

# ZOOM V3

U S E R   G U I D E



## **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 2005  
All rights reserved.

# Contents

OVERVIEW .....	5
<b>1 INSTALLATION INSTRUCTIONS.....</b>	<b>6</b>
1.1 WHAT'S IN THE PACKAGE .....	6
1.2 QUICK START INSTRUCTIONS.....	8
Step 1: Installing the Software .....	8
Step 2: Installing the Hardware .....	9
Step 3: Configuring Internet Explorer.....	12
Step 4: Configuring Your V3 .....	14
Step 5: Setting up VoIP Service .....	18
1.3 TIPS FOR MAKING VOIP CALLS .....	18
1.4 SETTING THE V3 FOR VOIP ONLY MODE .....	19
1.5 FRONT PANEL DESCRIPTION .....	20
1.6 IF YOU NEED HELP.....	20
1.7 CHANGING THE V3'S PASSWORD & RESETTING THE UNIT TO ITS DEFAULT SETTINGS.....	21
1.8 WINDOWS USERS: REMOVING THE V3 .....	22
<b>2 VOICE OVER IP SETTINGS .....</b>	<b>23</b>
2.1 CHANGING YOUR VOIP SETTINGS.....	23
If Your Unit Is Not Preset for VoIP .....	23
2.2 CALL FORWARDING AND CALL WAITING.....	28
Enabling Call Management Features.....	29
Activating Call Management Features.....	30
<b>3 PLAYING ONLINE GAMES.....</b>	<b>32</b>
3.1 USING YOUR V3 WITH XBOX® LIVE.....	32
3.2 USING YOUR V3 WITH PLAYSTATION® 2 .....	33
3.3 SETTING UP THE V3 FOR PEER-TO-PEER GAMING AND MULTIPLAYER GAME HOSTING .....	35
3.4 SETTING UP A VIRTUAL SERVER.....	36
3.5 SETTING UP A DMZ .....	44
<b>4 USING THE V3'S ADVANCED FIREWALL .....</b>	<b>50</b>
4.1 MAIN FIREWALL FEATURES.....	52
Protection Policy .....	52
Hacker Log.....	54
Service Filtering.....	55
4.2 CREATING INBOUND/OUTBOUND POLICIES .....	56
Inbound Policies .....	57
Outbound Policies.....	58

4.3 SETTING UP FIREWALL DATABASES .....	60
IP Group .....	60
Service Group.....	62
Time Group .....	62
<b>APPENDIX A DSL INTERNET SETTINGS TABLES .....</b>	<b>64</b>
<b>APPENDIX B VOIP PHONE INSTALLATION OPTIONS.....</b>	<b>67</b>
Plug Multiple Phones Directly into the V3 .....	67
Use Cordless Phones to Link to the V3 .....	67
<b>APPENDIX C MAC AND LINUX USERS: SETTING TCP/IP NETWORK SETTINGS .....</b>	<b>68</b>
Macintosh TCP/IP Settings .....	68
Linux TCP/IP Settings .....	69
<b>APPENDIX D TROUBLESHOOTING .....</b>	<b>71</b>
CONNECTION TROUBLESHOOTING TIPS .....	71
VOIP AND PHONE TROUBLESHOOTING TIPS .....	75
<b>APPENDIX E REGULATORY INFORMATION.....</b>	<b>79</b>

## Overview

---

The V3 is a gateway/router with a TelePort™ VoIP phone port. You use the V3 in conjunction with an Ethernet cable modem or Ethernet ADSL modem to connect to the Internet. The gateway/router provides an interface between the Internet and your local area network (LAN). It also includes an advanced firewall, which allows you to control Internet access from your local network and which protects your local network from unwanted Internet traffic. The TelePort lets you use an ordinary telephone to make VoIP calls over the Internet and regular calls through the familiar Public Switched Telephone Network (PSTN).

This User Guide contains installation instructions and explains how to configure the V3 for some popular applications. Most users should go now to the next chapter, Installation Instructions.

**Note:**

If you are an Internet service provider, a VoIP service provider, or a system administrator, additional information is available in the Technical Reference Manual at [www.zoom.com](http://www.zoom.com)

The Technical Reference manual includes information such as voice parameters and dialing plan configurations.

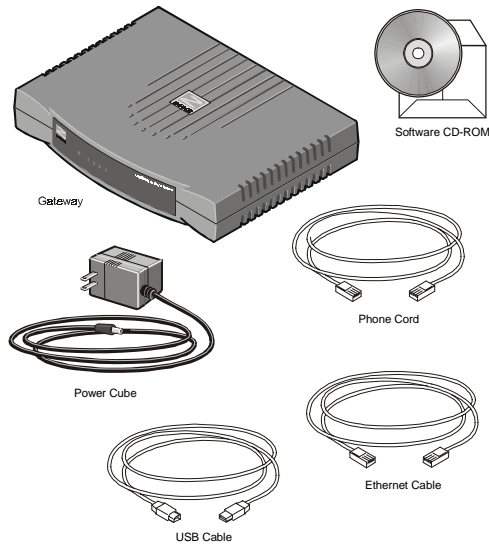
# 1

## Installation Instructions

---

*This chapter covers the basic instructions needed to install your V3 and place VoIP calls.*

### 1.1 What's in the Package



The CD contains the Installation Software, User Manual, Warranty, and Customer Support information.

In addition, you may have a **phone-jack adapter** to adapt the RJ-11 phone cord for a different phone jack (certain countries only).

**If anything is missing or damaged, contact Zoom Customer Support or your retailer or distributor.**

### *What You Will Need*

- **An Ethernet cable modem or Ethernet DSL modem.**
- **A Windows, Macintosh, or Linux computer** equipped with a **Network Interface Card (NIC)** or a **USB port**.
- **A telephone** to plug into the V3 if you plan to use VoIP.
- **An accessible telephone jack** (a jack where you can plug in a regular telephone and make calls).
- **A DSL phone filter.**

## 1.2 Quick Start Instructions

Installing the V3 involves five steps: **Installing the Software**, **Installing the Hardware**, **Configuring Internet Explorer**, **Configuring Your V3**, and **Setting Up VoIP Service**.

### *Step 1: Installing the Software*

Installing the software is only required for people connecting a Windows computer directly to the V3. All others should skip to Step 2: Installing the Hardware.

If your computer has an available Ethernet jack, we recommend that you use it instead of the USB jack. This will simplify installation.

**If you decide to use the V3's USB jack, you must remove any previously installed USB modem drivers on your computer before installing this software.** On the desktop, click the **Start** button, point to **Settings**, and select **Control Panel**. In **Control Panel**, double-click **Add/Remove Programs**, on the **Install/Uninstall** tab, select your old USB modem from the list, and click **Remove**. Now continue below.

- 1 Your computer must be on.** Insert the supplied CD into your computer's CD drive. The CD should start automatically and the **Select Language** screen should appear. (If the CD does not start automatically, on the desktop, click the **Start** button, click **Run**, and then type **D:\setup.exe**, where **D** is the letter of your CD drive.)
- 2 Select your language** and click the **Installation Wizard** button. The software installation proceeds automatically.
- 3** When the process is complete, you will be prompted to click **Finish** and then **Shut Down** to turn off your computer. Remove the CD from your CD drive before you shut down your computer.



## *Step 2: Installing the Hardware*

**Installing the Hardware** is a two-step process, **Making the Connections**, and **Powering Up**.

### *Making the Connections*

- 1 The software must be installed before you proceed.**  
Then, unplug or turn off the power to your PC and everything connected to your PC.
- 2 Plug your phone into the V3's PHONE jack.**  
If you have a cordless phone with one or more handsets, plug the **base station** into the V3's **PHONE** jack.  
**Note:** If RJ-11 phone jacks are not used in your country, you will need a phone adapter. Plug the adapter into the V3's **PHONE** jack and then plug in your phone.
- 3 Connect the V3 to the traditional telephone network.**  
Plug one end of the V3's phone cord into the V3's **TELCO** jack and the other end into a telephone jack where you would normally plug in a standard telephone. If you are using DSL, this jack should have a DSL phone filter installed on it. Phone filters block the DSL frequencies so that someone making a normal phone call won't hear noise on the line. They also keep phone conversations from interfering with DSL performance.  
**If you do not have a DSL phone filter, they are available at most retail stores that sell consumer electronics.**
- 4 Connect the V3 to your cable or DSL modem.**  
Plug one end of an Ethernet cable into your cable or DSL modem and plug the other end into the **WAN** port of the V3. If your cable or DSL modem is already connected to your PC with an Ethernet cable, leave the cable plugged into the cable or DSL modem. Then, unplug the other end from the PC and plug the end you just unplugged into the V3's **WAN** port.

- 5** **If you have an existing router**, we recommend that you replace the existing router with the V3, which has a built-in router. If, however, you need to connect the V3 behind another router, plug one end of the Ethernet cable into the **WAN** port of the V3 and the other end into a **LAN** port of the router.
  
- 6** **If you have a wireless access point or are using a wireless router as an access point**, unplug it from your computer or modem and plug it into one of the V3's **LAN** ports.
  
- 7** **Connect the V3 to your computer**. We recommend that you use the Ethernet port if possible, because Ethernet provides a more reliable connection.  
  
**Ethernet** - Plug one end of the included Ethernet cable into one of the V3's **LAN** ports (**1**, **2**, **3**, or **4**) and plug the other end into the computer's Ethernet port.  
  
**USB** - Plug one end of the USB cable into the V3's **USB** port and the other end into the computer's USB port.

## *Powering Up*

To ensure that all the devices you just connected to the V3 install correctly, you need to power up each device one at a time. Follow these steps carefully.

### **1 Plug in the modem's Power Supply, and turn on the modem's on/off switch if it has one.**

Plug the modem's power cube into a power outlet.

Wait for one-two minutes so that you are sure the modem has completed its power up process before proceeding to Step 2.

### **2 Plug in the V3's Power Supply.**

Plug the included power cube into a power outlet and then into the V3's power (**PWR**) jack.

Wait for one-two minutes so that you are sure the V3 has completed its power up process before proceeding to Step 3.

**Note:** Use only the power cube shipped with the V3 or you may cause damage to your hardware.

### **3 Turn the computer on.**

**If you are using USB,** a **Found New Hardware** box should display, showing the progress of the installation. Follow the prompts.

—**Windows XP users:** You may see **Hardware Installation** disclaimer boxes regarding Windows logo testing. You can safely disregard these messages and click **Continue Anyway**.

—**Windows 2000 users:** You may see a **Digital Signature Not Found** dialog box. You can safely disregard this message and click **Yes**.

—**Windows 98/Me users:** Restart your computer if you are prompted to do so.

## *Step 3: Configuring Internet Explorer*

**Macintosh and Linux users:** Your Web browser is set up automatically, so you can skip this section. Turn to page 68 to make sure that your computer's TCP/IP settings are configured correctly.

**Windows users:** The software that you use to make an Internet connection must be set for a **network connection**, not a **dial-up connection**. If you are already using a cable or DSL modem, you shouldn't need to do anything. If you are just setting up your cable or DSL Internet connection for the first time, we have included instructions. The following instructions are for Internet Explorer, a popular Web browser. If you are using Netscape Navigator or another browser, set it up now to use a **network connection** (this might be called a "Local Area Network" or "broadband" connection).

If you use Internet Explorer, you need Version 5 or later. Most people have the right version. If you don't, we suggest you get a free upgrade. If you want to check your version number, open Internet Explorer, select **Help**, then **About Internet Explorer**. Your version number is right under the Microsoft Internet Explorer logo. You can ignore all the numbers after the period following the first digit.

- 1 On the desktop, **right-click** (not left-click) the **Internet Explorer** icon, and select **Properties**.

### **If you cannot access Internet Explorer:**

**Windows XP users:** From the desktop, click the **Start** button, then click **Control Panel**. In **Control Panel**, click **Network and Internet Options** and then click the **Internet Options** icon.

**Windows 98/Me/2000 users:** From the desktop, click the **Start** button, point to **Settings**, and then click **Control Panel**. In **Control Panel**, click the **Internet Options** icon.

