

ZOOM

ADSL X6v

U S E R G U I D E



Important Safety Measures

- To reduce the risk of fire, use the supplied phone cord or an AWG 26 or larger UL-listed or CSA-certified phone cord.
- Do not use this product near water — for example, in a wet basement or next to a swimming pool.
- Avoid using a telephone (other than a cordless phone) during an electrical storm.
- Do not use the telephone to report a gas leak while you are in the vicinity of the leak.
- **WARNING:** If your modem has a removable antenna, attach only the antenna that was provided or an equivalent indoor antenna meeting local RF transmission regulations. **DO NOT** attach any antenna or antenna cable that has outdoor exposure.



Contents

Contents	3
Overview	7
Installation Instructions	8
Package Contents	8
Before You Begin	9
Installing the X6v	10
Windows Installation	10
Macintosh and Linux Installation	12
Installing the Hardware	13
Establishing Communication	15
Setting Up a Network	19
To Connect Additional Wired Computers	19
To Connect a Network Device	20
Universal Plug and Play	21
If You Need Help	21
Setting Up Your Wireless Network	22
Connecting a Windows Vista Computer with Built-in Wireless Capabilities	23
Connecting a Windows XP Computer with Built-in Wireless Capabilities	25
Connecting a Wireless-Enabled Computer to the X6v	26
Checking Your Settings	28
Setting Wireless Security	29
Overview	29
Setting Up Security Using WEP	29
Setting Up Security Using WPA2 or WPA	33
802.1x Authentication	35
Wireless Distribution System (WDS) Configuration	37
Wireless MAC Filtering	38

Setting Up VoIP Service.....	39
Using the Zoom Configuration Manager to Set Up VoIP Service	39
Changing Your VoIP Settings.....	44
Speed Dials.....	44
Call Forwarding.....	45
Ringing Based on Caller ID.....	45
Do Not Disturb	46
Call Waiting/Caller ID.....	46
Incoming Call Blocking.....	47
Outgoing Call Blocking.....	48
Advanced VoIP Configuration	49
VoIP System Settings	50
Date/Time	50
VoIP Subsystem Network Configuration.....	51
Static IP / DNS Configuration	51
HTTP/Telnet/FTP Server	52
STUN Settings	53
VoIP Parameters.....	54
Audio Settings.....	54
RTP Protocol Parameters.....	55
SIP Parameters.....	55
Regionalization Settings	56
SLAC Configuration	56
CODEC Configuration	57
Subscription Services	58
Dialing Parameters	58
Bridging from VoIP to PSTN.....	59
Bridging from PSTN to VoIP	64
Miscellaneous TELCO Parameters	68
Emergency Services.....	68
Controlling the X6v from Your Phone.....	70
Resetting Your VoIP Configuration	71

The X6v and Online Gaming.....	72
Setting Up the X6v for Online Gaming	73
Step 1: Choosing an IP Address for Gaming	73
Step 2: Setting Up a Virtual Server or DMZ	77
Setting Up a Virtual Server or DMZ on Your Computer	78
Setting Up a DMZ on an Xbox or Xbox 360.....	81
Setting Up a DMZ on a PlayStation 2 or 3.....	83
Using Router Setup	85
Viewing the Router Setup Options	86
Configuration Options	86
Status Options	89
Administration Options.....	89
Using the WAN Configuration Settings	91
Using the Ethernet Configuration Settings	97
Setting Up a Static Routing Table	98
Adding Extra Security with Advanced Firewall Filtering	100
Setting Security Logging	105
Configuring Intrusion Detection	106
Adding a DNS Server Name	109
Creating a Virtual Server or a DMZ	110
Using the ADSL Settings.....	112
Changing Your LAN Settings	113
Creating a Fixed (Static) IP Address	116
Assigning a Half Bridge Device.....	117
Enabling or Disabling UPnP	118
Assigning Ports to a PVC	119
Changing HTTP and Telnet Ports	121
Filtering Out MAC Addresses.....	122
Managing Access to Services	124
Configuring Quality of Service.....	125
TR-069	129
Monitoring ADSL, Wireless, and Ethernet Status.....	132

Changing Your Password.....	135
Restore/Reset Factory Settings	136
Backing Up and Restoring Your Configurations.....	137
Updating Your Firmware	138
Appendix A: ADSL Internet Settings Tables	139
Appendix B: Front and Back Panels.....	143
Appendix C: TCP/IP Network Settings	146
Macintosh TCP/IP Settings	147
Mac OS X	147
Mac OS 7.6.1 - 9.2.2.....	148
Linux TCP/IP Settings.....	149
RedHat.....	149
SuSE	149
Debian	149
Windows TCP/IP Settings.....	150
Windows XP	150
Windows 2000	151
Windows 98/Me	152
Appendix D: Troubleshooting	153
Appendix E: Configuring Your Web Browser	158
Configuring Internet Explorer	159
Configuring Mozilla Firefox.....	161
Appendix F: Wireless Channels by Country	162
Appendix G: Regulatory Information.....	163
Declaration of Conformity	165

Overview

This *User Guide* provides instructions for setting up your X6v, connecting the X6v to wired and wireless computers on a network, securing your network, setting up a Voice over Internet Protocol (VoIP) telephone service, and configuring the X6v for gaming.

For most customers, Chapter 1 covers what you need to get connected to the Internet. Chapter 2 applies if you want to set up a network. Chapter 3 provides security information, Chapter 4 covers VoIP setup, and Chapter 5 provides what you need for gaming.

Chapter 6, Router Setup, is primarily for System Administrators. This chapter explains how to use features such as adding extra security to the X6v with firewall filtering, backing up and restoring the X6v configuration, updating the firmware, and creating a fixed IP address.

You can find the latest information about the X6v at the Zoom Web site:

http://www.zoom.com/products/adsl_overview.html

1

Installation Instructions

This chapter includes the basic instructions needed to install your X6v and connect to the Internet using a Macintosh[®], Linux, or Windows[®] operating system.

*Note to Windows users: If you did not successfully set up the X6v using the **Install Assistant**, follow these instructions to install the X6v manually. If you already installed and connected your X6v (using the separate Quick Start booklet provided for Windows users), you can skip this chapter and begin with Chapter 2.*

Package Contents

Your package contains the following items:

- Zoom ADSL X6v modem
- Ethernet cable
- Phone cord
- Power cube
- CD

The CD contains the installation software, documentation, warranty, and Customer Support information.

If anything is missing or damaged, please contact Zoom Customer Support or whoever sold you the modem.

In addition, the package might include:

- A splitter to enable you to use a single ADSL wall jack for both an Internet connection and for telephone service (certain countries only)
- Phone-jack adapter to adapt the phone cord to a particular phone jack (certain countries only)
- ADSL line filter(s) (certain models only)

Before You Begin

You will need the following:

- ADSL service enabled on your telephone line. If you haven't already done so, you need to register with an ADSL service provider.
- One or more computers or laptops that you want to connect to the Internet. The X6v supports Macintosh, Linux, and Windows Vista, XP, 2000, Me and 98 operating systems.
- A Web browser. The minimum browser requirements on Windows are Internet Explorer v6, Firefox v1.0.3, Netscape v7.2, Opera v8.54, or Chrome v0.3.154.9; on Macintosh, Safari v3.0.4 or Firefox v2.0.3.
- For wireless connections, the computer(s) must have built-in wireless capability or be equipped with a wireless adapter. The X6v supports 802.11b and 802.11g compatible adapters.
- For direct wired connections to the X6v's ETHERNET ports, the computer(s) must have an Ethernet port.
- Additional Ethernet cables if you plan to connect more than one computer directly to the modem. The X6v supports up to four direct Ethernet connections.
- If you want to use your X6v's Internet calling capabilities but your unit does not include Voice over Internet Protocol (VoIP) service, you will need to sign up with a VoIP provider.
- For Internet calling you will also need a standard telephone (or telephones).

- If you want to be able to switch between Internet calling and standard landline calls, you will need a traditional landline telephone connection. This connection provides emergency backup if you lose power.

Installing the X6v

- Macintosh and Linux users: please go to page 12.

Important! If possible, use a computer that is centrally located in your home or office and that has easy access to an ADSL line. A central location helps assure good wireless performance. If you do not have a desktop computer located centrally in your home (if, for example, the desktop is in the basement), or you only have notebook computers, you should still directly connect this desktop computer or one of your notebooks to the X6v to configure it. Once the X6v is set up and your Internet connection is working, you can unplug the computer from the unit and move the X6v to a more central location.

Windows Installation

Windows users can quickly install the software and hardware then configure the X6v using Zoom's Install Assistant on the CD. If you have already run the Install Assistant, please go to [Setting Up a Network](#) on page 19.

If you encountered a problem using the Install Assistant, follow the instructions for Macintosh and Linux users starting on page 12.

- 1** Choose the Windows computer that you will use for setup. This can be any Windows Vista™, XP, 2000, Me or 98SE computer with an available Ethernet port.
- 2** Switch off the computer. Wait a few seconds, then switch it on. Wait until the computer completes its power-up process.
- 3** Close all open programs, including any anti-virus software or pop-up blockers.
- 4** Insert the X6v CD into the computer's CD drive. The CD should start automatically after a few seconds.

If the CD does not start automatically, click the Windows **Start** button (*Windows Vista users*: click **All Programs**, then **Accessories**), click **Run**, and then type **E:\setup.exe**, where **E** is the letter of your CD drive.

For Windows Vista only:

If the **AutoPlay** dialog box appears, click **Run Setup.exe**:



If a message appears stating that an unidentified program wants access to your computer, click **Allow**.

- 5 When the **Zoom ADSL Modems** screen opens, select **Install Assistant** from the menu.

The Install Assistant displays a series of screens that guide you through the installation process.

For Windows Vista and XP users: If a message appears, telling you that the Windows Firewall has blocked some features of this program, select **Unblock**, and continue with the installation.

- 6 On the **Install Assistant** screen, select your modem from the list of Zoom ADSL modem models, then click **Next**.
- 7 Follow the on-screen prompts to plug in the required cables and wired equipment, then set up the ADSL and VoIP service connections.

- 8 If you are prompted to enter your user name and password, remember that they are case-sensitive:



The screenshot shows a blue window titled 'X6v ADSL'. In the top left corner is the X6v logo. The main text reads: 'Your ADSL provider should have given you a Username (Usually your email address or the characters preceding the @ sign in your email address) and a Password. If you have a Username and Password, enter them below.' Below this text is a white form with three input fields: 'Username', 'Password', and 'Verify Password'. At the bottom of the window, it says 'Click Next To Continue' and has three buttons: 'Back', 'Next', and 'Cancel'.

- 9 When you complete the installation and setup, click **Finish** to update your modem and close the **Install Assistant**.

Congratulations! You have established communication and your computer is now connected to the Internet.

If you will not be using the VoIP feature, and you want to connect other computers to the X6v, continue with [Setting Up a Network](#) starting on page 19.


If you are or will be using the VoIP feature, first set up a network, if desired (as described on page 19), then go to [Chapter 4: Setting Up VoIP Service](#) on page 39.

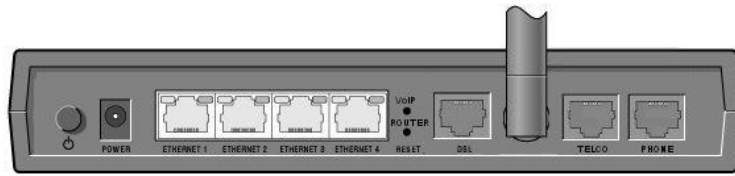
Macintosh and Linux Installation

Windows users: If you did not run the **Install Assistant** on the CD, follow these instructions to install the hardware and configure your X6v.

Installing the Hardware

- 1 Shut down and power off your computer.
(This can be any one of the computers that you plan to use with the X6v. In a typical situation, this would be the computer that is closest to your ADSL wall jack.)
- 2 Rotate the antenna on the back of the modem to a vertical position.
- 3 Connect the modem to the computer's Ethernet port.


Plug one end of the Ethernet cable  into any one of the X6v modem's **ETHERNET** ports (**Ethernet 1**, **Ethernet 2**, **Ethernet 3**, or **Ethernet 4**) and plug the other end into your computer's Ethernet port.



- 4 Plug the power cube into a power strip or wall outlet and then plug the power cube's other end into the modem's **POWER** jack.

Important!

Only use the power cube shipped with the X6v. Other power cubes might damage your hardware.

- 5 After you plug in the power cube, the **POWER** and **WLAN** lights on the front panel of the modem should become steady on, and the **DSL** light should flash. If the **POWER** light does not turn on, press the  button on the modem's rear panel and make sure that there is power at the wall outlet or power strip where you plugged in the power cube.

- 6 Turn on the computer.
- 7 Plug one end of the supplied phone cord into the modem's **DSL** port and the other into the ADSL wall jack. The flashing **DSL** light should become steady on. If it does not, refer to [Troubleshooting](#) on page 153.
- 8 If you want to use the modem's VoIP capability, plug a phone or cordless phone base station into the X6v's **PHONE** connector.

