem/Router. Cable modem users should click the Clone button to get the MAC address that was registered with your service provider for your device.

Go to [Step 4. Wireless Settings](#) on page 19.

### Configuring PPPoE

The page shown below only appears if you select the PPPoE button on the Select WAN Type menu. Otherwise skip this section.

The screenshot shows a web-based configuration interface for a Zoom device. At the top, there is a navigation bar with the Zoom logo, a language dropdown set to 'English', and menu items: 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area is titled 'Setup Wizard - PPP over Ethernet' and contains the following fields:

- ▶ PPPoE Account:
- ▶ PPPoE Password:
- ▶ Primary DNS:
- ▶ Secondary DNS:
- ▶ Service Name:  (optional)
- ▶ Assigned IP Address:  (optional)

At the bottom of the form, there is a '< Back' button on the left and a 'Next >' button on the right. A breadcrumb trail in the center reads: '[ Start > Password > Time > LAN/WAN > Wireless > Summary > Finish! ]'.

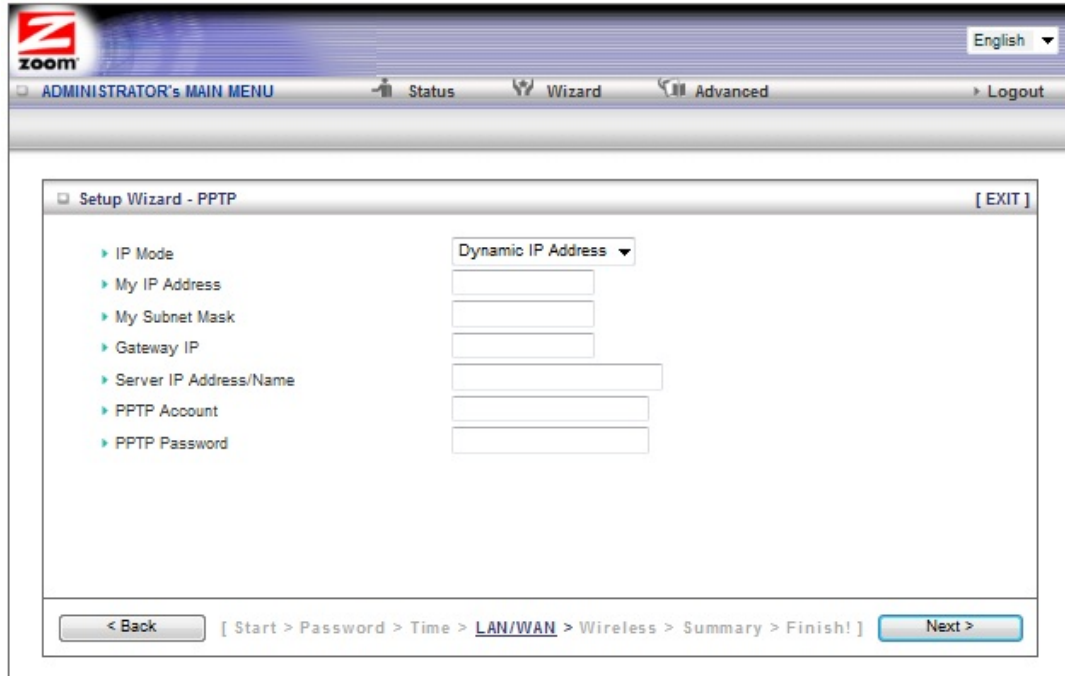
- **PPPoE Account**  
This is the PPPoE username supplied by your service provider.
- **PPPoE Password**  
This is PPPoE password supplied by your service provider.
- **Primary DNS**  
This is the Domain Name System (DNS) server's IP address. Your service provider supplies this address, if needed. Most users should not need to enter a DNS value.
- **Secondary DNS**  
This is the IP address of an alternate Domain Name System (DNS) server. Your service provider supplies this address, if needed.
- **Service Name**  
This is the name assigned by your service provider to identify your service. The Service Name is optional.
- **Assigned IP Address**  
This is the optional IP address assigned by your service provider. The Assigned IP Address is optional.

Go to [Step 4. Wireless Settings](#) on page 19.



## Configuring PPTP

The page shown below only appears if you select the **PPTP** button on the Select WAN Type menu. Otherwise skip this section.



The screenshot shows the Zoom Administrator's Main Menu interface. At the top, there is a navigation bar with the Zoom logo, a language dropdown set to 'English', and links for 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area is titled 'Setup Wizard - PPTP' and contains a list of configuration options on the left and corresponding input fields on the right:

- IP Mode: Dynamic IP Address (dropdown menu)
- My IP Address: [text input field]
- My Subnet Mask: [text input field]
- Gateway IP: [text input field]
- Server IP Address/Name: [text input field]
- PPTP Account: [text input field]
- PPTP Password: [text input field]

At the bottom of the wizard, there is a '< Back' button, a breadcrumb trail: '[ Start > Password > Time > LAN/WAN > Wireless > Summary > Finish! ]', and a 'Next >' button.

- **IP Mode**  
This is the mode used to generate the IP address. Select an option from the dropdown menu, based on your service provider's requirements.
- **My IP Address**  
This is the private IP address that your service provider assigned to your Modem/Router.
- **My Subnet Mask**  
This is the private subnet mask that your service provider assigned to your Modem/Router.
- **Gateway IP**  
This is the IP address of the service provider's server. Your service provider supplies this address.
- **Server IP Address/Name**  
This is the name and IP address of the PPTP server. Your service provider supplies this information, if needed.
- **PPTP Account**  
This is the PPTP account name that your service provider assigned to you.
- **PPTP Password**  
This is PPTP password that your service provider assigned to you.

Go to [Step 4. Wireless Settings](#) on page 19.

## **Configuring L2TP**

The page shown below only appears if you select the L2TP button on the Select WAN Type menu. Otherwise skip this section.

The screenshot shows the 'Setup Wizard - L2TP' configuration page in a web browser. The browser's address bar shows 'zoom' and the page title is 'ADMINISTRATOR's MAIN MENU'. The page has a navigation bar with 'Status', 'Wizard', 'Advanced', and 'Logout' options. The main content area is titled 'Setup Wizard - L2TP' and contains the following fields:

- IP Mode: Dynamic IP Address (dropdown menu)
- IP Address: [Text input field]
- Subnet Mask: [Text input field]
- WAN Gateway IP: [Text input field]
- Server IP Address/Name: [Text input field]
- L2TP Account: [Text input field]
- L2TP Password: [Text input field]

At the bottom of the page, there is a navigation bar with a '< Back' button, a breadcrumb trail '[ Start > Password > Time > LAN/WAN > Wireless > Summary > Finish! ]', and a 'Next >' button.

- **IP Mode**  
This is the mode used to generate the IP address. Select an option from the dropdown menu, based on your service provider's requirements.
- **IP Address**  
This is the IP address that identifies the L2TP server. Your service provider supplies this address.
- **Subnet Mask**  
This is the Modem/Router's subnet mask. Your service provider supplies this address.
- **WAN Gateway IP**  
This is the WAN Gateway IP address of the L2TP server. Your service provider supplies this address.
- **Server IP Address/Name**  
This is the name and IP address of the L2TP server. Your service provider supplies this information, if needed.
- **L2TP Account**  
This is the L2TP account name or user name supplied by your service provider.
- **L2TP Password**  
This is L2TP password supplied by your service provider.

Go to [Step 4. Wireless Settings](#) on page 19.

## Step 4. Wireless Settings

The Wireless Settings page lets you change the wireless settings for your Modem/Router. If you are happy with your wireless settings (set at the factory to wireless with WPA2/WPA security), click Next to go to Step 5. Otherwise, continue below. EITHER WAY, after running the Setup Wizard you will need to make sure that wireless devices connecting to the Modem/Router (computers, phones, tablets, game stations, etc.) are set up properly as discussed in [Chapter 3](#).

The screenshot shows the 'Setup Wizard - Wireless settings' window. It has a title bar with the Zoom logo and a language dropdown set to 'English'. Below the title bar is a navigation menu with 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area contains three settings: 'Wireless Module' with radio buttons for 'Enable' (selected) and 'Disable'; 'Network ID(SSID)' with a text input field containing 'Zoom'; and 'Channel' with a dropdown menu showing '1'. At the bottom, there is a '< Back' button, a breadcrumb trail '[ Start > Password > Time > WAN > **Wireless** > Summary > Finish! ]', and a 'Next >' button.

screen

new

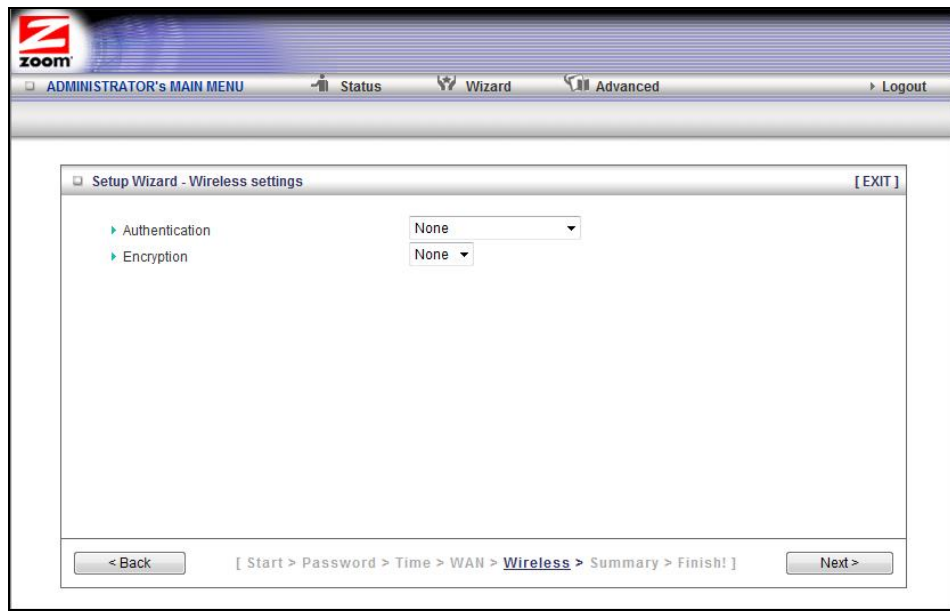
- Wireless Module Accept the default, Enable. Click the Disable checkbox only if you do not want wireless clients to access your network.
- Wireless Network Name (SSID) is the name of your wireless network. By default, the SSID for Model 4530 is Zoom-xxxxxx, where xxxxxx is 6 random alphanumeric digits. Your default SSID is printed on the label on the bottom of your unit. You can change the SSID to a name of your choice. The SSID can be up to 32 alphanumeric characters. If you change the name, make sure that all devices on your Modem/Router's wireless network use the new SSID as the access point.
- Channel refers to the wireless network channel assigned to your LAN. By default, the Modem/Router uses channel 10. You would only change this setting if you were concerned about possible interference from another wireless access point using the same channel.

**TIP:** Other wireless networks might be within range of your network. Your neighbors, for instance, may be within range. If you are having trouble connecting, try setting a different channel to see if that improves performance. You should try setting a channel that is 5 or more channels away from what you are using. By default, the

Modem/Router is set to 11. You may want to try channel 1 or 6, for instance, if you have trouble connecting with the default channel (11).

## Wireless Security Settings

If you accepted the default to Enable the Wireless Module (on the Wireless Settings page at Step 4), the following page opens when you click Next. **New screen**



## Configuring Authentication and Encryption

By default, Authentication and Encryption security services are set to **WPA2/WPA** and a random **Security Key** is programmed in at the factory. This key is printed on the label on the bottom of your unit. Most users should accept the default settings.

If you have devices on your network that only support WEP (for example, some gaming consoles) than you will need to setup WEP. Please see [WEP Authentication and Encryption](#).

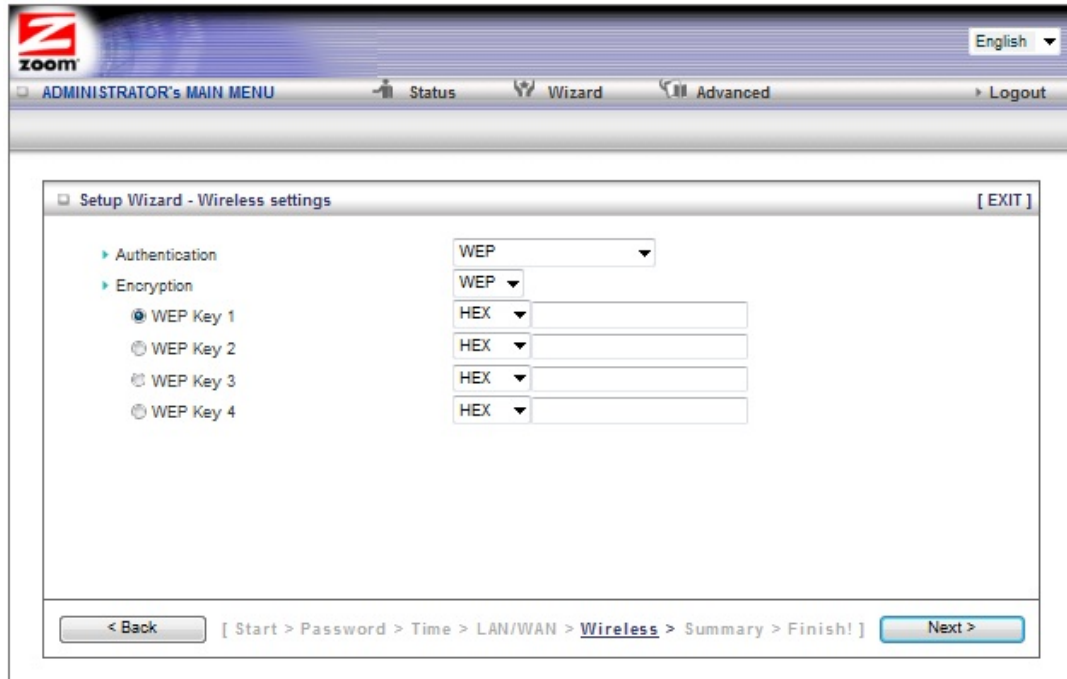
If you want to change the **Security Key** used by the Modem/Router. For example, you are replacing an existing wireless Modem/Router and want to use the same key. Enter the key you want to use in the **Security Key** field. This key should be from 8 to 64 characters long.

**Important:** If you are attaching other wireless devices to your Modem/Router you will need to enter the **Security Key** that is printed on the bottom label on your Modem/Router. If you have changed this key, you will need to enter the new key. See [Chapter 4: Connecting Devices Wirelessly to the Modem/Router](#) for more information.

## WEP Authentication and Encryption

If you have devices on your wireless network that support only WEP, (for example, some gaming consoles), you will need to select WEP as your Authentication method.

When you select WEP from the Authentication dropdown menu, the Encryption field expands, as shown in the following figure.



The screenshot shows the Zoom configuration wizard interface. At the top, there is a navigation bar with the Zoom logo, a language dropdown set to 'English', and menu items for 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area is titled 'Setup Wizard - Wireless settings' and contains the following configuration options:

- Authentication:** A dropdown menu set to 'WEP'.
- Encryption:** A dropdown menu set to 'WEP', which has expanded to show four 'WEP Key' options, each with a 'HEX' dropdown menu and an adjacent text input field.
- WEP Key 1:** Selected with a radio button.
- WEP Key 2:** Unselected with a radio button.
- WEP Key 3:** Unselected with a radio button.
- WEP Key 4:** Unselected with a radio button.

At the bottom of the wizard, there is a progress bar with a '< Back' button, a breadcrumb trail '[ Start > Password > Time > LAN/WAN > Wireless > Summary > Finish! ]', and a 'Next >' button.

Field	Entry
Authentication	Select <b>WEP</b>
Encryption	Select <b>WEP</b>
Encryption WEP Key 1, 2, 3, 4	We recommend selecting HEX as the key format as Ascii keys can have compatibility issues between different devices..

<p><b>Encryption</b> <b>WEP Key 1, 2, 3,</b> <b>4</b></p>	<p>You can choose to either use WEP 128 bit encryption or WEP 64 bit encryption. The difference is 128 bit is more secure and 64 bit is faster. We recommend selecting 64 bit.</p> <p><i>If you selected Hex format and you chose a 64-bit key length, 13 hexadecimal values are required. (Hexadecimal values include the numbers 0-9 and the letters A-F) Write the 13-hexadecimal key in the space below for future reference, and then enter it in the Key 1 box.</i></p> <p>-----</p> <p><i>If you selected Hex format and you chose a 128-bit key length, 26 hexadecimal values are required. (Hexadecimal values include the numbers 0-9 and the letters A-F) Write the 26-hexadecimal key in the space below for future reference, and then enter it in the Key 1 box.</i></p> <p>-----</p> <p>-----</p> <p>If you selected ASCII format, and you chose a 64-bit key length, 5 ASCII characters are required. Write the 5-ASCII-character key in the space below for future reference, and then enter it in the Key 1 box.</p> <p>-----</p> <p><i>If you selected ASCII format, and you chose a 128-bit key length, 13 ASCII characters are required. Write the 13-ASCII-character key in the space below for future reference, and then enter it in the Key 1 box.</i></p> <p>-----</p>
---	--

### Step 5. Summary

The Summary page displays the updated configuration settings for your Modem/Router and lets you accept, change, and test the configured values.

Setup Wizard - Summary [EXIT]

Please confirm the information below

[ WAN Setting ]	
WAN Type	3G/4G/LTE
APN	
PIN Code	
Dialed Number	
Account	
Password	*****
[ Wireless Setting ]	
Wireless	Enable
SSID	Zoom
Channel	1
Authentication	WPA-PSK / WPA2-PSK
Encryption	TKIP/AES

Do you want to proceed with the network testing?

The Ethernet Port will be used as LAN Port after saving. Confirm?

< Back [ Start > Password > Time > WAN > Wireless > Summary > Finish! ] Apply Settings

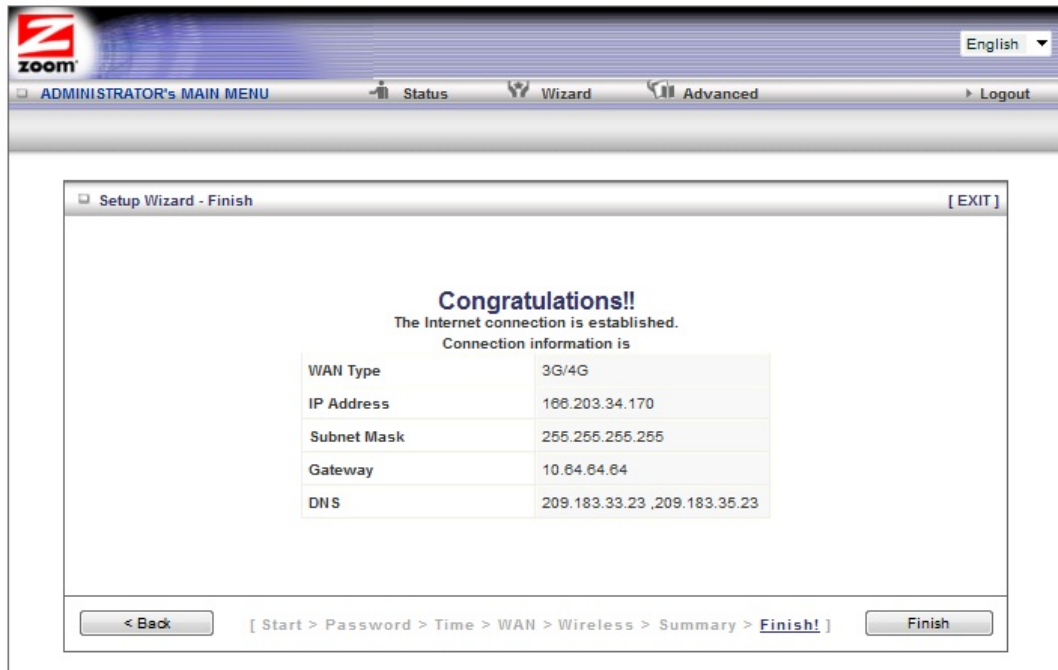
### New screen

- 1 To edit your entries, click Back as many times as needed to access the page for the field(s) to be edited, then click Next to continue with your edits or to return to the updated Summary page.
- 2 **If you are using the built-in 3G+ Modem** the Do you want to proceed with the network testing? checkbox is selected. We recommend that you leave this checked to test your 3G+ connection. If you do not want to test your 3G+ connection at this time uncheck the **Do you want to proceed with the Network testing box**.  
**Note:** If you are not using the built-in 3G+ modem this option does not appear.
- 3 When you're satisfied with the configured settings, click Apply Settings to save the new configuration.