- 2 In the **Internet Properties** dialog box, click the **Connections** tab.
- 3 On the **Connections** tab, click **Setup**.
- 4 Windows XP users: In the **Welcome to the New Connection Wizard** dialog box, click **Next**.  
If you see a **Location Information** dialog box, click **Cancel** to return to the **Welcome** dialog box, and click **Next** again.  
In the **Network Connection Type** dialog box, click **Connect to the Internet**.  
In the **Getting Ready** dialog box, click “**Set up my connection manually,**” and then click **Next**.  
In the **Internet Connection** dialog box, click “**Connect using a broadband connection that is always on,**” and click **Next**.
- 5 Windows 98/Me/2000 users: In the **Internet Connection Wizard** dialog box, select “**I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)**”, and click **Next**.  
In the **Setting up your Internet connection** dialog box, change the selection to “**I connect through a local area network (LAN)**” and click **Next**.  
In the **Local area network Internet configuration** dialog box, uncheck the box “**Automatic discovery of proxy server**”. Then click **Next**.  
A dialog box asks if you want to set up an email account. Click **No** and then **Next**.
- 6 When the configuration process is done, you will see a **Completing the Internet Connection Wizard** dialog box.  
Windows 98/Me/2000 users: Be sure to uncheck the box that says “**To connect to the Internet immediately, select this box....**”

**7** Click **Finish**.

**8** Windows XP users: Close **Control Panel**.

Windows 98/Me/2000 users: If Internet Explorer is open, close it before going to the next step of the installation, **Configuring Your V3**.

### *Step 4: Configuring Your V3*

- If you have a **Cable Modem**, see below
- If you have a **DSL Modem**, see page 15.

### *Configuring the V3 for a Cable Modem*

The V3 is set up by default to work with a cable modem, so additional configuration is normally not required.

**1** **Go to your Web browser** (i.e., Internet Explorer or Netscape Navigator) and **try to connect** to a familiar Web address.

**2** **If you connect successfully, your installation is complete and you're ready to browse the Web!** Continue with Step 5: Setting up VoIP Service on page 18.

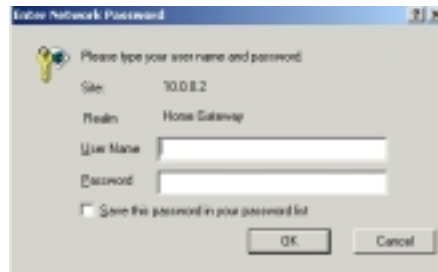
## *Configuring the V3 for a DSL Modem*

**1 Open the Zoom Configuration Manager.**  
You should have a **Zoom** icon on your desktop. You must double-click this icon to open up the **Zoom Configuration Manager**. (If you do not have an icon, open your Web browser, type **http://10.2.2.2** and press **Enter**.)

**2 Log in to the Zoom Configuration Manager.**  
Type the following User Name and Password in lowercase letters as shown. (You will need to use this User Name and Password each time you want to open up the **Zoom Configuration Manager**. See **Changing the V3's Password** in the User's Manual on the CD if you would like to choose a different Password.)

User Name: **admin**

Password: **zoomvoip**



**3** The **Basic Setup** page displays.

**At Internet Connection Type, pull down the list of selections and choose the type of DSL your provider uses.** If you don't know what type you have, read below.

The three most common types of DSL service are PPPoE, PPPoA, and 1483. There is also Static IP, but it is very unlikely that you are using it without knowing. You would have had to ask your service provider for it, and there is typically an additional monthly fee.

**It is very important that this selection is correct**, so if you don't know what type of service you have, we recommend that you call your service provider and ask them. If you can't call them, the tables beginning on page should help you figure it out.



**4** Click **Save Changes**. The screen may change slightly, depending on the type of DSL you select.



## 5 **Configuring the V3 for DSL PPPoE, PPPoA, 1483, or Static IP.**

### **If you selected DSL PPPoE:**

Your service provider should have given you a **username** (usually your email address or the characters preceding the @ sign in your email address) and a **password** (**NOT** the username and password that you used to get into the **Zoom Configuration Manager**.) If you cannot remember or cannot find your username and password, call your service provider and tell them you have misplaced your username and password. Then enter them as well. Skip to Step 7.

### **If you selected DSL PPPoA or DSL 1483:**

To make the V3 work with DSL PPPoA or 1483, you will have to configure your DSL modem. For PPPoA, you need to “pass through” your DSL modem’s IP Address to the V3. For DSL 1483, you need to “turn off NAT.” NAT is a kind of firewall.

You will have to do this through your DSL modem configuration software. Unfortunately there are many different DSL modem manufacturers and each one handles this a little bit differently, so we can’t give specific instructions for your modem. You should find these settings in your DSL modem user’s manual or configuration software under “Advanced Features” or “Advanced Configuration.”

—**If you have DSL PPPoA**, the setting that you are looking for is commonly called **PPP Half Bridge, ZIPB, DHCP Spoofing**, or just **IP Passthrough**. When you find it, **check or select it**.

—**If you have DSL 1483**, look for **Setting NAT, NAT Configuration**, or something similar. When you find it, **turn off NAT**.

### **If you selected DSL with Static IP:**

Enter the **static IP address, subnet mask, default gateway**, and **DNS Server** IP address assigned to you by your service provider, and then click **Add**.

- 6** Click **Save Changes**, then **Write Settings to Flash and Reboot**, and then **Confirm**.
- 7** Go to your **Web browser** (i.e., Internet Explorer or Netscape Navigator) and **try to connect** to a familiar Web address.
- 8** **If you connect successfully, your installation is complete and you're ready to browse the Web!** Continue with Step 5: Setting up VoIP Service  
If you do not connect successfully, refer to the **Troubleshooting Tips** on page 71.

### *Step 5: Setting up VoIP Service*

If you purchased a V3 Model 5567, your unit has been set up for VoIP service, so continue below with 1.3 Tips for Making VoIP Calls. If you purchased another Model V3, please go to Chapter 2 on page 23.

## 1.3 Tips for Making VoIP Calls

**Distinctive Ring and Dial Tone** - The V3's ring and dial tone sound different from your normal phone. This means that you can easily tell by the ring that you are receiving a VoIP call. Perhaps more important, when you make a VoIP call, you will hear a different dial tone than you hear on the public phone network, so that you can be sure you are making a VoIP call.

**Speed dialing** - If the phone that you plugged into the V3 has a speed dialing feature, you can use it for your VoIP calls and your regular calls. Just be sure to start the VoIP calls with the # symbol (except in VoIP Only Mode where you don't use the #).

**Redial** - You may redial a VoIP number just as you would redial any other number, using the redial feature on your phone.

**Hook Flash** - If you receive a second call while you are on a VoIP call, you will hear a call waiting tone. Momentarily press the hook button on your phone to talk to the second caller, and press it again to go back to your first conversation. After you have completed a VoIP call, you can press the hook button to get a fresh VoIP dial tone and make another VoIP call without dialing # (Note that redial or speed dialing will not work in this case, however. You must hang up for at least one second if you need to make a conventional phone call.

## 1.4 Setting the V3 for VoIP Only Mode

For models outside of the US, the V3 can be set to operate in **VoIP Only Mode**. While in **VoIP Only Mode**, you do not need to dial # before dialing a number. Use **VoIP Only Mode** when:

- You have a cable modem and you are not near a phone jack that you can plug the V3 into.
- You are using a DSL modem and your DSL line also provides your ISDN service.
- You are using “unbundled” DSL—that is, a line without any telephone service attached to it.
- You intend to use the phone connected to the V3 **solely** for VoIP calls. That way, you do not have to hit # before every call.

To put the V3 in **VoIP Only Mode**, follow these steps:

- 1 From the **Zoom Configuration Manager**, click the **Voice Over IP** icon at the top of the page.
- 2 Check the **VoIP Only Mode** box.
- 3 Click **Save Changes, Write Settings to Flash and Reboot, and Confirm**.

## 1.5 Front Panel Description



Light	Description
PWR	Lights when the V3 is plugged into a power source.
LINK	Lights when the V3 is connected to its broadband WAN connection device.
DATA	Blinks when data is being transferred through the broadband line.
USB	Lights when the USB port of the V3 is plugged into a powered-up computer's USB port.
LAN 1-4	Lights when a LAN port of the V3 is plugged into the Ethernet port of a powered-up device.
VoIP	Lights when a Voice over IP call is taking place.

If you have followed the manual to this point, your V3 gateway and VoIP should be working. Congratulations, you're ready to enjoy the V3!

## 1.6 If You Need Help

- If you have hardware installation problems, our Technical Support Staff will be happy to assist you.  
**Windows Users:** Please see the Customer Support portion of the CD for contact information. You may also want to refer to the Frequently Asked Questions on the CD.  
**Macintosh and Linux Users:** You will find Customer Support information and User Documentation in Adobe PDF format in the appropriately named folders in the directory of the CD-ROM that came with your V3.

- From time to time, Zoom may release improved firmware. This is available at [www.zoom.com](http://www.zoom.com) , along with upgrade instructions. We recommend that you check this site periodically for updates.

## 1.7 Changing the V3's Password & Resetting the Unit to Its Default Settings

To change the V3's Password, click the **Advanced Setup** icon at the top of the **Zoom Configuration Manager**. Under the **Administration** heading, click **Admin Password**.

- Type the new password, then retype it for verification purposes.
- Click **Save Changes, Write Settings to Flash and Reboot**, and **Confirm**.

Note:

The password must be at least 8 characters. If you change your password and then forget it, your only recourse is to reset it to the default by performing a hardware system reset (see below).

If you have changed the system settings on your V3 unit and for some reason want to restore them to the factory default settings, you can do so in one of two ways: You can perform a software reset or a hard reset.

If you can open your Web browser and access your V3's user interface, here's how to perform a software reset:

- From the **Advanced Setup** page, under **Administration**, click **Reset to Default**. You will be prompted to click the **Write Settings to Flash and Reboot** button. Once this process is complete, your unit is reset to its factory settings. Click on any of the icons at the top of the page to continue.

If you lose your link to the unit and cannot communicate with it via the Web browser, here's how to perform a hard reset.

- Using a paper clip, press the **RESET** button on the unit's back panel. While holding in this button, count to five, and then release the button. You are now guaranteed that all system settings are restored to the unit's factory defaults.

## 1.8 Windows Users: Removing the V3

If you have Windows and want to remove your V3—for instance, if you move your computer to a location without broadband service—you should remove the software before disconnecting the hardware.

- 1 From the desktop, select Start | Programs | Zoom VoIP Gateway | Uninstall.
- 2 When prompted to confirm your choice, click Yes.
- 3 When the process is complete, you will be prompted to click Finish.
- 4 Unplug your V3 hardware.

# 2

## Voice Over IP Settings

---

*If you purchased a V3 Model 5567, you do not need this chapter. If you have another V3 model, please continue below.*

### 2.1 Changing Your VoIP Settings

**The V3 needs to be configured with specific information for the VoIP service that you plan to use.**

**If you received the V3 from your service provider, it is likely that it is preset for their VoIP service.** In most cases the service provider will tell you that the unit has been preset. If you're not sure you can check by going to the **Advanced VoIP Setup** page (Double-click the **Zoom V3** icon on your desktop, then the **Voice over IP** button on the opening page, then the **Advanced VoIP Setup** button.) If the **User ID** box is filled in, your V3 is preset; you can now refer to **Section 1.3 Tips for Making VoIP Calls** on page 18 or **Section 2.2 Call Forwarding and Call Waiting** on page 28. If your V3 is not preset, continue below.

#### *If Your Unit Is Not Preset for VoIP*

**There are two ways to configure the V3 for VoIP.** Both require that you enter specific information provided to you by your service provider.

Some service providers use **Auto Account Configuration**. If your service provider gave you a **Server Address**, they are using Auto Account Configuration. Go to Auto Account Configuration on page 24.

If your service provider did not give you a Server Address but provided you with a **User ID** and a **Password**, you will configure your V3 manually. Go to Manual Account Configuration on page 26.

## Auto Account Configuration

### **1** Open the **Voice Over IP** page.

Click the **Zoom V3** icon on your desktop, then the **Voice over IP** icon at the top of the opening page to display the **Voice over IP** setup page.