To be able to switch between Internet and standard landline phone service, plug one end of the supplied phone cord into the X6v's **TELCO** (i.e., **TELE**phone **CO**mpany) connector and the other end into the wall jack where you would normally plug in a standard telephone.

We recommend that you put an ADSL filter on every phone connected to the ADSL phone line. If you received a filter or filter/splitter from Zoom, you can use that. You can also purchase an ADSL filter from a retailer of telephone accessories. ADSL filters and filter/splitters come in a variety of styles and sizes and might not look identical to the filter/splitters shown here.



- a Plug the **LINE** or **PHONE LINE** connector of the filter into the wall jack that is enabled for DSL service.
- b Plug the X6v into the filter's **MODEM** connector.
- c Optionally, connect a phone cord between the filter's **PHONE** connector and your X6v's **TELCO** port.

Congratulations! You have installed the hardware. Now continue with the next section, **Establishing Communication**.

Establishing Communication

Important!

Macintosh and Linux users must make sure that the computer's TCP/IP settings are configured properly **BEFORE** starting this section. See **Macintosh TCP/IP Settings** on page 147 or **Linux TCP/IP Settings** on page 149 for instructions.

You must set up the X6v so that it can communicate with your Internet service provider. Follow these steps:

- 1 Close all programs including antivirus software and pop-up blockers.
- 2 Log into the **Zoom Configuration Manager**:
 - a Open your Web browser and type <http://192.168.0.1> in the browser's address field.
 - b When the authentication dialog opens, type **user** in the **User Name** field and **password** in the **Password** field, as shown here.

User Name: **user**

Password: **password**

Note: The **User Name** (**user**) and **Password** (**password**) that you type in this dialog are used by the Zoom Configuration Manager for non-administrative users and must be typed as shown, using lower-case characters. (The **User Name** and **Password** for administrative users are described in **Using Router Setup** on page 86.) These identifiers are not the user name and password that your Internet Service Provider might have given you nor are they names that you choose.

If you are not prompted for a **User Name** and **Password**, do the following, in this order: Recheck all connections; restart the modem and computer; then reset the modem by inserting a paper clip into the **Reset** pinhole in the modem's back panel and holding it for at least 3 seconds.

Important:

To protect your configuration, choose your own X6v password after the setup is complete. See **Changing Your Password** on page 135.

- 3 After you log in, use the **ADSL Setup** page to configure the modem so it can connect with your Internet service provider.



- To use *Automatic Configuration* (recommended):

At **Configure my connection**, click **Start**.

On the **Settings successfully detected** dialog, click **OK** to return to the **ADSL Setup** page.

If the X6v finds a PPPoE or PPPoA connection, on the **ADSL Setup** page, enter the user name and password given to you by your Internet Service Provider.

If the X6v finds a 1483 Bridged or 1483 Routed connection, you have the option of using either dynamic or static IP addressing. Depending on your situation, select the appropriate option button:

- [MOST USERS] Ensure that **Obtain an IP address Automatically** is selected if you are using Dynamic Host Configuration Protocol (also known as DHCP or dynamic IP addressing). This option is selected by default because most Internet service providers use DHCP.
- Select **Use the following IP Address** only if you are using a static IP address. (You should know if you are using static IP addressing. There is typically an extra charge for a static IP address and

you usually have to make special arrangements with your Internet service provider to get one.)

Enter the **IP Address**, **Subnet Mask**, **Default Gateway**, and **DNS** that you plan to use. Click **Save Changes**, then click **Write Settings to Flash**.

- *To configure your settings manually if Automatic Configuration does not work:*
 - a On the **ADSL Setup** page, enter your **Protocol**, **Encapsulation**, **VPI**, and **VCI** settings in the appropriate fields. Your service provider should supply these values. If you do not know these settings, refer to Appendix A on page 139.
 - b **NAT** (Network Address Translation) is **Enabled** by default. This feature lets multiple users access the Internet sharing a single IP address. **Enabled** is typically the correct setting. Select **Disable** in the unlikely event that you want to assign different public IP addresses to each network user.
 - c Depending on the **Protocol** setting you selected, the bottom half of the page will change so that you can enter additional information.
 - **If you selected PPPoA or PPPoE**, enter your **ADSL Username** and **Password** in the appropriate boxes. Your Internet Service Provider should have given this information to you. (Your **Username** is typically your email address or the characters preceding the @ sign in your email address.) These entries are not the same **Username** and **Password** that you used earlier to open the **Zoom Configuration Manager**.
 - **If you selected 1483 Bridged or 1483 Routed**, you have the option of using either dynamic or static IP addressing. Depending on your situation, select the appropriate option button:
 - [MOST USERS] Ensure that **Obtain an IP address Automatically** is selected if you are using Dynamic Host Configuration Protocol (also known as DHCP or dynamic IP addressing). This option is selected by default

because most Internet service providers use DHCP.

- Select **Use the following IP Address** only if you are using a static IP address. (You should know if you are using static IP addressing. There is typically an extra charge for a static IP address and you usually have to make special arrangements with your Internet service provider to get one.)

Enter the **IP Address**, **Subnet Mask**, **Default Gateway**, and **DNS** that you plan to use. Click **Save Changes**, then click **Write Settings to Flash**.

- 4 Verify that your Internet connection is working. Open your Web browser and try to connect to a familiar Web address. If you connect successfully, you are ready to set up the rest of your network.

If you cannot connect to the Internet, see [Troubleshooting](#) on page 153.

Tip!

If you configured the X6v using a notebook computer, you can keep it plugged in or you can disconnect it from the unit's ETHERNET port. As long as the X6v remains plugged into an ADSL wall jack and a power source, the X6v can function as a stand-alone device. You can then make the notebook part of your wireless network.

Congratulations! You have established communication and your computer is connected to the Internet.

If you want to configure a VoIP account, first set up your network - if desired - and then continue with [Chapter 4, Setting Up VoIP Service](#) on page 39.

If you want to connect other computers to the X6v, continue with **Setting Up a Network** below.

Setting Up a Network

When a computer that is directly connected to the X6v modem is able to browse the Web, you know for certain that your Web connection is working. Now you can set up the rest of your network.

It is up to you to decide whether you want to have some computers connected directly to the X6v and others connected wirelessly. The X6v supports both wired and wireless connections. You can have up to 253 connections, four of which can be wired directly through the X6v's four **ETHERNET** ports. You can also plug a network device (such as a hub, switch, or router) into one of the ETHERNET ports.

To set up your network, you can do any or all of the following, in any order that you choose:

- If you want to connect additional computers directly to the X6v, see **To Connect Additional Wired Computers** below.
- If you want to connect a hub, switch, or router directly to the X6v, see **To Connect a Network Device** on page 20.
- If you want to connect additional computers using a wireless network, see [Chapter 2: Setting Up Your Wireless Network](#) on page 22.

To Connect Additional Wired Computers

You can connect up to four computers that have Ethernet ports directly to the X6v.

- 1 Shut down and power off the computer you want to connect to the X6v. (This is important because the computer must locate the correct IP address for the modem. This is done when the computer is turned back on in step 3 below.)
- 2 Plug one end of an Ethernet cable into one of the modem's ETHERNET ports and plug the other end into the computer's Ethernet port.

- 3 Turn on the computer.
- 4 Verify that your Internet connection is working. Open your Web browser and connect to a familiar Web address.
- 5 Repeat steps 1 through 4 for each computer you want to add.

To Connect a Network Device

You can use one of the **ETHERNET** ports on the X6v to plug in a network device (for example, a hub, switch, or router). If you want to connect a game console, please see [Step 1: Choosing an IP Address for Gaming](#) in **Chapter 5, The X6v and Online Gaming**. And should the X6v's DHCP server become disabled, the instructions starting on page 73 will tell you how to configure a static IP.

- 1 Plug one end of an Ethernet cable into one of the modem's **ETHERNET** ports and the other end into the network device's Ethernet port. (For a hub or a switch, this is typically called an **Uplink** or **Expansion port**. For a router, this is typically called a **WAN port**.)
- 2 Set up your network. Refer to the documentation provided with your particular network device for instructions on how to do this.
- 3 Once your network is set up, reboot any computer that is part of the network.
- 4 Verify that your Internet connection is working. Open the Web browser on each computer and connect to a familiar Web address.

Congratulations! You have set up your wired devices. If you have wireless devices that you want to add to your network, go to **Setting Up Your Wireless Network** on page 22.

Universal Plug and Play

The X6v supports Universal Plug and Play (UPnP™). This means that other devices plugged into your computer or network (for example, a gaming application, router, or stand-alone firewall) that use UPnP should automatically detect the X6v and make the needed configurations for them to work together. There is no setup for you to do.

If You Need Help

Zoom has many Technical Support services available to its customers. You can access these services in a variety of ways:

- Visit our Web site at www.zoom.com and select **Technical Support**. From there, you can register your X6v, contact our technical support experts, use our intelligent database, SmartFacts™, and get warranty information.

Tip:

From time to time, Zoom may release improved firmware. This is also available at www.zoom.com, along with upgrade instructions. We recommend that you check our Web site periodically for updates.

- Call our support office. The appropriate number depends on your country:
US: (617) 753-0961
(617)753-0968 for VoIP product assistance
UK: 0870 720 0090
Other country (US number): (617) 753-0967
For more information about Zoom's Technical Support services, go to <http://www.zoom.com/techsupport/>.
- Some retailers of Zoom products provide support or can recommend a convenient support center.

2

Setting Up Your Wireless Network

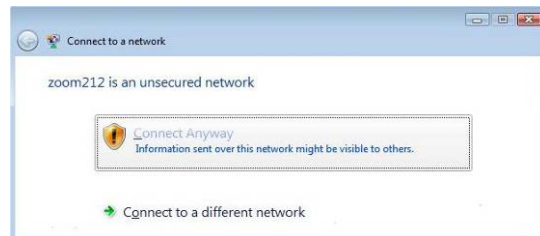
This chapter discusses how to set up a wireless network using computers that have built-in wireless capabilities and/or a wireless adapter. Chapter 3 provides information about implementing network security.

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

- 1** Some newer Windows Vista and XP notebooks and desktops have built-in wireless networking capabilities and do not require the installation of a wireless component. If this is the case, you should set up that computer's wireless connection using the Windows Vista or XP connect utility. See the sections below on connecting Windows Vista (page 23) or XP (page 25) computers with built-in wireless capabilities.
- 2** Some desktop and notebook computers may have built-in wireless networking capabilities, but do not use the Windows Vista or XP utility to configure their device. If this is so, set up your computer's wireless connection using the instructions on page 26 for **Connecting a Wireless-Enabled Computer to the X6v**.
- 3** Some desktop and notebook computers may need a wireless network adapter installed. This can be a USB adapter, PC Card adapter, or PCI adapter. When you install the adapter, make sure that it is set to **infrastructure** or **access point** mode (NOT **ad-hoc** or **peer-to-peer** mode). If you need help installing your wireless adapter or setting its mode, refer to the documentation that came with it. After you install the adapter, see **Connecting a Wireless-Enabled Computer to the X6v** on page 26.

Connecting a Windows Vista Computer with Built-in Wireless Capabilities

- 1 From the **Start** menu select **Connect to**.
- 2 In the **Connect to a network** dialog, highlight the desired network and click **Connect**.
 - If your desired network is secured, in the next dialog box enter the security key or password and click **Connect**.
 - If your desired network is unsecured, in the message box select **Connect Anyway**.



Note: We strongly recommend that you set up a secured network. For information on wireless security, see [Setting Wireless Security](#) on page 29.

If you have difficulty connecting, make sure you have entered the correct password. Then perform a power cycle on your computer and the X6v as described in the [Troubleshooting Tips](#) on page 153.

- 3 In the **Successfully connected to [desired network]** dialog, you have three options. You can:
 - Select **Save the network** and **Start this connection automatically** if you always want to connect to the same network. Then click **Close**. The next time you start your computer you will automatically connect to the selected network.
 - Select **Save the network** and clear the **Start this connection automatically** check box if you don't want to

automatically connect to this network every time you start your computer but you will want to connect in the future. Click **Close** to display the **Select a location . . .** dialog box where you choose a location.

If the **User Account Control** dialog box appears, click **Continue**.

- Click **Close** to complete the connection procedure. Select this option if you are connecting to this network only one time.

To disconnect from the current network:

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

Connecting a Windows XP Computer with Built-in Wireless Capabilities

- 1 On your Windows desktop, click the **Start** button then click **Control Panel**.
- 2 **Double-click** the **Network Connections** icon.
- 3 **Right-click** the **Wireless Network Connection** icon, then select **Properties**.
- 4 On the **Wireless Network Connection Properties** dialog, select the **Wireless Networks** tab. Windows will automatically scan for available wireless networks in your area. Any compatible networks within range will appear in the **Available networks** list. It should find the wireless network of the X6v—named **zoom**. (The scan is done automatically because the **Use Windows to configure my wireless network settings** check box is selected by default).
- 5 Select **zoom** from the **Available networks** list, then click the **Configure** button to add it to the **Preferred networks** list. The notebook will try to connect to the Internet using the wireless networks listed here, in the order in which they appear. (If you already have networks listed here, we recommend you either remove them or use the **Move up** button to move **zoom** to the top of the list.)
- 6 Click **OK**.
- 7 Test your wireless connection. From the computer or notebook that you set up, open your Web browser (for instance, Internet Explorer or Netscape Navigator) and try to connect to a familiar Web address.