## Step 6. Finish

If you are not using the built-in 3G+ modem or you decided not to test your mobile broadband connection the **Configuration is Completed** page displays. Click **Finish** to restart the router and save the new configuration settings for your router.

If your Internet connection test was successful, the **Congratulations!!** screen will appear. Click **Finish** to restart the router and save the new configuration settings for your router.



new screen

If your Internet connection test was not successful, try running the test again by clicking **Connect Again**. If the test still fails please see [Troubleshooting your Built-in 3G+ Modem Connection](#).

Congratulations! Your Modem/Router should now be configured.


- If you want to learn how to attach other wireless devices to the Modem/Router go to [Chapter 4: Connecting Devices Wirelessly to the Modem/Router](#).
- If you want to learn about the Modem/Router's voice features including viewing a list of incoming, outgoing or missed calls, or setting up advanced voice features like Call forwarding, call waiting, or speed dialing go to [Chapter 5: Understanding your Modem/Router's Voice Features](#).
- To learn how to use Model 4530 for text messaging go to [Chapter 6: Working with Text Messages](#).
- In the unlikely event that you want to use the **Advanced** configuration



program to tailor the Modem/Router's configuration to your needs, for example, to set up a Virtual Server or DMZ so that your games or gaming consoles can access the Internet through your Modem/Router's firewall, please continue to [Chapter 7: Using the Configuration Manager's Advanced Program](#). (Most users will not need to do this.)

Your Modem/Router's setup is complete. **Congratulations!**

### **Troubleshooting your Built-in 3G+ Modem Connection**

If you are unable to connect to the Internet through your router, please first check Signal Strength light  on the Modem/Router's front panel.

If the light is red that means either your SIM card is not inserted or not working, or your Modem/Router is not receiving a mobile broadband signal. If your Signal Strength light is red please try the following:

- Check that your SIM card is properly inserted into the back of your Modem/Router.
- Verify that you are in a mobile broadband coverage area. You may want to move the antenna to optimize signal strength; putting the antenna in a vertical position normally gives the best performance. You may also want to try changing the location of your router, for example, by moving the router closer to a window.

If your Signal Strength Light is amber or green that means you are connected to the mobile broadband network but most likely your mobile broadband settings are wrong. If your Signal Strength light is green or amber please try the following:

- If you used auto-configure to detect your service provider, the Modem/Router may have used the wrong settings for your provider. Auto-configure can only detect your service provider, it can not detect the actual settings. Once it detects your provider it tries the most common setting for that provider. To check if this is the problem, run the setup wizard again. When you get to the **Setup 3G+** page select **Manual**. Select your country and then select your service provider. If you have multiple settings for your service provider you will need to run the wizard again until you have tried each setting. If none of the predefined settings work, contact your service provider and ask if they can provide you with your **APN, Dialed Number, Account, Password, and Pin Code**. Some of these settings are optional and your service provider may not need them.
- If your Signal Strength light is amber, you may want to move the antenna to optimize signal strength; putting the antenna in a vertical position normally gives the best performance. You may also want to try changing the location of your router, for example, by moving the router closer to a window.

If you are still having problems connecting to the Internet please contact Zoom Technical Support as described in [Appendix C: Registering Your Product and Getting Help](#).

# 4

## Connecting Devices Wirelessly to the Modem/Router

---

*This chapter provides tips for connecting devices (computers, phones, tablets, game stations, etc.) wirelessly to the Modem/Router. If you are familiar with this already, **or if you prefer to use the instructions associated with each device**, you don't need to read this chapter. You do need to make sure that each device connecting to the Modem/Router is set up for wireless security that is compatible with the Modem/Router's wireless security settings.*

### Establishing your Wireless Network

Note that for **each** computer or other device added to your wireless network, you will need to take appropriate steps for setting up that computer or other device. To do that, select one of the possibilities for that computer or other device below:

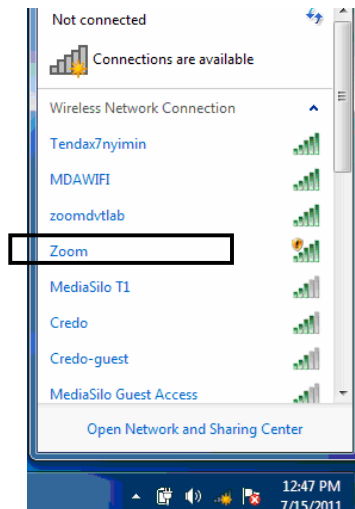
- Many newer **Windows 7, Vista, and XP computers have built-in wireless networking** capabilities and do not require the installation of a wireless component. If this is the case, you should set up that computer's wireless connection using the Windows 7, Vista, or XP connect utility. See the sections below on connecting **Windows 7** (page 27) , **Vista** (page 28), or **XP** (page 29) computers with built-in wireless capabilities.
- Some **computers** may have **built-in wireless networking** capabilities, but do not use the Windows 7, Vista, or XP utility to configure their device. If this is so, set up your computer's wireless connection using the instructions on page 29 for **Connecting a Wireless-enabled Computer or Device to the Modem/Router**.
- If you are using a Macintosh computer see the instructions on page 29 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, iPod Touch**, etc., see the instructions on page 29 for **Connecting a Wireless-enabled Computer or Device to the Modem/Router**.
- Some **computers** may need a **wireless network adapter installed**. This can be a USB adapter, PC Card adapter, or PCI adapter. When you install the adapter, make sure that it is set to **infrastructure** or **access point** mode (NOT **ad-hoc** or **peer-to-peer** mode). If you need help installing your wireless adapter or setting its mode, refer to the documentation that came with it. After you install the adapter, see the instructions on page 29 for **Connecting a Computer with a wireless adapter to the Modem/Router**.

## Connecting a Windows 7 Computer with Built-in Wireless Capabilities

- 1 From the taskbar, click on the wireless symbol.



- 2 In the wireless network options box, highlight the Wireless Network Name (SSID) you gave your wireless network in Step 4 of the Setup Wizard. If you did not change the Wireless Network Name (SSID), select the default name **Zoom\_XXXXXX**, where XXXXXX are 6 random alphanumeric characters. The complete Wireless Network Name is printed on the bottom label of your unit. If you want to automatically connect to the Modem/Router, click the **Connect Automatically** box. Then click **Connect**.



- When prompted, enter the **Security Key** found on the bottom label of your unit. If you changed the key in Step 4 of the Setup Wizard, enter the new security key and click **Connect**.
  - If you disabled wireless security in Step 4 of the Setup Wizard select **Connect Anyway** when warned that your network is unsecure.
- When you click on the wireless network option box, Windows will scan for available networks. More than one wireless network may appear in the list. These are other wireless networks that are within range of your network. Your neighbors, for instance, may be within range of your network. Each wireless network has a channel associated with it. We recommend there be at least a five-channel difference between your network and those of your neighbors. Having less than a five-channel difference may result in interference with your connection. By default, the Modem/Router uses channel 10. If you need to change this channel, you must do so using the **Wireless Setup** page of the **Zoom Configuration Manager**. For instructions on how to log in to the **Zoom Configuration Manager**, see page 8. After logging in, select **Wireless** from the left-hand menu. On the **Wireless** page you can select a new channel from the drop-down menu.

### 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 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 wireless network options box, highlight the Wireless Network Name (SSID) you gave your wireless network in Step 4 of the Setup Wizard. If you did not change the Wireless Network Name (SSID), select the default name **Zoom\_XXXXXX**, where XXXXXX are 6 random alphanumeric characters. The complete Wireless Network Name is printed on the bottom label of your unit. If you want to automatically connect to the Modem/Router, click the **Connect Automatically** box. Then click **Connect**.
    - When prompted, enter the **Security Key** found on the bottom label of your unit. If you changed the key in Step 4 of the Setup Wizard, enter the new security key and click **Connect**.
    - If you disabled wireless security in Step 4 of the Setup Wizard select **Connect Anyway** when warned that your network is unsecure.
- When you click on the wireless network option box, Windows will scan for available networks. More than one wireless network may appear in the list. These are other wireless networks that are within range of your network. Your neighbors, for instance, may be within range of your network. Each wireless network has a channel associated with it. We recommend there be at least a five-channel difference between your network and those of your neighbors. Having less than a five-channel difference may result in interference with your connection. By default, the Modem/Router uses channel 10. If you need to change this channel, you must do so using the **Wireless Setup** page of the **Zoom Configuration Manager**. For instructions on how to log in to the **Zoom Configuration Manager**, see page 8. After logging in, select **Wireless** from the left-hand menu. On the **Wireless** page you can select a new channel from the drop-down menu.
- 3 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 connect 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.

**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 In the wireless network options box, highlight the Wireless Network Name (SSID) you gave your wireless network in Step 4 of the Setup Wizard. If you did not change the Wireless Network Name (SSID), select the default name **Zoom\_xxxxxx**, where xxxxxx are 6 random alphanumeric characters. The complete Wireless Network Name is printed on the bottom label of your unit. If you want to automatically connect to the Modem/Router, click the **Connect Automatically** box. Then click **Connect**.
    - When prompted, enter the **Security Key** found on the bottom label of your unit. If you changed the key in Step 4 of the Setup Wizard, enter the new security key and click **Connect**.
    - If you disabled wireless security in Step 4 of the Setup Wizard select **Connect Anyway** when warned that your network is unsecure.
- When you click on the wireless network option box, Windows will scan for available networks. More than one wireless network may appear in the list. These are other wireless networks that are within range of your network. Your neighbors, for instance, may be within range of your network. Each wireless network has a channel associated with it. We recommend there be at least a five-channel difference between your network and those of your neighbors. Having less than a five-channel difference may result in interference with your connection. By default, the Modem/Router uses channel 10. If you need to change this channel, you must do so using the **Wireless Setup** page of the **Zoom Configuration Manager**. For instructions on how to log in to the **Zoom Configuration Manager**, see page 8. After logging in, select **Wireless** from the left-hand menu. On the **Wireless** page you can select a new channel from the drop-down menu.

**To disconnect from the current network:**

- 1 On your Windows desktop, click the **Wireless Network Icon** in the System Tray.
- 2 **Select** your Wireless Network Name. And click on **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 documentation on how to enable wireless.



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

- 2 Select the Wireless Network Name (SSID) you gave your wireless network in Step 4 of the Setup Wizard. If you did not change the Wireless Network Name (SSID), select the default name **Zoom\_XXXXXX**, where XXXXXX is 6 random alpha numeric characters.
  - When prompted for the wireless password, enter the **Security Key** found on the bottom label of your unit. If you changed the key in Step 4 of the Setup Wizard, enter the new security key. Click **OK** to connect to the Modem/Router.
  - More than one wireless network may appear in the list. These are other wireless networks that are within range of your network. Your neighbors, for instance, may be within range of your network. Each wireless network has a channel associated with it. We recommend there be at least a five-channel difference between your network and those of your neighbors. Having less than a five-channel difference may result in interference with your connection. By default, the Wireless-N Router uses channel 10. If you need to change this channel, you must do so using the **Wireless Setup** page of the **Zoom Configuration Manager**. For instructions on how to log in to the **Zoom Configuration Manager**, see page 8. After logging in, select **Wireless** from the left-hand menu. On the **Wireless** page you can select a new channel from the drop-down menu.

**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 Computer or Device (including the iPhone or other cellular phones, the iPod Touch, etc.) to the Modem/Router**

- 1 Go to 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 Wireless Network Name (SSID) (Service Set Identifier) that you gave the Modem/Router Step 4 of the Setup Wizard. If you did not change the Wireless Network Name (SSID), select the default name **Zoom\_XXXXXX**, where XXXXXX are 6 random alphanumeric

characters. The complete Wireless Network Name is printed on the bottom label of your unit. Select it as the network you want to use to connect to the Internet.

When prompted, enter the **Security Key** found on the bottom label of your unit. If you changed the key in Step 4 of the Setup Wizard, enter the new security key and click **Connect**.

**Tip!**

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

There are several site scan issues you should be aware of:

- More than one wireless network may appear in the list. These are other wireless networks that are within range of your network. Your neighbors, for instance, may be within range of your network. Each wireless network has a channel associated with it. We recommend there be at least a five-channel difference between your network and those of your neighbors. Having less than a five-channel difference may result in interference with your connection. By default, the Modem/Router uses channel 10. If you need to change this channel, you must do so using the **Wireless Setup** page of the **Zoom Configuration Manager**. For instructions on how to log in to the **Zoom Configuration Manager**, see page 8. After logging in, select **Wireless** from the left-hand menu. On the **Wireless** page you can select a new channel from the drop-down menu.
- 2 Test your wireless connections. From each computer or device that you set up, open your Web browser (for instance, Internet Explorer, Firefox, or Chrome) and try to connect to a familiar Web address.

**If you connect successfully, you are ready to browse the Web!**

**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 **Zoom\_XXXXXX**, where XXXXXX are 6 random alphanumeric characters.
- 3 Select or click on **Disconnect** or similarly-named button.

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

- 1 Go to the computer that is set up with a wireless adapter that you want to add to the network. The computer should have software that will let it perform a **site search** to scan for available wireless networks in your area. When the Wireless Network Name (SSID) that you set in step 4 of the Setup Wizard of your Modem/Router's wireless network appears in the list select it as the network you want to use to connect to the Internet. If you did not change the Network ID (SSID), select the default name **Zoom\_XXXXXX**. Where XXXXXX are 6 random alphanumeric characters. The complete Network ID is printed on the bottom label of your unit.

**Tip!**

For most wireless adapters, you will use its wireless 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. If you need help, refer to the documentation that came with your wireless adapter.

- 2 When prompted, enter the **Security Key** found on the bottom label of your unit. If you changed the key in Step 4 of the Setup Wizard, enter the new security key.

There are several site scan issues you should be aware of:

- If you are trying to connect to a wireless network that already has security enabled, your wireless adapter might not recognize what type of security is on the network. You may need to manually set up the security for your adapter. If you need help, refer to the documentation that came with your wireless adapter.
  - **Windows 7, XP, and Vista users:** If you installed a wireless adapter on a Windows 7, XP, or Vista 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.
  - More than one wireless network may appear in the list. These are other wireless networks that are within range of your network. Your neighbors, for instance, may be within range of your network. Each wireless network has a channel associated with it. We recommend there be at least a five-channel difference between your network and those of your neighbors. Having less than a five-channel difference may result in interference with your connection. By default, the Modem/Router uses channel 10. If you need to change this channel, you must do so using the **Wireless Setup** page of the **Zoom Configuration Manager**. For instructions on how to log in to the **Zoom Configuration Manager**, see page 8. After logging in, select **Wireless** from the left-hand menu. On the **Wireless** page you can select a new channel from the drop-down menu.
- 2 Test your wireless connections. From each desktop or notebook computer that you set up, open your Web browser (for instance, Internet Explorer or Firefox) and try to connect to a familiar Web address.

**If you connect successfully, you are ready to browse the Web!**

**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 Modem/Router's Wireless Network Name.
- 3 Select or click on **Disconnect** or similarly-named button.

## Setting up your Network using WPS

---

If all the wireless devices you plan to connect to your network support **Wi-Fi Protected Setup (WPS)**, you can use WPS to connect and secure your devices in one step. To use WPS follow the instructions below.



**Note:** WPS configures one client device at a time. Please repeat the configuration method for each client on your wireless network that supports WPS security.

## Configuration Methods

WPS offers three configuration methods. Choose the method that is compatible with the hardware and software options available on your “client device,” which is the device you’re connecting wirelessly to the Modem/Router.

### Method One

Use this method if your client device has a **WPS** button. This button can be either a physical button on the unit or a software button in its application.

- 1 Press the WPS button on your Modem/Router and hold it in for seven (7) seconds until the Wireless LED starts blinking rapidly.

**Important!** The Registrar (the device configuring the WLAN) goes into the WPS mode and the Enrollee (the device joining the WLAN) then looks for it. You should always start the Registrar first. By default your Modem/Router is configured as a Registrar.

- 2 Click or press the WPS button on the client device.
- 3 Refer to your client device's documentation for further instructions, if necessary.

### Method Two

Use this method if your client device already has a WPS PIN number. The client is the Enrollee.

- 4 If you haven't already done so, open a Web browser and type **http://192.168.2.1** in the address bar.
  - a When the Configuration Manager launches, log in as admin, then select Advanced > Basic Settings > Wireless to open the Wireless Setup page.
  - b Click the **WPS Setup** button to open the **Wi-Fi Protected Setup** page.
  - c Select **PIN Code** from the **Config method** dropdown menu.
  - d Enter the **PIN number** from your client device.
  - e Click **Trigger** to start the connection process on the Modem/Router.

**Important!** You must do this within two minutes after starting the Modem/Router.
  - f On the Modem/Router, when the program displays a message that the process succeeded, click **Save** to save the configuration

### Method Three

Use this method if your client device requests the Modem/Router’s PIN number. The client is the Registrar. Use this method if the client(s) are to connect to multiple access points so that a client will control the configuration instead of the Modem/Router.

- 1 If you haven't already done so, open a Web browser and type **http://192.168.2.1** in the address bar.

- a When the Configuration Manager launches, log in as admin, then select **Advanced > Basic Settings > Wireless** to open the Wireless Setup page.
- b Click the **WPS Setup** button.
- c Select **Enrollee** from the **Config Mode** dropdown menu.
- d Click **Generate Pin** to generate a new Pin number.
- e Enter the Modem/Router's **Pin Number** into your client device. Refer to your client's documentation for further details.  
**Important!** You must do this within two minutes after starting the Modem/Router.
- f Click **Trigger** to start the connection process on the Modem/Router.
- g On the Modem/Router, when the program displays a message that the process succeeded, click **SET** to keep the Modem/Router from receiving new configuration parameters from another WPS Registrar.
- h Click **Save** to save the configuration.