Item	Status
User ID	
Auto-Configuration Status	AutoConfigActive
World Wide Number	0

### Basic Setup

Auto Account Configuration

Server:

Filename:

Encryption:

Select Ring & Tone by Country/Region:

Display Name:

VoIP only Mode:

---

After you have saved your changes, you must write the new settings to flash and reboot. Click the button below to do this.

### **2** Under **Basic Setup**, in the **Server** box enter the Server address given to you by your provider.



- 3 If your service provider gave you a **Filename**, enter it in the Filename box. If you did not get a Filename from your service provider, leave the box as it is.
- 4 Go to the box labeled **Encryption**. Your service provider should have told you whether encryption should be on (box checked) or off (box unchecked). It is important that this is right, so if you don't have this information contact your service provider before proceeding.
- 5 Click the **Download Configuration** button.
- 6 You can now use **Select Ring & Tone by Country/Region** to decide what kind of ring and ring tone you would like for your incoming VoIP calls. You can either choose to have your ring and ring tone be the same as your normal phone ring, slightly different, or completely different. We recommend that you make the ring different from your normal ring so that you can tell the difference between an incoming VoIP call and a regular call.

**To make your incoming ring the same as your normal ring**, choose your country from the pulldown menu.

**To make your incoming ring slightly different** from your normal ring, choose your country from the pulldown menu and pick the "VoIP" option. This will give you the same tone as your normal ring with a different ring pattern.

**For a completely different ring tone** for your VoIP calls, you can choose any ring listed for any country.

- 7 Click **Save Changes**, then **Write Settings to Flash and Reboot**, and then **Confirm**.

**8 Check that your settings are okay.** Look at the **User ID** box near the top of the page. If this box is now filled in, your settings are okay.

**If this box is not filled in, contact your provider.**

**9** You can now refer to **Section 1.3 Tips for Making VoIP Calls** on page 18 or **Section 2.2 Call Forwarding and Call Waiting** on page 28.

## Manual Account Configuration

**1** **Open the Advanced VoIP Setup page.**

Double-click the **Zoom V3** icon on your desktop. In lowercase letters, enter **admin** for the username and **zoomvoip** for the password. Click the **Voice over IP** icon at the top of the opening page to display the **Voice over IP** setup page. Then click the **Advanced VoIP Setup** button at the bottom of the **Voice Over IP** page to display the **Advanced VoIP Setup** page.

The screenshot displays the 'Advanced VoIP Setup' interface. At the top, there is a red header bar labeled 'Service Configuration'. Below this, there are three checkboxes: 'Enable VoIP' (checked), 'Enable SIP Registration' (unchecked), and 'Auto Account Configure' (unchecked). The main configuration area is divided into two columns of fields. The left column includes: 'User ID' (empty), 'Password' (empty), 'Domain/Host' (empty), 'SIP Proxy Address' (empty), 'Outbound Proxy Address' (empty), 'SIP Registration Interval' (3600), 'Local SIP Port' (5060), and 'Caller ID Modulation' (GD\_BELL202). The right column includes: 'Authorization ID' (empty), 'Display Name' (Zoom V3), 'SIP Port' (5060), 'SIP Proxy Port' (5060), 'Outbound Proxy Port' (5060), 'Authentication Method' (AUTH\_MD5), 'RTP Media Port' (5000), and 'Select Ring & Tone by Country/Region' (US/Canada - VoIP). Below these fields is a 'Codec Preferences' section with three dropdown menus set to G.711u, G.729, and G.711a. At the bottom, there is an 'Enable STUN' section with radio buttons for 'Yes' (selected) and 'No', followed by 'STUN Server' and 'STUN Port' input fields.

- 2 Under **Service Configuration**, click the **Auto Account Configure** box to remove the checkmark.
- 3 Enter the **User ID, Authorization ID, Password, Domain/Realm**, and **SIP Proxy Address** in the appropriate boxes. These five boxes must be filled in correctly. Enter them carefully and check to make sure they match the information given to you.
- 4 If you installed the V3 behind a router or your service provider told you to enable **STUN**, click **Yes** to enable **STUN**. Then, enter the **STUN server** name and **port number**. These should have been given to you by your service provider.
- 5 Enter any **additional information required by your service provider**. If your provider gave you any other information, enter it in the appropriate boxes.
- 6 You can now use **Select Ring & Tone by Country/Region** to decide what kind of ring and ring tone you would like for your incoming VoIP calls. You can either choose to have your ring and ring tone be the same as your normal phone ring, slightly different, or completely different. We recommend that you make the ring different from your normal ring so that you can tell the difference between an incoming VoIP call and a regular call.

**To make your incoming ring the same as your normal ring**, choose your country from the pulldown menu.

**To make your incoming ring slightly different** from your normal ring, choose your country from the pulldown menu and pick the “VoIP” option. This will give you the same tone as your normal ring with a different ring pattern.

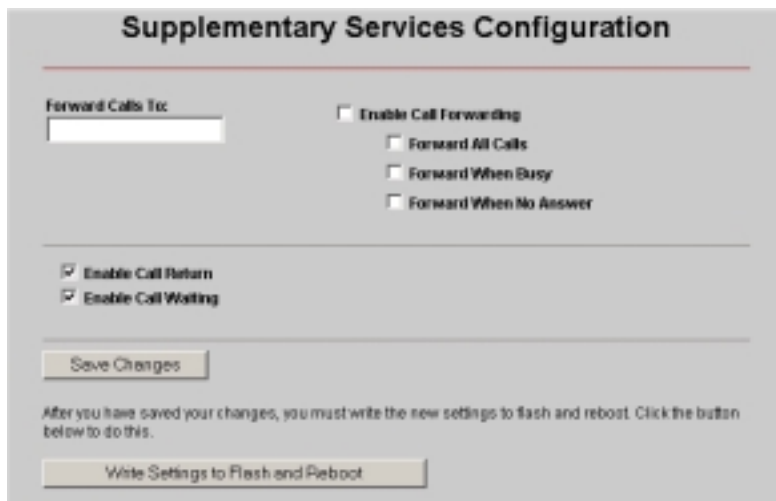
**For a completely different ring tone** for your VoIP calls you can choose any ring listed for any country.

**7** Click **Save Changes**, then **Write Settings to Flash and Reboot**, and then **Confirm**.

**8** **Wait** for 30 seconds. You can now refer to Section 1.3 Tips for Making VoIP Calls on page 18 or continue below.

## 2.2 Call Forwarding and Call Waiting

The **Supplementary Services** page displays the V3's VoIP call management features such as call forwarding and call waiting. Click its button on the bottom of the **Voice Over IP** page.



**Supplementary Services Configuration**

Forward Calls To:

Enable Call Forwarding

- Forward All Calls
- Forward When Busy
- Forward When No Answer

Enable Call Return

Enable Call Waiting

After you have saved your changes, you must write the new settings to flash and reboot. Click the button below to do this.

**Important:** The V3's call forward capabilities are displayed on this page. However, **to activate these functions**, you must enter the V3's VoIP call management commands using your telephone keypad. The section immediately following the table, **Activating Call Management Features**, explains how to do this.

## *Enabling Call Management Features*

<b>Enable Call Forwarding</b>	Click to turn on the call forwarding feature. Then select (click) the options listed below that you want to use.
<b>Forward Calls To</b>	Enter the phone number of the location where you want to forward incoming VoIP calls. You must also enter the forwarding number using your telephone keypad, as explained below this table.
<b>Forward All Calls</b>	Enables the forwarding of all VoIP calls to the specified forwarding number.
<b>Forward When Busy</b>	Enables the forwarding of VoIP calls to the specified forwarding number when the V3's phone is busy.
<b>Forward When No Answer</b>	Enables the forwarding of VoIP calls to the specified forwarding number when there is no answer.
<b>Enable Call Waiting</b>	Enabled by default. Call waiting signals you with a tone when another caller tries to contact you while you are on the phone. Press the hook button on your phone to be connected to the second caller, and the person you were talking with will be placed on hold. Press it again to return to the first conversation. If you disable it, callers will either hear a busy signal or they will be given the option to leave a voice mail message; this depends on your service provider.
<b>Enable Call Return</b>	Enabled by default. Dial the call return number for your region, preceded by the # sign, if you want the V3 to dial the last number that attempted to call you. if you do not know the call return number or it does not work, dial # and then * 6 9

## *Activating Call Management Features*

**Note:**

Call forwarding works only for calls that arrive over VoIP. The V3 cannot forward calls from the PSTN. However, if you have VoIP to PSTN service, you can forward VoIP calls from the V3 to the PSTN.

The command sequence to control call management is simple. We have included a sample table below. On your telephone keypad, enter

# <**Forward code**> <**Forward Number**> #

The V3 will attempt to place a call to the Forward Number.

If someone answers within 15 seconds, the forwarding feature will become active. If not, you need to re-enter the command:

# <**Forward code**> <**Forward Number**> #

Then the forwarding feature you have selected will become active.

You will hear a stutter dial tone while call forwarding is active.

### Sample Table of Enable/Disable Codes

Function	USA	UK
Forward All	* 7 2	* 2 1 *
Forward Busy	* 7 4	* 6 7 *
Forward No Ans	* 7 5	* 6 1 *
Forward Deactivate	* 7 3	# 2 1 *
Call Waiting Disable	*7 0	# 4 3 #

To deactivate Call Forwarding, enter

# < **Forward Deactivate code** > #

Note:

Deactivating call forward from the keypad only *deactivates* the last phone number programmed—that is, the currently active forwarding function. It does not turn off the V3's call forwarding capability. This must be done from the V3's **Supplementary Services** page or by your service provider.

To deactivate Call Waiting, enter

# < **Call Waiting Disable code** > #

Now go to **Section 1.3 Tips for Making VoIP Call** on page 18.

# 3

## Playing Online Games

---

*Setting up the V3 for online gaming depends on what you want to do:*

- *If you have Xbox<sup>®</sup> Live, continue below.*
- *If you have PlayStation 2<sup>®</sup>, go to page 33.*
- *If you have another online game, go to page 35.*

### 3.1 Using Your V3 with Xbox<sup>®</sup> Live

Follow these steps:

- 1 Update the Xbox Dashboard:** Make sure you have your Xbox Live Starter Kit at hand. Insert the Xbox Live CD into your Xbox. Once the upgrade is complete, the main menu will include an **Xbox Live** entry.
- 2 Connect the V3 and the Xbox:** Using an Ethernet cable, plug one end into the Xbox's jack and the other end into one of the V3's Ethernet (**LAN**) jacks. Note: If you didn't use the Ethernet cable that came in your V3 package to connect the V3 to your computer, you can use that cable. Otherwise, you can buy one at your local electronics or computer store. Insert the Xbox Communicator module into the Xbox Controller expansion slot (top slot) and then insert the headset plug into the Communicator module.



- 3 Activate your Xbox Live account:** The Xbox Live CD should still be in your Xbox. We recommend that you watch a video that explains the installation process: Select **Xbox Live** from the menu. Then, from the Dashboard, select **Xbox Live** and follow the prompts. **Note:** You will need your subscription code to activate your account—this number is located on the CD's sleeve. (If you require more detailed instructions, please refer to your Xbox Live documentation.)

That's it! You can load one of the demo games included on your Xbox Live CD or use any other Xbox Live-enabled game to begin.

## 3.2 Using Your V3 with PlayStation® 2

Your PlayStation 2 must be connected to your V3: Using an Ethernet cable, plug one end into the PlayStation's **Network** jack and the other end into one of the V3's Ethernet (**LAN**) jacks.

Note: If you didn't use the Ethernet cable that came in your V3 package to connect the V3 to your computer, you can use that cable. Otherwise, you can buy one at your local electronics or computer store. Then follow the steps below.

- 1** Load the PS2 **Network Adapter Start-up Disc** that was supplied with the PS2 network adapter into the PlayStation 2.
- 2** At the PlayStation's main menu, select **ISP Setup**.
- 3** If you have pre-existing network settings on your PlayStation 2, you will be prompted to select **New Network Setting** before selecting **Local Area Network (LAN)**. Otherwise, simply select **Local Area Network (LAN)**.
- 4** Select **Advanced Setup** and then **Set Manual IP**.

5 Fill out these fields:

<b>IP Address</b>	10.2.2.50
<b>Subnet Mask</b>	255.255.255.0
<b>Default Gateway or Router</b>	10.2.2.2

Then select **Continue**.