If you connect successfully, your notebook's wireless capability is configured and you are ready to browse the Web!

Important!

If you want to add security to your network, please see [Setting Wireless Security](#) on page 29.

Connecting a Wireless-Enabled Computer to the X6v

- 1 For a new wireless network, go to the wireless-enabled computer that you want to add to the network. The computer should have software that will scan for available wireless networks in your area. When the Service Set Identifier (**SSID**) of your X6v wireless network appears in the list—the SSID is **zoom**—select it as the network you want to use to connect to the Internet.

Tip!

For most wireless adapters, you will use their wireless configuration manager software and click a **Scan** button or select a **Site Scan, Scan Networks**, or other similarly named tab to scan for wireless signals. If you need help, refer to the documentation that came with your wireless adapter.

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

- If you installed a wireless adapter on a Windows XP computer, Windows XP may try to automatically configure the adapter (rather than let you use the software provided with the wireless adapter). You will know this is happening because you will be prompted with a message about one or more wireless networks being available. You will also be able to click a link to open the **Wireless Network Connection Properties** dialog. If this happens, click the link, clear the **Use Windows to configure my wireless network settings** check box, and then click **OK**. You can then use the software provided with your wireless adapter without interruption from Windows.
- More than one wireless network might appear in the list. These are other wireless networks that are within range of your network. Each wireless network has a channel associated with it. We recommend that there be at least a five-channel difference between your network and neighboring networks with strong signals. Having less than a five-channel difference may result in interference with your connection. By default, the

X6v uses channel 10. If you need to change this channel, do so using the **Wireless Setup** page of the **Zoom Configuration Manager**.

- If you want to secure your wireless network so it won't be accessible by others, you should specify security settings. To learn how, see [Setting Wireless Security](#) on page 29. (By default, the wireless connections provided by the X6v do not have any security applied.)
- 2 Test your wireless connections. From each desktop or notebook computer that you set up, open your Web browser (for instance, Internet Explorer or Mozilla Firefox) and try to connect to a familiar Web address.

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

Important!

To add security to your network, see [Setting Wireless Security](#) on page 29.

Checking Your Settings

If you ever need to check your wireless settings, you can do so from the **Wireless Setup** page. This page is available in the **Zoom Configuration Manager** by clicking the **Wireless** icon.

The following table explains the settings.

This setting...	Lets you specify...
Wireless Status	Enable shows that your wireless network is up. Disable indicates that your wireless network is down.
SSID	The Service Set Identifier for your wireless network. By default, the SSID for the X6v is zoom . You can change the SSID to any name that you want.
Hide SSID	Lets you specify whether or not to broadcast the SSID of your network. If you do not want to broadcast the SSID, set this option to True .
Default Channel	The channel your wireless connection uses by default for your wireless connection. The X6v is set for channel 10 .
Profile	The standard used by your wireless adapters. This drop-down list contains 802.11b Only , 802.11g Only , or Mixed Long . The default is Mixed Long, (800.11b+g) which allows you to mix both b and g wireless adapters.
Encryption	The type of encryption used for your wireless Internet signal. This drop-down list contains None , WEP-64 bit , WEP 128 bit , WPA and WPA2 . The default is None , meaning that no security is enabled.
Region	If your country is not listed, select Other .

3

Setting Wireless Security

When you first set up your X6v wireless network, security is turned off by default. This means that your wireless signal is not encrypted and that anyone with compatible wireless technology can access your computer network and the Internet using your wireless connection. This chapter explains how to set up wireless security to protect your network and Internet connection.

Overview

To set up wireless security on a new wireless network, you will create and enter a unique passphrase or an alphanumeric key. Once entered, only devices with the proper key or passphrase will be allowed to establish a connection to the network.

There are two basic ways to configure and implement a passphrase or key. They are **WEP** (**W**ired **E**quivalent **P**rivacy) and **WPA**™ (**W**iFi® **P**rotected **A**ccess™) or **WPA2**™. WPA2 is the most secure, but you can use it only if all your wireless devices support the 802.11g profile.

If you are replacing an existing wireless router with the X6v, you might want to retain whatever security settings you use on your network. Enter your previously defined settings when instructed.

Setting Up Security Using WEP

WEP can be configured two ways: 64-bit and 128-bit. 128-bit WEP provides a bit more security than 64-bit, but 128-bit WEP also tends to diminish network performance. We recommend that you use WEP 64-bit security, because WEP-64 works with most 802.11 wireless equipment.

To set WEP security, follow these steps:

- 1 Verify that your modem's Ethernet connection is active.
- 2 Open the **Zoom Configuration Manager** by typing the following in your Web browser's address bar:
<http://192.168.0.1>
- 3 In the authentication dialog, type the following User Name and Password in lower case, then click **OK**.


User Name: **user**

Password: **password**



You can safely ignore the warning message. It is for informational purposes only.

(The User Name and Password entered here are for the Configuration Manager only, and are not the same as the user name and password that your Internet service provider might have given you.)

- 4 On the X6v **ADSL Setup** page, click the **Wireless** icon  at the top of the screen to open the **Wireless Setup** page:

Wireless Setup

Name	Value
Wireless Status	Enable
SSID	sarahsecure
Hide SSID	false
Default Channel	10
Profile	802.11g + b
Encryption	None
Region	UNITED STATES

[802.1x Authentication](#) [WDS Configuration](#) [Wireless MAC Filtering](#)

Save Changes

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

Write Settings to Flash

- 5 In the SSID box, enter a NEW name for your network, such as **sarahsecure**. DO NOT use **zoom** as the SSID.
- 6 Normally you should not change the Hide SSID and Default Channel settings.
- 7 Go to **Encryption** and select **WEP-64** bit from the drop-down menu. Several new boxes open directly below the **Encryption** box:

Encryption	WEP-64 bit
Passphrase <input type="checkbox"/>	
Default Key	1
Key 1	00-00-00-00-00
Key 2	00-00-00-00-00
Key 3	00-00-00-00-00
Key 4	00-00-00-00-00
Region	UNITED STATES

- 8 If you are replacing an existing wireless router with the X6v, you might want to retain whatever security settings you use on your network. Enter the SSID, encryption type, and the security key or passphrase that you previously defined for your network. You must enter a dash (–) between each pair of characters in a security key.
- 9 If you are setting up a new wireless network, select the check box marked **Passphrase** and then enter a word or phrase in the Passphrase text box. For best security, enter a combination

of numbers and letters. The Passphrase should be at least eight characters. Click **Save Changes**, then **Write Settings to Flash**.

When the Wireless Setup page refreshes, note that your passphrase is no longer displayed and that security keys 1-4 have been automatically generated.


- 10** Leave the Default Key as **1**, and write down the 10 digits of **Key 1**. Put this security key where you can find it — on the bottom of the X6v case, for instance.
- 11** Now you need to set up each of your wireless devices with the SSID and security key, as follows:
 - a** First, make sure that the network device on which you are setting security has its wireless capability turned on. (Many notebooks have a hardware switch for wireless.)
 - b** Next, go to the network device's area for configuring a wireless network connection.
 - c** For a Windows computer, click the **Wireless Networking** icon at the lower right corner of the screen.
 - d** Select the **Site Survey** or **Scan** option to see a list of the access points in your area. That list should include the SSID that you just set up on the X6v.
 - e** Select that SSID and enter the WEP-64 Key 1 that you just wrote down in step 10. Omit the hyphens when entering the key.
 - f** **Save** your settings.
 - g** Repeat substeps **a** through **f** for all wireless devices on your network.

That's it! Your security setup is now complete!

In the unlikely event that you experience performance issues with your wireless network, you might want to set up your network on a channel that's different from the factory-set channel of 10. To do that, follow these steps:

- 1** Open the Zoom Configuration Manager by typing <http://192.168.0.1> in your Web browser's address bar:
- 2** In the authentication dialog, type your User Name and your new Password (or, if you haven't yet changed your password,


type **user** for User Name and **password** for Password, each in lower-case letters). Click **OK**.

- 3 On the **ADSL Setup** page, click the **Wireless** icon  at the top of the screen to open the **Wireless Setup** page.
- 4 On the **Wireless Setup** page, enter a new channel. If possible, this channel should be 5 channels away from other strong channels in use in your area. The default channel is 10.
- 5 Be sure to click **Save**, then **Write Settings to Flash** after you change the channel. All devices connecting wirelessly to the X6v will automatically switch to the new channel.

Your basic security setup is complete. Please see the following sections to configure 802.1x Authentication, a Wireless Distribution System, and Wireless MAC Filtering.

Setting Up Security Using WPA2 or WPA

WPA2 and WPA use a **passphrase** that you choose and enter on the X6v and other wireless devices on the network to set up security. To use WPA2 or WPA, **all** of the wireless devices on your network must support that encryption method.

- 1 Check to make sure that all other clients that you plan to put on the network support WPA2 or WPA. If they do not, return to **Setting Up Security Using WEP** on page 29 and follow the instructions.
- 2 Click the **Wireless** icon  in the **Zoom Configuration Manager** to open the **Wireless Setup** page. Go to **Encryption** and select **WPA2** or **WPA** from the drop-down menu. A new field labeled **WPA Passphrase** will open directly below the **Encryption** box.



- 3 Normally you should not change the Hide SSID and Default Channel settings.
- 4 If you are replacing an existing wireless router with the X6v, you may want to retain whatever security settings you use on your network. Enter the SSID, encryption type, and the passphrase that you previously defined for your network.
- 5 If you are setting up a new wireless network, choose and enter a **Passphrase**. You can enter a word or phrase, or for greater security you can enter a combination of numbers and letters. The passphrase that you enter is case-sensitive.
- 6 Every wireless network client needs to be set individually by entering the **Passphrase** on all wireless devices on the network. Open the software that came with the device, which should be running on the computer where the device is installed. Find the configuration menu for security, choose **WPA2** or **WPA**, and enter the **Passphrase**, exactly as you entered it on the X6v **Wireless Setup** page.

Your basic WPA or WPA2 security setup is complete. Please refer to the following sections for information on 802.1x Authentication, WDS (Wireless Distribution System) configuration, and Wireless MAC Filtering.

802.1x Authentication

The IEEE 802.1x standard can authenticate requests to use your wireless network, and can dynamically update your encryption keys.

On the Wireless Setup page, click **802.1x Authentication** to open the 802.1x Authentication page:

802.1x Authentication

Name	Value
Auth Server:	Local <input type="button" value="v"/>
Radius Server IP:	<input type="text" value="0.0.0.0"/>
Shared Secret:	<input type="text"/>
Auth Control Enabled:	false <input type="button" value="v"/>
Identity String:	<input type="text" value="DSL gateway 00:01:38:bb:b9:41"/>
Rekey Timeout:	<input type="text" value="600"/>
Key Transmission Enabled:	true <input type="button" value="v"/>
Entropy Pool:	<input type="text" value="••••••••"/>
Version:	2.01

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

The following table describes the values that you can select or enter.

Setting	Description
Auth Server	Local - No external Radius Server is used, 802.1x not being used RADIUS - External (LAN) Radius Server is used for authentication
RADIUS server IP	If you selected RADIUS, enter the server's IP address.

Setting	Description
Shared Secret	If you selected RADIUS. Shared secrets are used to verify that RADIUS messages, with the exception of the Access-Request message, are sent by a RADIUS-enabled device that is configured with the same shared secret. You must use the same case-sensitive shared secret on both RADIUS devices (Client and Server).
Auth Control Enabled	Enable or disable Authentication Control which allows AP to act as 802.1x Authenticator for wireless devices
Identity String	Identity String or IP address of the 802.1x Authentication Server (Radius Server)
Rekey Timeout	Default is 600 seconds. Specifies time in which WEP keys for the current session will timeout and new ones are issued as a deterrent to any attacker.
Key Transmission Enabled	Determines whether or not the Authenticator (AP) is configured to send WEP keys to supplicants (WL Clients)
Entropy Pool	Can manually enter in “pool” of characters. WEP keys dynamically generated will be automatically generated at random from this pool.

After you enter your values, click **Save Changes** and then **Write Settings to Flash**.

Wireless Distribution System (WDS) Configuration

A **Wireless Distribution System (WDS)** expands a wireless network by using multiple Access Points connected wirelessly.

WDS Configuration

Name	Value
WDS Status	Disable <input type="button" value="v"/>
AP1	<input type="text" value="00:00:00:00:00:00"/>
AP2	<input type="text" value="00:00:00:00:00:00"/>
AP3	<input type="text" value="00:00:00:00:00:00"/>
AP4	<input type="text" value="00:00:00:00:00:00"/>

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

To set up a Wireless Distribution System, make the following entries:

Setting	Description
WDS Status	Select Enable to configure WDS.
AP 1, AP2, AP3, AP4	Enter the 12-digit MAC address of each Access Point (AP) that you want to include in the Wireless Distribution System.