# 5

## Understanding your Modem/Router's Voice Features

---

*Most users will just plug their home phone into the Modem/Router's phone port and begin placing calls over the cellular voice network. This chapter is only for users who want to monitor their incoming, outgoing or missed calls, to setup call waiting or speed dialing, or to setup advanced telephony features.*

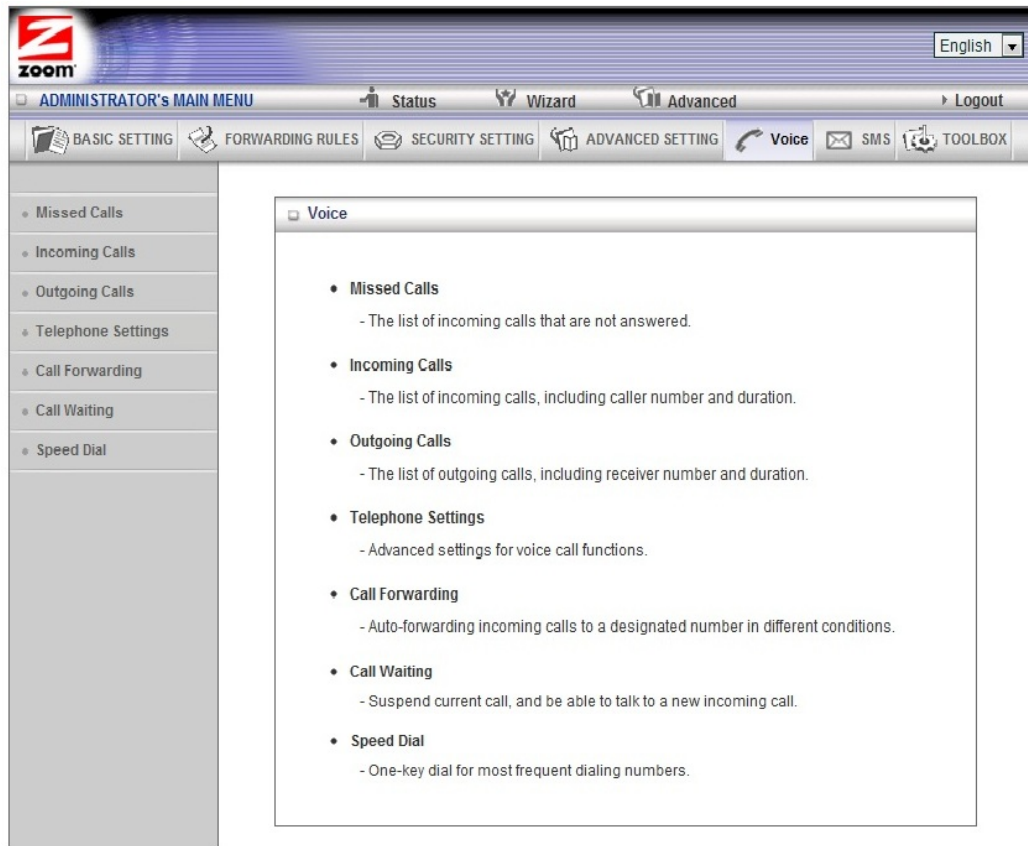
If you are using the Modem/Router's built-in 3G+ modem to make voice calls and are connected to the Modem/Router through your computer's Ethernet port, you can go right ahead and log into the configuration manager. If you are using a wireless connection to access the Modem/Router you must first establish the wireless connection. If you are unsure how to set up a wireless connection see [Establishing your Wireless Network](#) on page 26.

- 4 Turn on your computer and Modem/Router, then launch the computer's Web browser.
- 5 In the Web browser address bar, type the Modem/Router's default IP address, **http://192.168.2.1** and then click Enter.  
When the MAIN MENU opens for the first time, it displays a System Status page that summarizes the current settings and values for your system.
- 6 On the Toolbar, type **admin** (the default password) in the System Password field, then click Login.



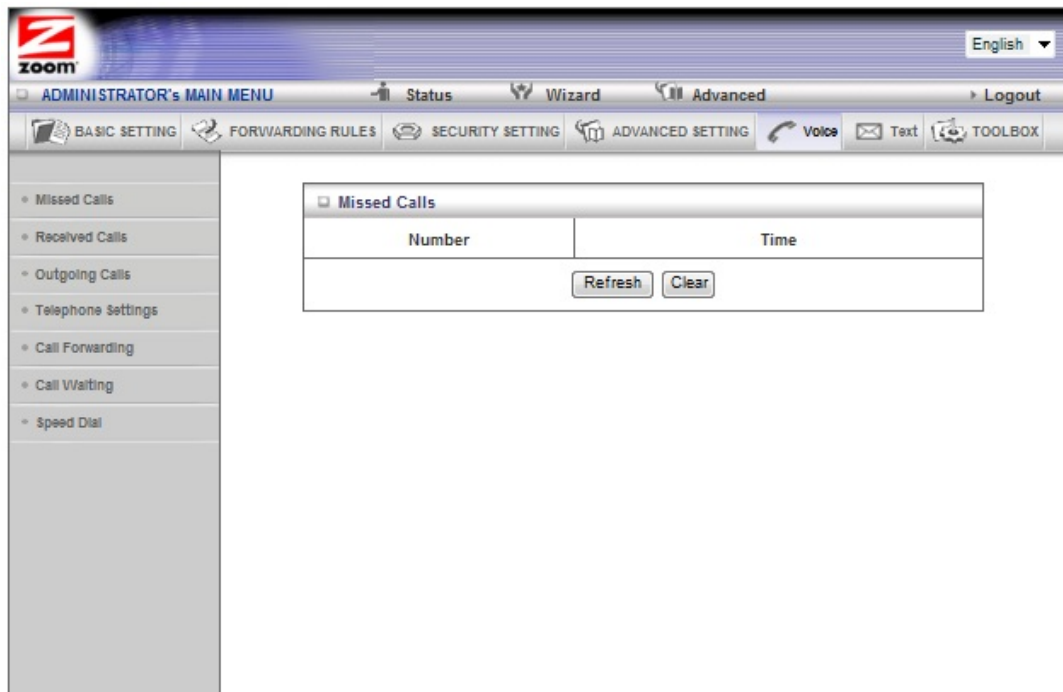
**Note:** if you have changed the System Password, you will use the new password to log in.

- 7 When you log in, the Configuration Manager opens its Main Menu. Select **Voice** on the top menu.



## Missed Calls

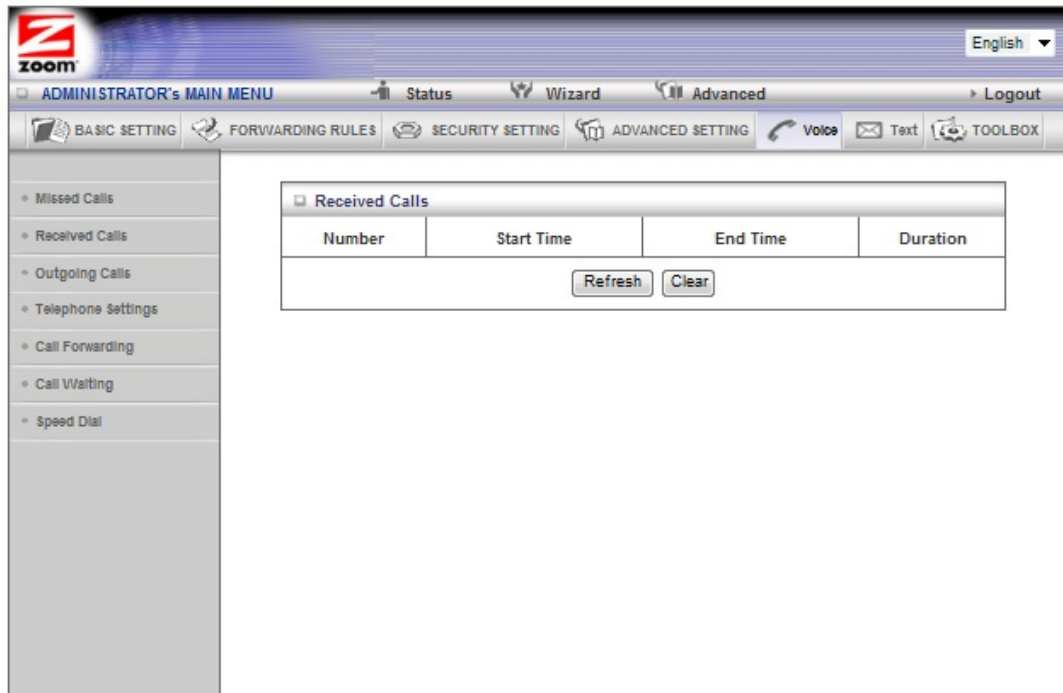
When you click on **Missed Calls** on the left hand menu the following screen appears:



This page displays the calls that you missed. Clicking on **Refresh** updates the screen and clicking on **Clear** erases the existing missed calls.

## Received Calls

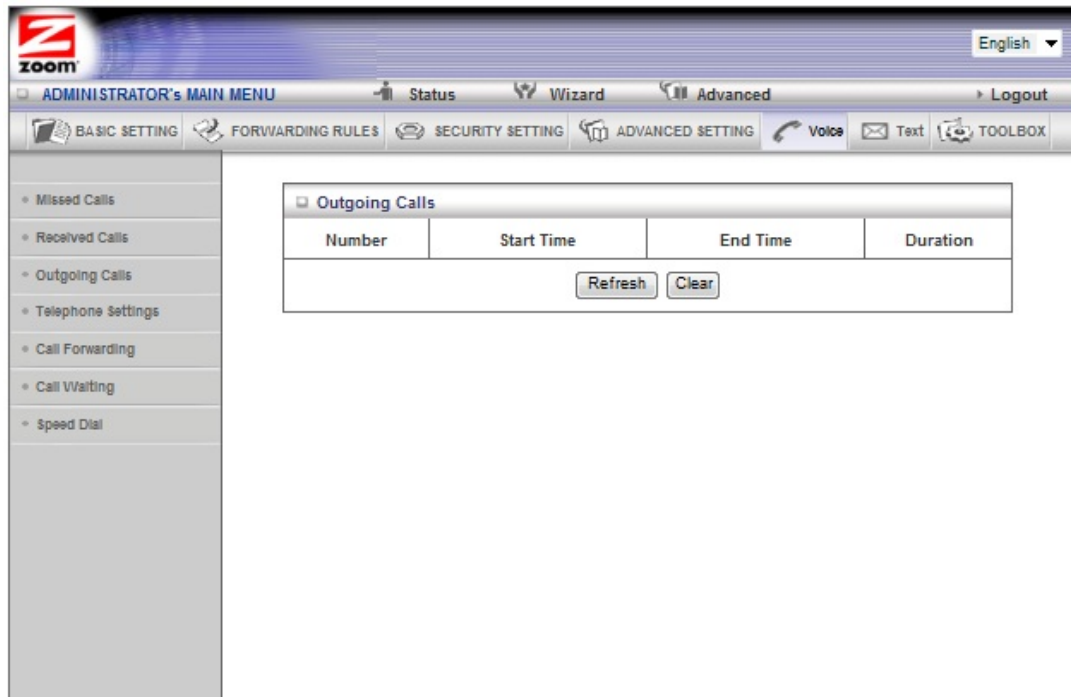
When you click on **Received Calls** on the left hand menu the following screen appears:



This page displays the calls that you received including the number that called, the starting and ending time of the call and the duration. Clicking on **Refresh** updates the screen and clicking on **Clear** erases the existing missed calls.

## Outgoing Calls

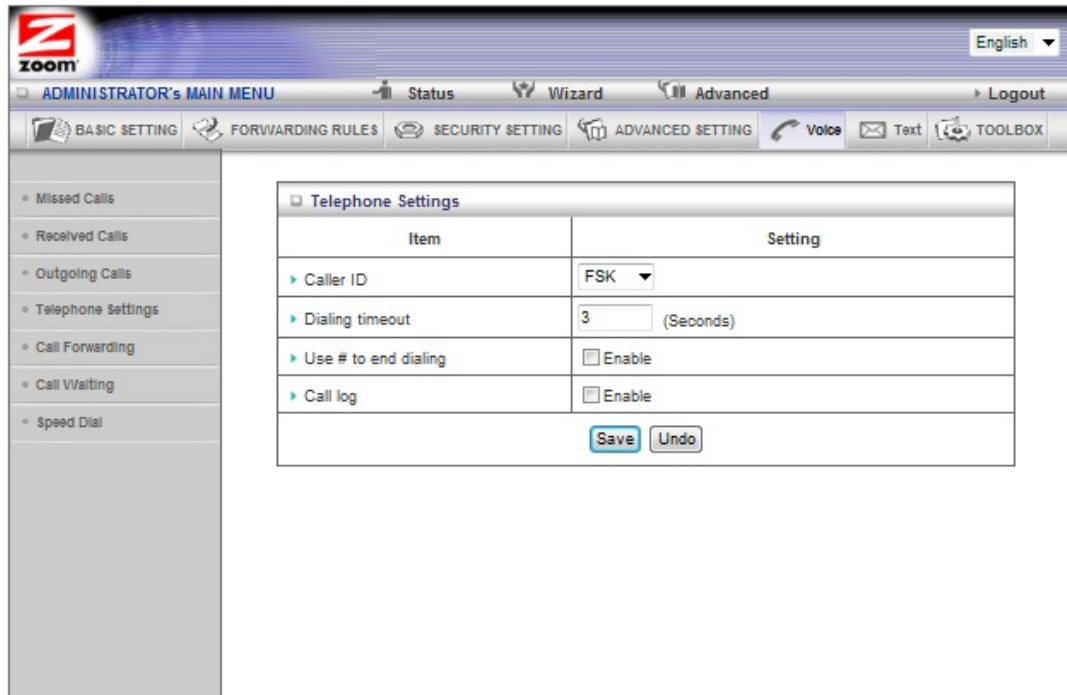
When you click on **Outgoing Calls** on the left hand menu the following screen appears:



This page displays the calls that you made including the number that you called, the starting and ending time of the call and the duration. Clicking on **Refresh** updates the screen and clicking on **Clear** erases the existing missed calls.

## Telephone Settings

When you click on **Telephone Settings** on the left hand menu the following screen appears:



#### Caller ID

Your Modem/Router supports both **FSK** and **DTMF** caller id. If you are not receiving caller ID on your phone try changing the setting.

#### Dialing Timeout

This is how long the Modem/Router will wait after you press a digit before it starts to dial.

#### Use # to end dialing

If you enter the # sign at the end of the phone number you are dialing, the Modem/Router will immediately dial the phone number and not wait for the **Dialing Timeout** to expire.

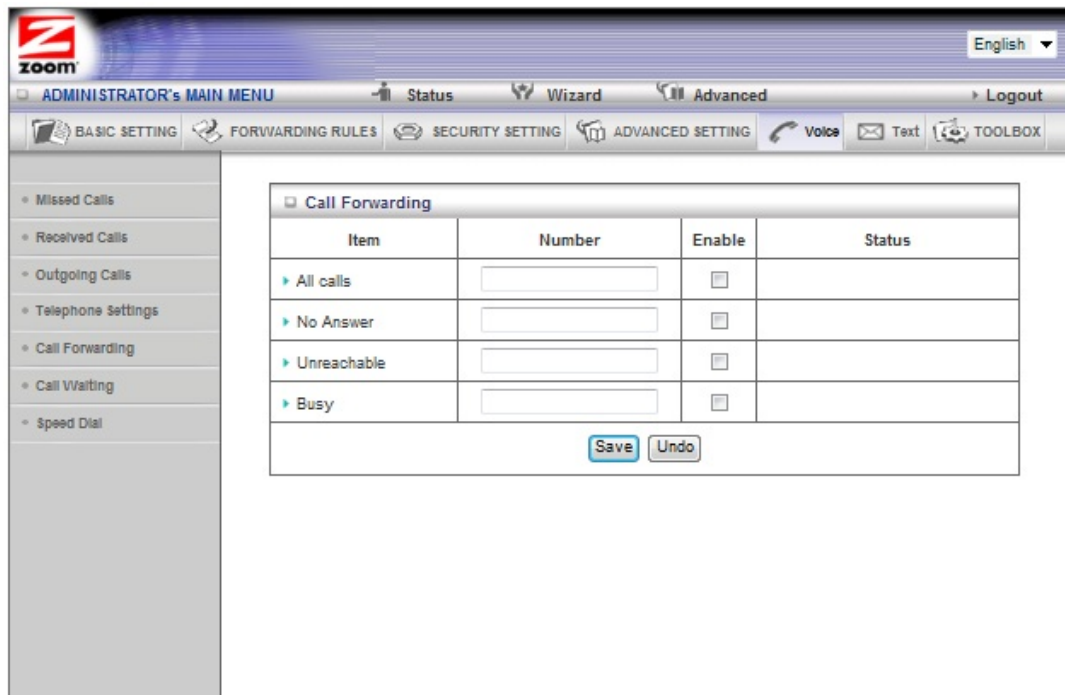
#### Call Log

When the Call log is enabled, all your Missed, Received, and Outgoing calls are logged by the Modem/Router.

#### Call Forwarding

When you click on **Call Forwarding** on the left hand menu the following screen appears:

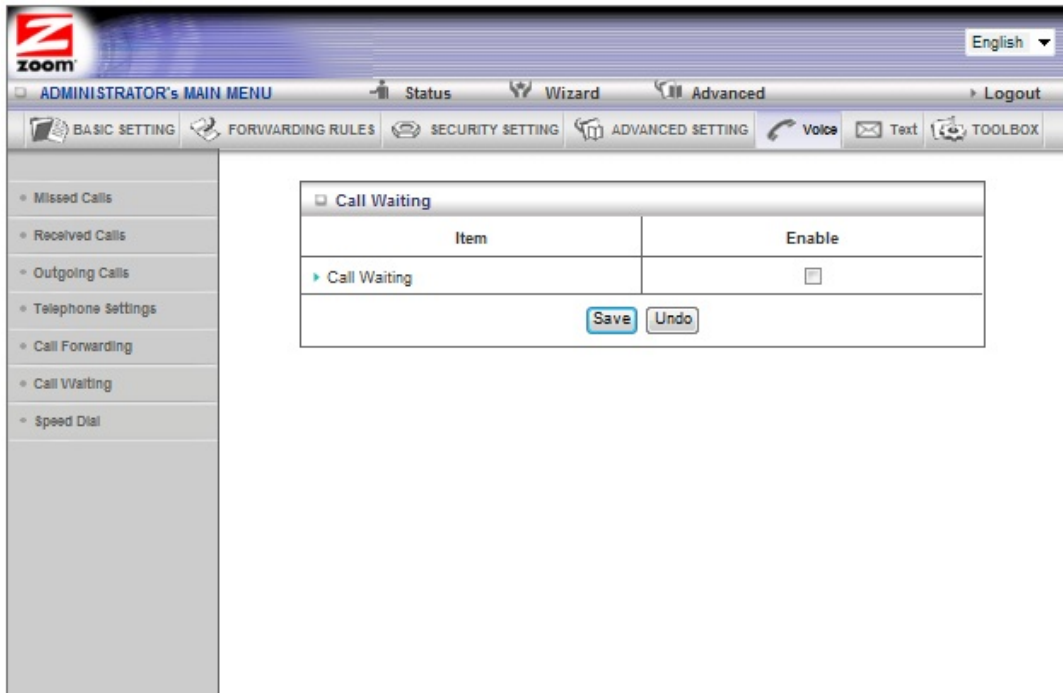




On this page you can forward your phone calls to a different number. You have the option of forwarding either all calls, or calls where there is No Answer, you are Unreachable or if your line is Busy. Enter the **Number** that you want to forward the call to for each case and click the **Enable box**. Click **Save** to store your settings.

## Call Waiting

When you click on **Call Waiting** on the left hand menu the following screen appears:



Click the **Enable** checkbox to enable Call Waiting. If you receive a voice call while you are on another call will receive a beep indicating that there is another call present. Press down on the flash hook of your phone to transfer over to the new call. When you are done with that call press the flash hook again to transfer back to your original call.

## Speed Dial

When you click on **Speed Dial** on the left hand menu the following screen appears:

zoom

English

ADMINISTRATOR's MAIN MENU   Status   Wizard   Advanced   Logout

BASIC SETTING   FORWARDING RULES   SECURITY SETTING   ADVANCED SETTING   Voice   Text   TOOLBOX

- Missed Calls
- Received Calls
- Outgoing Calls
- Telephone Settings
- Call Forwarding
- Call Waiting
- Speed Dial

Speed Dial

Number	Telephone Number	Enable
0	<input type="text"/>	<input type="checkbox"/>
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/>

Save   Undo

On this page you can program your Modem/Router. You have the option of forwarding either all calls, or calls where there is No Answer, you are Unreachable or if your line is Busy. Enter the **Number** that you want to forward the call to for each case and click the **Enable box**. Click **Save** to store your settings.