6 Fill out these fields:

<b>Primary DNS</b>	10.2.2.2
<b>Secondary DNS</b>	10.2.2.2

Then select **Continue**.

7 Select **Test Settings**. A connection test runs. You will then see the message, “**The test for connecting to your ISP was successful! Please save your network setting.**” If you are unsuccessful, re-check the information you entered in Steps 5 and 6.

Then select **Continue**.

8 Now enter a **Network Setting Name** (anything you choose) and then select **Save**. Your Service Provider setup is now complete. Follow the prompts for online registration.

9 Now, using the computer connected to the V3, go to the V3’s **Advanced Setup** page and click the **DMZ** button. Then select **Enable** from the **DMZ** dropdown list, and enter the static IP address **10.2.2.50** in the **DMZ Host IP** field. Click **Save Changes**, then **Write Settings to Flash and Reboot**, and then **Confirm** to complete the process.

Important:

Outside game players need to know the V3’s **WAN IP address**. To find this address, click the **System Status** icon at the top of any **Zoom Configuration Manager** page and scroll down to the **WAN Status** section.

## 3.3 Setting Up the V3 for Peer-to-Peer Gaming and Multiplayer Game Hosting

There are only two cases where you need to set up your V3 for online gaming.

- If you are using your computer to play a “**peer-to-peer**” or “**head-to-head**” game over the Internet, you **always** have to set up the V3 **unless** you linked up to your partner by going to a web site. A peer-to-peer game is a game where two players are competing directly against one another. Popular peer-to-peer games include Age of Empires, Command and Conquer, Dark Reign 2, and Unreal Tournament. If you are unsure whether your game is a peer-to-peer game, check the game instructions.
- If you are using your computer to play a **multiplayer game and you want to host the game**. Popular multiplayer games include Half Life, Diablo II, Delta Force, Hexen II, Myth, Quake II, and Warcraft II, III.

In both these cases you will need to open one or more ports in the V3’s built-in firewall as described below, so that the firewall doesn’t block the other players. **The two ways to accomplish this are to Set up a Virtual Server if you only need to open a few ports, or to Set up a DMZ, which opens all the V3’s ports.**

### Important!

#### **If your computer already has firewall software installed:**

If you have third-party firewall software installed on your computer, such as the Windows XP firewall, you may need to deactivate it before opening ports by setting up a virtual server or a DMZ. If you don’t, your computer may block the ports you are trying to open.

If you do not know how to deactivate the software, consult your Windows Help or the documentation that came with your software or computer.

- **For Virtual Server instructions, continue below.**
- **For DMZ instructions, go to page 44.**

## 3.4 Setting Up a Virtual Server

### 1 Find out which ports need to be opened for gaming.

Most peer-to-peer and multiplayer game manuals will tell you exactly which port or ports need to be opened. If yours didn't, you may be able to look up the information at:

**[www.practicallynetworked.com/sharing/app\\_port\\_list.htm](http://www.practicallynetworked.com/sharing/app_port_list.htm)**

If you have found your games port settings, we recommend that you **print them out, write them down now, or keep the game manual handy.**

Different games require different numbers of ports to be open. This can be a single port, or it can be a hundred ports or more. **Each required port needs to be set individually, so the more ports that your game requires, the more time it will take to do the configuration.** Some games even use "dynamic" ports, meaning that the ports used by the game are constantly changing, so you can't set the ports.

**There is a setting that opens all your ports for gaming**, called a **DMZ**. If you can't find the port settings in your game manual or on the web site shown above, or if you have to open more than 20 ports (which is the maximum allowed by the V3), or if your game documentation says that the game uses dynamic ports, or if you don't want to spend the time to open multiple ports, refer to the DMZ instructions on page 44.

#### **Warning!**

Every time you open an additional port, it decreases the effectiveness of your firewall, so the less ports you open the better.

## 2 Choose an IP address for Gaming.

Double-click the **Zoom V3 icon** on your desktop (or type 10.2.2.2 in your Web browser just the way you would normally type a web address) to get to the V3's **Zoom Configuration Manager**. Click the **Advanced Setup** icon, then click **LAN Settings**. There you will see the starting and ending range of the V3's dynamic (DHCP) LAN IP addresses. You need to choose an IP Address that is outside this range. Normally you should pick the next **higher** number. For example, if the range shown is 10.2.2.4 to 10.2.2.15, your Host IP Address should be the next IP address after 10.2.2.15, which would be 10.2.2.16. Unless you have changed the V3's IP address settings, which is very unlikely, just use that number. Write down the number you choose for reference. The rest of the instructions will assume that you are using 10.2.2.16.

Gaming IP Address: \_\_\_\_\_

**Windows users continue below.**

**Macintosh users jump to Step 5 (page 39).**

**Linux users jump to Step 6 (page 40).**

## 3 Windows Users Only: Open the TCP/IP Properties dialog box.

**For Windows XP:** From the desktop click the **Start** button, point to **Control Panel** and then **Network Connections**. Then right-click (NOT left-click) **Local Area Connection**, select **Properties**, highlight your NIC card's **TCP/IP** entry (it should start with **TCP/IP** and have the characters **10/100**, **NIC**, or **Ether** in it – and not have the words **AOL**, **Dial-up**, or **Adapter**). Click **Properties** to display the Windows **TCP/IP Properties** dialog box.

**For Windows 2000:** From the desktop click the **Start** button, point to **Settings** and then **Network and Dial-up Connections**. Then right-click (NOT left-click) **Local Area Connection**, select **Properties**, highlight your NIC card's **TCP/IP** entry (it should start with **TCP/IP** and have the characters **10/100**, **NIC**, or **Ether** in it – and not have the words **AOL**, **Dial-up**, or **Adapter**). Click **Properties** to display the Windows **TCP/IP Properties** dialog box.

**For Windows 98 and Me:** From the desktop click the **Start** button, then point to **Settings** and then **Control Panel**. Double-click the **Network** icon to display the **Network** configuration screen. Highlight your NIC card's **TCP/IP** entry (it should start with **TCP/IP** and have the characters **10/100**, **NIC**, or **Ether** in it – and not have the words **AOL**, **Dial-up**, or **Adapter**). Click **Properties** to display the Windows **TCP/IP Properties** dialog box.

## **4 Windows Users Only: Enter the IP Settings.**

### **For Windows 2000 and XP:**

Click the **Use the following IP address** and **Use the following DNS server addresses** buttons so that a black dot appears. Then enter the settings for **IP address**, **Subnet mask**, **Default gateway**, and **Preferred DNS server**. Most users can copy the information exactly as it is shown in the chart below. However, **if you chose an IP address in Step 2 other than 10.2.2.16**, enter the number that you chose instead of 10.2.2.16. When done, click **OK** and **continue with Step 7**.

IP address	10.2.2.16
Subnet mask	255.255.255.0
Default gateway (V3's LAN IP address)	10.2.2.2
Preferred DNS server	10.2.2.2

### **For Windows 98 and Me:**

Click **Specify an IP Address** and enter the settings for **IP Address** and **Subnet Mask** shown below, **unless you chose an IP address in Step 2 other than 10.2.2.16**, in which case you should enter the number that you chose instead of 10.2.2.16.

<b>IP address</b>	<b>10.2.2.16</b>
<b>Subnet mask</b>	<b>255.255.255.0</b>

Now click the **DNS Configuration** tab at the top of the menu. Then click **Enable DNS**. Enter any name (i.e., your name, the words “My Computer”, a favorite word, or any other letters or numbers) in the box labeled **Host**. A **Host**: name is required.

Fill in the **DNS Server Search Order** box with the number **10.2.2.2**, click **Add**, and then click the **Gateway** tab. Fill in the **New gateway**: box with the number **10.2.2.2** and click **Add** and then **continue with Step 7**.

## **5 Macintosh Users Only: Open the TCP/IP Pane or Window and enter the IP settings.**

### **For Mac OS X:**

From the **Dock**, choose **System Preferences** and then **Network** to display the **Network** pane. (For OS X 3, you also have to click the **Configure** button.)

Under the **TCP/IP** tab, highlight **Manually** in the **Configure**: list box and enter the settings for **IP Address**, **Subnet Mask**, **Router**, and **DNS Servers** shown below, **unless you chose an IP address in Step 1 other than 10.2.2.16**, in which case you should enter the number that you chose instead of 10.2.2.16. When done, click **Save** or **Apply Now**, and **continue with Step 7**.

<b>IP Address</b>	<b>10.2.2.16</b>
<b>Subnet Mask</b>	<b>255.255.255.0</b>
<b>Router (V3's LAN IP address)</b>	<b>10.2.2.2</b>
<b>DNS Servers</b>	<b>10.2.2.2</b>

### **For Mac OS 7.6.1 – 9.2.2:**

From the **Apple** menu, choose **Control Panels** and then **TCP/IP** to display the **TCP/IP** Window. Under the **TCP/IP** tab, highlight **Manually** in the **Configure:** list box and enter the settings for **IP Address, Subnet mask, Router address, and Name server addr.** shown below, **unless you chose an IP address in Step 1 other than 10.2.2.16**, in which case you should enter the number that you chose instead of 10.2.2.16. When done, close the Window and you will be prompted to click **Save**. Then **continue with Step 7**.

IP address	10.2.2.16
Subnet mask	255.255.255.0
Router address (V3's LAN IP address)	10.2.2.2
Name server addr.	10.2.2.2

### **6 Red Hat Linux Users Only:**

- a **Edit /etc/sysconfig/network-scripts/ifcfg-eth0 so that it contains the following lines:**

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
BROADCAST=10.2.2.255
NETMASK=255.255.255.0
IPADDR=10.2.2.16
GATEWAY=10.2.2.2
NETWORK=10.2.2.2
```

- b **Then edit or create /etc/resolv.conf so that it contains the following line:**