After you enter your values, click **Save Changes** and then **Write Settings to Flash**.

Wireless MAC Filtering

This page lets you grant or deny network access to devices with the listed MAC addresses.

Wireless MAC Filtering

MAC Address Auth

Existing Wireless MAC Filtering

MAC Address	Delete?
-------------	---------

Add Wireless MAC Filtering

MAC Address	Add
<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="button" value="Add"/>

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

Setting	Description
MAC Address Auth	Select Disabled , White List or Black List . White List allows network access only to the devices in the Existing Wireless MAC Filtering list. Black List allows network access to all devices except those in the Existing Wireless MAC Filtering list.
Existing Wireless MAC Filtering	List of devices currently authenticated by MAC address
Add Wireless MAC Filtering	Enter the 12-digit MAC address of the device you want to add to your network, and click Add .

Click **Save Changes**, then **Write Settings to Flash**.

4

Setting Up VoIP Service

This chapter covers the setup of the X6v for Internet telephone service, using the X6v's built-in VoIP capabilities.

To complete the installation, you need the following:

- An account set up with a VoIP service provider. If your X6v did not come with an account set up, go to your service provider's Web site and sign up for service if you have not already done so.
- A telephone so you can place and receive phone calls.

Using the Zoom Configuration Manager to Set Up VoIP Service

You may want to connect the X6v to your landline. If you connect the X6v's **TELCO** (i.e., **T**elephone **C**ompany) port to a landline telephone service, you can choose to make some calls through your landline and other calls over the Internet. If the landline is also set for DSL service, be sure to connect an ADSL filter between the telephone line and the X6v's TELCO jack. Then follow these steps:

- 1 To log into the Zoom Configuration Manager, follow these steps:
 - a Open your Web browser and, in its address bar, type **http://192.168.0.1**, then press the **Enter** key on your keyboard.

- b In the **authentication** dialog, type the following user name and password in lower-case letters, then click **OK**. (The **User Name** and **Password** you enter here are not the same as the User Name and Password that your Internet service provider may have given you.)

User Name: **user**

Password: **password**



You can safely ignore the warning message.

If you are not prompted for a **User Name** and **Password**, do the following in this order: Recheck all connections; restart the modem and computer; and reset the modem by inserting a paper clip into the lower **Reset** pinhole in the modem's back panel and pressing it three times.

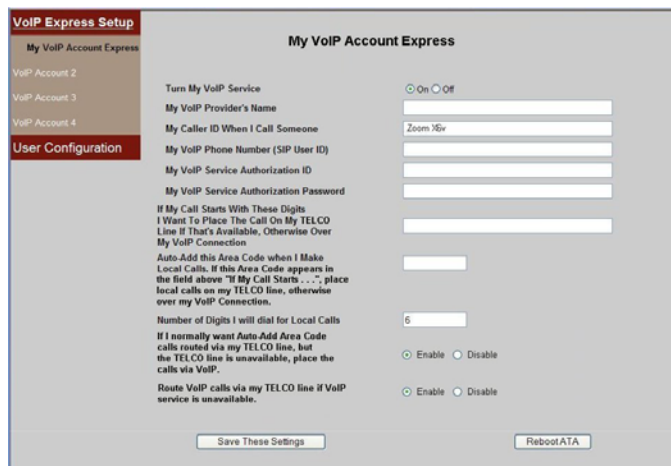
Important:

To protect your configuration, choose your own password after the setup is complete. See **Changing Your Password** on page 135.

2 At the top of the **ADSL Setup** page, click the **VoIP**  icon:



The **My VoIP Account Status** page will open. Click **VoIP Express Setup** to display the parameters for your account on the **My VoIP Account Express** page:



Make the following entries.

Setting	Description
Turn my VoIP service . . .	Click the On button to enable VoIP.

Setting	Description
My VoIP provider's name	Type your provider's name for reference.
My Caller ID when I call someone	Type your name or the ID that people see in the Caller ID display when you call them. Your VoIP provider might have assigned this identifier. If not, you can enter your name or another identifier for your account.
My VoIP phone number (SIP User ID)	Assigned by your VoIP provider. This is usually the number that people use to call you. Do not change this number.
My VoIP Service Authentication ID	The ID (often the same as your VoIP phone number) that your VoIP provider might have assigned. Enter the ID if it does not appear in the field.
My VoIP Service Authentication Password	The password that your VoIP provider might have assigned. Enter the password if it does not appear in the field.
If My Call Starts With ...	<p>Specifies when to use the landline (TELCO) connection when you connect the X6v's TELCO port to a standard telephone service jack.</p> <p>Enter area codes, city and/or country codes, or entire numbers. Include any required prefixes such as 011, 00, or 1. Separate the entries with a comma or a comma and a space.</p> <p>The numbers that you enter will be dialed on your TELCO line. All other numbers will be dialed over your VoIP connection.</p> <p>There is a limit of 18 entries.</p>

Setting	Description
Auto-add this Area Code...	Type the area or city code that the X6v will automatically add to local calls.
Number of digits I will dial for Local Calls	If you entered an area or city code in the previous field, specify the number of additional digits for local calls. For example, if local calls have this format: 555-1234, type 7. (Ignore the dash.)
If I normally want Auto-Add Area Code calls...	Select Enable (the default) or Disable .
Route VoIP calls via my TELCO line if...	Select Enable (the default) or Disable .

The X6v automatically sends all emergency calls (911, 999, 100, and 11x numbers) over your landline.

Another advantage of connecting the **TELCO** port to your landline is that if the X6v's Internet connection is disrupted, by default your phone calls are automatically switched to your landline service. (You can disable this feature on the **My VoIP Account Express** page.)

- 3 Click **Save These Settings** to save the account information and write it to flash memory.

Note: The only time you need to click **Reboot VoIP** is when you change an IP address.

Changing Your VoIP Settings

The **User Configuration** link on the **Your VoIP Account** page lets you add or change settings such as Speed Dials, Call Forwarding, and Call Waiting/Caller ID. Click the **Help** button on each page for configuration tips.

On each page, when you complete your changes, click **Save These Settings** to save your information and write it to flash memory.

Note: Many VoIP settings can be controlled from your telephone keypad. See [Controlling the X6v from Your Phone](#) on page 70.

Speed Dials

To open the **Speed Dials** page, where you can enter up to 28 numbers into your speed dial list, click **User Configuration**:



Enter a complete phone number opposite a Speed Dial number. For example, opposite *20 enter (123) 456-7890. Save your changes. The next time you want to call (123) 456-7890, for example, just dial *20.

Calls will be placed via VoIP or via your standard telephone service according to the settings you entered on the **My VoIP Account** page. In other words, if you configured calls starting with **(456)** to go to your landline service, if you enter (456) 123 4567 as a Speed Dial, that number will be dialed out over your TELCO line when you invoke it through the Speed Dial feature.

Call Forwarding

On the **User Configuration** menu, click **Call Forwarding** to enable or disable **Call Forwarding** parameters and enter up to 30 priority call forwarding numbers.



The screenshot shows the Zoom ATA Express Setup interface. The top navigation bar includes the Zoom logo and links for Basic VoIP Setup, Advanced VoIP Setup, Call Log, Other, and Help. The left sidebar lists various configuration options, with 'Call Forwarding' selected. The main content area is titled 'Call Forwarding' and contains the following settings:

- Call Forward Always: Enable Disable
- Call Forward On Busy: Enable Disable
- Call Forward On No Answer: Enable Disable
- Call Forward Priority: Enable Disable

Below these are input fields for the following parameters:

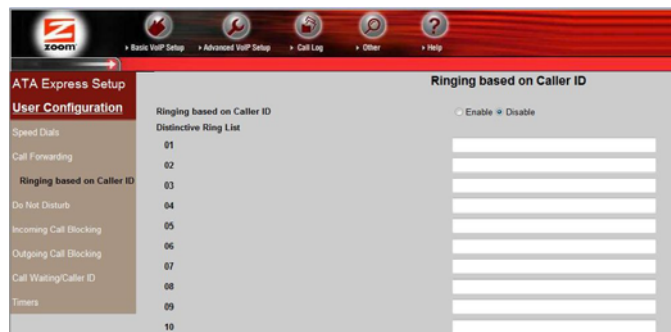
- Call Forward Always Number
- Call Forward On Busy Number
- Call Forward No Ans Number
- Call Forward Priority Number: 16177530548
- Priority Call Forward List

The Priority Call Forward List contains four entries:

Priority	Number
01	8000122
02	16173570236
03	
04	

Ringling Based on Caller ID

On the **User Configuration** menu, click **Ringling Based on Caller ID** to specify distinctive ring tones for up to 30 phone numbers:



The screenshot shows the Zoom ATA Express Setup interface. The top navigation bar is the same as in the previous screenshot. The left sidebar lists various configuration options, with 'Ringling based on Caller ID' selected. The main content area is titled 'Ringling based on Caller ID' and contains the following settings:

- Ringling based on Caller ID: Enable Disable

Below this is a table for the Distinctive Ring List:

Priority	Number
01	
02	
03	
04	
05	
06	
07	
08	
09	
10	

Click **Enable** to turn on the distinctive ring feature, and enter the numbers to which you want to assign a distinctive ring. The ring patterns are the Bellcore-r1 through Bellcore-r8 tones.

Do Not Disturb

Note: This feature applies to VoIP calls only.

On the **User Configuration** menu, click **Do Not Disturb** to enable or disable this feature, which allows you to block all calls except those from the phone numbers on the **Do Not Disturb Exceptions List**:

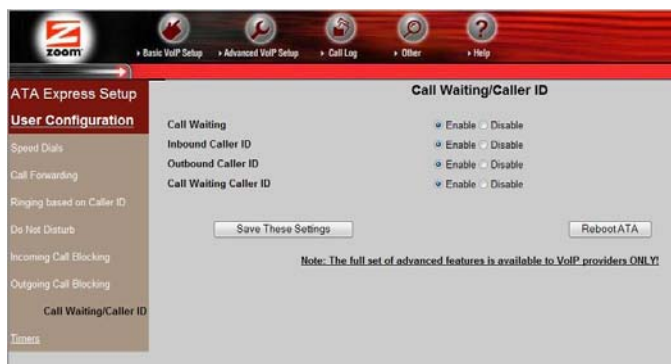


Your phone will not ring unless you get a call from one of the phone numbers that you enter on the Exceptions list.

Call Waiting/Caller ID

This feature applies to VoIP calls only.

On the **User Configuration** menu, click **Call Waiting/Caller ID** to configure Call Waiting, Inbound and Outbound Caller ID, and Call Waiting Caller ID:



There are two cases where you should disable **Call Waiting**:

- If you have enabled **Call Forward on Busy** on the **Call Forwarding** page. (See page 45.)
- If you have configured a **Fax Transmission Mode** on the **Audio Settings** page. (See page 54.)

Incoming Call Blocking

This feature applies to VoIP calls only.

On the **User Configuration** menu, click **Incoming Call Blocking** to enable or disable blocking of anonymous calls (calls that do not provide Caller ID) and specify phone numbers from which you will not accept calls:



You can enter up to 30 phone numbers that will be blocked by the X6v.

By default, **Block Anonymous Calls** and **Block Listed Incoming Calls** are both disabled.

Outgoing Call Blocking

This feature applies to both VoIP and standard telephone calls. On the **User Configuration** menu, click **Outgoing Call Blocking** to prevent certain phone numbers from being dialed from the X6v.




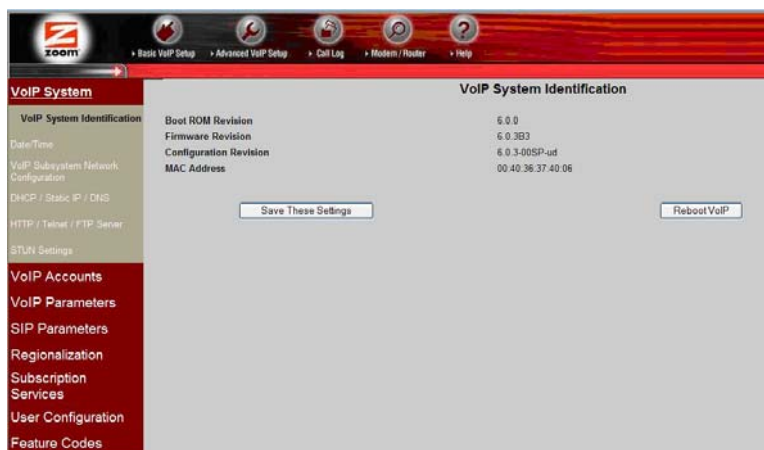
At the **Block Listed Outgoing Numbers** option, select the **Enable** check box. In the **Blocked Call List**, enter up to 30 complete numbers or numbers starting with particular digits. For example, to block all 900 numbers, enter 900x.7. This will block all numbers that start with 900 followed by 7 digits.

To remove a number from the **Blocked Numbers List**, delete it.

To remove all entries from the list, at the **Block Listed Outgoing Numbers** option, select the **Disable** check box.