# 6

## Working with Text Messages

---

*Your 3G+ Modem/Router with Phone Port can be used to send and receive text messages. This chapter shows you how to use your Modem/Router to send a text message and how to manage your received text messages.*

### Using your Modem/Router to Send Text Messages

---

If you want to use the Modem/Router's built-in 3G+ modem to send text messages and are connected to the Modem/Router through your computer's Ethernet port you can go right ahead and log into the configuration manager. If you are using a wireless connection to access the Modem/Router you must first establish the wireless connection. If you are unsure how to set up a wireless connection see [Establishing your Wireless Network](#) on page 26.

- 1 Turn on your computer and Modem/Router, then launch the computer's Web browser.
- 2 In the Web browser address bar, type the Modem/Router's default IP address, **http://192.168.2.1** and then click Enter.

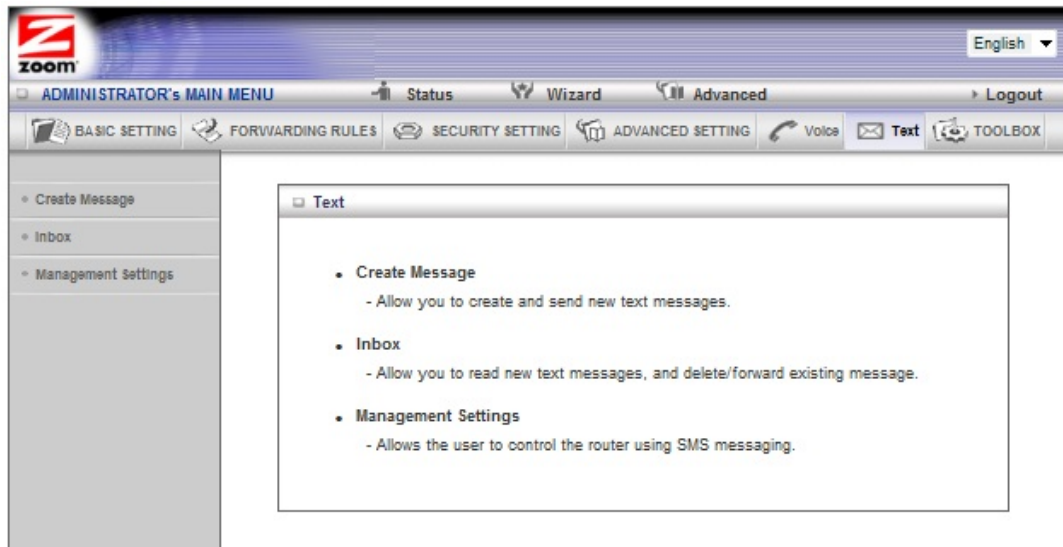
When the MAIN MENU opens for the first time, it displays a System Status page that summarizes the current settings and values for your system.

- 3 On the Toolbar, type **admin** (the default password) in the System Password field, then click Login.

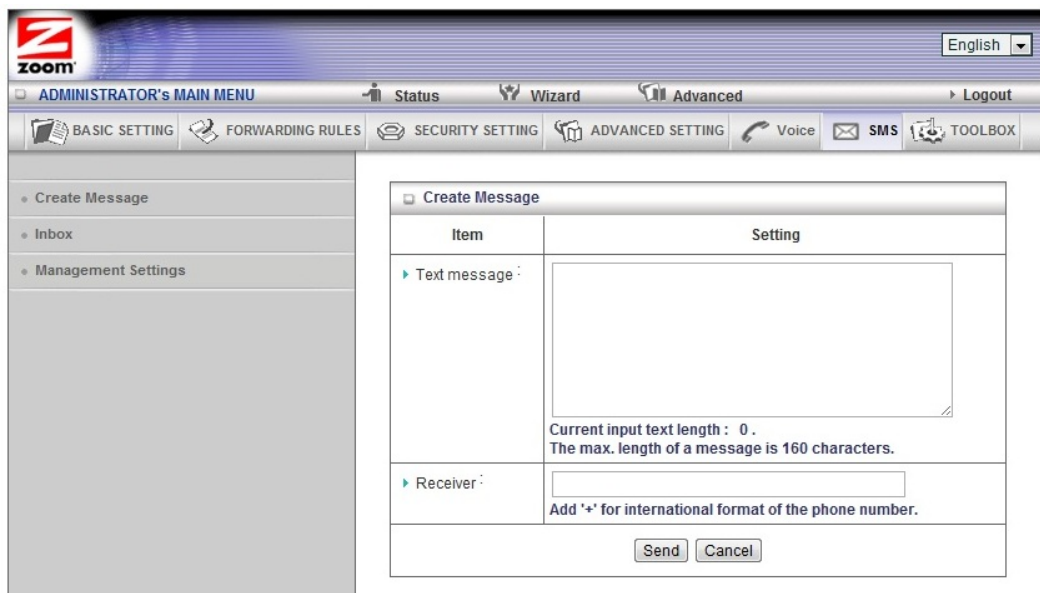


**Note:** If you have changed the System Password, you will use the new password to log in.

- 4 When you log in, the Configuration Manager opens its Main Menu. Select **Text** on the top menu.



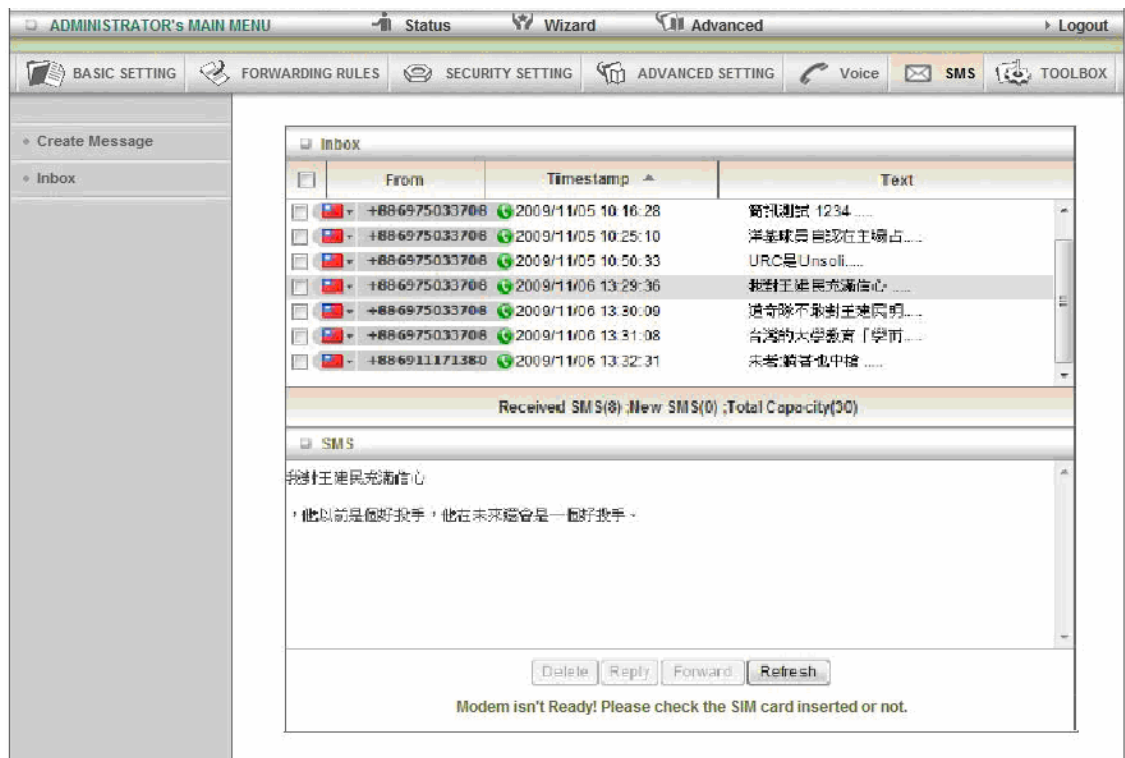
- 5 To send a message, select **Create Message** from the left hand menu. The following page appears:



- 6 Enter the message you want to send in the box next to **Text message**. The maximum length of the text message is 160 characters.
- 7 Enter the phone number of the person you want to send the text to in the **Phone number** box.
- 8 Click **Send** to send your text message. The Modem/Router will respond with a **Sent OK** message to let you know the message was sent.

## Working with your Inbox

The Modem/Router will store incoming text messages on your SIM card. From your Inbox you can read, delete, reply, and forward text messages. To access your Inbox, click on Inbox from the left hand menu. The following page appears: **new screen**



To read a text message, click on the message you want to view. The text message will now appear in the box at the bottom of the screen.

To reply to a text message, click on the checkbox next to the message then click on **Reply**. Type your message and click **Send** to send it. To return to the Inbox, click on **Inbox** on the left hand menu

To forward a text message, click on the checkbox next to the message then click on **Forward**. Type your message and enter the phone number of the person you want to forward it to in the **Phone number** box. Click **Send** to send it. To return to the Inbox, click on **Inbox** on the left hand menu.

To delete a text message, click on the checkbox next to the message then click on **Delete**. The message will be deleted from your Inbox.

## The Management Settings Page

When you click on **Management Settings** the following page appears:

The screenshot shows the Zoom Management Settings page. The interface includes a top navigation bar with the Zoom logo, a language dropdown set to English, and a main menu with options like Status, Wizard, and Advanced. Below this is a secondary menu with icons for BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, Voice, SMS, and TOOLBOX. The left sidebar contains a tree view with 'Create Message', 'Inbox', and 'Management Settings' (selected). The main content area is divided into four sections:

- Management Settings**: A table with two columns, 'Item' and 'Setting'.

Item	Setting
Remote Management via SMS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Delete All Received SMS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Delete SMS for Remote Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Security Key	<input type="text"/>
- Command Settings**: A table with two columns, 'Item' and 'Setting'.

Item	Setting
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Connect	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Disconnect	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Reconnect	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Reboot	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
- Notification Settings**: A table with two columns, 'Item' and 'Setting'.

Item	Setting
WAN Link Down	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WAN Link Up	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Secondary WAN Link is Up	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Secondary WAN Link is Down	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
- Access Control List**: A table with two columns, 'Item' and 'Setting'.

Item	Setting
Access Control	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Any Phone Number	<input type="checkbox"/> Management
Phone 1	<input type="checkbox"/> Management <input type="checkbox"/> Notification
Phone 2	<input type="checkbox"/> Management <input type="checkbox"/> Notification
Phone 3	<input type="checkbox"/> Management <input type="checkbox"/> Notification
Phone 4	<input type="checkbox"/> Management <input type="checkbox"/> Notification
Phone 5	<input type="checkbox"/> Management <input type="checkbox"/> Notification

At the bottom of the main content area, there are 'Save' and 'Undo' buttons.

Your Modem/Router can be controlled remotely by text messaging. You are able to

connect, disconnect, reboot, and receive status updates from the Modem/Router.

### **Remote Management via SMS**

Click **Enable** to enable remote control of your Modem/Router using Text messaging.

### **Delete All Received SMS**

Click **Enable** to delete all received text messages including both regular text messages and remote management text messages. If you do not want to store your text messages on your SIM card you should enable this feature.

### **Delete SMS for Remote Management**

Click **Enable** if you want to delete remote control text messages. Normal text messages will still be stored on the SIM card.

### **Security Key**

If you enable remote management you must enter a **Security Key**. This key gives a user access to the system. When you send a command through text messaging to the modem you will need to include this key.

**Need to finish**



# 7

## Using the Configuration Manager's Advanced Program

---

Most users will not need to manually set up their Modem/Router. In the unlikely event that you do, you can use the Configuration Manager's Advanced program to change the Modem/Router's default settings.

This chapter includes:

- Suggestions for settings that you might want to change
- A brief description of the online and context-sensitive help that is available
- Instructions for launching the Advanced program
- An overview of the available configuration menus and settings

### Changing Default Settings

---

Here are some reasons why you might want to use the Advanced program to change the Modem/Router's default settings.

- **Manually entering your APN settings.**
- You want to block access to certain URLs or set up Scheduling usage rules. See [The URL Blocking Page](#) on page 65 and [The Schedule Rule and Schedule Rule Setting Pages](#) on page 75 for details.
- You want to hide the SSID name so other network users cannot see your wireless network. See [The Wireless Setting Page](#) on page 54 for details.
- You want to change Modem/Router settings to establish a firewall to guard against unauthorized access to your network. See [The MAC Address Control Page](#) on page 67 for details.
- You want to set up a Virtual Server or DMZ so that your games or gaming consoles can access the Internet through your Modem/Router's firewall. See [Configuring Forwarding Rules](#) on page 59 for details.
- You want your Mobile Broadband connection to be terminated by the Modem/Router if you haven't used the Internet for a specified period of time. The default setting is **Auto Reconnect (always on)**. See [The Basic Setup Page \(Connection Control\)](#) on page 51 for details.

- You want to connect the Modem/Router to your ADSL or cable modem, using the built-in 3G+ modem as a backup Internet connection. See [The Basic Setup Page](#) on page 51 for details.
- You want to change the default wireless security on your Modem/Router. See [Wireless Security](#) on page xx for details.
- You want to enable security on the built-in 3G+ modem. See Pin Codes on page xx
- You want to back up Modem/Router settings that you made using the Configuration Manager. See [The Backup Setting Dialog](#) on page 79 for details.

## Online Help

---

The Advanced program provides both online and context-sensitive help that guides you in changing the settings on each menu. **Need to check**

- To access **online help**, click **[HELP]** on the menu's Toolbar. Each **[HELP]** page describes the fields on the active page and, when applicable, the required or recommended entries.
- The **context-sensitive help** automatically displays a question mark to the right of the cursor, then opens a message box in the left pane of the page. The message box contains text that describes the active field and its required or recommended entry.

## Launching the Configuration Manager's Advanced Program

---

If you are connected to the Modem/Router through your computer's Ethernet port, you can go right ahead and log into the configuration manager. If you are using a wireless connection to access the Modem/Router, you must first set up the wireless connection. If you are unsure how to set up a wireless connection see [Establishing your Wireless Network](#) on page 26. Turn on your computer and Modem/Router, then launch your Web browser.

- 9 In the Web browser address bar, type the Modem/Router's default IP address, **http://192.168.2.1** and then click Enter to launch the Configuration Manager.

When the Configuration Manager's MAIN MENU opens, it displays a Status page that summarizes the basic settings and current values for your setup.

- 10 On the Toolbar, type the login password -- **admin** is the default password -- in the System Password field, and then click Login.



- 11 Click Advanced on the Toolbar to launch the Advanced program.

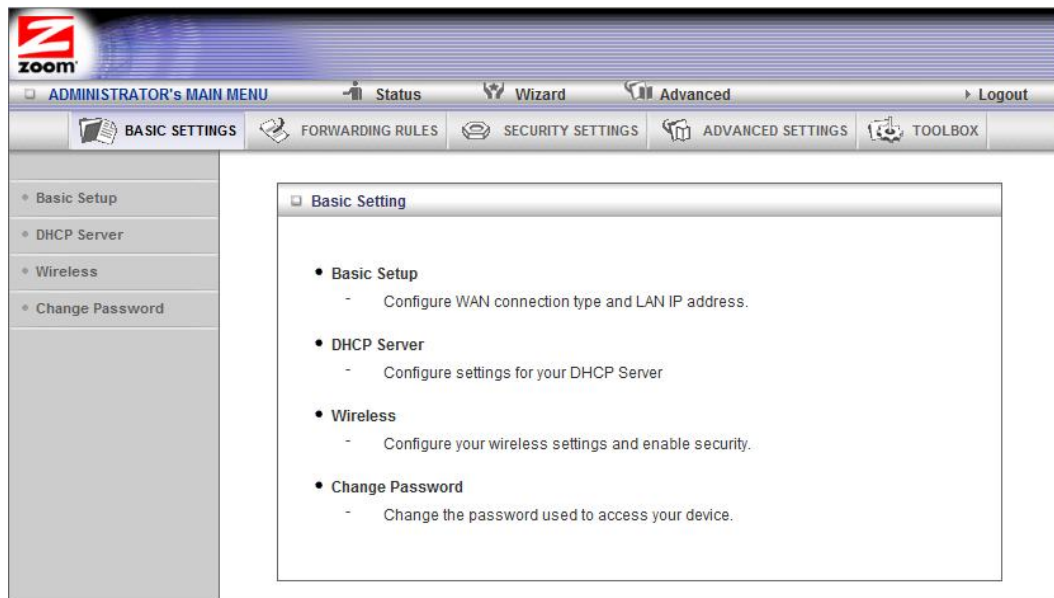


- 12 On the Basic Settings page, click one of the Toolbar buttons (Basic Settings, Forwarding Rules, Security Settings, Advanced Settings, or Toolbox).

The corresponding window opens. Each window contains a description of the configuration options at center and a configuration menu on the left pane.

## Configuring Basic Settings

The Basic Settings page lists the four configuration menus on the left pane and provides a description of the configuration menus at center.



## The Basic Setup Page

You can use the Basic Setup page to configure your LAN and WAN setup.

**Note:** The following image depicts the fields that the program displays when 3G+ is selected as the WAN Type. The fields will differ for each WAN Type. See the online help for a description of each WAN Type and its corresponding fields. If you want to use the built-in 3G+ modem as a backup to your cable or ADSL modem, go to [Using the 3G+ modem as a backup](#) on page 53.

BASIC SETTINGS		FORWARDING RULES	SECURITY SETTINGS	ADVANCED SETTINGS	TOOLBOX																																
<ul style="list-style-type: none"> <li>Basic Setup</li> <li>DHCP Server</li> <li>Wireless</li> <li>Change Password</li> </ul>	<div style="text-align: right;">[ HELP ]</div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>Ethernet port configuration</td> <td>LAN</td> </tr> <tr> <td>LAN IP Address</td> <td>192.168.1.1</td> </tr> <tr> <td>WAN Type</td> <td>3G/4G/LTE</td> </tr> <tr> <td>APN (Not required by all providers)</td> <td></td> </tr> <tr> <td>PIN Code</td> <td></td> </tr> <tr> <td>Dialed Number</td> <td></td> </tr> <tr> <td>Username</td> <td></td> </tr> <tr> <td>Password</td> <td></td> </tr> <tr> <td>Authentication</td> <td> <input checked="" type="radio"/> Auto           <input type="radio"/> PAP           <input type="radio"/> CHAP         </td> </tr> <tr> <td>Primary DNS</td> <td></td> </tr> <tr> <td>Secondary DNS</td> <td></td> </tr> <tr> <td>Connection Control</td> <td>Auto Reconnect (always-on)</td> </tr> <tr> <td>Maximum Idle Time</td> <td>0 seconds</td> </tr> <tr> <td rowspan="3">Keep Alive</td> <td> <input checked="" type="radio"/> Disable  <input type="radio"/> Use LCP Echo Request         </td> </tr> <tr> <td>           Icp-echo-interval: 10 seconds         </td> </tr> <tr> <td>           Icp-echo-failure: 3 times         </td> </tr> </tbody> </table> <div style="text-align: center;"> <input type="button" value="Save"/> <input type="button" value="Undo"/> </div>					Item	Setting	Ethernet port configuration	LAN	LAN IP Address	192.168.1.1	WAN Type	3G/4G/LTE	APN (Not required by all providers)		PIN Code		Dialed Number		Username		Password		Authentication	<input checked="" type="radio"/> Auto <input type="radio"/> PAP <input type="radio"/> CHAP	Primary DNS		Secondary DNS		Connection Control	Auto Reconnect (always-on)	Maximum Idle Time	0 seconds	Keep Alive	<input checked="" type="radio"/> Disable <input type="radio"/> Use LCP Echo Request	Icp-echo-interval: 10 seconds	Icp-echo-failure: 3 times
Item	Setting																																				
Ethernet port configuration	LAN																																				
LAN IP Address	192.168.1.1																																				
WAN Type	3G/4G/LTE																																				
APN (Not required by all providers)																																					
PIN Code																																					
Dialed Number																																					
Username																																					
Password																																					
Authentication	<input checked="" type="radio"/> Auto <input type="radio"/> PAP <input type="radio"/> CHAP																																				
Primary DNS																																					
Secondary DNS																																					
Connection Control	Auto Reconnect (always-on)																																				
Maximum Idle Time	0 seconds																																				
Keep Alive	<input checked="" type="radio"/> Disable <input type="radio"/> Use LCP Echo Request																																				
	Icp-echo-interval: 10 seconds																																				
	Icp-echo-failure: 3 times																																				

new screen

### LAN IP Address

The local IP address of the Modem/Router. **192.168.2.1**, by default. All wireless or wired devices on your network must use the LAN IP address of your Modem/Router as their default gateway.