```
NAMESERVER=10.2.2.2
```

Note:

If you are using another version of Linux and you are unsure how to enter this information, consult the help file or documentation that came with your operating system.



c **Continue with Step 7.**

## **7 All Users: Go back to the V3's Advanced Setup page and click the Virtual Server button.**

If you already closed the **Zoom Configuration Manager**, double-click the Zoom V3 icon on your desktop (or type 10.2.2.2 in your Web browser) and click the **Advanced Setup** icon.

## **8 Configure the Virtual Server.**

This is where you'll need to enter the information that you got from your gaming manual or the **www.practicallynetworked.com** web site. **Unfortunately, you can only configure one port at a time.** Each time you configure a new port, your computer will reboot when you hit **Write Settings to Flash and Reboot**.

Tip:

If you have more than a few ports, this process could take a long time. An option is to set up a DMZ, **which opens all your ports at once.** See page 44 for instructions.

**Enter the information shown below now on the Virtual Server Configuration page.**

<b>Public Port</b>	Inbound port from the Internet that you want to open. This is the port number, or one of the port numbers, that you got from your gaming manual or the web site at <a href="http://www.practicallynetworked.com">www.practicallynetworked.com</a>
<b>Private Port</b>	Enter the same port number that you entered in the Public Port field above. (Technically, the Private Port is the inbound port from the V3 that you want to open to the LAN side.) Note: You cannot leave the Private Port field blank.
<b>Port Type</b>	The default is TCP. Some games use both TCP and UDP. If your game uses both port types, you will have to create two Virtual Server entries for each port you want to open. Once you will have to enter the Public Port, Private Port, and Host IP address, and select TCP, and then you will have to fill in the same fields again and select UDP.
<b>Host IP Address</b>	Fixed IP address of the host computer— <b>this is the same IP address that you chose in Step 2 and entered in Step 4</b> , probably 10.2.2.16.

**9** After entering the above information, click **Add This Setting**.

**10** Click **Write Settings to Flash and Reboot**.

Your computer will reboot. **If you need to open additional ports, go back to Step 8** on page 41 and repeat.

Important:

Outside game players will need to know the V3's **WAN IP address**. To find this address, click the **System Status** icon at the top of any **Zoom Configuration Manager** page and scroll down to the **WAN Status** section.

## 3.5 Setting Up a DMZ

If you are playing a game or using an application that requires a **specific port or ports to be open**, go to page 36 for instructions on setting up a Virtual Server. A virtual server can have a maximum of 20 ports open.

If you need more than 20 ports open, or you don't know which ports to open (some games or applications like NetMeeting use "dynamic" ports, meaning that the ports used by the game are constantly changing, so it is not possible to set specific ports), you have to set up what is called a DMZ (Demilitarized Zone).

To set up a DMZ, you need to make all four of the settings in the chart below. You make these settings on the computer where you set up the DMZ, no matter whether the computer is a Windows, Macintosh, or Linux computer.

**Important!**

**If your computer already has firewall software installed:** If you have third-party firewall software installed on your computer, such as the Windows XP firewall, you may need to deactivate it before opening ports by setting up a virtual server or a DMZ. If you don't, your computer may block the ports you are trying to open.

If you do not know how to deactivate the software, consult your Windows Help or the documentation that came with your software or computer.

IP address	10.2.2.16 (see Step 1 below)
Subnet mask	255.255.255.0
Default gateway or router (V3's LAN IP address)	10.2.2.2
Preferred DNS server or Name server	10.2.2.2

## 1 Choose an IP address.

Double-click the **Zoom V3 icon** on your desktop (or type 10.2.2.2 in your Web browser just the way you would normally type a web address) to get to the V3's **Zoom Configuration Manager**. Click the **Advanced Setup** icon, then click **LAN Settings**. There you will see the starting and ending range of the V3's dynamic (DHCP) LAN IP addresses. You need to choose an IP Address that is outside this range. Normally you should pick the next **higher** number. For example, if the range shown is 10.2.2.4 to 10.2.2.15, your Host IP Address should be the next IP address after 10.2.2.15, which would be 10.2.2.16. Unless you have changed the V3's IP address settings, which is very unlikely, just use that number. Write down the number you choose for reference. The rest of the instructions will assume that you are using 10.2.2.16.

DMZ IP Address: \_\_\_\_\_

**Windows users continue below.**

**Mac users jump to Step 4 (page 47).**

**Linux users jump to Step 5 (page 48).**

## 2 Windows Users Only: Open the TCP/IP Properties dialog box.

**For Windows XP:** From the desktop click the **Start** button, point to **Control Panel** and then **Network Connections**. Then right-click (NOT left-click) **Local Area Connection**, select **Properties**, highlight your NIC card's **TCP/IP** entry (it should start with **TCP/IP** and have the characters **10/100**, **NIC**, or **Ether** in it – and not have the words **AOL**, **Dial-up**, or **Adapter**). Click **Properties** to display the Windows **TCP/IP Properties** dialog box.

**For Windows 2000:** From the desktop click the **Start** button, point to **Settings** and then **Network and Dial-up Connections**. Then right-click (NOT left-click) **Local Area Connection**, select **Properties**, highlight your NIC card's **TCP/IP** entry (it should start with **TCP/IP** and have the characters **10/100**, **NIC**, or **Ether** in it – and not have the words **AOL**, **Dial-up**, or **Adapter**). Click **Properties** to display the Windows **TCP/IP Properties** dialog box.

**For Windows 98 and Me:** From the desktop click the **Start** button, then point to **Settings** and then **Control Panel**. Double-click the **Network** icon to display the **Network** configuration screen. Highlight your NIC card's **TCP/IP** entry (it should start with **TCP/IP** and have the characters **10/100**, **NIC**, or **Ether** in it – and not have the words **AOL**, **Dial-up**, or **Adapter**). Click **Properties** to display the Windows **TCP/IP Properties** dialog box.

### **3 Windows Users Only: Enter the IP Settings.**

**For Windows 2000 and XP:**

Click the **Use the following IP address** and **Use the following DNS server addresses** buttons so that a black dot appears. Then enter the settings for **IP address**, **Subnet mask**, **Default gateway**, and **Preferred DNS server**. Most users can copy the information exactly as it is shown in the chart below. However, **if you chose an IP address in Step 1 other than 10.2.2.16**, enter the number that you chose instead of 10.2.2.16. When done, click **OK** and **continue with Step 6**.

IP address	10.2.2.16
Subnet mask	255.255.255.0
Default gateway (V3's LAN IP address)	10.2.2.2
Preferred DNS server	10.2.2.2

**For Windows 98 and Me:**

Click **Specify an IP Address** and enter the settings for **IP Address** and **Subnet Mask** shown below, unless you chose an IP address in Step 1 other than 10.2.2.16, in which case you should enter the number that you chose instead of 10.2.2.16.

<b>IP address</b>	<b>10.2.2.16</b>
<b>Subnet mask</b>	<b>255.255.255.0</b>

Now click the **DNS Configuration** tab at the top of the menu. Then click **Enable DNS**. Enter any name (i.e., your name, the words “My Computer”, a favorite word, or any other letters or numbers) in the box labeled **Host**: A **Host**: name is required.

Fill in the **DNS Server Search Order** box with the number **10.2.2.2**, click **Add**, and then click the **Gateway** tab. Fill in the **New gateway**: box with the number **10.2.2.2**, click **Add**, and then **continue with Step 6**.

#### **4 Macintosh Users Only: Open the TCP/IP Pane or Window and enter the IP settings.**

##### **For Mac OS X:**

From the **Dock**, choose **System Preferences** and then **Network** to display the **Network** pane. (For OS X 3, you also have to click the **Configure** button.)

Under the **TCP/IP** tab, highlight **Manually** in the **Configure**: list box and enter the settings for **IP Address**, **Subnet Mask**, **Router**, and **DNS Servers** as shown below, **unless you chose an IP address in Step 1 other than 10.2.2.16**, in which case you should enter the number that you chose instead of 10.2.2.16. When done, click **Save** or **Apply Now**, and **continue with Step 6**.

<b>IP Address</b>	<b>10.2.2.16</b>
<b>Subnet Mask</b>	<b>255.255.255.0</b>
<b>Router</b> (V3's LAN IP address)	<b>10.2.2.2</b>
<b>DNS Servers</b>	<b>10.2.2.2</b>

##### **For Mac OS 7.6.1 – 9.2.2:**

From the **Apple** menu, choose **Control Panels** and then **TCP/IP** to display the **TCP/IP** Window. Under the **TCP/IP** tab, highlight **Manually** in the **Configure:** list box and enter the settings for **IP Address, Subnet mask, Router address, and Name server addr.** shown below, **unless you chose an IP address in Step 1 other than 10.2.2.16**, in which case you should enter the number that you chose instead of 10.2.2.16. When done, close the Window and you will be prompted to click **Save**. Then **continue with Step 6**.

IP address	10.2.2.16
Subnet mask	255.255.255.0
Router address (V3's LAN IP address)	10.2.2.2
Name server addr.	10.2.2.2

## 5 **Red Hat Linux Users Only:**

- a **Edit /etc/sysconfig/network-scripts/ifcfg-eth0 so that it contains the following lines:**

```

DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
BROADCAST=10.2.2.255
NETMASK=255.255.255.0
IPADDR=10.2.2.16
GATEWAY=10.2.2.2
NETWORK=10.2.2.0

```

- b **Then edit or create /etc/resolv.conf so that it contains the following line:**