Advanced VoIP Configuration

On any VoIP system page, click the **Advanced VoIP Setup** icon  to display the full VoIP user configuration menu in the left pane. Basic read-only system information is displayed in the main window:

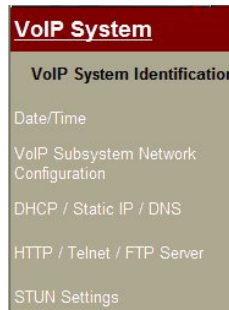


(There are a number of highly technical Advanced VoIP Setup parameters that are available to VoIP providers only. For information, please see the [X6v VoIP Features Technical Reference](#).)

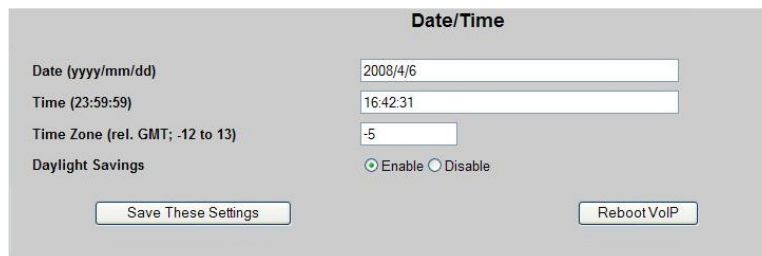
Note: The discussion of advanced VoIP configuration uses the term **PSTN** (**P**ublic **S**witched **T**elephone **N**etwork), which is also described in this *User Guide* as TELCO or landline service.

VoIP System Settings

Click **VoIP System** to select a parameter from this menu:



Date/Time

A screenshot of a web-based configuration form titled "Date/Time". The form has a light gray background and contains the following fields and controls:

- Date (yyyy/mm/dd)**: A text input field containing "2008/4/6".
- Time (23:59:59)**: A text input field containing "16:42:31".
- Time Zone (rel. GMT; -12 to 13)**: A text input field containing "-5".
- Daylight Savings**: Two radio buttons, "Enable" (which is selected) and "Disable".
- At the bottom, there are two buttons: "Save These Settings" on the left and "Reboot VoIP" on the right.

The date and time are set automatically by the time server, and the Daylight Savings adjustment is enabled by default.

You may need to change your **Time Zone** relative to Greenwich Mean Time. For help, please see <http://www.greenwichmeantime.com/info/timezone.htm>

VoIP Subsystem Network Configuration

The screenshot shows a web interface titled "VoIP Subsystem Network Configuration". It contains four input fields: "VoIP Name" with the value "ZOOM_VoIP", "VoIP Host Name" with the value "ZOOM_VoIP", "VoIP Domain Name" which is empty, and "MTU" with the value "1492". At the bottom, there are two buttons: "Save These Settings" and "Reboot VoIP".

The VoIP names are informational only.

You can change the network **MTU** (**M**aximum **T**ransmission **U**nit) value if you are instructed by your system administrator or by Zoom Customer Support.

Static IP / DNS Configuration

The screenshot shows a web interface titled "Static IP / DNS". It contains four input fields: "Static IP Address" with the value "192.168.0.234", "Subnet Mask" with the value "255.255.255.0", "Gateway IP Address" with the value "192.168.0.1", and "Primary DNS Address" with the value "192.168.0.1". At the bottom, there are two buttons: "Save These Settings" and "Reboot VoIP".

Setting	Description
Static IP Address	The VoIP System IP Address must always be in the same subnet as the modem/router LAN IP Address. The Host ID must always be 234 . These are last three digits in the dotted-decimal entry: x.x.x.234. The default value is 192.168.0.234.

Setting	Description
Subnet Mask	The default value of 255.255.255.0 defines a class C network that will support up to 254 devices connected to your LAN.
Gateway IP Address	This is the LAN IP Address assigned to your modem/router. By default it is 192.168.0.1 .
Primary DNS Server	This must always be the same as the Gateway IP Address.

HTTP/Telnet/FTP Server

HTTP / Telnet / FTP Server

HTTP Server Port

Telnet Server Port

FTP Server Port

Setting	Description
HTTP Server Port	The default is 8080.
Telnet Server Port	The default is 8023.
FTP Server Port	The default is 8021.

STUN Settings

This page lets you configure STUN (Simple Traversal of UDP through NATs), which helps the X6v route VoIP packets through the NAT firewall.

STUN Settings

STUN Enable Enable Disable

STUN Server Address

STUN Symmetric Deterministic Enable Enable Disable

Setting	Description
STUN Enable	STUN permits discovery of Network Address Translation (NAT) mapping. If your VoIP service uses Outbound Proxy, disable STUN (your provider will tell you to do this). Generally, you should leave STUN enabled (the default).
STUN Server Address	Enter the Domain Name or IP address of your VoIP provider's STUN server. By default, the Zoom STUN server address is displayed here.
STUN Symmetric Deterministic Enable	Not applicable.
Save These Settings	Click to save your changes to flash memory.

VoIP Parameters

Click the **VoIP Parameters** menu to display the Audio Settings and RTP Protocol Parameters configuration pages.

Audio Settings

Audio Settings

Preferred Codecs G.711u | iLBC | G.729B | G.711A

Silence Suppression Enable Enable Disable

Fax Transmission Mode Off

DTMF Transmission Method RTP Out-of-band

Save These Settings
Reboot VoIP

Setting	Description
Preferred Codecs	Lets you arrange the Codec names in order of preference. The default sequence is G.711u, iLBC, G.729B, G.711A. If your upstream bandwidth is ≤ 256 kbps, set your first preference for G.729B or iLBC. Otherwise, for better voice quality, use G.711u or G.711A.
Silence Suppression Enable	Prevents audio frames from being sent during periods of silence, thus reducing the network traffic necessary for making calls. (Note: This feature is useful only with G.729B.) The default is Disabled .
Fax Transmission Mode	Select the FAX processing method: Off, μ Law Passthrough or ALaw Passthrough. The default is Off .
DTMF Transmission Method	Select the DTMF processing method: Off, Audio Passthrough, RTP Out-of-Band, SIP Out-of-Band. The default is RTP Out-of-Band .
Save These Settings	Click to save your changes to flash memory.

RTP Protocol Parameters

This page displays the VoIP system's **Real-time Transport Protocol** jitter buffer parameters. The page is informational only.

RTP Protocol Parameters	
RTP Jitter Buffer Start Depth (ms)	20
RTP Jitter Buffer Minimum Depth (ms)	20

SIP Parameters

- 1 Select the **SIP (Session Initiation Protocol) Parameters** menu to display the SIP Protocol Parameters configuration page.

SIP Protocol Parameters	
SIP Local Port (1024-65535)	<input type="text" value="5060"/>

- 2 Change the **SIP Local Port** setting only if you have a conflict – for example, if you have multiple VoIP devices on your Local Area Network.

If this is the case, change the port in even-numbered increments: 5062, 5064, etc.

- 3 Click **Save These Settings**.

Regionalization Settings

Select the **Regionalization** menu to display the following two configuration pages.

SLAC Configuration

Use the **SLAC** (Subscriber Line Audio-processing Circuit) **Configuration** page to support the Caller ID mode required by your phone.

The defaults shown in the illustration are for North America. Different Caller ID defaults will appear according to the X6v's region.

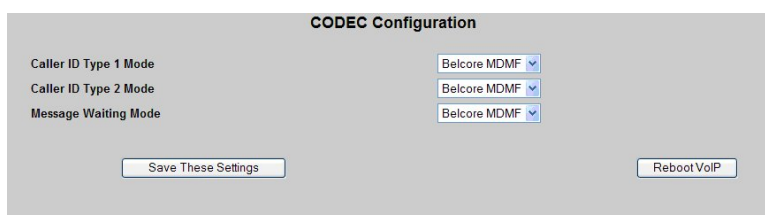
The screenshot shows a web interface titled "SLAC Configuration". It features three dropdown menus on the right side, each labeled with a setting name on the left: "Caller ID Type 1 Mode", "Caller ID Type 2 Mode", and "Message Waiting Mode". All three dropdown menus are currently set to "Belcore MDMF". Below the dropdowns, there are two buttons: "Save These Settings" on the left and "Reboot VoIP" on the right.

Setting	Description
Caller ID Type 1 Mode	Select the on-hook mode: None, Belcore MDMF, Belcore SDMF, ETSI WINK, ETSI RING, DTMF. The default is Belcore MDMF .
Caller ID Type 2 Mode	Select the off-hook mode: None, Belcore MDMF, Belcore SDMF, ETSI WINK, ETSI RING, DTMF. The default is Belcore MDMF . The default is Belcore MDMF .
Message Waiting Mode	Select None, Belcore MDMF, Belcore SDMF, ETSI. The default is Belcore MDMF .
Save These Settings	Click this button to save your settings to flash memory.

CODEC Configuration

Use the **CODEC (COde/DECode) Configuration** page to support the Caller ID modes used by your PSTN service provider on the line connected to the X6v's TELCO port.

The defaults shown in the illustration are for the United States. In other regions, the appropriate defaults will appear.



The screenshot shows a configuration page titled "CODEC Configuration". It contains three dropdown menus: "Caller ID Type 1 Mode", "Caller ID Type 2 Mode", and "Message Waiting Mode". All three dropdown menus are currently set to "Belcore MDMF". Below the dropdowns are two buttons: "Save These Settings" and "Reboot VoIP".

Setting	Description
Caller ID Type 1 Mode	Select the on-hook mode: None, Belcore MDMF, Belcore SDMF, ETSI WINK, ETSI RING, DTMF. The default is Belcore MDMF .
Caller ID Type 2 Mode	Select the off-hook mode: None, Belcore MDMF, Belcore SDMF, ETSI WINK, ETSI RING, DTMF. The default is Belcore MDMF .
Message Waiting Mode	Select None, Belcore MDMF, Belcore SDMF, ETSI. The default is Belcore MDMF .
Save These Settings	Click this button to save your settings to flash memory.

Subscription Services

When you select this item from the VoIP system menu, the **Dialing Parameters** page appears.

Dialing Parameters

The screenshot shows the 'Dialing Parameters' configuration page. On the left is a list of settings: 'Your VoIP Account Unavailable', 'No VoIP Accounts Available', 'PSTN Not Available', 'Configure PSTN Dial Pattern', 'Hot Line Dialing', 'Warm Line Dialing', 'Hotwarm Dial String', 'Polarity Dialing', 'Polarity Dial Done', 'Polarity Connect', 'Polarity Answer', and 'Polarity Idle'. On the right, each setting has a corresponding control: three dropdown menus for 'Alternate Dial Tone', two radio button groups for 'Enable/Disable', and three radio button groups for 'Forward/Reversed'. At the bottom are 'Save These Settings' and 'Reboot VoIP' buttons.

In a given location, normally only a few types of dialed numbers need to be defined. There is dialing for local calls, there is dialing for domestic toll calls, and there is dialing for international toll calls. In addition, there are specific short strings that are set aside for emergency dialing, and there may be other special strings that invoke telephone features.

By default, the X6v is configured to handle number patterns in every country in the world. Emergency calls are by default routed to the PSTN, and all other calls are routed via VoIP.

To change which calls are sent to the PSTN, your first option is to open the **My VoIP Express** page, where you can simply define most numbers that you want to send to the PSTN.

If you want to use the **Dialing Parameters** page to tailor a dial pattern to precisely reflect the format of telephone numbers in your location, please see the discussion of dial patterns in the [X6v VoIP Features Technical Reference](#).

Bridging from VoIP to PSTN

The VoIP bridge modes let you use the X6v as a mini telephone switch. You are probably familiar with telephone switches at companies, government offices and the like. When you call a main number, the telephone switch (or switchboard) answers, and you can typically dial any extension you want inside the office.

When you make a VoIP call to the X6v in VoIP to PSTN bridge mode, you are connected to the landline that is plugged into the X6v. This is like being connected to a switchboard when you call a company or government office. Unlike the case of a company or government office switchboard, however, you are not limited to dialing extensions within the office. You can dial any call that the PSTN line supports.

This can be useful and convenient if people you know or work with have a way to make free or low cost VoIP calls to your X6v. If they can do this, then they can make PSTN calls from your X6v. Often this will save considerable amounts of money relative to making the call directly.

- Suppose you are in Los Angeles, and you have a friend in Hong Kong who needs to make frequent calls to local numbers in L.A. Your friend can make free or very low cost VoIP calls to your X6v. Once she has connected to your X6v, she can make local PSTN calls from your X6v to anywhere in L.A.
- Suppose your company has offices in L.A. and in Frankfurt. You can sign up for a VoIP number that is local to Frankfurt. Now when colleagues in Frankfurt want to call local numbers in L.A., they can do so for the price of a local call in Frankfurt: they can call the local Frankfurt number that is assigned to your X6v, and when they connect to your X6v in bridge mode, they can dial local PSTN calls to anywhere in L.A.
- Some cell or mobile phone plans offer free or reduced rate calling to particular numbers. If you designate your X6v's VoIP number under such a plan, then you can make calls under that plan from your cell phone to your X6v. Once you connect to the X6v, you can make a bridge call to

anywhere in L.A. You can do this when you travel anywhere within the area covered by your cell phone plan.