### WAN Type

Set to 3G+, by default. You can choose another option from the dropdown menu, based on the WAN connection type that your service provider supports.

### APN, PIN Code, Dialed Number, Username and Password

Identifiers assigned by some service providers, if needed. This information should be supplied with your SIM card. Contact your service provider if this information is missing.

#### Authentication

Set to Auto, by default. Optionally, click **Password Authentication Protocol (PAP)**, or **Challenge Handshake Authentication Protocol (CHAP)**, if supported by your service provider.

#### Primary DNS and Secondary DNS

Identifiers for the **Domain Name Servers**. These identifiers are provided by your service provider.

#### Connection Control

Specifies the method for connecting or disconnecting the WAN session based on network activity. Auto Reconnect (always on) is the default. Other options are Connection-on-Demand or Manual.

#### Maximum Idle Time

Specifies the duration (in seconds) of inactivity before the device disconnects. The default is **0**, which disables this feature.

#### Keep Alive

Disabled by default. Select LCP Echo Request to keep the connection alive.

### Using your 3G+ modem as a Backup

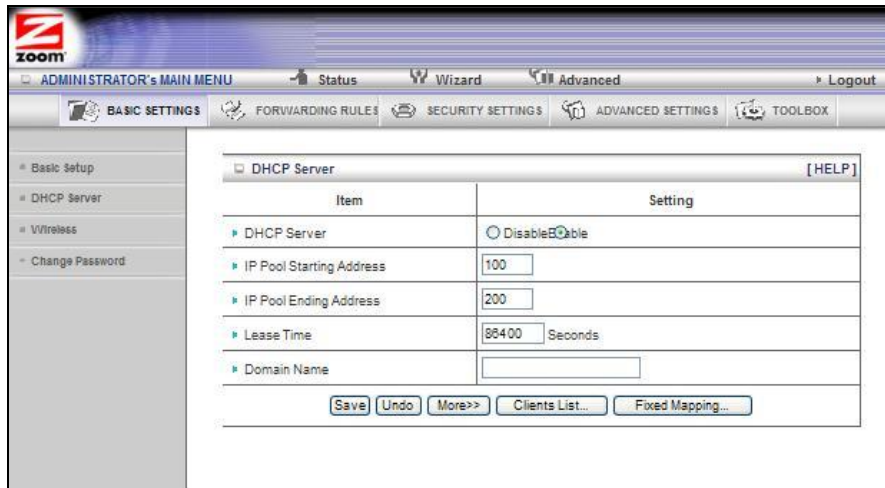
You can use the built-in 3G+ modem to provide Internet access if your DSL or Cable service stops working.

To set up the 3G Failover, follow the instructions below:

- 1 You should have already set up your cable or DSL modem using the built in Setup Wizard. If not, see Launching the Configuration Manager's Setup Wizard on page 10.
- 2 Select Basic Settings from the Configuration Manager's Advanced Page. See Launching the Configuration Manager's Advanced Program on page 50 if you don't know how to access the Advanced setting page.
- 3 On the Basic Setup page click the **Wan Connection Checkbox**.
- 4 Enter an IP address in the **Internet host** textbox. This is the IP address that the Modem/Router will ping to verify that your DSL or Cable connection is active. (We recommend using your Domain Name Server for this purpose.) To get the IP address of your Domain Name server:
  - a Go to the **Status** page from the Zoom Configuration Manager. Locate the Domain Name Server.
  - b In the **WAN Status** column, copy one of the displayed IP addresses (either the primary or secondary DNS IP address).
  - c From the Configuration Manager, click on **Advanced** and then **Basic Setup** and paste the IP address into the **Internet host** textbox.
- 5 Click **Save**.

## The DHCP Server Page

You can use the DHCP Server page to configure your DHCP server. If you want to change the default values, please click [HELP], which opens a page that describes each item and the recommended values.



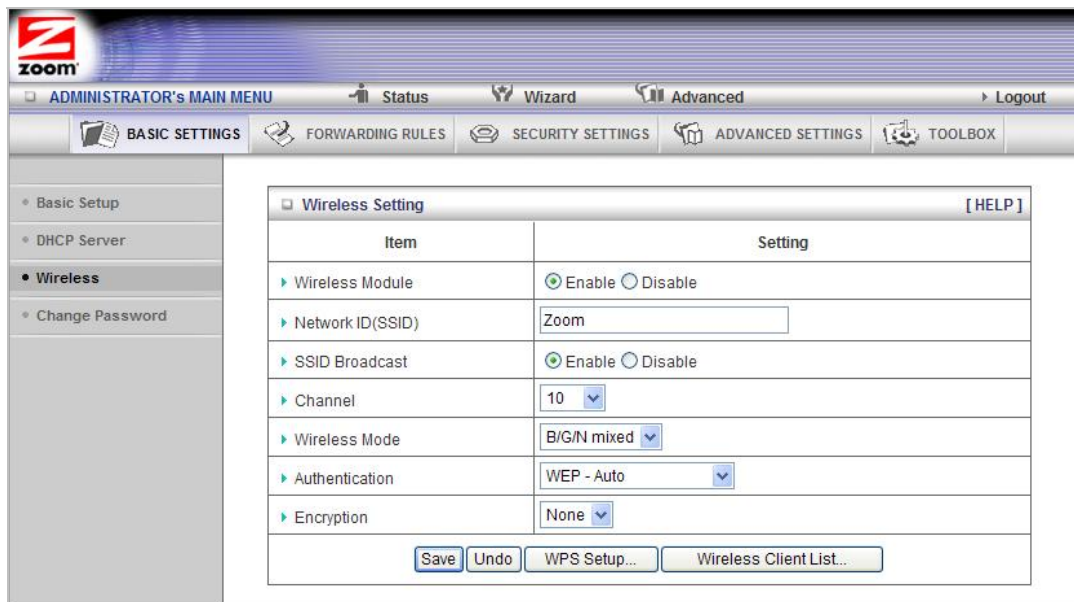
The screenshot shows the Zoom DHCP Server configuration page. The interface includes a top navigation bar with 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary navigation bar with 'BASIC SETTINGS', 'FORWARDING RULES', 'SECURITY SETTINGS', 'ADVANCED SETTINGS', and 'TOOLBOX'. A left sidebar contains a tree view with 'Basic Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'DHCP Server' and contains a table with the following settings:

Item	Setting
DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IP Pool Starting Address	100
IP Pool Ending Address	200
Lease Time	86400 Seconds
Domain Name	

At the bottom of the table are buttons for 'Save', 'Undo', 'More>>', 'Clients List...', and 'Fixed Mapping...'. A '[HELP]' link is located in the top right corner of the table area.

## The Wireless Setting Page

You can use the Wireless Setting page to configure your wireless LAN setup. If you want to change the default values, please click [HELP], which opens a page that describes each item and the recommended values.



The screenshot shows the Zoom Wireless Setting configuration page. The interface is similar to the DHCP page, with a top navigation bar and a secondary navigation bar. The left sidebar has 'Basic Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Wireless Setting' and contains a table with the following settings:

Item	Setting
Wireless Module	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID(SSID)	Zoom
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	10
Wireless Mode	B/G/N mixed
Authentication	WEP - Auto
Encryption	None

At the bottom of the table are buttons for 'Save', 'Undo', 'WPS Setup...', and 'Wireless Client List...'. A '[HELP]' link is located in the top right corner of the table area.

### Wireless Module

Accept the default, Enable. Click the Disable checkbox only if you do not want wireless clients to access your network.

### Transmit Power

Allows you to lower the amount of power transmitted by the WiFi connection to save battery. Lowering the transmit power will also reduce how far the device can be from the Travel Modem/Router and still connect. When operating in Battery Power saving mode the transmit power is reduced to 25%. See Battery Power saving mode on page 80.

### Network ID (SSID)

Refers to the **S**ervice **S**et **I**dentifier for your device. By default, the SSID for the Modem/Router with Wireless-N is Zoom. You can change the SSID to a name of your choice. The SSID can be up to 32 alphanumeric characters. If you change the name, make sure that all devices on your network use the new SSID as the access point.

### SSID Broadcast

To hide your network's SSID name, which disables automatic broadcasting of the SSID and makes the wireless access point (your Modem/Router) invisible to wireless clients on the network, click the Disable radio button.

### Channel

Refers to the wireless network channel assigned to your LAN. By default, the Travel Modem/Router uses channel 10.

### Wireless Mode

Accept the default, B/G/N mixed if the client devices on your network use various wireless standards. Otherwise, select the wireless standard used by all wireless devices on your network. Having a single standard will speed up the wireless throughput.

### Authentication

Select an Authentication method for all devices on your wireless network. If you are using gaming devices that require WEP, then you must configure all devices with this method.

For WEP Authentication:

You can accept the default, WEP-Auto or select one of the available options. Select WEP-Open to use Open System authentication. Select WEP-Shared to use Shared Key authentication.

For WPA-PSK/WPA2-PSK Authentication:

You can select WPA-PSK/WPA2 PSK if your devices support both authentication methods. Optionally, select WPA-PSK or WPA2-PSK if all devices on your network support only one of these authentication methods.

Encryption

Select an Encryption method that corresponds to the Authentication method that you chose.

If you chose a WPA-PSK/WPA2-PSK Authentication method:

Accept TKIP/AES encryption (the WPA-PSK/WPA2-PSK default), which supports dynamic encryption keys using TKIP or AES algorithms, or choose one of the other options.

Select AES if you chose WPA2-PSK for the authentication method.

Select TKIP if you chose WPA-PSK for the authentication method.

In the Preshare Key field, enter a 26-character key.

If you chose a WEP Authentication method:

Select WEP.

Key Format

We recommend using Hex because not all Ascii keys are compatible. Hex keys use the numbers 0-9 and the letters A-F.

Encryption WEP Key 1, 2, 3, 4

*If you selected Hex format* and you chose a 128-bit key length, 26 hexadecimal values are required. Write the 26-hexadecimal key in the space below for future reference, and then enter it in the Key 1 box.

-----  
-----

*If you selected Hex format* and you chose a 64-bit key length, 13 hexadecimal values are required. Write the 13-hexadecimal key in the space below for future reference, and then enter it in the Key 1 box.

-----

*If you selected ASCII format*, and you chose a 128-bit key length, 13 ASCII characters are required. Write the 13-ASCII-character key in the space below for future reference, and then enter it in the Key 1 box.

-----



If you selected ASCII format, and you chose a 64-bit key length, 5 ASCII characters are required. Write the 5-ASCII-character key in the space below for future reference, and then enter it in the Key 1 box.

— — — — —

Click WPS Setup to launch the **WiFi Protected Setup (WPS)** Setup program. For instructions, please refer to [WPS Configuration](#) on page 32.

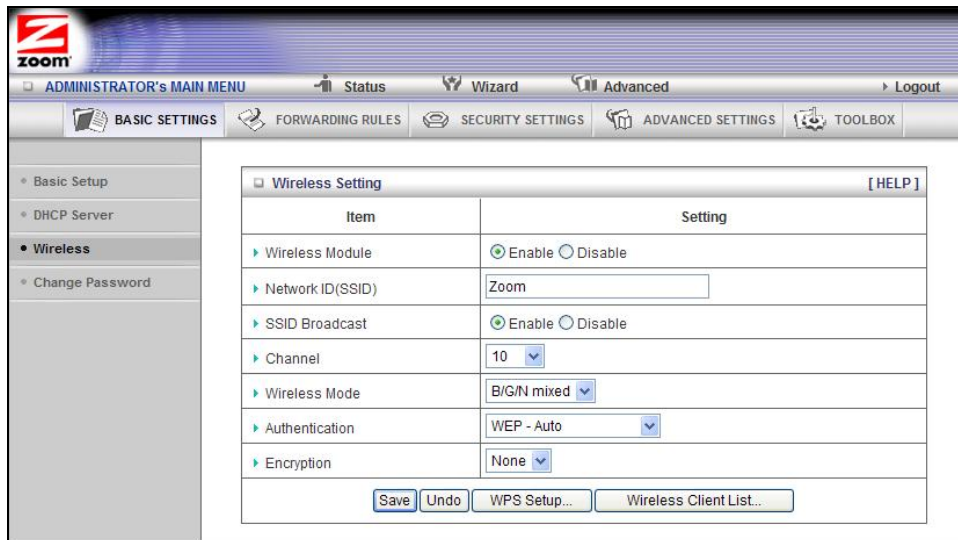
We recommend you set WPA2/WPA security unless you know that you will be connecting devices to your network that support only WEP. If you know you have some devices that only support WEP, go to **WEP Configuration** on page 40. Otherwise continue to **WPA2/WPA Configuration**.

### WPA2/WPA Configuration

**Wi-Fi Protected Access (WPA)** is an encryption method that offers a stronger security standard than WEP.

**Important!** If you choose to configure your Modem/Router using either WPA2 or WPA encryption, then you must configure all devices on your wireless network with the same WPA encryption method and shared key.

You can configure WPA2 or WPA encryption using the [Wireless Setting Page](#) of the Configuration Manager's Advanced program.



The screenshot shows the Zoom Administrator's Main Menu. The navigation menu on the left includes: Basic Setup, DHCP Server, **Wireless**, and Change Password. The main content area displays the **Wireless Setting** page with a table of settings:

Item	Setting
Wireless Module	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID(SSID)	Zoom
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	10
Wireless Mode	B/G/N mixed
Authentication	WEP - Auto
Encryption	None

At the bottom of the table are buttons for **Save**, **Undo**, **WPS Setup...**, and **Wireless Client List...**

- 13 In the **Authentication** drop down bar select **WPA – PSK/WPA2 – PSK**. If you know all your devices support WPA2-PSK you can select it instead.
- 14 In the **Preshare Key** field enter a value for the key. The maximum value is 42 characters. The minimum value is 8 characters.

- 15 Write down this passphrase and put it where you can find it – on the bottom of the case, for instance.
- 16 Click **Save**. If you are connected wirelessly to the travel Modem/Router you will lose the connection as soon as you click **Save**. When you re-establish your wireless connection you will be prompted for the preshared key that you just entered. You must enter this key to be able to connect to the Travel Modem/Router.
- 17 Now you need to set up each of your wireless devices with the Preshared Key that you entered. See [Establishing your Wireless Network](#) on page 26 for instructions on connecting devices to the Modem/Router.

## WEP Configuration

**Wired Equivalent Privacy (WEP)** is a basic encryption method that does not offer the security strength of WPA or WPA2. Use this method only if some of your network's wireless devices, such as a gaming console, do not support WPA2/WPA.

**Important!** If you choose to configure your Modem/Router using WEP encryption, then you must configure all devices on your wireless network with the same WEP encryption method and key.

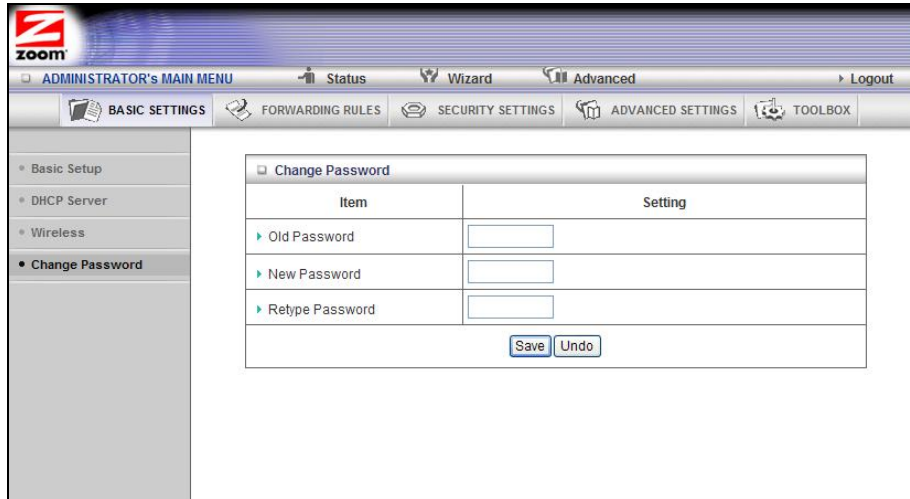
You can configure WEP encryption using the [Wireless Setting Page](#) of the Configuration Manager's Advanced program.

- 18 In the **Encryption** drop down bar select **WEP**.
- 19 In the WEP KEY 1 box you have the choice of entering either a 64-bit key or a 128-bit key. If you want to use a 64-bit key enter 13 hex characters. (Hex characters are the numbers 0-9, and the characters A-F.) If you want to use a 128-bit key enter 26 Hex characters. A 64-bit key provides slightly faster performance while a 128-bit key provides slightly better security. We recommend using a 64-bit key.
- 20 Write down this key and put it where you can find it – on the bottom of the Modem/Router case, for instance.
- 21 Click **Save**. If you are connected wirelessly to the Modem/Router you will lose the connection as soon as you click **Save**. When you re-establish your wireless connection you will be prompted for the key that you just entered. You must enter this key to be able to connect to the Modem/Router.
- 22 Now you need to set up each of your wireless devices with the Key that you entered. See [Establishing your Wireless Network](#) on page 26 for instructions on connecting devices to the Modem/Router.

## The Change Password Page

You can use this page to change your login password. To view or change configuration settings, you must enter a password. Your Modem/Router has a default

password (**admin**) that was set by the factory and that you used to access the Configuration Manager initially. To safeguard your configuration, particularly if you make changes, we recommend that you change the login password.



The screenshot shows the Zoom Configuration Manager interface. At the top, there is a navigation bar with the Zoom logo, 'ADMINISTRATOR'S MAIN MENU', and buttons for 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTINGS', 'FORWARDING RULES', 'SECURITY SETTINGS', 'ADVANCED SETTINGS', and 'TOOLBOX'. On the left side, a sidebar lists configuration categories: 'Basic Setup', 'DHCP Server', 'Wireless', and 'Change Password' (which is selected). The main content area displays the 'Change Password' form, which includes a table with two columns: 'Item' and 'Setting'. The table has three rows: 'Old Password', 'New Password', and 'Retype Password', each with a corresponding text input field. Below the table are 'Save' and 'Undo' buttons.

Item	Setting
▶ Old Password	<input type="text"/>
▶ New Password	<input type="text"/>
▶ Retype Password	<input type="text"/>

**Note:** If you forget the new password, you won't have access to the Configuration Manager and will need to [restore the device to its factory settings](#) thus losing any changes you made to your Modem/Router's configuration. To avoid this problem, we recommend that you write the new password and save it in a convenient location.

## Configuring Forwarding Rules

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

A virtual server will allow access to your computer or gaming station on certain ports. A port is a channel that is used by applications (such as games) for communication. For example, the directions for the game you want to play over the Internet might tell you to open up port 6000.