```

NAMESERVER=10.2.2.2

```

Note:

If you are using another version of Linux and you are unsure how to enter this information, consult the help file or documentation that came with your operating system.

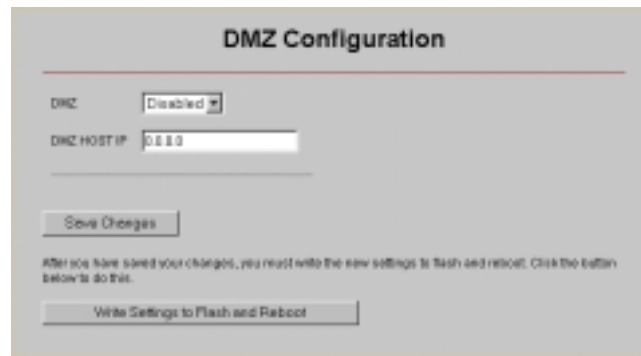


c Continue with Step 6.

**6 All Users: Go back to the V3's Advanced Setup page and click the DMZ button to open the DMZ Configuration page.**

If you already closed the **Zoom Configuration Manager**, double-click the Zoom V3 icon on your desktop (or type 10.2.2.2 in your Web browser) and click the **Advanced Setup** icon.

**7 Configure the DMZ.**



Select **Enable** from the **DMZ** list, and enter **10.2.2.16** in the **DMZ Host IP** box. Click **Save Changes** and then click **Write Settings to Flash and Reboot**. You're done!

Important:  
Outside users will need to know the V3's **WAN IP address**. To find this address, click the **System Status** icon at the top of any **Zoom Configuration Manager** page and scroll down to the **WAN Status** section.

# 4

## Using the V3's Advanced Firewall

---

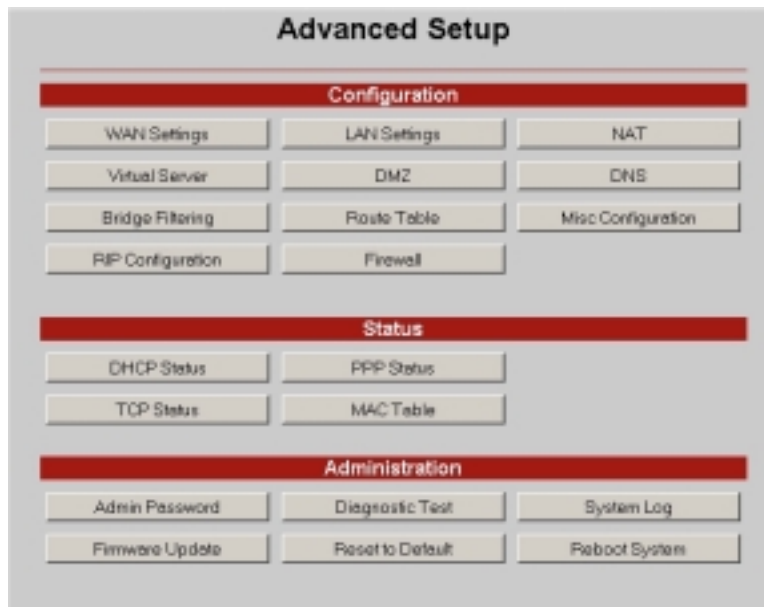
*This chapter describes the V3's advanced firewall and the types of protection it offers. If you are like most users, you probably will not need to modify your firewall settings. If, however, you are an administrator or an expert user who wants to customize the firewall to protect a network against specific threats, you should refer to this chapter.*

You can think of the firewall as playing a role like that of a guard at the gate of an ancient walled city. The guard has a great scroll, which lists allowed and proscribed traffic. In one possible set of rules, visitors may enter only if they show an invitation from a citizen of the city. Children may not leave the city. The guard may allow entry of carts of flour, but only for delivery to the bakery. Any messenger who doesn't know the password to the city is thrown in the moat, and can't pass through the gate.

You may set the policies of your firewall, which is like writing the rules on the great scroll in the example. The firewall will then follow the rules, acting like the guard. Instead of controlling entry and exit of goods and people, you control entry and exit of particular types of IP packets. In general, you will want to do this to prevent unwanted packets from entering your network (this is the purpose of the wall in the first place).

By default, the firewall will allow only those packets to enter that you are likely to need; for example, in response to a request for a web page, or as part of a VoIP call you make. You may want to accept other, specific packets, perhaps to facilitate Internet gaming, or because you want people outside your network to access a server you have set up. You may want to prevent some users from accessing the Internet at all.

To access the V3's firewall settings, from the **Advanced Setup** page, click the **Firewall** button. (If you have exited from the V3 and have forgotten how to establish communication with it, refer to page 15.)



The main Firewall page displays.

**Note:** If you ever want to disable the advanced firewall, there is an option to do so at the bottom of the page.



## 4.1 Main Firewall Features

The V3's (DoS) Denial of Service firewall features are grouped together in the top section, under **Advanced Options**. These DoS features mean that the V3 provides protection from a potentially devastating attack on your computer. Such attacks can overwhelm and shut down a computer or a server. The V3's DoS features are grouped together as follows:

- Protection Policy
- Hacker Log
- Service Filtering.

### *Protection Policy*

Click the **Protection Policy** link to display the basic and advanced protections. Protection policies provide a defense from the most common methods of tampering with the security of a network. All the defense mechanisms listed below are enabled by default.



<b>IP Spoof checking</b>	Inspects so-called “trusted” IP addresses to ensure legitimacy.
<b>Ping of Death checking</b>	Prevents oversized ping packet fragments (totaling more than 65,536 bytes) from getting through—which cause the computer to hang or crash.
<b>Land Attack checking</b>	Guards against attackers who mimic source and destination ports and IP addresses, causing infinite loops and system crashes.
<b>Reassembly checking</b>	Ensures correct reassembly of datagrams—prevents attackers from sending a continuous stream of identical, invalid datagram fragments that can cause system state problems.
<b>SYN (synchronize) Flooding checking</b>	Prevents attackers from flooding the system with incomplete synchronization connection requests, which can exhaust server resources and cause operating system crashes.
<b>ICMP Redirection checking</b>	Keeps route information hidden, ensuring that ICMP messages cannot be compromised, or forged, and redirected to the attacker’s destination of choice.
<b>Source Routing checking</b>	Prevents attackers from illegally obtaining network data by stipulating that data packets must follow strict source routing.
<b>Winnuke checking</b>	Only applicable to Windows 95, NT, and 3.11 systems. Prevents OOB (out of band) data from reaching an IP address, which can cause lost connections and system crashes.

## Hacker Log

Whenever the firewall prevents a packet from being delivered because of a perceived security threat, the **Hacker Log** feature keeps track. You have the option of specifying which types of messages are logged in and displayed. **Note:** These options are directly related to the **Protection Policy** page described above.

<p><b>Alert Log</b></p>	<p>Click to add any of these types of attacks—SYN Flooding, Ping of Death, IP Spoofing, Win Nuke—to the log entries in the system log of policy violations. (To view the log, go to the <b>Advanced Setup</b> page and click <b>System Log</b>.)</p>
<p><b>Log Database Properties</b> <b>Log Frequency</b></p>	<p>You have the option of selecting how often a particular type of hacker event can occur before the V3 generates a system log entry. The default is every 100 records or events. Available range is 1-65535 records/events.</p>
<p><b>General Log</b></p>	<p>Click to add General Attacks, Deny Policies, or Allow Policies to the log entries in the system log of policy violations. (To view the log, go to the <b>Advanced Setup</b> page and click <b>System Log</b>.) General Attacks are those most likely to occur—Land Attack, Reassembly Attack, ICMP Redirection, and Source Routing. Deny Policy and Allow Policy are tied to inbound and outbound firewall policies (see page 56).</p>

Once you've made your selections, click **Save Changes** and **Write Settings to Flash and Reboot**.

## *Service Filtering*

The Service Filtering feature lets you give certain users permission to access the V3 from outside the network—that is, over the Internet. If you enable one of the services listed on this page, the V3's firewall will open up the appropriate port to allow the service to work.

<b>PING from External Network</b>	Disabled by default. Enable it to allow an external user to ping your V3. This can be useful if you need to troubleshoot your unit.
<b>FTP from External Network*</b>	Disabled by default. Enable it to allow an external user to ftp into your V3. Typically, you would do this if you wanted someone to check the V3's configuration.
<b>DNS from External Network</b>	Disabled by default. Enable it to allow your V3 to accept DNS requests from an external source.
<b>IKE from External Network</b>	Disabled by default. Enable it to allow a VPN (virtual private network) connection to your network.
<b>RIP from External Network</b>	Disabled by default. Enable it to allow your V3 to receive RIP (Routing Information Protocol) requests from an external source. The Technical Reference Manual contains details about RIP; go to <b><a href="http://www.zoom.com">www.zoom.com</a></b>
<b>DHCP from External Network</b>	Disabled by default. Enable it to allow your V3 to receive DHCP requests from an external source.

**\*Important:** To complete the step of allowing remote users to FTP into the V3, you must go to the V3's **Advanced Setup** page, click the **Misc. Config.** button, and do the following: Enable FTP Server in the dropdown list and **uncheck** the box "**Disable WAN side FTP access.**" FTP must be enabled in both places for this feature to work.

Once you've made your selections, click **Save Changes** and **Write Settings to Flash and Reboot.**

## 4.2 Creating Inbound/Outbound Policies

The V3 offers ways to tailor, or restrict, incoming and outgoing Internet traffic to increase security. Your V3 comes with three inbound/outbound policies preconfigured for VoIP: 1) SIP Port 5060; 2) RTP Media Base 5000; 3) TFTP Port 60.

To create additional policies, from the main **Firewall** page, click the **Inbound Policy** or **Outbound Policy** link, depending on what you want to do.

**Tip:** When setting up policies, it may help to think of inbound and outbound policies as mirror images of each other. In each case, the source and destination IP addresses, subnet masks, and ports are reversed. That is, for an inbound policy, the source address appears on the WAN side, and the destination appears on the LAN side; for an outbound policy, the source is on the LAN side and the destination is on the WAN side.



## Inbound Policies

Inbound firewall policies allow you to filter the traffic that arrives over the Internet—from the WAN side to the V3 LAN side—based on rules that you set up.

**Firewall Inbound Policy**

No Entries in Inbound Policy Database

... Adding New Policy ...

Src IP: [ ] - [ ] Any IP [v] DB: [None v]

Dest IP: [ ] - [ ] Any IP [v] DB: [None v]

Src Port: [ ] - [ ] Any Port [v]

Dest Port: [ ] - [ ] Any Port [v] DB: [None v]

Transport Protocol: [All Protocol v]

Filtering Action: [Allow v]

Time Window Filtering: [None v]

Add/Modify Inbound Policy

<b>Src IP</b>	Source IP address to which this rule should apply.*
<b>Dest IP</b>	Destination IP address to which this rule should apply.*
<b>Src Port</b>	Source Port number to which this rule should apply.*
<b>Dest Port</b>	Destination Port number to which this rule should apply.*
<b>Transport Protocol</b>	Protocol to be used. Choices are All, TCP, UDP, ICMP, AH, ESP, GRE.
<b>Filtering Action</b>	Choices are Allow or Deny.
<b>Time Window Filtering</b>	Default is none. If you set up Time Groups (see page 62), they appear in this list as options.

<b>DB</b>	Short for Database. Default is none. If you set up IP Groups or Service Groups (see page 60 and 62), they appear in this list as options.
-----------	---

*\*For each of these fields, choices are any IP address, a single IP address, an IP range, or a mask range.*

Once you have entered all applicable information, click **Add Inbound Policy**. From the subsequent page that displays, you can move or edit this policy using the **Up**, **Dn** (short for Down), **Edit**, and **Delete** buttons. **Important:** The firewall applies all inbound policies in a top-down order according to their location in the policy table. Once you have completed the creation of your rules, use the **Up** and **Dn** buttons to put them in order in the table from top to bottom. You can always add an **All** policy at the bottom of the list, so that if there are any packets that don't match any of the above policies in the list, they will be denied (if you set up **Deny All**), or permitted (if you set up **Allow All**).

### Outbound Policies

Outbound firewall policies allow you to filter the traffic that users inside the firewall—on the V3's LAN side—are allowed to send out over the Internet—to the WAN side.



<b>Src IP</b>	Source IP address to which this rule should apply.*
---------------	---

<b>Dest IP</b>	Destination IP address to which this rule should apply.*
<b>Src Port</b>	Source Port number to which this rule should apply.*
<b>Dest Port</b>	Destination Port number to which this rule should apply.*
<b>Transport Protocol</b>	Protocol to be used. Choices are All, TCP, UDP, ICMP, AH, ESP, GRE.
<b>Filtering Action</b>	Choices are Allow or Deny.
<b>Time Window Filtering</b>	Default is none. If you set up Time Groups (see page 62), they would appear in this list as options.
<b>DB</b>	Short for Database. Default is none. If you set up IP Groups or Service Groups (see page 60 and 62), they would appear in this list as options.

*\*For each of these fields, choices are any IP address, a single IP address, an IP range, or a mask range.*