- You can enable single-step dialing, which allows people to dial just the destination number when they make a VoIP to PSTN bridge call. (Enable this feature only if your VoIP service provider tells you to do so.)

There are many more permutations that this feature lets you take advantage of. (For example, see [Bridging from PSTN to VoIP](#) for a description of how to set up pairs of devices in bridge mode in two different locations to facilitate low cost calling between those locations using standard local phones, including cell/mobile phones).

There are several options you can set when you configure a VoIP to PSTN bridge. You can control which callers can access bridge mode:

- You can allow all callers to access bridge mode.
- You can restrict access only to callers with Caller ID.
- You can restrict access only to particular callers based on their Caller ID.
- For whichever callers you allow, you can require that they enter a security code.

If you activate a security code, callers who enter an incorrect code will ring through to the phone that is connected to the X6v. This is convenient for someone who is traveling, and who may some of the time want to use the bridge feature to make local calls, but who other times may want to reach someone in their home or office.

To configure a bridge from VoIP to PSTN, in the VoIP area of the Configuration Manager, click the **Advanced VoIP Setup** icon , in the left menu pane select **Subscription Services**, and then select **Bridging from VoIP to PSTN**:

Setting	Description
Bridge from VoIP to PSTN	Enables or disables the bridge. The default is Disabled .
Auto-Answer VoIP Bridge Calls	Enables auto-answer of VoIP calls. The default is Disabled .
VoIP Bridge Accept Any Call	Enables answering calls with or without Caller ID. The default is Disabled .
VoIP Bridge Accept Anonymous Calls	Enables answering calls without Caller ID. The default is Disabled .
Caller Password	Enables a security code for access to the bridge. The default is Disabled .
Password Dial String	Enter any sequence of up to 24 telephone keypad digits and special characters: 1 2 3 4 5 6 7 8 9 0 # *

Setting	Description
VoIP Bridge Accept Only These Numbers (01 to 10)	Enter up to 10 phone numbers that can access the bridge feature
VoIP Bridge Billing Delay Duration (10 ms)	Time after auto-answer that X6v sends indication to server. The default is 10 x 10 ms = 100 ms.
VoIP Bridge Security Entry Duration (10 ms)	Timeout for entry of security code. The default is 1000 x 10 ms = 10 seconds.

Quick setup tips

To quickly set up a VoIP to PSTN bridge:

- 1 At **Bridge from VoIP to PSTN**, select **Enable**.
- 2 At **Auto-Answer VoIP Bridge Calls**, select **Enable**.
- 3 At **VoIP Bridge Accept Any Call**, select **Enable**.
- 4 Click **Save These Settings**.

With these settings, if you call the X6v's VoIP account, the X6v will answer the call and play the PSTN dial tone. When you hear this tone, you can call any number supported by your standard telephone service, and the call will be bridged to the PSTN.

To add security to a VoIP to PSTN Bridge:

- 1 At **Bridge from VoIP to PSTN**, select **Enable**.
- 2 At **Auto-Answer VoIP Bridge Calls**, select **Enable**.
- 3 In the **VoIP Bridge Accept Only These Numbers** list, enter numbers authorized to make bridge calls.
- 4 If you want to accept anonymous calls in addition to the numbers you list, at **VoIP Bridge Accept Anonymous Calls**, select **Enable**.
- 5 Click **Save These Settings**.

To add a security code for making a bridge call (you can add this feature whether or not you list numbers that you will accept):

- 1** At **Bridge from VoIP to PSTN**, select **Enable**.
- 2** At **Auto-Answer VoIP Bridge Calls**, select **Enable**.
- 3** At **Caller Password**, select **Enable**.
- 4** At **Password Dial String**, enter any sequence of up to 24 telephone keypad digits and special characters:
1 2 3 4 5 6 7 8 9 0 # *
- 5** Click **Save These Settings**.

Once the security code is enabled, callers who dial into your X6v will hear a special tone prompting them to enter the security code. When they successfully enter the security code, they will receive a regular TELCO dial tone, and they can dial the number they want to call over the VoIP network.

To enable single-stage dialing to a VoIP to PSTN bridge:

If your service provider supports single-stage dialing, when the remote caller dials a PSTN number, the VoIP service will direct that call to your X6v. Your X6v will answer the call. The service provider will include in a message to your X6v the PSTN number that the remote caller originally dialed. Your X6v will bridge the call by dialing that PSTN number out its TELCO port.

Follow these steps:

- 1** At **Bridge from VoIP to PSTN**, select **Enable**.
- 2** At **Auto-Answer VoIP Bridge Calls**, select **Enable**.
- 3** At **VoIP Bridge Accept Any Call**, select **Enable**.
- 4** At **VoIP Bridge Single Stage Dialing**, select **Enable**.
- 5** Click **Save These Settings**.

Bridging from PSTN to VoIP

When you make a PSTN (TELCO) call to the X6v in PSTN to VoIP bridge mode, you are connected to the VoIP service that is connected to the X6v. This is like being connected to a switchboard when you call a company or government office.

Unlike the case of a company or government office switchboard, however, you are not limited to dialing extensions. You can dial any call that your VoIP service supports.


This can offer a useful and convenient way to make free or low cost VoIP calls from your X6v even if you are out of your home or office. For example, you can make a local PSTN call to your X6v from your cell or mobile phone, and bridge the call to a low-cost long distance or international call via VoIP. Often this will save considerable amounts of money compared to making the call directly.


- Suppose you live in London, and you have friends and family in Calcutta. You don't have to be at home in order to call them. You can call your X6v's PSTN phone number from any standard phone including your cell phone, and make a low-cost VoIP call to Calcutta.
- Suppose your company has offices in Dubai and in Buenos Aires. You can set the X6v so that when customers call the Dubai office after hours, the X6v automatically bridges the call to Buenos Aires, and staff can answer the call in that office.
- Again, if your company has offices in Dubai and Buenos Aires, you can set up an X6v in bridge mode in each location. Staff off site in Buenos Aires can call into the PSTN number of the X6v in the Buenos Aires office and make a VoIP bridge call to the VoIP number of the X6v in Dubai. Once connected to the X6v in Dubai, they can bridge to the PSTN connection in Dubai, and contact customers and vendors outside the office in Dubai, all for the cost of a local call in Buenos Aires. You can set up a double bridge in each direction. In this way, calls can also be made in the opposite direction, from Dubai to Buenos Aires.

There are several options you can set when you configure a PSTN to VoIP bridge.

- You can control which callers can access bridge mode.
- You can allow all callers to access bridge mode.
- You can restrict access only to callers with Caller ID.[†]
- You can restrict access only to particular callers based on their Caller IDs.[†]
- For the callers you allow, you can require that they enter a security code.

If you activate a security code, callers who enter an incorrect code will ring through to the phone that is connected to the X6v. This is convenient for someone who is traveling, and who may some of the time want to use the bridge feature to make local calls, but who other times may want to reach someone in their home or office.

To configure a bridge from PSTN to VoIP, in the VoIP area of the Configuration Manager, click the **Advanced VoIP Setup** icon , in the left menu pane select **Subscription Services**, and then select **Bridging from PSTN to VoIP**:



Bridging From PSTN to VoIP

Bridge From PSTN to VoIP Enable Disable

PSTN Caller ID Forward to VoIP Enable Disable

Auto-Answer PSTN (TELCO) calls Enable Disable

TELCO Port Accept Any Call Enable Disable

TELCO Port Accept Anonymous Calls Enable Disable

Caller Password Enable Disable

Password Dial String

TELCO Port Accept Only These Numbers

01

02

03

04

05

06

07

08

09

10

Note: To use this feature, your PSTN service must include Caller ID Display.

Setting	Description
Bridge from PSTN to VoIP	Enable or disable the bridge
PSTN Caller ID Forward to VoIP	Your X6v normally forwards your VoIP account Caller ID on any VoIP calls you make, including PSTN to VoIP calls. If you enable 'PSTN Caller ID Forward to VoIP,' then your X6v will forward to the VoIP leg of the call the Caller ID of the PSTN line that originated the bridge call.
Auto-answer PSTN (TELCO) calls	Enables/disables entrance to bridge mode. Set this to Enable.
TELCO Port Accept Any Call	Enables/disables answering calls with or without Caller ID
TELCO Port Accept Anonymous Calls	Enables/disables answering calls without Caller ID
Caller Password	Enables/disables security code to access bridge feature
Password Dial String	Enter any sequence of up to 24 telephone pad digits and special characters: 1 2 3 4 5 6 7 8 9 0 # *
TELCO Port Accept Only These Numbers (01 to 10)	Enter up to 10 numbers that can access the bridge.
Save These Settings	Click this button to save your settings to flash memory.

Quick setup tips

To quickly set up a PSTN to VoIP bridge:

- 1** At **Bridge from PSTN to VoIP**, select **Enable**.
- 2** At **Auto-Answer PSTN Calls**, select **Enable**.
- 3** At **TELCO Port Accept Any Call**, select **Enable**.

4 Click Save These Settings.

With these settings, if you call the X6v's PSTN number, the X6v will answer the call and play a dial tone. When you hear this dial tone, you can call any number supported by your VoIP service, and the call will be bridged to the Internet.

To add security to a PSTN to VoIP Bridge by accepting calls only from authorized numbers:

- 1** At **Bridge from PSTN to VoIP**, select **Enable**.
- 2** At **Auto-Answer PSTN Calls**, select **Enable**.
- 3** At **TELCO Port Accept Any Call**, select **Disable**.
- 4** At **TELCO Port Accept Only These Numbers**, in the boxes 01 to 10 enter numbers authorized to make bridge calls.
- 5** Click **Save These Settings**.

To add a security code for making a bridge call (you can add this feature whether or not you list numbers that you will accept):

- 1** At **Bridge from PSTN to VoIP**, select **Enable**.
- 2** At **Auto-Answer PSTN Calls**, select **Enable**.
- 3** At **Caller Password**, select **Enable**.
- 4** At **Password Dial String**, enter any sequence of up to 24 telephone keypad digits and special characters:
1 2 3 4 5 6 7 8 9 0 # *

5 Click **Save These Settings**.

Once the security code is enabled, callers who dial into your X6v will hear a special tone prompting them to enter the security code. When they successfully enter the security code, they will receive the VoIP dial tone, and they can dial the number they want to call over the VoIP network.

To forward the Caller ID of the incoming PSTN number when someone makes a bridge call:

At **PSTN Caller ID Forward to VoIP**, select **Enable**.

(If this parameter is disabled, the X6v will send its own VoIP Caller ID as the Caller ID of the bridged call).

Miscellaneous TELCO Parameters

If you are having problems with your Caller ID display, Zoom Customer Support may ask you to modify one or more of the Caller ID settings on this page.

The screenshot shows a configuration page titled "Miscellaneous TELCO Parameters". It contains several settings:

- TELCO Port Display Caller ID: Enable Disable
- TELCO Port Caller ID Sent After One Ring: Enable Disable
- TELCO Caller ID Wait Duration (10 ms):
- TELCO Caller ID Clear Duration (10 ms):
- Billing Delay Duration (10 ms):
- TELCO Security Entry Duration (10 ms):

At the bottom of the page are two buttons: "Save These Settings" and "Reboot VoIP".

Emergency Services

The screenshot shows a configuration page titled "Emergency Services". It contains the following information and input fields:

- Emergency Numbers Currently Routed via VoIP: 100, 11x, 911, 999
- Emergency Numbers Currently Routed via the PSTN: (empty field)
- Emergency Numbers to be Routed via VoIP if Either the PSTN Line is Not Available or These Numbers Are Not Configured to be Routed on the PSTN:
- Emergency Numbers to be Routed via the PSTN if the PSTN line is available:

At the bottom of the page are two buttons: "Save These Settings" and "Reboot VoIP".

Setting	Description
Emergency Numbers Routed via VoIP	(Display only) These numbers are automatically routed via VoIP by your VoIP service provider.
Emergency Numbers Routed via the PSTN	(Display only) These numbers are automatically routed via the PSTN.
Emergency Numbers to be Routed via VoIP if Either the PSTN Line is Unavailable or These Numbers Are Not Configured to be Routed on the PSTN	Enter emergency numbers here.
Emergency Numbers To Be Routed via the PSTN if the PSTN is Available	Enter emergency numbers here.

Controlling the X6v from Your Phone

Many VoIP features can be controlled from the phone plugged into your X6v. **For all these commands, pick up the receiver and then enter the command.**

(These commands do not apply to non-VoIP calls. Features for the traditional phone network are normally available from your traditional phone company.)