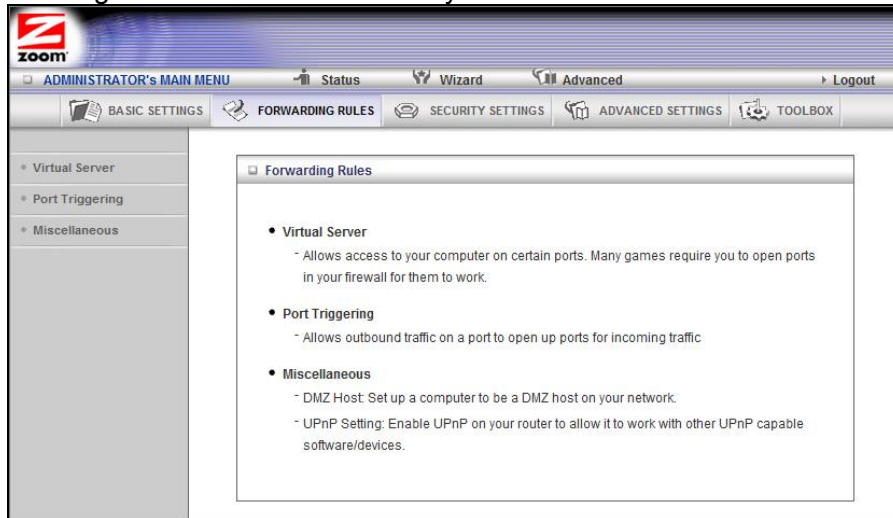
Port triggering works by sensing when data is sent out on the predetermined outgoing port and then automatically opening up the corresponding incoming port(s). It will automatically forward the traffic on the incoming port to the computer that accessed the outgoing port. If your game uses one port to send outgoing data and a different port (or ports) for incoming data, you may want to use port triggering. The advantage of port triggering is that it is more secure than setting up a virtual server since the incoming port is only open when you are using it, and since it tracks which computer sent the outgoing data. Port triggering can also be easier to set up because you do not need to know the IP address of your gaming station. The disadvantage of port triggering is that only 1 host can be accessing the port at one time, so if you have two computers or game stations playing the same game on your network you will need to use a virtual server or DMZ.

A DMZ differs from a virtual server in that it allows access on all ports of the computer. Because of this, DMZ's are less secure and should be used with caution on your

computer. However DMZ's work well with your gaming stations since security is not as much of an issue for gaming stations as it is for computers.

Some games support UPnP. If your game supports UPnP then you do not need to set any forwarding rule since UPnP will automatically set up the Modem/Router to work with the game.

You can use the Forwarding Rules page to configure the options mentioned above, for allowing access to devices behind your Modem/Router.



## The Virtual Server Page

You can use the Virtual Server page to configure a virtual server.

Because your Modem/Router's firewall filters out unrecognized packets to protect your network, all computers behind this product are invisible to the outside world. If you want, you can make some of them accessible by enabling Virtual Server mapping.

A virtual server will allow access to your computer on certain ports. A port is like a channel that is used by applications (such as games) to communicate on. For example, the directions for the game you want to play over the Internet might tell you to open port 6000.

### Service Ports

This is the port number you want to allow access to your computer on. To enter multiple ports use the dash format; for example, 2004-2009.

### Server IP

This is the IP Address of the computer or gaming device that you want to allow access to. If you do not know the IP address you can look it up by selecting Basic Settings > DHCP Server, then clicking on Client List. To make this virtual server permanent, then you should set up a fixed mapping to your computer or gaming device on the DHCP Server page. Doing this ensures that your computer will keep the same IP address

## Protocol

Select UDP, TCP, or Both depending on what type of protocol your game or application uses.

## Enable

Click to enable the Virtual Server

## Use Rule#

You can enable your virtual server for certain periods of time by assigning it a Rule #. You must first set up the appropriate Scheduling Rule. See [The Schedule Rule and Schedule Rule Setting Pages](#) on page 75 for more information.

For example, if you have an FTP server (port 21) at 192.168.1.5, a Web server (port 80) at 192.168.1.6, and a game at 192.168.1.7, then you need, at minimum, to specify the following mapping.

ID	Service Port	Server IP	Enable
1	21	192.168.1.5	Yes
2	80	192.168.1.6	Yes
3	5000	192.168.1.7	Yes

## The Port Triggering Page

Port triggering opens an incoming port when your computer is using a specified *outgoing port* for specific traffic. This provides a way for you to automate setting up a Virtual Server with some applications. You can use the Port Triggering page to configure which packets are allowed access.

The screenshot shows the 'Port Triggering' configuration page in the Zoom Firewall Administrator interface. The page has a navigation bar with 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below the navigation bar are tabs for 'BASIC SETTINGS', 'FORWARDING RULES', 'SECURITY SETTINGS', 'ADVANCED SETTINGS', and 'TOOLBOX'. The 'FORWARDING RULES' tab is active, and the 'Port Triggering' sub-tab is selected. A sidebar on the left contains a tree view with 'Virtual Server', 'Port Triggering', and 'Miscellaneous'. A text box in the sidebar explains: 'When the trigger packet is detected, the inbound packets on the specified port numbers are allowed to pass through the firewall.' The main content area shows a table with 8 rows for configuration. The columns are 'ID', 'Trigger', 'Incoming Ports', and 'Enable'. The 'Enable' column contains checkboxes. At the top of the table is a 'Popular applications' dropdown menu with a 'Copy to' button. At the bottom of the table are 'Save' and 'Undo' buttons.

ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

### Trigger

The outbound port number used by the application.

### Incoming Ports

When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

### Enable

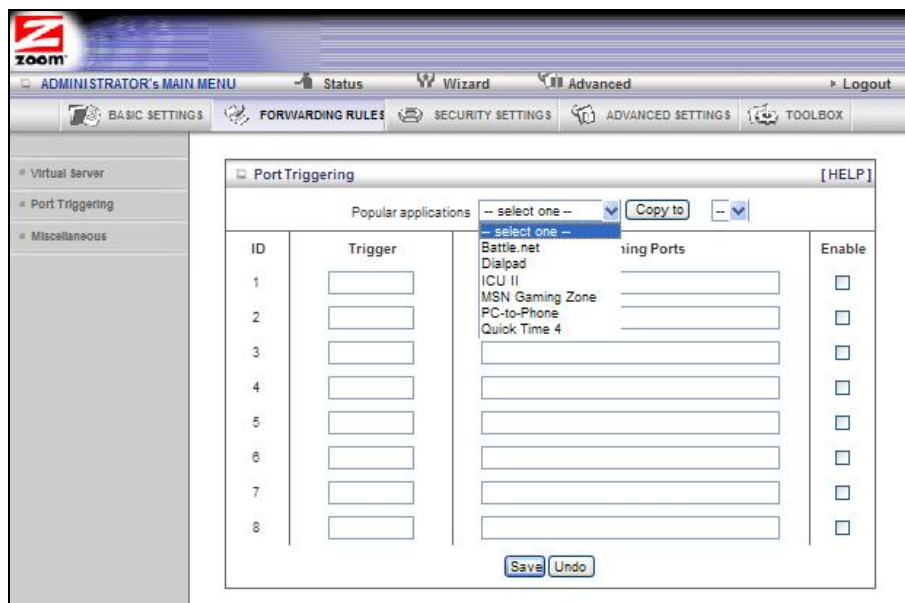
Enables access for the specified application.

### Popular applications

Provides a menu of applications from which to choose.

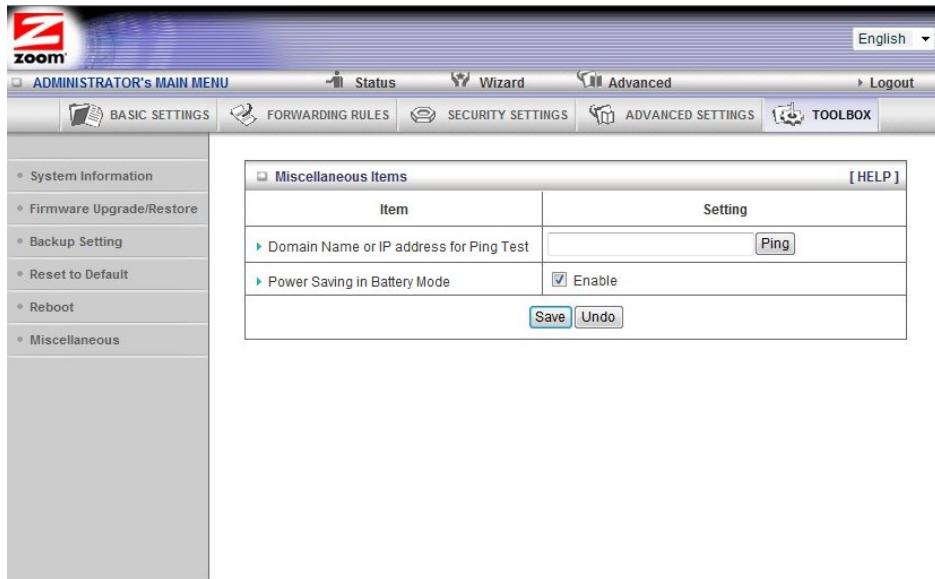
Select an application and click Copy to to add the application to your list.

Click Save to store your selection or Undo to remove the entry.



## The Miscellaneous Page

The Miscellaneous Page lets you set up and enable a DMZ Host on your network, and enable UPnP settings for software and devices. In this way, specific ports can open for incoming traffic that must pass through your firewall. You can also enable IGMP on this page in the unlikely event that your service provider is using it.



### Set IP Address of DMZ Host

A **DMZ** (Demilitarized Zone) **Host** is a host without the protection of the firewall. It allows a computer or gaming system to be exposed to unrestricted two-way communication for Internet games, video conferencing, Internet telephony and other special applications. Use caution when using a DMZ because your firewall no longer protects the computer that is set up as a DMZ.

### UPnP setting

This feature is enabled by default. Games and applications that are UPnP compatible will automatically open ports for you on your Modem/Router.

### IGMP Setting

Enable IGMP (Internet Group Management Protocol ) if your service provider tells you to. IGMP is typically used for IPTV applications.

## Configuring Security Settings

The Security Setting page lists six configuration menus on the left pane and provides a description of the configuration menus at center.




[BASIC SETTINGS](#)
[FORWARDING RULES](#)
[SECURITY SETTINGS](#)
[ADVANCED SETTINGS](#)
[TOOLBOX](#)

- Status
- Packet Filters
- Domain Filters
- URL Blocking
- MAC Control
- Miscellaneous

**Security Setting**

- Packet Filters**
  - Allows you to control access to a network by analyzing the incoming and outgoing packets and either letting them pass or halting them based on the IP address of the source and destination.
- Domain Filters**
  - Let you prevent users behind this device from accessing specific URLs.
- URL Blocking**
  - URL Blocking will block LAN computers to connect to pre-defined websites.
- MAC Address Control**
  - MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a MAC address
- Miscellaneous**
  - Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.
  - Administrator Timeout: Amount of inactive time before the device will automatically log you off the session. Set this to zero to disable it.
  - Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.


[ADMINISTRATOR'S MAIN MENU](#)
[Status](#)
[Wizard](#)
[Advanced](#)
[Logout](#)

[BASIC SETTINGS](#)
[FORWARDING RULES](#)
[SECURITY SETTINGS](#)
[ADVANCED SETTINGS](#)
[TOOLBOX](#)

- Status
- Packet Filters
- Domain Filters
- URL Blocking
- MAC Control
- Miscellaneous

**Outbound Filter** [\[Modify\]](#)

Item	Status
Outbound Filter	Disable
Local Client	Only Deny Remote Host Service Working Time

**Inbound Filter** [\[Modify\]](#)

Item	Status
Inbound Filter	Disable
Remote Host	Deny Remote Host to access Service Working Time

**Domain Filter** [\[Modify\]](#)

Item	Status
Domain Filter	Disable
Domain	Access
All other Domains	Yes

[Refresh](#)

## Status Page

The Status page shows you the status of the inbound and outbound Packet Filters and the Domain Filters. Inbound, Outbound, and Domain filters are disabled, by default.



## Packet Filtering Page

Packet Filtering allows you to control what packets are allowed to pass through the Modem/Router. Outbound Packet filters control outbound packets and Inbound Filtering controls packets coming from the Internet. Inbound Filters applies only to packets going to a Virtual Server or DMZ. Most users will not need to setup Packet Filtering.

When you click on **Packet Filters** from the left-side menu, it takes you to the **Outbound Packet Filtering page**. If you need to set up an Inbound Filter, click on **Inbound Filter** button at the bottom of the page.

## Filtering Policies

You can select one of the two filtering policies:

Allow all to pass except those that match the specified rules

Deny all to pass except those that match the specified rules

## Filtering Rules

You can specify eight rules for each direction: inbound or outbound. For each rule, you can define the following:

Source IP address

Destination IP address

Destination Port

Use Rule#

For the Source or Destination IP address, you can define a single IP address (4.3.2.1). An empty field implies any IP address.

For Destination Port, you can define a single port (80) or a range of ports (1000-1999). No prefix indicates both TCP and UDP are defined. Leaving this empty implies that all port addresses apply.

Each Rule can be enabled or disabled individually.

You can use packet filters with scheduling rules for more access control flexibility.

## The Domain Filters Page

You can use the Domain Filters page to enable or deny user access to specified URLs. Domain filtering and URL Blocking perform similar functions. The major difference between Domain Filtering and URL Blocking is that Domain Filtering requires the user to input a suffix whereas URL Blocking requires the user to input a keyword only. In other words, Domain Filtering can block a specific web site, whereas URL Blocking can block hundreds of web sites by specifying a keyword.

Domain Filter

Use to prevent users behind this device from accessing specific URLs.

Log attempted URL Access

Check if you want to log the action when someone accesses the specific

URLs.

Privilege IP Address Range

Domain filtering rules do not apply to IP addresses in this range.

Domain Suffix

The suffix of the restricted URL; for example, **xxx** .com.

Action

The action to be taken when a user accesses the restricted domain suffix URL. Check Drop to block access. Check log to record the attempted access.

Enable

Click the checkbox to enable a rule.

## The URL Blocking Page

You can use the URL Blocking page to block LAN computers from connecting to pre-defined Web sites or to limit their access to specific websites. The major difference between Domain Filtering and URL Blocking is that Domain Filtering requires the user to input a suffix whereas URL Blocking requires the user to input a keyword only. In other words, Domain Filtering can block a specific web site, whereas URL Blocking can block hundreds of web sites by specifying a keyword.

URL Blocking [HELP]		
Item	Setting	
URL Blocking	<input checked="" type="checkbox"/> Enable	
Block Setting	<input checked="" type="radio"/> Blacklist <input type="radio"/> Whitelist	
ID	URL	Enable
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="checkbox"/>

Save Undo

URL Blocking Enable

Check if you want to enable URL Blocking.

Block Setting

Select Blacklist to block access to any words or URLs that you specify.  
Select Whitelist to allow access only to the URLs that you specify.

## URL

If any part of the Website's URL matches the pre-defined word, the connection will be blocked if Blacklist is set, or allowed if Whitelist is set. For example, if you set up blacklisting, you can use the pre-defined word, sex, to block all website URLs that contain the pre-defined word, sex.

## Enable

Click the checkbox to enable each rule.

## The MAC Address Control Page

You can use the MAC Address Control page to provide an added layer of security to your Modem/Router. MAC Address control is used to define connection and association rights for clients whose IP and MAC addresses are specified. Click on the **HELP** button page for a detailed explanation including examples for setting up MAC address control.

ID	MAC Address	IP Address	C	A
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

### MAC Address Control

Check Enable to enable MAC Address Control. All of the settings on this page will take effect only if Enable is checked.

### Connection control

Check Connection control to specify which wired and wireless clients can connect to this device. If a client is denied a connection to this device, then that client is also denied Internet access. Choose allow or deny to indicate

which clients can connect to this device.

## Association control

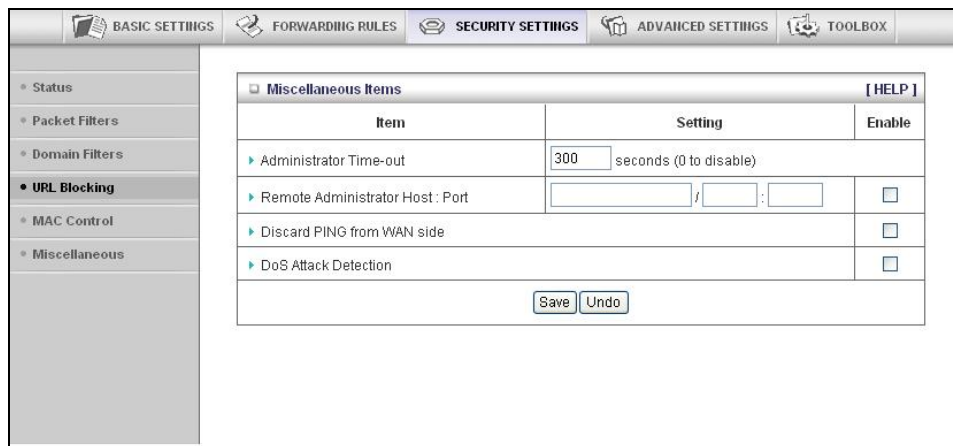
Check Association control to specify which wireless clients can associate to the wireless LAN. If a client is not allowed to associate to the wireless LAN, then the client can't send or receive any data via this device. Choose allow or deny to indicate which clients can associate to the wireless LAN. If selected, the specified wireless client will obtain any radio connection to the access point.

## DHCP clients

Displays a list of computers that are currently connected to the Modem/Router. Select a client from the menu then copy to the selected ID. The client IP and MAC addresses are written in the fields below the menus.

## The Miscellaneous Page

You can use the Miscellaneous Items page to enable additional security features.



The screenshot shows a web interface with a navigation bar at the top containing tabs for BASIC SETTINGS, FORWARDING RULES, SECURITY SETTINGS, ADVANCED SETTINGS, and TOOLBOX. The SECURITY SETTINGS tab is active. On the left side, there is a sidebar menu with the following items: Status, Packet Filters, Domain Filters, URL Blocking (highlighted with a black dot), MAC Control, and Miscellaneous. The main content area displays the 'Miscellaneous Items' configuration page, which includes a table with the following data:

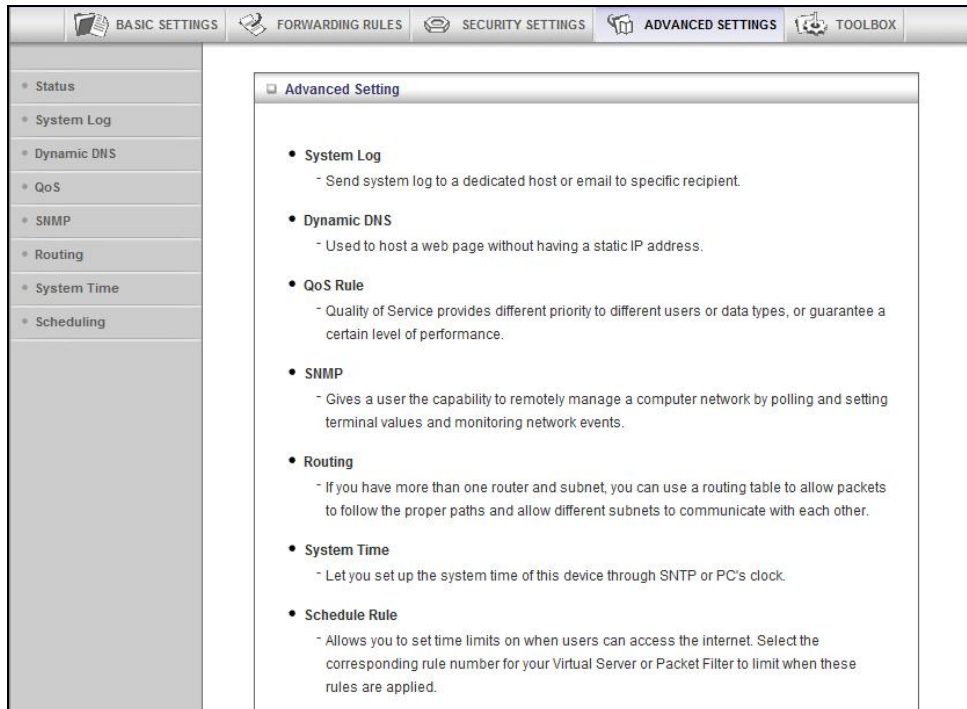
Item	Setting	Enable
▶ Administrator Time-out	300 seconds (0 to disable)	
▶ Remote Administrator Host: Port	<input type="text"/> / <input type="text"/> : <input type="text"/>	<input type="checkbox"/>
▶ Discard PING from WAN side		<input type="checkbox"/>
▶ DoS Attack Detection		<input type="checkbox"/>

At the bottom of the configuration area, there are 'Save' and 'Undo' buttons. A '[ HELP ]' link is located in the top right corner of the configuration area.