Once you have entered all applicable information, click **Add Outbound Policy**. From the subsequent page that displays, you can move or edit this policy using the **Up**, **Dn** (short for Down), **Edit**, and **Delete** buttons. **Important:** The firewall applies outbound policies in a top-down order according to their location in the policy table page. Once you have created all your rules, or policies, use the **Up** and **Dn** buttons to put them in order in the table from top to bottom. You can always add an **All** policy at the bottom of the list, so that if there are any packets that don't match any of the above policies in the list, they will be denied (if you set up **Deny All**), or permitted (if you set up **Allow All**).

## 4.3 Setting Up Firewall Databases

The V3 includes options to set up databases of user information, so you can create different combinations of user groups. Drawing from these groups, or databases, you can then create and apply certain inbound and outbound policies and restrict Internet traffic. For example, if you don't want your children accessing the Internet during the day, you can set up a time group that blocks access from 8am to 5pm. For instructions on how to create inbound and outbound policies, refer to the section above.

- IP Group
- Service Group
- Time Group.

### *IP Group*

The **IP Group** page lets you specify IP addresses and subnet masks and assign a group name to them. That way, you can create a set of inbound and outbound firewall policies pertaining to multiple individuals simultaneously. For example, if you have a small office and you don't want certain computers (or users) to have Internet access, you can set up an IP group that includes those computers and then set up an outbound policy that blocks Internet access for that IP group.

Firewall IP Group

No Entries in IP Group Database

IPMask	IP Entry Name	IP addr. 1	IP addr. 2
Single IP			

Add/Modify this entry

Save Changes

After you have saved your changes, you must write the new settings to flash and reboot. Click the button below to do this.

Write Settings to Flash and Reboot

<b>IP/Mask</b>	There are three ways to use this database. Choices are <b>Single IP</b> , <b>IP Range</b> , or <b>Subnet Mask</b> . Your selection depends on whether you want to specify one IP address for an entire group, a range of IP addresses for a group, or a range of subnet masks for a group.
<b>IP Entry Name</b>	Name of your choosing. Purpose is to identify the IP group you want to set up. Maximum field length=19 characters.
<b>IP addr.1</b>	<p>IP address that you want to assign to a group.</p> <p>If you selected <b>Single IP</b>, enter that IP address here.</p> <p>If you selected the <b>IP Range</b> option because you want to designate a range of addresses, enter the beginning of the range here and enter the ending range in the <b>IP addr.2</b> field.</p> <p>If you selected the <b>Subnet Mask</b> option, enter the desired IP address here and enter the subnet mask in the <b>IP addr.2</b> field. All addresses falling within that subnet will be included in the group you set up.</p>
<b>IP addr.2</b>	<p>If you are using the <b>Single IP</b> option, this field is not applicable.</p> <p>If you are using the <b>IP Range</b> option, enter the end of the IP address range here. Note: <b>IP addr.1</b> has to contain the beginning of the range.</p> <p>If you are using the <b>Subnet Mask</b> option, enter the subnet mask here. The subnet mask divides IP addresses into groups. In the <b>IP addr.1</b> field, you must enter an IP address of the group that you want in the database. All IP addresses within the same group as the address in the <b>IP addr.1</b> field will be affected.</p> <p>For example, if you enter the IP address 192.168.0.1 in the <b>ip addr.1</b> field and the subnet mask 255.255.255.0 in the <b>ip addr.2</b> field, the group will include the addresses 192.168.0.1 to 192.168.0.255 (for a total of 255 addresses). If you enter the IP address 192.168.0.1 in the <b>ip addr.1</b> field, and the subnet mask 255.255.255.240 in the <b>ip addr.2</b> field, the group will include the addresses 192.168.0.1 to 192.168.0.15 (a total of 15 addresses).</p>

Once you have filled in these fields, click **Add/Modify this entry**. A new page displays, showing the new entry at the top, with two buttons **Modify** and **Delete**. You can change or delete this entry at any time. From this page, you can also add new entries.

## Service Group

The Service Group page lets you specify a port and assign a group name to it. This is useful if you want to identify a group by a particular port. You can then use that service group when creating an inbound or outbound policy.

<b>Service Entry Name</b>	Name of your choosing. Purpose is to identify the group that you want to assign to a particular port. Maximum field length=19 characters.
<b>TCP/UDP</b>	Specify which protocol this group should use, TCP (Transmission Control Protocol) or UDP (User Datagram Protocol).
<b>Port #</b>	Port number of your choosing that should be associated with this group.

Once you have filled in these fields, click **Add/Modify this entry**. A new page displays, showing the new entry at the top, with two buttons **Modify** and **Delete**. You can change or delete this entry at any time. From this page, you can also add new entries.

## Time Group

The **Time Group**, or **Time Window**, page lets you specify a particular time period and assign a group name to it. For example, if you don't want your children accessing the Internet during the day, you can set up a time group that blocks Internet access from 8am to 5pm. Time windows are useful when configuring inbound and outbound firewall policies for a particular group of individuals.

**Firewall Time Group**

*No Entries in Time Window Database*

Time Window Name	Time Period	
	from Monday 01 00 AM to Monday 01 03 AM	<input type="button" value="Add/Modify this entry"/>

<b>Time Window Name</b>	Name of your choosing. Purpose is to identify the group that you want to associate with a given time period. Maximum length=19 characters.
<b>Time Period</b>	Starting and ending time window—day, hour, minute, and AM or PM.

Once you have filled in these fields, click **Add/Modify this entry**. A new page displays, showing the new entry at the top, with two buttons **Modify** and **Delete**. You can change or delete this entry at any time. From this page, you can also add new entries.

# Appendix A

## DSL Internet Settings Tables

---

*You can use the information in these tables if you need help making your DSL selection on page 16.*

*Many DSL providers use different settings depending on the region in which they are operating, which is why there may be more than one setting for your service provider. The setting for your service provider labeled (1) is the most commonly used setting and should be tried first. The next most common is labeled (2), and so on. You may have to try more than one setting, which is why it is better to get the correct setting from your service provider if possible.*

*If your service provider is not shown, and the settings for **Service Provider Not Shown** don't work, try the settings for the company that provides local phone service in your area.*



<b>USA Service Providers</b>	<b>DSL Connection Type</b>
AllTel (1)	PPPoE
AllTel (2)	1483
August.net (1)	1483
August.net (2)	1483
BellSouth	PPPoE
CenturyTel (1)	PPPoE
CenturyTel (2)	1483
Covad	PPPoE
Earthlink (1)	PPPoE
Earthlink (2)	PPPoE
GWI	1483
Qwest (1)	PPPoA
Qwest (2)	PPPoA
SBC (1)	PPPoE
SBC (2)	1483
SBC (3)	1483
Sprint (1)	PPPoA
Sprint (2)	PPPoE
Verizon (1)	PPPoE
Verizon (2)	1483
<b>Service Provider Not Shown</b>	PPPoE

<b>Outside USA</b>	<b>DSL Connection Type</b>
Australia-Telstra	PPPoA
Argentina	PPPoA
Belgium-ADSL Office	1483
Belgium-Turboline	PPPoA
Bolivia	1483
Colombia - EMCALI	PPPoA
Denmark-Cybercity, Tiscali	PPPoA
France (1)	PPPoE
France (2)	PPPoA
France (3)	PPPoA
Germany	PPPoE
Hungary-Sci-Network	PPPoE
Iceland-Islandssimi	PPPoA
Iceland-Siminn	PPPoA

Israel	PPPoA
Italy	PPPoA
Jamaica (1)	PPPoA
Jamaica (2)	1483
Kazakhstan	PPPoA
Netherlands-BBNED	PPPoA
Netherlands-MX Stream	PPPoA
Portugal	PPPoE
Saudi Arabia (1)	PPPoE
Saudi Arabia (2)	PPPoE
Saudi Arabia (3)	1483
Saudi Arabia (4)	1483
Saudi Arabia (5)	1483
Saudi Arabia (6)	1483
Spain-Albura, Tiscali	PPPoA
Spain-Colt Telecom, Ola Internet	PPPoA
Spain-EresMas, Retevision	PPPoA
Spain-Telefonica (1)	PPPoE
Spain-Telefonica (2), Terra	1483
Spain-Wanadoo (1)	PPPoA
Spain-Wanadoo (2)	PPPoE
Spain-Wanadoo (3)	1483
Sweden-Telenordia	PPPoE
Sweden-Telia	1483
Switzerland	PPPoE
Turkey(1)	PPPoE
Turkey(2)	PPPoA
UK (1)	PPPoA
UK (2)	PPPoE
Venezuela-CANTV	1483
Vietnam	PPPoE

# Appendix B

## VoIP Phone Installation Options

---

*Your V3 gateway makes it easy to make both VoIP calls over the Internet and regular phone calls using your standard phone service. You can plug a single telephone into the V3's **PHONE** jack. You may prefer to connect more than one phone to the V3 so that you can make VoIP calls from other rooms. You have a choice of two ways to accomplish this without running wires.*

- *Plug Multiple Phones Directly into the V3*
  - *Use Cordless Phones to Link to the V3*
- Each of these ways is very easy and virtually foolproof.*

### ***Plug Multiple Phones Directly into the V3***

If you want more than one phone near the V3—in a small office, for example—you can use standard telephone adapters to connect multiple phones. These adapters are called T-adapters or 2-jack modular adapters; many people use them to plug in their answering machines. You can plug in as many phones as you'd like. (If you plug multiple phones directly into the V3, just be sure that when you add up all their Ringer Equivalence Numbers (RENs), the total is 5 or lower. Virtually all phones show the REN somewhere. Most phones have a REN that's 1 or lower.)

### ***Use Cordless Phones to Link to the V3***

If you have a cordless phone that has more than one handset, simply plug the base station into the V3—you can then make VoIP and regular calls using all the handsets.

**Note:** If you have a wireless network that operates over the typical 2.4GHz frequency and you want to use cordless phones, it is best if you use 900MHz or 5GHz phones; that way, you will minimize any chance of interference.

# Appendix C

## Mac and Linux Users: Setting TCP/IP Network Settings

---

*If you are using the Linux operating system, or if you are using a Macintosh computer, you must ensure that your computer's network, or TCP/IP, settings are configured correctly.*

*Otherwise, you will not be able to connect to the Internet.*

*Windows automatically configures your network settings, so you don't have to perform this task.*

*Linux users: Turn to page 69.*

*Macintosh users: Continue below.*

### **Macintosh TCP/IP Settings**

Depending on your Mac OS, the directions to configure your Macintosh's network settings will differ. For OS X, follow the instructions below. Otherwise go to page 69.

For Mac OS X

- 1 From the **Dock**, choose **System Preferences** and then **Network** to display the **Network** pane. (For OS X 3, you also have to click the **Configure** button.)
- 2 From the **Location:** list box, make sure **Automatic** is selected.
- 3 Under the **Show** drop-down tab, choose **Built-in Ethernet**.
- 4 Under the **TCP/IP** tab, make sure that **Using DHCP** is highlighted in the **Configure:** list box. Do not enter anything into the **DHCP Client ID** field.
- 5 Click **Apply Now** (or **Save** if prompted) and close the **Network** pane.
- 6 For Mac OS X, you're done with your network settings. Now return to **Configuring Your V3** on page 14.

For Mac OS 7.6.1 - 9.2.2

- 1 From the **Apple** menu, choose **Control Panels** and then **TCP/IP** to display the **TCP/IP** Window.
- 2 Under **Connect via:**, select **Ethernet built-in**.  
Under **Configure:**, select **Using DHCP Server**.  
Do not enter anything in the **DHCP Client ID** field.
- 3 Close the **TCP/IP** Window. You will be asked if you want to save the changes. Click **Save**.
- 4 Now return to **Configuring Your V3** on page 14.

### *Linux TCP/IP Settings*

The instructions for setting up boot-time DHCP vary dramatically by distribution, so you may want to refer to your particular version's documentation.

Note: If you have more than one network card installed, you will need to pick distinct Ethernet identifiers for each (eth0, eth1, eth2, etc.). If you select an identifier other than eth0 for your ADSL modem, use that identifier throughout.

For RedHat

Edit or create `/etc/sysconfig/network-scripts/ifcfg-eth0` so that it contains the following three lines:

```
DEVICE=eth0  
ONBOOT=yes  
BOOTPROTO=dhcp
```

For SuSE

Edit the file `/etc/rc.config`; search for the variables **NETCONFIG**, **NETDEV\_0**, and **IFCONFIG\_0**.

Set them as follows (see the instructions in `rc.config`):

```
NETCONFIG="_0"  
NETDEV_0="eth0"  
IFCONFIG_0="dhcpcplient"
```

Reboot with this command: `/sbin/shutdown -r now`.

For Debian

Add this line to the file `/etc/network/interfaces`: **iface eth0 inet dhcp**. Reboot with this command: `/sbin/shutdown -r now`.

Now return to **Configuring Your V3** on page 14.

# Appendix D

## Troubleshooting

---

*Our Technical Support staff is ready to help you with any questions you may have. However, if you are having trouble, you may find an easy solution below. Otherwise, refer to the Frequently Asked Questions (FAQs) on the CD (click **Support**), or visit our web site for the latest tips: [www.zoom.com](http://www.zoom.com)*

### Connection Troubleshooting Tips

In order to troubleshoot your Internet connection problem, we recommend you first determine if the V3 has a WAN IP address or not. The first tip below tells you how to determine if you have a WAN IP address. Depending on your answer, we will recommend other troubleshooting steps you should take to solve the problem.

**If you can't connect to the Internet, first make sure that you have a WAN IP address:**

Go to the V3's **System Status** page and click **WAN Status**. You should see a WAN IP address listed.

To get to the V3's **System Status** page, double-click the **Zoom** icon on your desktop (or type **10.2.2.2** in your Web browser).

Then log in by entering the User Name **admin** and the Password **zoomvoip**, and click the **System Status** icon.

**If you have a WAN IP address, skip to page 72.**

**If you don't have a WAN IP address and you are using a Cable Modem or a DSL PPPoA or 1483 Modem, your next step should be to do a Release/Renew operation.**

- 1** Go to the V3's **Advanced Setup** page and click **WAN DHCP Status**.
- 2** Select **Release** and click **Save Changes**.
- 3** Select **Renew** and click **Save Changes**.
- 4** **Go to your Web browser** (i.e., Internet Explorer or Netscape Navigator) and **try to connect** to a familiar Web address. If you are unsuccessful, check to see if you have a WAN IP address (see page 71). If you do not, you should contact Zoom Technical Support.

**If you have a WAN IP address, but can't connect to the Internet, make sure that:**

**Your Ethernet or USB cable connections are okay.**

Check that the appropriate V3 front panel light is lit (**LAN 1, 2, 3, or 4** or **USB**). This will confirm that the connection is good.

**Your WAN connection is okay.**

Check that the V3 front panel **LINK** light is lit. This will confirm that the connection to your cable or DSL modem is good.

**Your computer's TCP/IP properties are correct.**

**Macintosh users:** TCP/IP instructions are on page 68.

**Linux users:** TCP/IP instructions are on page 69.

**Windows users:**



**1** First open the Windows **TCP/IP Properties** dialog box. How you do this depends on your version of Windows:

—**For Windows 2000:** From the desktop click the **Start** button, point to **Settings** and then **Network and Dial-up Connections**. Then right-click (NOT left-click) **Local Area Connection**, select **Properties**, highlight your NIC card's **TCP/IP** entry (it should start with **TCP/IP** and have the characters **10/100**, **NIC**, or **Ether** in it – and not have the words **AOL**, **Dial-up**, or **Adapter**). Click **Properties** to display the Windows **TCP/IP Properties** dialog box.

—**For Windows XP:** From the desktop click the **Start** button, point to **Control Panel** and then **Network Connections**. Then right-click (NOT left-click) **Local Area Connection**, select **Properties**, highlight your NIC card's **TCP/IP** entry (it should start with **TCP/IP** and have the characters **10/100**, **NIC**, or **Ether** in it – and not have the words **AOL**, **Dial-up**, or **Adapter**). Click **Properties** to display the Windows **TCP/IP Properties** dialog box.

—**For Windows 98 and Me:** From the desktop click the **Start** button, then point to **Settings** and then **Control Panel**. Double-click the **Network** icon to display the **Network** configuration screen. Double-click NIC card's **TCP/IP** entry (it should start with **TCP/IP** and have the characters **10/100**, **NIC**, or **Ether** in it – and not have the words **AOL**, **Dial-up**, or **Adapter**) to display the **TCP/IP Properties** dialog box.

**2** If you are using DHCP (most users), check that your DHCP settings are okay. If you are using a static IP address, skip to Step 3.

**For Windows 2000 and XP:**

Make sure that “**Obtain an IP address automatically**” is selected on the **General** tab and that “**Obtain a DNS server address automatically**” is selected on the **DNS Configuration** tab. All fields should be blank.

**For Windows 98 and Me:**

Make sure that “**Obtain an IP address automatically**” is selected at the **IP Address** tab and that “**Enable DNS**” is selected on the **DNS Configuration** tab. All fields should be blank.

### **3 If you are using a static IP address, check that your IP settings are okay.**

#### **For Windows 2000 and XP:**

Click the **Use the following IP address** and **Use the following DNS server addresses** buttons so that a black dot appears. Then enter the settings for **IP address**, **Subnet mask**, **Default gateway**, and **Preferred DNS server** assigned by your provider.

#### **For Windows 98 and Me:**

Click **Specify an IP address** and enter the settings for **IP Address** and **Subnet Mask** as assigned by your provider.

Now click the **DNS Configuration** tab. Then click **Enable DNS**. Enter any name (i.e., your name, the words “My Computer”, a favorite word, or any other letters or numbers) in the box labeled **Host:**. A **Host:** name is required.

Fill in the **DNS Server Search Order** box with the number **10.2.2.2**, click **Add**, and then click the **Gateway** tab near the top of the page. Fill in the **New gateway:** box with the number **10.2.2.2**, and click **Add**.

#### **Your service provider’s broadband connection is functioning properly.**

Unplug the Ethernet cable that you plugged into the V3’s **WAN** jack (the one that you unplugged from your PC). Plug it back into the PC and see if you are able to connect to the Internet. If you are not able to connect, contact your service provider.

- Your service provider’s broadband connection is functioning properly by placing a call to customer support.

**I type http://10.2.2.2 into my Web browser’s address bar, but the V3’s Network Password box won’t open so I can’t communicate with the V3.**

- If you are using a Macintosh or Linux computer, your Internet settings may need adjustment; turn to page 68 for instructions.
- If you are using Mac OS X 10.3 and above, renew your IP address: Go to **System Preferences | Network**. Click the **Configure** button and then the **Renew DHCP Lease** button.
- If you are using a Windows computer, perform a Release/Renew operation.

For Windows 2000/XP: From the desktop, click **Start | (All) Programs | Accessories | Command Prompt**. Then type **ipconfig /all** and press Enter. In the subsequent dialog box, make sure the NIC adapter is highlighted in the dropdown list, click **Renew** and then click **Release**. Then type **10.2.2.2** into your browser's address bar, and the Network Password box should display.

For Windows 95/98/Me: From the desktop, click **Start | Run**, type **winipcfg**, and click **OK**. In the subsequent dialog box, make sure the NIC adapter is highlighted in the dropdown list, click **Renew** and then click **Release**. Then type **10.2.2.2** into your browser's address bar, and the Network Password box should display.

## VoIP and Phone Troubleshooting Tips

**When I pick up the phone and press #, I don't get a VoIP dial tone.**

- Your V3 may be in VoIP only mode. If so, you shouldn't press # to begin a call. See page 19 for instructions on changing modes.
- Your Internet Protocol connectivity may not be working. Try browsing the Internet. If you can't, refer to the **Connection Troubleshooting Tips** above.
- Check that your VoIP service is properly configured.

- If your service supports automatic configuration downloads, go to the V3's **VoIP** page to see if the V3 has received a configuration download. If not, press the **Download Configuration Now** button, or reboot the V3.
- If your service doesn't support automatic configuration downloads, double-check all the settings for your account and service provider on the **VoIP** page and **Advanced VoIP Setup** page. Check the **User ID**, **Authorization ID**, **Password**, **Domain/Realm**, and **SIP Proxy Address** in the appropriate boxes. These five boxes must be filled in correctly. Also check with your service provider to see if **STUN** should be enabled. If so, enable **STUN** and enter a server and port address.

If none of the above helps, contact your VoIP service provider

**When I try to make a VoIP call to another VoIP phone, the call doesn't go through.**

The person or persons you are calling may not be available. Try again later. Or, if there is a chance you may have the wrong number, go to the provider's Web site and check the directory.

Check if the person you are trying to call uses the same VoIP service as you. If not:

- You will have to precede your call by dialing a code for that person's VoIP service. Ask the person you are attempting to call for the code, or check the service provider's web site for a list.
- In some cases, there may not be a way to make direct VoIP calls from your service to people subscribing to another VoIP service. Check the web site, or email your provider.

**When I try to make a VoIP call to a standard PSTN number, the call doesn't go through.**

Make sure that:

- You have signed up for PSTN service with your VoIP service provider. Contact your provider's customer support department if necessary.

- You are dialing according to the guidelines your service provider gave you. Your provider's web site should provide instructions and examples. For instance, you may need to dial local calls as though they were long distance. Or, you may need to dial a call within your country as though you were calling from outside the country—beginning with an international prefix such as 00, followed by the country code, city code or area code, and local number.
- You aren't taking too long between digits when you dial a number. If you take a very long time, the V3 may register that you have completed dialing before you are through. If this is a possibility, hang up and try again.

### **When I pick up the phone, I don't hear a dial tone.**

For aV3 used normally, the dial tone you hear when you first pick up your phone comes from the local phone company. Check that:

- You have installed any phone adapters required for your country.
- Your **TELCO** line is firmly plugged into the telephone wall jack.

If you have another phone jack for the same phone line, plug your phone into that jack and make sure you hear a dial tone. If you don't, contact your local phone service provider. If you do, then check that:

### **When some people call me, my Caller ID display doesn't work.**

Some phones that display caller ID are very sensitive to ring type. If you are using the VoIP version of the ring and tone sounds but find that the Caller ID display on your phone is unreliable, try switching back to the standard ring and tone configuration. See page 25 for instructions on changing your ring.

The Caller ID setting may not be set to the right value for your phone. You have one of two choices, Bell 212 or V.23. Go to the V3's **Advanced Voice** page and click the **Advanced VoIP Setup button** to check your setting.

Your service provider may not pass through caller information for all calls, in particular, DID calls to your VoIP connection that come from the PSTN. Check with your provider's customer support.

**My phone's ring sounds strange.**

If you don't like the ring for incoming VoIP calls, you can change it. Go to the V3's **VoIP** page and click **Select Tone & Ring by Country/Region** (see page 25 for instructions on changing your ring). **Note:** Some country selections include two choices, one of which is a special VoIP ring. This ring sounds a little different from the standard ring for that country or region.

**When I start to dial, I sometimes forget whether I'm dialing over the PSTN or over the Internet (VoIP).**

The V3 has a distinctive, lower-pitched dial tone when it is in VoIP mode, compared to the standard phone dial tone for your country. If you do not notice the V3's change in dial tone after you press # to begin a VoIP call, we recommend that you change your VoIP dial tone to make it more easily recognizable. See page 25 for help changing your ring tones.

# Appendix E

## Regulatory Information

---

### U.S. FCC Part 68 Statement

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. The unit bears a label on the back which contains among other information a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the telephone company.

This equipment uses the following standard jack types for network connection: RJ11C.

This equipment contains an FCC compliant modular jack. It is designed to be connected to the telephone network or premises wiring using compatible modular plugs and cabling which comply with the requirements of FCC Part 68 rules.

The Ringer Equivalence Number, or REN, is used to determine the number of devices which may be connected to the telephone line. An excessive REN may cause the equipment to not ring in response to an incoming call. In most areas, the sum of the RENs of all equipment on a line should not exceed five (5.0).

In the unlikely event that this equipment causes harm to the telephone network, the telephone company can temporarily disconnect your service. The telephone company will try to warn you in advance of any such disconnection, but if advance notice isn't practical, it may disconnect the service first and notify you as soon as possible afterwards. In the event such a disconnection is deemed necessary, you will be advised of your right to file a complaint with the FCC.

From time to time, the telephone company may make changes in its facilities, equipment, or operations which could affect the operation of this equipment. If this occurs, the telephone company is required to provide you with advance notice so you can make the modifications necessary to obtain uninterrupted service.

There are no user serviceable components within this equipment. See Warranty flyer for repair or warranty information.

It shall be unlawful for any person within the United States to use a computer or other electronic device to send any message via a telephone facsimile unless such message clearly contains, in a margin at the top or bottom of each transmitted page or on the first page of the transmission, the date and time it is sent and an identification of the business, other entity, or individual sending the message and the telephone number of the sending machine or of such business, other entity, or individual. The telephone number provided may not be a 900 number or any other number for which charges exceed local or long distance transmission charges. Telephone facsimile machines manufactured on and after December 20, 1992, must clearly mark such identifying information on each transmitted message. Facsimile modem boards manufactured on and after December 13, 1995, must comply with the requirements of this section.

This equipment cannot be used on public coin phone service provided by the telephone company. Connection to Party Line Service is subject to state tariffs. Contact your state public utility commission, public service commission, or corporation commission for more information.

### 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.

### Industry Canada Emissions Statement

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations. Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

### Industry Canada CS03 Statement

Notice: The Industry Canada label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing the equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of concern. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas. Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

Notice: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

### European Declaration of Conformity

The manufacturer declares under sole responsibility that this equipment is compliant to Directive 1999/5/EC (R&TTE Directive) via the following. This product is CE Marked.



Directive	Standard	Test Report
73/23/EEC-Low Voltage	EN 60950-1 : 2001 IEC 60950-1 :2001	electrical safety
89/336/EEC-EMC	EN 55022 : 1998/A1:2000/A2:2003 EN 55024 : 1998/A1:2001/A2:2003	EMC-emissions

### Electrostatic Discharge Statement

The unit may require resetting after a severe electrostatic discharge event.

Note: If you do not use the supplied phone cord, use an equivalent of minimum AWG 26 line cord.

Note: The V3's WAN port is not allowed to connect directly to the telecommunications network.





## Declaration of Conformity

We, the undersigned,

<b>Company</b>	Zoom Technologies, Inc.
<b>Address, City</b>	207 South Street, Boston, Massachusetts 02111
<b>Country</b>	USA
<b>Phone number</b>	617 423 1072
<b>Fax number</b>	617 542 8276

certify and declare under our sole responsibility that the following equipment:

<b>Product description / Intended use</b>	
<b>EU / EFTA member states intended for use</b>	EU: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, The Netherlands, Portugal, Spain, Sweden, United Kingdom EFTA: Switzerland, Iceland, Liechtenstein, Norway
<b>Member states with restrictive use</b>	None
<b>Manufacturer</b>	Zoom Technologies, Inc.
<b>Brand</b>	Zoom V3 VoIP Gateway/Router
<b>Type</b>	Series 0225; Models 5567, 5570, 5577, 5580, 1612, 1615, 1622, 1625, 9222, 9225, 9232, 9235

is tested to and conforms with the essential requirements for protection of health and the safety of the user and any other person and Electromagnetic Compatibility, as included in following standards:

Standard	Issue Date
EN60950-1	2001
IEC60950-1	2001
EN55022	1998/A1:2000/A2:2003
EN55024	1998/A1:2001/A2:2003

and therefore complies with the essential requirements and provisions of the **Directive 1999/5/EC** of the European Parliament and of the council of March 9, 1999 on Radio equipment and Telecommunications Terminal Equipment and the mutual recognition of their conformity and with the provisions of Annex II (Conformity Assessment procedure referred to in article 10(3)).

The following Notified Body has been consulted in the Conformity Assessment procedure:

<b>Notified body number</b>	<b>Name and address</b>
N/A	

The technical documentation as required by the Conformity Assessment procedure is kept at the following address:

<b>Company</b>	Zoom Technologies, Inc.
<b>Address, City</b>	207 South Street, Boston, Massachusetts 02111
<b>Country</b>	USA
<b>Phone number</b>	617 423 1072
<b>Fax number</b>	617 542 8276



TCF/TF reference nr.	<b>0225-ITF</b>
Drawn up in	Boston, MA USA
Date	December 19, 2005
Name and position	 Andy Pollock, Hardware Engineering Manager