- *55** Enable Call Waiting on all calls. When a call is waiting, you will hear a tone. You can then press the Flash button on your phone to go back and forth between your 2 callers.
- *56** Disable Call Waiting on all calls.
- *59** Disable Caller ID for call waiting calls.
- *70** Turn off Call Waiting for the next call.
- *71** Turn on Call Waiting for the next call.
- *72** Forward all calls to <phone number>. After you dial *72, dial 8, enter the phone number, then press #.
- *73** Disable Call Forwarding.
- *82** Enable Caller ID for all outbound calls.
- *62** Block Caller ID on all outbound calls.
- *65** Enable Caller ID on all inbound calls.
- *85** Disable Caller ID for all inbound calls.
- *67** Enable Caller ID for the next outbound call.
- *68** Block Caller ID for the next outbound call.
- *66** Redial the last number you dialed.
- *69** Call the last person who called you.

- *77 Block all calls that don't have a Caller ID.
- *87 Stop blocking calls that don't have a Caller ID.
- *78 Do Not Disturb. Your phone won't ring.
- *79 Turn off Do not Disturb. Lets your phone ring.

Resetting Your VoIP Configuration

To reset the X6v to your most recently saved VoIP configuration, put the end of a pin or paper clip into the **VoIP RESET** hole (the top one of two reset holes) in the back panel and hold the button down for 5 seconds or more.

To restore the X6v to the most recent settings given to you by your VoIP service provider, press and hold the **VoIP RESET** button for 5 seconds or more, and then release. Wait two minutes, then press and hold the button for at least 5 more seconds.

To restore the factory default VoIP configuration, press and hold the **VoIP RESET** button for 15 seconds.

5

The X6v and Online Gaming

This chapter covers the setup of the X6v for online gaming with a desktop, notebook, Xbox® or Xbox 360, or PlayStation® 2 or 3.

Do I Need to Do Anything?

There are three cases where you need to set up your modem in order to play online games:

- 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 modem 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 **World in Conflict™**, **Madden NFL 08**, **Counterstrike™**, **Age of Mythology®**, and **Unreal Tournament 2004®**. 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 multi-player game. Popular multi-player games include **StarCraft®**, **Everquest® I and II**, **Diablo II®**, **Hexen II**, the **Myth**

series, **Quake II**, **Half-Life** and **Half-Life II**, **Warcraft® II and III**, **World of Warcraft** and **Lord of the Rings**.

- If you are playing an online game using Xbox or Xbox 360 Live or PlayStation 2 or 3.

In all three cases you will need to follow the steps described in the next section, **Setting Up the X6v for Online Gaming**.

Setting Up the X6v for Online Gaming

Setting up the X6v for online gaming involves two basic steps: **Choosing an IP Address for Gaming** and **Setting Up a Virtual Server or DMZ**. This section provides instructions for doing these tasks on your computer, Xbox, or PlayStation.

Step 1: Choosing an IP Address for Gaming

You need to make sure that the computer or gaming system you use for playing games always has the same IP address. By default, the X6v assigns addresses dynamically (using **Dynamic Host Configuration Protocol** or **DHCP**) to the devices on the local area network whenever they reboot. These addresses won't necessarily always be the same. Therefore, you need to assign a **Static** (unchanging) IP address to every computer or gaming system in the network.

- If you are using a computer for gaming, continue below.
- If you are using an Xbox or Xbox 360, go to page 75.
- If you are using a PlayStation 2 or 3, go to page 76.

If you are using a computer to play an online game:

- 1 If you know the name of your computer or if you have only one computer connected, you can find the MAC address under **DHCP Clients** at the bottom of the **Create New DHCP Server Fixed Host** page. You can also find the MAC address

on the **System Status** page. Click the **System Status** icon and scroll down until you see **DHCP Client Status**.

If you do not know the name of your computer or you have more than one computer connected, follow these steps to find the MAC address:

- a On the computer you want to use for gaming, click the **Start** button (Windows Vista users: you must also click **All Programs**, then **Accessories**) and select **Run**.
- b In the Run dialog box, type **command** and click **OK** to open the **Command** or **MS-DOS** window
- c In the Command Prompt or MS-DOS window (after **C:\>** or **C:\WINDOWS>**), type **ipconfig**, leave a space, then type **/all**

It should look like this: **ipconfig /all**

- d Press **Enter**. The MAC address is displayed as the 12-digit **Physical Address** or **Internet Adapter** address. Write this address down and keep it handy.

2 Now that you have determined the MAC address, you can assign your computer a Static IP address.

- a In the Zoom Configuration Manager, click the **Router Setup** button.
- b On the **Router Setup** page, click the **LAN Configuration** button.
- c On the **LAN Configuration** page, click the **Add DHCP Fixed Host** button. The **Create New DHCP Server Fixed Host** page appears:

Create new DHCP server fixed host IP/MAC mapping

Item	Value
<small>Define your new fixed mapping here. The IP address you choose will be given to the host with the MAC address you specify. The IP address must not clash with an IP address already present in a dynamic address range. You should also ensure that there is a suitable subnet defined for the IP address to reside in. The MAC address should be expressed as 6 hexadecimal pairs separated by colons, e.g. 00:20:2b:01:02:03</small>	
IP address	<input type="text"/>
MAC address	<input type="text"/>
Maximum lease time	86400 <input type="text"/> seconds

Make these entries:

Setting	Values
IP Address	Enter 192.168.0.50 . If you are setting up more than one computer, use different IP addresses. For example, enter 192.168.0.50 for the first computer and 192.168.0.51 for the next computer.
MAC Address	Type the computer's MAC address.
Maximum Lease Time	Leave the default setting.

- d Click **Save Changes** and then **Write Setting to Flash** to save the IP address to permanent memory. Now your computer will always be assigned this address.
- e Now go to [Setting Up a Virtual Server or DMZ on Your Computer](#) on page 78.

If you are using the Xbox or Xbox 360 to play an online game

Follow these steps to assign a static IP to the Xbox:

- 1 Turn on the Xbox.
- 2 In the **System** area of the Dashboard, select **Network Settings**, then **Edit Settings**.

- 3 Select the **IP Settings** tab and then select **Manual**.
 - Enter a Static **IP Address** for the Xbox. Choose any address from 192.168.0.101 to 192.168.0.233.
 - Enter the following **Subnet Mask**: 255.255.255.0
 - Enter the following **Gateway** (X6v) address: 192.168.0.1
 - Click **Done**.
- 4 Turn off the Xbox.
- 5 Connect the Xbox to the X6v.
- 6 Now go to page 81 for instructions on setting up a DMZ on the Xbox. This will prevent the X6v's firewall from stopping connections to the Xbox.

If you are using PlayStation 3 to play an online game

Follow these instructions to assign a Static IP address to your PlayStation:

- 1 Insert your Network Access Disc into the PlayStation.
- 2 On the home menu, select **Settings**, then **Network Settings**.
- 3 Select **Internet Connection Settings**.
- 4 Select **Yes** to disconnect from the Internet.
- 5 For your network type, select **Wireless**.
- 6 Select **Address Settings**, then **Custom**.

- 7 Under **IP Address Setting**, select **Manual** and enter the following:
 - For **IP Address**, choose any address from 192.168.0.101 to 192.168.0.233.
 - For **Subnet Mask**, enter 255.255.255.0
 - For **Default router** (X6v) address, enter 192.168.0.1
- 8 Now go to page 83 for instructions on setting up a DMZ on the PlayStation 3. This will prevent the X6v's firewall from stopping connections to the PlayStation.

Step 2: Setting Up a Virtual Server or DMZ

You set up either a virtual server or a DMZ (Demilitarized Zone) so that the modem's firewall won't block the other players from your system during your gaming. The main difference between the virtual server and the DMZ is the amount of access someone has to your system.

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

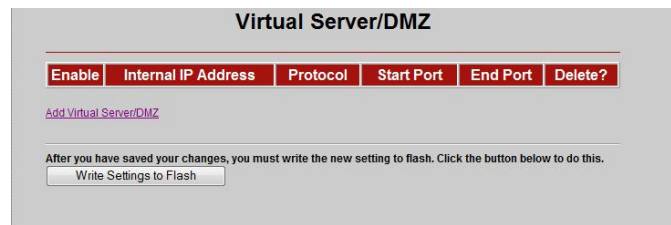
A DMZ differs from a virtual server in that it allows access on all ports to the computer. Because of this, DMZ's are less secure than virtual servers and should be used with caution on your computer. For Xbox Live and PlayStation 2, a DMZ is OK since security is not as much of an issue as it is for your computer.

- If you are playing a **peer-to-peer** or **multi-player game** on your computer, go to [Setting Up a Virtual Server or DMZ on Your Computer](#) on page 78.
- If you are using Xbox Live, go to [Setting Up a DMZ on an Xbox or Xbox 360](#) page 81.
- If you are using PlayStation 2, go to [Setting Up a DMZ on a PlayStation 2 or 3](#) on page 83.

Setting Up a Virtual Server or DMZ on Your Computer

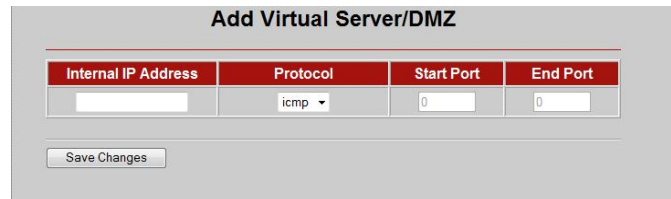
Note: If you have third-party firewall software, such as the Windows XP firewall, installed on your computer, you may need to deactivate it before setting up the virtual server or DMZ. Otherwise your computer may block the ports you want to open.

- 1 Click the **Router Setup** icon. Then, click the **Virtual Server/DMZ** button to display this page:



The screenshot shows the 'Virtual Server/DMZ' configuration page. At the top, there is a table with columns: 'Enable', 'Internal IP Address', 'Protocol', 'Start Port', 'End Port', and 'Delete?'. Below the table is a link labeled 'Add Virtual Server/DMZ'. At the bottom, there is a text instruction: 'After you have saved your changes, you must write the new setting to flash. Click the button below to do this.' followed by a 'Write Settings to Flash' button.

- 2 On the **Virtual Server/DMZ** page, click the **Add Virtual Server/DMZ** link to display the **Add Virtual Server/DMZ** page:



The screenshot shows the 'Add Virtual Server/DMZ' configuration page. It features a table with four columns: 'Internal IP Address', 'Protocol', 'Start Port', and 'End Port'. The 'Protocol' column is currently set to 'icmp'. Below the table is a 'Save Changes' button.

3 Make the following entries:

Setting	Values
Internal IP Address	Enter the IP address that you specified on the Create New DHCP Fixed Host Server page.
Protocol	<p>If you know your protocol (udp or tcp) and port number(s) from your game instructions, select the protocol from the list.</p> <p>If you do not know your protocol or port number(s), you need to set up your computer as a DMZ by selecting DMZ from the Protocol list. This will open up all ports on the computer to all communication over the Internet.</p> <p>Warning: Setting up a DMZ removes the protection provided by the ADSL Ethernet's firewall. We therefore recommend that a DMZ be used only when necessary.</p>
Start Port	<p>If you designated your computer as a DMZ, you do not have to enter anything here.</p> <p>If you are playing another peer-to-peer or multi-player game, your game instructions should tell you what ports to enter here. To enter a number, you must enter tcp or udp in the Protocol box.</p> <p>If you only need to open one port, enter the same port number for both Start Port and End Port. If you need to open a range of ports, enter the starting port number of the range here.</p> <p>The highest supported port number is 65535.</p>

Setting	Values
End Port	<p>If you designated your computer as a DMZ, you do not have to enter anything here.</p> <p>If you are playing another peer-to-peer or multi-player game, your game instructions should tell you what ports to enter here. To enter a number, you must enter tcp or udp in the Protocol box.</p> <p>If you only need to open one port, enter the same port number for both Start Port and End Port. If you need to open a range of ports, enter the starting port number of the range here.</p> <p>The highest supported port number is 65535.</p>

4 Click **Save Changes** and then **Write Settings to Flash**.

Important: If you have not already configured the computer for wireless security, see page 29 for instructions on setting WEP or page 33 for setting WPA.

If your security has been configured, your online gaming setup is complete.

Setting Up a DMZ on an Xbox or Xbox 360

- 1 Click the **Router Setup** icon. Then, click the **Virtual Server/DMZ** button to display this page:

- 2 On the **Virtual Server/DMZ** page, click the **Add Virtual Server/DMZ** link to display the **Add Virtual Server/DMZ** page:

- 3 Make the following entries:

Setting	Values
Internal IP Address	Enter the IP address that you specified on the Xbox IP Settings screen.
Protocol	Select DMZ to enable your Xbox as a DMZ.
Start Port	The field remains unavailable because you selected DMZ. No entry is required.
End Port	The field remains unavailable because you selected DMZ. No entry is required.

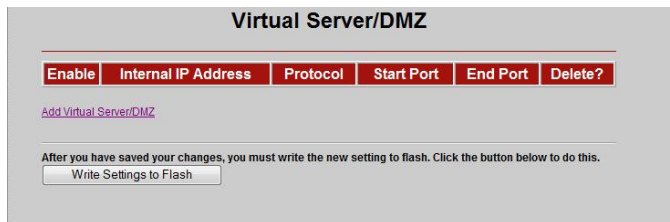
- 4 Click **Save Changes** and then **Write Settings to Flash**.
- 5 **Update the Xbox Dashboard:**
Make sure you have your Xbox Live Starter Kit at hand. Insert the Xbox Live CD into your Xbox. When the update is complete, the main menu will include an **Xbox Live** entry.
- 6 **Insert the Xbox Communicator module into the Xbox Controller expansion slot** (top slot). Then insert the headset plug into the Communicator module.
- 7 **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.)