Please refer to the online help for details about each of the menu items.

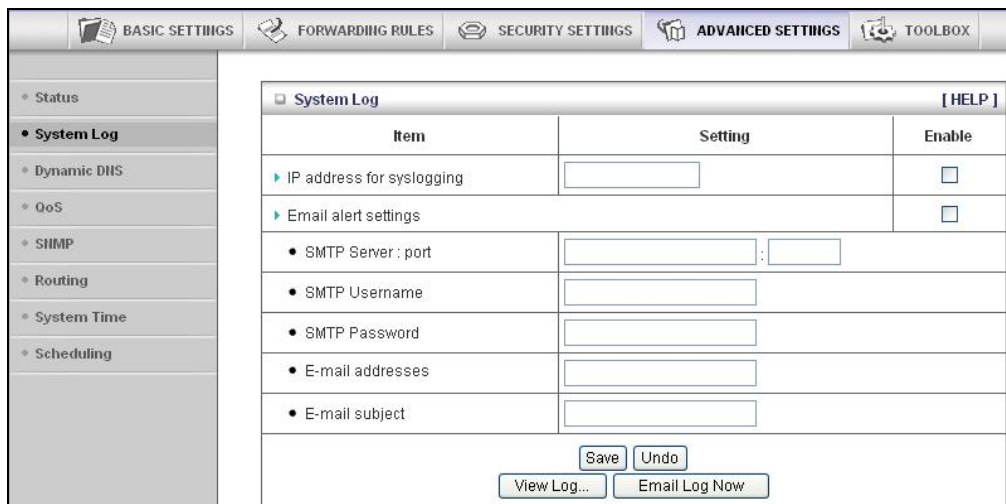
## Configuring Advanced Settings

The Advanced Settings page lists eight menus on the left pane and provides a description of the configuration menus at center.



## The System Log Page

You can use the System Log page to define how and where system logs will be exported via syslog (UDP) or SMTP(TCP).



### IP Address for Syslogging

Host IP address of the destination where the Sys log will be sent.  
Click the Enable checkbox to set the IP Address as the destination.

### E-mail alert settings

Check Enable if you want to send syslog via email.

### SMTP Server IP and Port

Input the SMTP server IP and port; for example, **mail.your\_url.com** or **192.168.2.100:26**. If you do not specify a port number, the port value will be set to 25.

### SMTP Username and Password

Input the SMTP Username and Password.

### E-mail addresses

The email address of each syslog recipient.

### E-mail Subject

The subject of the email alert. This setting is optional.

## The Dynamic DNS Page

You can use the Dynamic DNS page to define the **Dynamic Domain Name Service** (DDNS) that will host your server. For example, the DDNS could host your server when you want to host a website on your network but you do not have a static IP. Your DDNS provider keeps track of changes to your IP address and automatically routes users trying to access your web site to the correct location

**Note:** Before you enable DDNS, you must register an account with one of the DDNS servers listed in the Provider field.

The screenshot shows a web interface with a navigation menu on the left and a main configuration area. The navigation menu includes: Status, System Log, **Dynamic DNS** (selected), QoS, SHMP, Routing, System Time, and Scheduling. The main area is titled 'Dynamic DNS' and contains a table with the following items and settings:

Item	Setting
DDNS	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Provider	DynDNS.org(Dynamic) [v]
Host Name	<input type="text"/>
Username / E-mail	<input type="text"/>
Password / Key	<input type="text"/>

At the bottom of the configuration area are 'Save' and 'Undo' buttons.

Your DDNS provider will provide the HostName, Username/E-mail, and Password/Key that you will enter into the fields on the Dynamic DNS page.

## The QoS Page

You can use the **Quality of Service** (QoS) page to provide different priorities to different users or data flows, or to guarantee a certain level of performance.

QoS Rule [ HELP ]					
Item		Setting			
▶ QoS Control		<input type="checkbox"/> Enable			
▶ Available Upstream bandwidth		<input type="text"/> kbps (Kilobits per second)			
ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
1	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▾	<input type="checkbox"/>	(0) Always ▾
2	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▾	<input type="checkbox"/>	(0) Always ▾
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▾	<input type="checkbox"/>	(0) Always ▾
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▾	<input type="checkbox"/>	(0) Always ▾
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▾	<input type="checkbox"/>	(0) Always ▾
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▾	<input type="checkbox"/>	(0) Always ▾
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▾	<input type="checkbox"/>	(0) Always ▾
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▾	<input type="checkbox"/>	(0) Always ▾

### QoS Control

Click the Enable checkbox to enable QoS.

### Available Upstream bandwidth

Set the upstream speed. The best way to find your throughput is to use one of the free speed tests widely available on the Web. Some examples of sites with good speed tests are [www.speedtest.net](http://www.speedtest.net) and [www.speakeasy.net/speedtest](http://www.speakeasy.net/speedtest). When you know your actual upstream throughput, enter it in this field. The value should be in kilobits per second (Kbps).

### Local: IP

Define the local IP address of packets.

### Local: Ports

Define the local port of packets.

### Remote: IP

Define the remote IP address of packets.

### Remote: Ports

Define the remote port of packets.

### QoS Priority

Select a value from the dropdown menu to define the priority level for the local and remote settings. Packets will be serviced based upon the priority level set. For critical applications, select High or Normal. For non-critical applications, select Low. High is the default value.

### Enable

Click the Enable checkbox to apply the settings.



## User Rule#

Select a rule from the dropdown menu to indicate when the policy applies. (0) Always is the default value.

## The SNMP Page

You can use the **Simple Network Management Protocol (SNMP)** page to set up the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events. Most users do not need to set up SNMP.

Item	Setting
▶ Enable SNMP	<input type="checkbox"/> Local <input type="checkbox"/> Remote
▶ Get Community	<input type="text"/>
▶ Set Community	<input type="text"/>
▶ IP 1	<input type="text"/>
▶ IP 2	<input type="text"/>
▶ IP 3	<input type="text"/>
▶ IP 4	<input type="text"/>
▶ SNMP Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c
▶ WAN Access IP Address	<input type="text"/>

Save Undo

### Enable SNMP

Click the Local, Remote, or both checkboxes to enable the SNMP function. Check Local if you want the Modem/Router to respond to requests from the LAN. Check Remote if you want the Modem/Router to respond to requests from the WAN.

### Get Community

Set Get Community to the GetRequest to which your device will respond.

### Set Community

Set Set Community to the SetRequest that your device will accept.

### IP 1, IP 2, IP 3, IP 4

Enter the IP address of your SNMP Management PCs. You must specify where the Modem/Router should send SNMP Trap messages.

### SNMP Version

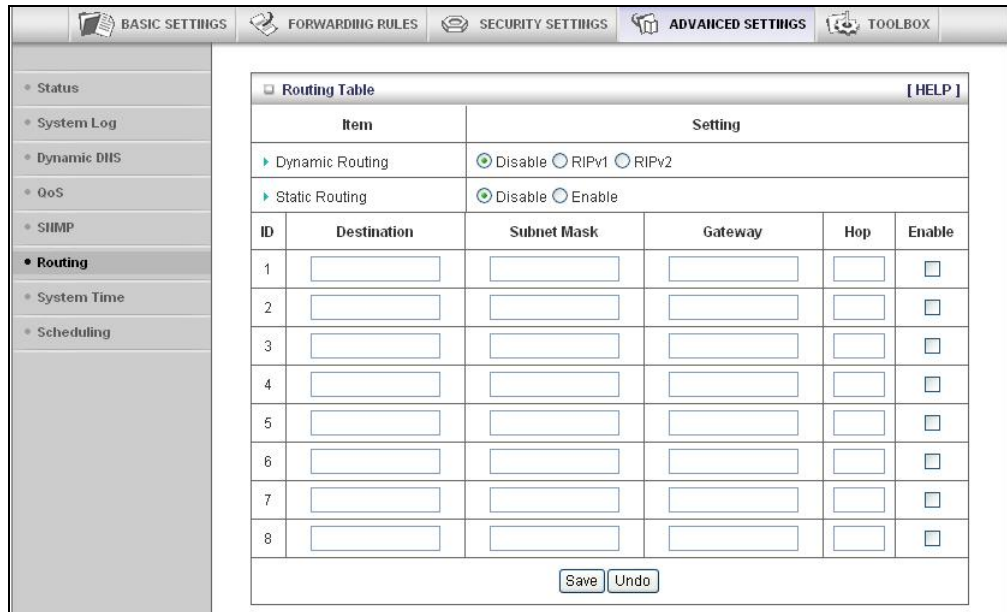
Select the SNMP Version that your SNMP Management software supports.

### WAN Access IP Address

Enter the IP address for WAN access. The default value of **0.0.0.0** indicates that every IP address can get some information about this device, using the SNMP protocol.

## The Routing Table Page

You can use the Routing Table page to enable/disable both Dynamic and Static Routing. If routing is enabled, you can specify which physical interface address to use for outgoing IP data grams. If you have more than one Modem/Router and subnet, you will need to define a routing table that lets packets find the proper routing path and allows different subnets to communicate with each other. Most users do not need to set up Dynamic or Static Routing.



The screenshot shows a web interface for configuring a routing table. At the top, there are navigation tabs: BASIC SETTINGS, FORWARDING RULES, SECURITY SETTINGS, ADVANCED SETTINGS (selected), and TOOLBOX. On the left, a sidebar menu lists various settings: Status, System Log, Dynamic DNS, QoS, SHMP, Routing (selected), System Time, and Scheduling. The main content area is titled 'Routing Table' and includes a '[HELP]' link. It contains two sections: 'Dynamic Routing' with radio buttons for 'Disable' (selected), 'RIPv1', and 'RIPv2'; and 'Static Routing' with radio buttons for 'Disable' (selected) and 'Enable'. Below these is a table with 8 rows for static routing rules. Each row has columns for ID, Destination, Subnet Mask, Gateway, Hop, and Enable. The 'Enable' column contains checkboxes. At the bottom of the table are 'Save' and 'Undo' buttons.

Routing Table		Setting			
Item					
Dynamic Routing	<input checked="" type="radio"/> Disable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2				
Static Routing	<input checked="" type="radio"/> Disable <input type="radio"/> Enable				
ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Save Undo

### Dynamic Routing

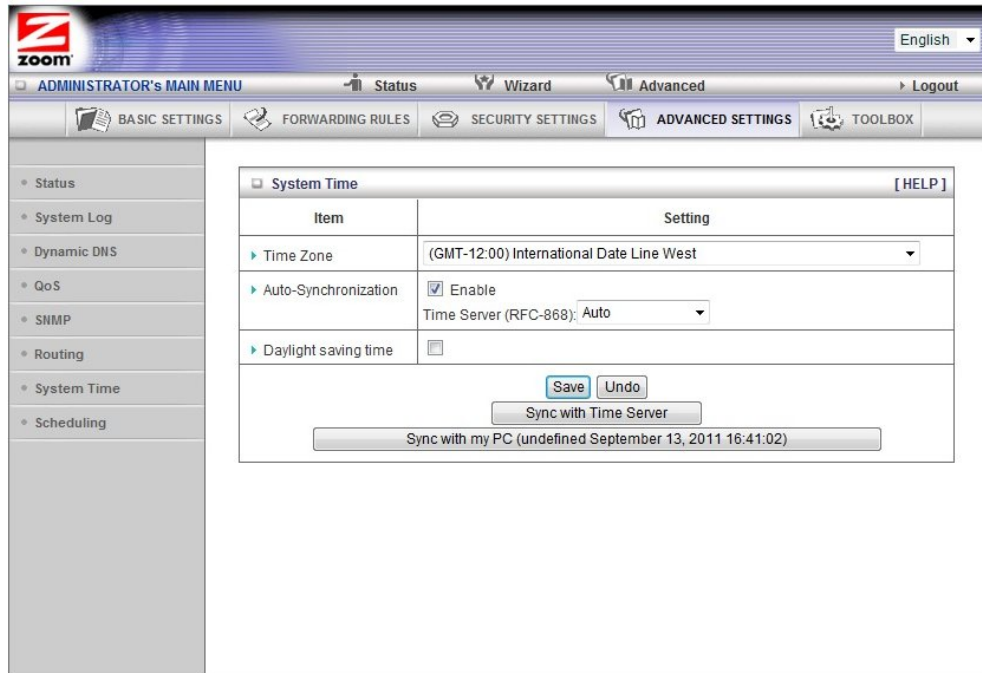
The **Routing Information Protocol (RIP)** will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network. Otherwise, please select RIPv1 if you need this protocol.

### Static Routing

For static routing, you can specify up to eight routing rules. You can enter the Destination IP address, Subnet Mask, Gateway, Hop for each routing rule. Click the Enable checkbox to activate the routing table entry.

## The System Time Page

You can use the System Time page to set and synchronize your Modem/Router with the local time zone, the Time Server and your PC.



### Time Zone

Select the local time zone from the dropdown menu.

### Auto-Synchronization

Click the Enable checkbox to enable this function.

Select an item from the Time Server dropdown menu to specify the server with which to synchronize. The default value is Auto.

Click Sync with Time Server to set Date and Time by NTP Protocol.

Click Sync with my PC to set Date and Time using your PC's Date and Time

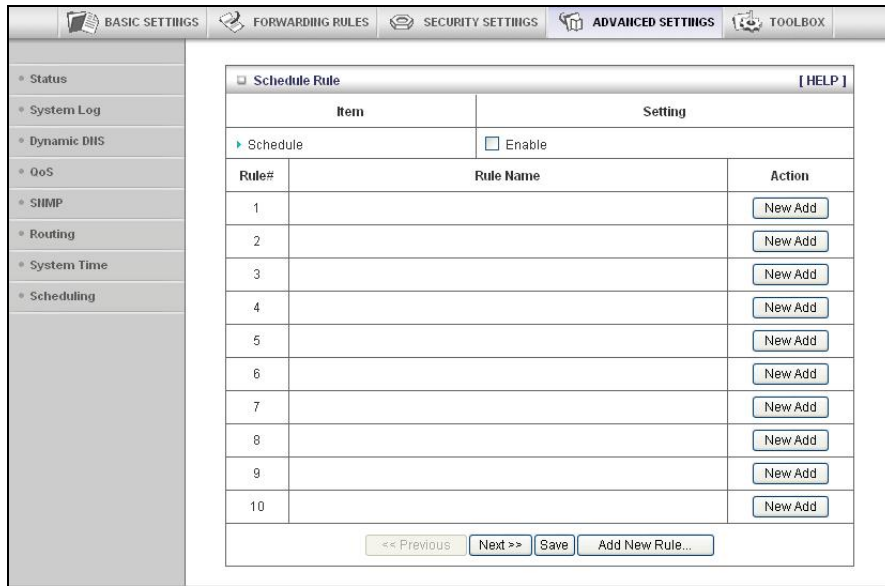
### Daylight Saving time

Select enable if you live in an area that uses daylight savings time. You need to enter the start and end dates for daylight savings time.

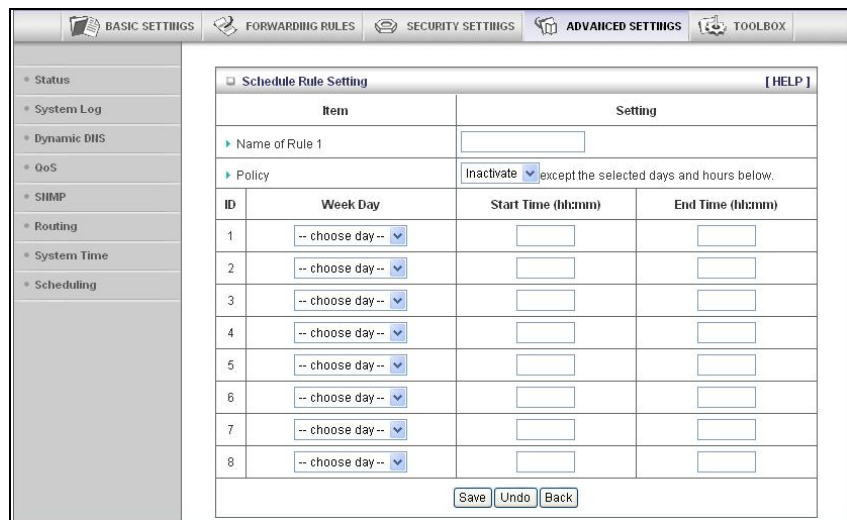
## The Schedule Rule and Schedule Rule Setting Pages

You can use the Schedule Rule and Schedule Rule Setting pages to define when services will be turned on and off based on rules that you define.

- 1 On the Schedule Rule page, click the Enable checkbox to enable the scheduling rules, which are defined on the Schedule Rule Setting page.



a. Click Add New Rule to open the Schedule Rule Setting page.



b. On the Schedule Rule Setting page, specify a Rule name, a Policy that defines whether the rule is Active or Inactive, Week Day and the Start Time and End Time for each rule that you are creating.

Navigation: BASIC SETTINGS | FORWARDING RULES | SECURITY SETTINGS | **ADVANCED SETTINGS** | TOOLBOX

Left sidebar: Status, System Log, Dynamic DNS, QoS, SHMP, Routing, System Time, **Scheduling**

**Schedule Rule Setting** [HELP]

Item: Name of Rule 1:

Policy:  except the selected days and hours below.

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	Monday	09:00	10:00
2	-- choose day --		
3	-- choose day --		
4	-- choose day --		
5	-- choose day --		
6	-- choose day --		
7	-- choose day --		
8	-- choose day --		

Save | Undo | Back

- c Click **Save** for each rule that you create.
- d Click **Back** to return to the **Schedule Rule** page.

- e When the **Schedule Rule** page opens, the rule(s) that you created and saved appear in the **Rule Name** column.

Navigation: BASIC SETTINGS | FORWARDING RULES | SECURITY SETTINGS | **ADVANCED SETTINGS** | TOOLBOX

Left sidebar: Status, System Log, **Dynamic DNS**, QoS, SHMP, Routing, System Time, Scheduling

**Schedule Rule** [HELP]

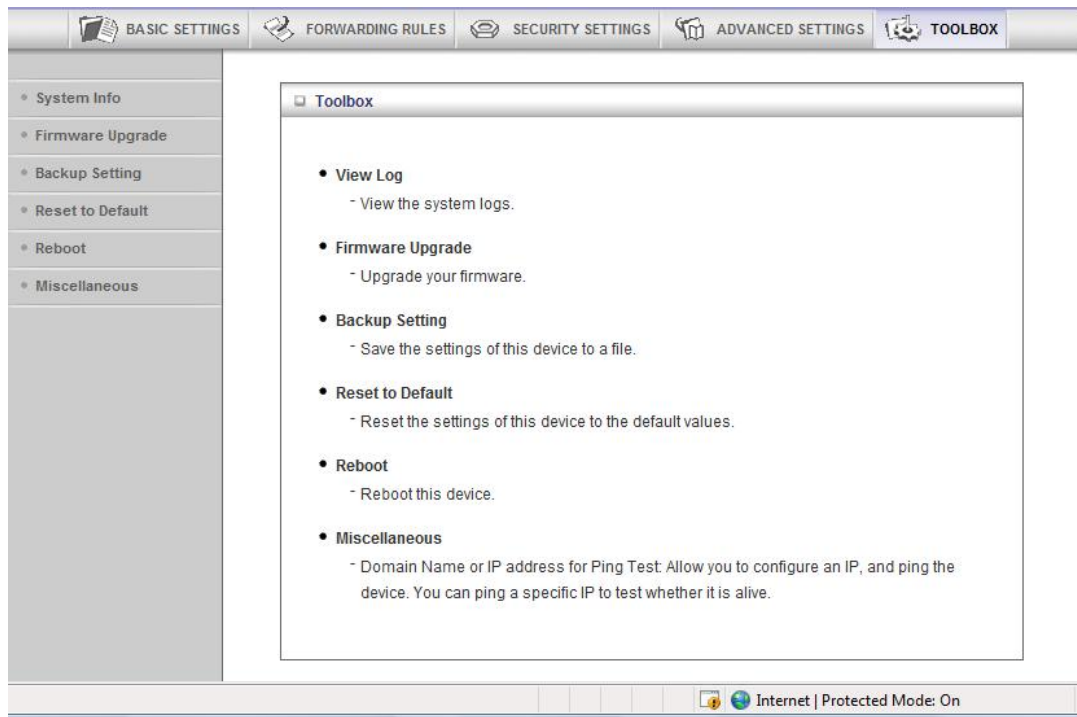
Item: Schedule:  Enable

Rule#	Rule Name	Action
1	test1	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
2	test2	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
3	test3	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
4		<input type="button" value="New Add"/>
5		<input type="button" value="New Add"/>
6		<input type="button" value="New Add"/>
7		<input type="button" value="New Add"/>
8		<input type="button" value="New Add"/>
9		<input type="button" value="New Add"/>
10		<input type="button" value="New Add"/>

- f Click **Edit** to make changes to a scheduled rule.
- g Click **Delete** to remove a scheduled rule.

## Configuring Toolbox Settings

The Toolbox Settings page lists six configuration menus on the left pane and provides a description of the configuration menus at center.

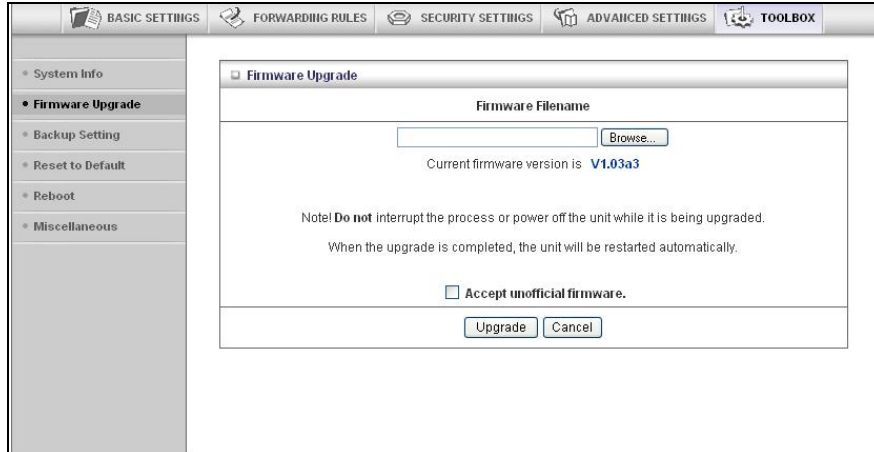


## The System Information Page

You can use the System Information page to view information about your Modem/Router, and to view download, and delete system logs.

## The Firmware Upgrade Page

You can use the Firmware Upgrade page to get the most recent version of the Modem/Router firmware, if available.



- 1 Click Browse to open the location where you saved the Firmware Update file that you downloaded from the Zoom web site or received via email.
- 2 Click Upgrade.

### The Backup Setting Dialog

You can back up your Modem/Router settings by clicking the Backup Setting item from the left pane of the Toolbox menu. The following dialog opens.



- 1 Click Save to write and save your Modem/Router settings as a binary file.

### The Reset to Default Dialog

You can reset the Modem/Router to its factory settings by clicking the Reset to Default item from the left pane of the Toolbox menu. The following dialog opens.



- 1 Click OK to reset the Modem/Router.  
We recommend that you back up and save your configuration first if you've made changes and want a record of that configuration

## The Reboot Dialog

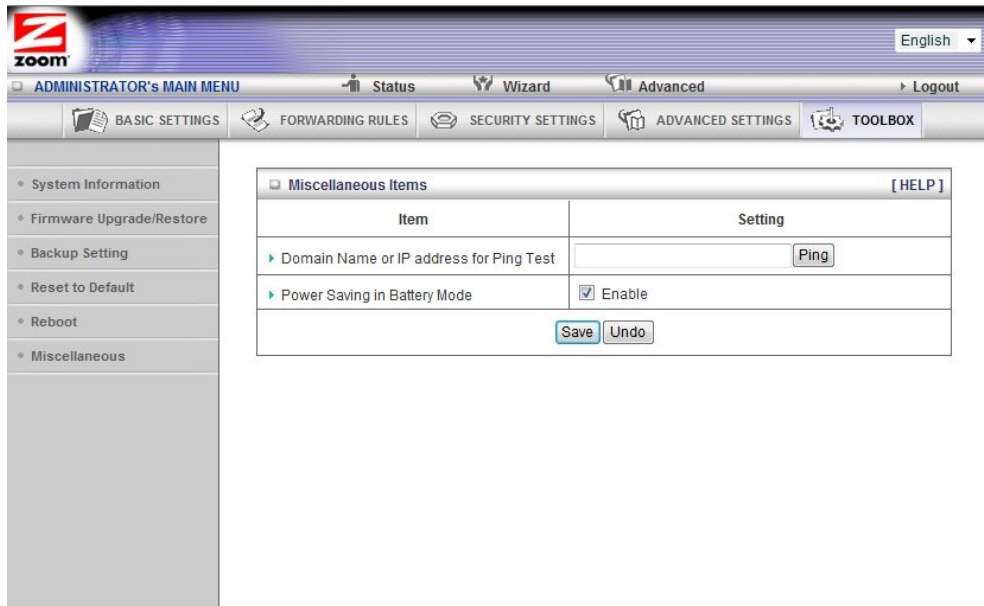
You can reboot the Modem/Router by clicking the Reboot item from the left pane of the Toolbox menu. The following dialog opens.



- 1 Click OK to reboot the Modem/Router.

## The Miscellaneous Page

You can use this page to Ping a remote device on your network or to enable Power Saving in Battery mode. When in Power Saving mode, if the Modem/Router is operating off its battery, the transmit power for WiFi will be reduced to 25%. This will limit the wireless range of the Modem/Router.





## Appendix A: Mobile Broadband Settings

Your Modem/Router works with a large number of different mobile broadband modem models. In most cases when you plug your mobile broadband modem or phone into the Modem/Router, the proper APN (Access Point Name), Dialed Number, PIN Code, Username, and Password for the provider is automatically entered. In some cases, the modem does not know this information, and the Modem/Router needs to be set up to include that information. For instructions on how to do this, please refer to [Chapter 2: Using the Configuration Manager](#) and use the Setup Wizard to enter these settings.

If you are unable to connect to the Internet using the Modem/Router, you should try entering the different settings for your service provider. Begin by entering the first setting for your provider. If that doesn't work, try entering the next setting. If a field is empty in the chart, then leave that setting blank in the Setup Wizard.

### U.S. Mobile Broadband Service Providers

Provider	APN	Dialed Number for 3G	Dialed Number for 4G	Username	Password	Other Settings
<b>Alltel (1)</b>	Check with provider	#777		Check with provider	Check with provider	
<b>Alltel (2)</b>		#777		<your 3G phone number>@alltel.net	alltel	
<b>AT&amp;T (1)</b>	Check with provider	*99#	*99***3# OR *99***1#			
<b>AT&amp;T (2)</b>	ISP.CINGULAR	*99***1#	*99***3# OR *99***1#			
<b>AT&amp;T (3)</b>	ISP.CINGULAR	*99#	*99***3# OR *99***1#	WIXDC001@W5.MYCINGULAR.COM	CINGULAR1	
<b>AT&amp;T voice/data or iPhone SIM card</b>	WAP.CINGULAR	*99#	*99***3# OR *99***1#	WAP@CINGULAR.COM	CINGULAR1	
<b>Cingular ex-AT&amp;T</b>	proxy			guest	guest	
<b>Cingular with acceleration</b>	ISP.CINGULAR			ISPDA@CINGULARGPRS.COM	CINGULAR1	
<b>Cingular w/o acceleration</b>	ISP.CINGULAR			ISP@CINGULARGPRS.COM	CINGULAR1	

<b>Cingular</b> non-contract	WAP.CINGULAR			WAP@CING ULARGPRS. COM	CINGULAR1	
<b>Sprint</b>	Not Required	#777		Check with provider	Check with provider	
<b>T-Mobile</b>	Check with provider	*99#	*99***3# OR *99***1#			
<b>T-Mobile</b> US GPRS Internet	internet2.voicestre am.com					
<b>T-Mobile</b> Internet	internet2.voicestre am.com			guest	guest	
<b>T-Mobile</b> VPN	internet3.voicestre am.com			guest	guest	
<b>T-Mobile</b> non-contract	wap.voicestream.c om			guest	guest	
<b>Verizon (1)</b>		#777	*99***3# OR *99***1#	Check with provider	Check with provider	
<b>Verizon (2)</b>		Leave blank OR check with provider		<your 3G phone number>@vz w3g.com	vzw	

#### U.K. Mobile Broadband Service Providers

Provider	APN	Dialed Number	Username	Password	Other Settings
<b>3</b>	three.co.uk		guest	guest	
<b>Anvil Mobile (1)</b>	m2m.sim4life.com	*99#			
<b>Anvil Mobile (2)</b>	m2m.aql.net	*99#			
<b>ASDA</b>	asdamobiles.co.uk		wap	wap	Gateway Address: 212.183.137.12
<b>BT Mobile Business</b>	btmobile.bt.com	*99***1#	bt	bt	

<b>BT Mobile</b> Customer Value	btmobile2.bt.com	*99***1#	bt	bt	
<b>Jersey Telecom</b>	pepper		abc	abc	
<b>Jersey Telecom</b>	pepper	*99#			
<b>Manx Telecom</b>	internet				
<b>Meteor</b>	isp.mymeteor.ie		my	meteor	
<b>O2 (1)</b> with contract	mobile.o2.co.uk		web	password	
<b>O2 (2)</b> with contract	mobile.o2.co.uk	*99# OR *99***1#	o2web OR faster	password	DNS Address (if needed): 193.113.200.201
<b>O2 (1)</b> faster, with contract	mobile.o2.co.uk		faster	password	
<b>O2 (2)</b> faster, with contract	mobile.o2.co.uk	*99# OR *99***1#	faster OR o2web	password	DNS Address (if needed): 193.113.200.201
<b>O2</b> pre-pay	payandgo.o2.co.uk		payandgo	payandgo	
<b>Orange</b> Pay Monthly	orangeinternet		user	pass	
<b>Orange</b> Pay and Go	orangewap		Multimedia	Orange	
<b>T-Mobile</b>	general.t-mobile.co.uk		user	pass	
<b>Tesco Mobile</b>	prepay.tesco-mobile.com		tescowap	password	
<b>Virgin Mobile (1)</b>	goto.virginmobile.com		user	[space]	
<b>Virgin Mobile (2)</b>	goto.virginmobile.com	*99#	Leave blank	Leave blank	Authentication: PAP
<b>Vodafone</b>	ppbundle.internet		web	web	
<b>Vodafone</b> contract	internet		web	webs	

<b>Vodafone contract</b>	wap.vodafone.co.uk		wap	wap	
<b>Vodafone pre-pay</b>	pp.vodafone.co.uk		wap	wap	
<b>Three UK</b>	three.co.uk		guest	guest	
<b>Three Ireland</b>	3ireland.ie		guest	guest	

# Appendix B: How to Set Up Tethering on the iPhone

---

These instructions are based on using the iPhone in the USA with Verizon and AT&T, and may vary slightly depending on the model of your iPhone, your firmware version, and service provider. These instructions assume that you have a service contract that supports tethering. Please consult your iPhone user manual for more information.

- 1 Connect one end of the USB cable to the Modem/Router and the other end to the iPhone.
- 2 Turn on tethering on the iPhone. For GSM models used by AT&T, select **Settings** → **General** → **Network** → **Internet Tethering**. For CDMA models used by Verizon, select **Settings** → **General** → **Network** → **Personal Hotspot**.
- 3 **Note:** If you see a choice between Bluetooth tethering or USB, you need to select **USB**.

For most carriers you will need to set up your APN information in the Modem/Router. To do this first enter the Modem/Router **Configuration Manager**, then select **Basic Settings** → **Basic Setup**. On the **Basic Setup** page, enter the APN settings for your provider. If you don't know the APN settings please contact your provider or see [Appendix A](#), which contains the settings for many of the most popular wireless providers.

For example, if you are using your iPhone with AT&T, use the following settings for the items shown:

Item	Setting
APN	WAP.CINGULAR
Username	WAP@CINGULAR.COM
Password	CINGULAR1
Dial Number	Leave blank

Basic Setup [HELP]	
Item	Setting
▶ Ethernet port configuration	LAN ▾
▶ LAN IP Address	192.168.1.1
▶ 3G Fallback	<input type="checkbox"/> Check for Wan Connection Internet host: <input type="text"/>
▶ WAN Type	3G ▾
▶ APN (Not required by all providers)	WAP.CINGULAR
▶ PIN Code	<input type="text"/>
▶ Dialed Number	<input type="text"/>
▶ Username	WAP@CINGULAR.COM
▶ Password	*****
▶ Authentication	<input checked="" type="radio"/> Auto <input type="radio"/> PAP <input type="radio"/> CHAP
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ Connection Control	Auto Reconnect (always-on) ▾
▶ Maximum Idle Time	0 seconds
▶ Keep Alive	<input checked="" type="radio"/> Disable <input type="radio"/> Use LCP Echo Request ▶ lcp-echo-interval: 10 seconds ▶ lcp-echo-failure: 3 times
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

## Appendix C: Registering Your Product and Getting Help

---

Zoom supports this Modem/Router. If you need assistance, please contact Zoom directly. We encourage you to register your product and to notice the many support options available from Zoom. Please go to [www.zoomtel.com](http://www.zoomtel.com) and select **Technical Support**. From here you can register your new Modem/Router, contact our technical support experts, use our SmartFacts™ intelligent database, and get warranty information.

If you need to contact Zoom Customer Support, you can call us by dialing:

**U.S.:** (617) 753-0965

**U.K.:** London: +44 2033180660

Manchester: +44 1618840074

## Limited Warranty

---

Zoom Telephonics, Inc. (hereinafter "Zoom") warrants this product against defects in material and workmanship for a warranty period of one year. The one year warranty may be extended only by Zoom as required by local law in the country where this modem is sold by Zoom. This warranty applies to the original end-user purchaser.

For all Zoom products other than software, Zoom will, solely at its option, repair or replace this product with a functionally equivalent new or factory-reconditioned product during the warranty period. The consumer will deliver the product to Zoom. All transportation risks and costs in connection with this warranty service are the responsibility of the consumer.

Zoom will replace software at no charge if there is a defect in materials or workmanship for a period of 30 days from date of original retail purchase, provided the defective software is returned to Zoom. Shipments from Zoom will normally be via U.S. Mail. Software products supplied by Zoom are sold "as is," without warranty, either expressed or implied, as to function, application, merchantability, performance, and quality.

Zoom is not responsible for incidental or consequential damages, and is not responsible for damages resulting from the breach of any expressed or implied warranty. Zoom is not responsible for any costs of recovering, reprogramming, or reproducing any programs or data stored or used with the Zoom products, damage to property, and to the extent permitted by law, damages for personal injury.

This warranty is in lieu of all other warranties, expressed or implied. We do not assume or authorize assumption for us of any other warranty expressed or implied. Some states and countries do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusions may not apply to you.

This warranty does not apply if the Zoom product has been damaged by accident, abuse, lightning or other natural disasters, misuse or misapplication, or if it has been modified without the written permission of Zoom, or if any serial number has been removed or defaced.

This warranty shall not be applicable to the extent that any provisions of this warranty are prohibited by any federal, state, or municipal law that cannot be preempted. This warranty gives you specific legal rights, and you may also have other rights that vary from state to state or country to country.



## CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 5022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC.

### Declaration of Conformity

	Declaration of Conformity Déclaration de conformité Konformitätserklärung Dichiarazione di conformità Declaração de Conformidade Konformitetsdeklaration	Overensstemmelseserklæring Conformiteitsverklaring van de EU Δήλωση Συμμόρφωσης Deklaracja zgodności Declaración de conformidad Cam kết về sự tuân thủ ở Châu Âu
Manufacturer/Producent/Fabrikant/ Constructeur/Hersteller/Κατασκευαστής / Fabbricante/ Fabricante/Tillverkare/ Nhà sản xuất	<b>Zoom Telephonics, Inc.</b> <b>207 South Street</b> <b>Boston, MA 02111 USA /</b> <b>617-423-1072</b> <b>www.zoomtel.com</b>	
Brand/Varemærke/Merk/Marque/Marke / Μάρκα/Marchio/Marka/Marca/Thương hiệu	<b>Zoom Wireless-N Router w</b> <b>3G+Modem &amp;Voice</b>	
Type/Typ/Μάρκα/Tipo/Kiểu mẫu	<b>Model 4530 Series 1098</b>	

The manufacturer declares under sole responsibility that this equipment is compliant to Directive EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC via the following. This product is CE marked.

Producenten erklærer under eneansvar, at dette udstyr er i overensstemmelse med direktivet EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC via følgende. Dette produkt er CE-mærket.

De fabrikant verklaart geheel onder eigen verantwoordelijkheid dat deze apparatuur voldoet aan Richtlijn EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC op grond van het onderstaande.

Dit product is voorzien van de CE-markering. Le constructeur déclare sous son entière responsabilité que ce matériel est conforme à la Directive EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC via les documents ci-dessous. Ce produit a reçu le marquage CE.

Hiermit erklärt Zoom die Übereinstimmung des Gerätes modem mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC. Dieses Produkt ist das gekennzeichnete CE.

Ο κατασκευαστής δηλώνει με αποκλειστική του ευθύνη ότι αυτό το προϊόν συμμορφώνεται με την Οδηγία EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC μέσω των παρακάτω. Αυτό το προϊόν φέρει τη Σήμανση CE.

Il fornitore dichiara sotto la sola responsabilità che questa apparecchiatura è compliant a EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC direttivo via quanto segue. Questo prodotto è CE contrassegnato.

Producent stwierdza że to urządzenie zostało wyprodukowane zgodnie z Dyrektywą EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC. Jest to potwierdzone poprzez umieszczenie znaku CE na urządzeniu.

O fabricante declara sob sua exclusiva responsabilidade que este equipamento está em conformidade com a Directiva 1 EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC através do seguinte. Este produto possui Marcação CE.

El fabricante declara bajo su exclusiva responsabilidad que este equipo satisface la Directiva EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC por medio de lo siguiente. Este producto tiene marca CE.

Nhà sản xuất cam kết với trách nhiệm của mình là thiết bị này tuân theo Hướng dẫn EN 55022/A1 Class B, 2004/108/EC, 2006/95/EC, and ErP Directive 2009/125/EC thông qua các mục sau. Sản phẩm này được đánh dấu là CE.

EN 60950-1:2006/A11:2009 / IEC 60950-1:2005+A1:2009
EN 301 908-1 V4.2.1:2010-03 / EN 300 328 V1.7.1 :2006
EN 301 511 (TS151 010-1 V6.6.0 (2006-1) 3GPP TS 51.010-1 Version 6.6.0 Release 6)
EN50385:2002 / EN 62311 :2008



Director, /Direktør, /Director, /Directeur /Direktør, /Διευθυντής,  
/Direttore, /Dyrektor /Director, /Director, Đốc

Paul Prohodski  
7 August, 2012  
1077/TF, Boston, MA, USA

## U.S. FCC Part 15 Emissions Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

Operations in the 2.4GHz band are restricted to indoor usage only.

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

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

**2591-A**

**27672**

**©2011**