Important: If you have not already configured the Xbox for wireless security, see page 29 for instructions on setting WEP or page 33 for setting WPA.

If your security has been configured, your online gaming setup is complete.

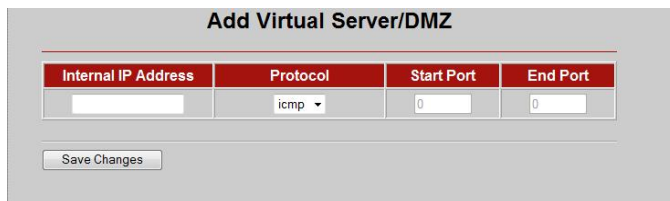
Setting Up a DMZ on a PlayStation 2 or 3

- 1 Click the **Router Setup** icon. Then, click the **Virtual Server/DMZ** button to display this page:



The screenshot shows the 'Virtual Server/DMZ' configuration page. At the top, there is a table with columns: 'Enable', 'Internal IP Address', 'Protocol', 'Start Port', 'End Port', and 'Delete?'. Below this table is a link labeled 'Add Virtual Server/DMZ'. At the bottom of the page, there is a text instruction: 'After you have saved your changes, you must write the new setting to flash. Click the button below to do this.' followed by a button labeled 'Write Settings to Flash'.

- 2 On the **Virtual Server/DMZ** page, click the **Add Virtual Server/DMZ** link to display the **Add Virtual Server/DMZ** page:



The screenshot shows the 'Add Virtual Server/DMZ' configuration page. It features a table with four columns: 'Internal IP Address', 'Protocol', 'Start Port', and 'End Port'. The 'Protocol' column has a dropdown menu currently set to 'icmp'. Below the table is a 'Save Changes' button.

- 3 Make the following entries:

Setting	Values
Internal IP Address	Enter the IP address that you specified on the PlayStation's IP Address setting screen.
Protocol	Select DMZ to enable your PlayStation as a DMZ.
Start Port	The field remains unavailable because you selected DMZ.
End Port	The field remains unavailable because you selected DMZ.

4 Click **Save Changes** and then **Write Settings to Flash**.

Important: If you have not already configured wireless security on the PlayStation, see page 29 if your network uses WEP, or page 33 if your network uses WPA.

If your security has been configured, your online gaming setup is complete.

6

Using Router Setup

Router Setup is primarily for technically advanced users. For most people, the options that are set by default when the X6v is installed are sufficient.

*However, those who want or need to change the advanced X6v settings can do so by logging in as **admin** and using the **Router Setup** page in the **Zoom Configuration Manager**. This chapter explains the advanced options and features of the X6v modem and how to apply them to your network.*

The information in this chapter applies to you if:

- *Your Internet service provider instructs you to enable, disable, or change the default settings for your X6v*
- *You need to change your Wide Area Network settings*
- *You want to change the default firewall settings to block particular IP addresses and intrusive hosts*
- *You want to change your ADSL password*
- *You have customized your configuration and want to back it up for future use or apply it to additional modems*
- *You want to set up fixed IP addresses for your computer(s)*

Note: *Users who want to set up Quality of Service (described in this section) can do so more easily using the Zoom Install Assistant.*

Viewing the Router Setup Options

You open the **Router Setup** page by clicking the **Router Setup** icon at the top of the **Zoom Configuration Manager** page. The page opens and displays buttons organized into three groups: **Configuration**, **Status**, and **Administration**:



Configuration Options

When you click a **Configuration** button, a page opens to the option you selected. The following table describes each option and the tasks you can perform.

This button...	Opens a page that lets you...
WAN Configuration	Specify how the Wide Area Network (WAN) setup is configured. Some of the values need to be supplied by your ISP/ADSL provider.

This button...	Opens a page that lets you...
Advanced Firewall Filter	Define an additional layer of security for the computers in your network. For example, if you create a DMZ interface using the Virtual Server/DMZ page (see below), you can enable the firewall filtering and add a security policy that blocks certain protocols from reaching the DMZ machine.
ADSL Configuration	Adjust the ADSL settings on your modem. Typically, you do not need to change these ADSL settings unless instructed by your service provider.
Ethernet Configuration	View and change the settings on the Ethernet ports on your X6v. Typically you should not need to change these settings.
DNS	Allows you to specify multiple DNS servers. Typically, most users do not need to enter a DNS server unless instructed by their ISP.
LAN Configuration	Specifies the settings that control the connection between the X6v modem and your Ethernet jack. Sets a fixed IP address for your computer. Do not change the LAN configuration unless instructed to do so. See the online Help for LAN configuration details.
Routing Table	Set up the routes on which you want the X6v to send data that it receives on a particular interface, such as a LAN or Ethernet interface. Routes specify the IP address of the next device, interface, or Internet destination to forward data to, based on the ultimate destination of the data.

This button...	Opens a page that lets you...
Virtual Server/DMZ	Open access to your computer by creating a virtual server or a DMZ (Demilitarized Zone). By default, your modem uses NAT (Network Address Translation) to hide your networked computers from users on the Internet. However, there are times when you may want to give outside access to the computers in your network. If so, you can set up a virtual server or DMZ to allow outside users access to a computer on your network. You may want to allow access, for example, if a LAN computer is hosting Internet games or running a Web server.
PPP Half Bridge	Share the public IP address assigned by your ISP with a single PC on the LAN. This avoids problems caused by certain applications having to work through NAT (such as online games or FTP servers) and avoids the need to run a PPP software stack on the PC.
UPnP (Universal Plug and Play)	Connect automatically with other UPnP-enabled software and hardware. The Internet Gateway Device (IGD) protocol makes it possible for applications running on the network to automatically configure NAT routing.
Per Port PVC	Assign an Ethernet port to a Permanent Virtual Circuit (PVC) . This feature is commonly used for delivering video.
Port Settings	Conveniently change the default port settings. You will need to use this feature if the X6v is hosting a web or Telnet server.
MAC Filtering	Prevent network devices with the specified MAC addresses from accessing the Internet.
Management Control	Enable or deny access to X6v services – HTTP, Telnet, SNMP – to local network devices and/or remote users.

This button...	Opens a page that lets you...
QoS (Quality of Service)	Assign each port (ETHERNET ports 1-4 and the wireless port) a priority of High or Medium. This lets you assure better performance for gaming and VoIP, for example.
TR 069 (Technical Report 069)	Allow an Access Control Server (ACS) to control and configure your X6v.

Status Options

The **Status** buttons open reports that provide real-time information about your connections and networks. The reports refresh themselves to give you the most current information.



Typically, these reports are used for maintenance purposes and troubleshooting.

The following table describes each report in the **Status** group:

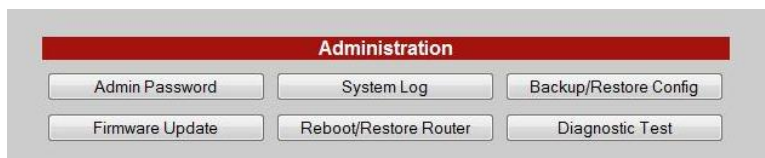
This button...	Opens a page that lets you...
ADSL Status	View information, such as the ADSL Line State, and Upstream and Downstream speeds.
Wireless Status	View information, such as your Link Speed, SSID, Default Channel, and Mac Address of your wireless computer.
Ethernet Status	View information about Rx (Receive) and Tx (Transmit) Packets.

To see sample reports, go to page 129.

Administration Options

The buttons in the **Administration** group are typically used for administrative tasks, such as updating the modem's firmware,

changing your **Zoom Configuration Manager** password, and putting back your modem's configuration file.



The following table lists each button in the **Administration** group and gives a brief description of the things that you can do with that feature.

This button...	Opens a page that lets you...
Admin Password	Change the Admin password to the Zoom Configuration Manager . The original user name and password for the administrator are: User name: admin Password: zoomadsl
Firmware Update	Specify the path to the upgrade file you need to update your firmware. Use the Browse button on this page to navigate to the file, then click the Upload button to perform the firmware update.
System Log	View data generated or acquired by routine system communication with other devices. This information does not necessarily represent unexpected or improper functioning and is not captured by the system traps that create alarms. You can save the system log to a file.
Reboot/Restore Router	Reboot the X6v and reset its configuration to the factory defaults.
Backup/Restore Config	Save your current configuration settings so that they may be restored at a later time.

Setting	Description
Diagnostic Tests	Run a diagnostic test to help isolate any problems you may be having.

Using the WAN Configuration Settings

When do I need the WAN Configuration page?

The **WAN Configuration** page contains critical information about your Wide Area Network (WAN), ADSL setup, and Internet access. Some of these values are provided by your ISP/ADSL provider and need to be entered on this page. To determine if you need to add other values, read the table descriptions that follow the picture. Note that **Protocol, Encapsulation, VPI, VCI, PPP, and NAT** also appear on the **ADSL Setup** page. Most likely you have already entered values for these settings and only need the WAN Configuration page for setting up an advanced feature such as enabling a disconnect timeout on your PPP connection.

WAN Configuration Page

The screenshot shows the WAN Configuration page with the following settings:

Section	Setting	Value
Selected PVC	Selected PVC	PVC 0
	Protocol	PPPoE
	Encapsulation	LLC
	VPI	0
VCI	VCI	35
	PPP	
Username	ppp4@zoom.com	
Password	*****	
Service Name		
Disconnect timeout	0 minutes	
Authentication	AUTO	
NAT	Enabled	
ATM	ATM Traffic Class	UBFR
	Peak Cell Rate	2000
	Burst Tolerance	0
	Max Cell Rate	0
	Max Burst Size	0
	Sustainable Cell Rate	0
RIP	Accept V1	false
	Accept V2	false
	Send V1	false
	Send V2	false

Buttons: [Select PVC](#),

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

The following table describes the settings on the **WAN Configuration** page and the values that you can enter. After you enter your values, click **Save Changes** and then **Write Settings to Flash**.

Note: The table shows settings in addition to the ones shown in the picture. Depending upon your protocol setting, your WAN configuration might have all or only some of the settings.

Setting	Description
Protocol (Internet Connection type)	Your Internet Service Provider supplies this value. If your service provider instructs you to use 1483 Bridged mode, select 1483 Bridged + NAT to take advantage of your modem's advanced routing and firewall features.
Encapsulation	The encapsulation value should match your ADSL provider's encapsulation. The value refers to the way that data is passed over the Internet. An example value is LLC (Logical Link Control). Your ADSL provider supplies this value when you sign up for ADSL service.
VPI	Virtual Path Identifier ranges from 0 – 256. Your ADSL provider supplies the VPI when you sign up for ADSL.
VCI	Virtual Circuit Identifier ranges from 0 – 65536. Your ADSL provider supplies the VCI when you sign up for ADSL service.
Username	Your ADSL provider supplies this username when you sign up for ADSL service. (It is not the same as the username and password for the Zoom Configuration Manager .)
Password	Your ADSL provider supplies this password when you sign up for ADSL.

Setting	Description
Service Name	This is an optional value that your service provider may ask you to enter.
Disconnect timeout	The amount of time before the PPP connection drops if there is no activity. A value of 0 means stay connected even if your network stays idle.
Authentication	The type of authentication protocol used during the negotiation of the PPP connection. This protocol may be specified by your ISP. One option, CHAP (C hallenge H andshake A uthentication P rotocol), encrypts your user name and password during the negotiation. P assword A uthentication P rotocol does not.
NAT	Network Address Translation. By default, this setting is Enabled . NAT keeps a table of individual private IP addresses in your network and refers to the table when incoming requests are made. If no matches are found, the incoming data cannot come into your network. An Enabled setting keeps your IP addresses hidden from outside users. Disabled is some times used if you want to use Public IP addresses.
MTU	Maximum Transmission Unit. Largest physical packet size, measured in bytes, that the modem can send. Any messages larger than the MTU have to be fragmented before being sent.
Obtain IP Address	Enable this button if your service provider is using DHCP and you are using the 1483 protocol. If you are unsure of what your service provider is using select this button.

Setting	Description
Specify an IP Address	Enable this button if you are using a static IP address and you are using 1483 protocol. Typically you have to request and pay extra for a static IP address.
IP Address, Subnet Mask, Default Gateway, and DNS	If you are using a Static IP address, enter the values for IP Address , Subnet Mask , Default Gateway , and DNS server that your service provider gave you. You must also be using the 1483 protocol.
Ethernet Filter Type	Specifies the type of Ethernet filtering that is performed by the bridge interface. All -Allows all types of Ethernet packets through the port. Ip -Allows only IP/ARP types of Ethernet packets through the port. PPPoE -Allows only PPPoE types of Ethernet packets through the port.
ATM Traffic Class Peak Cell Rate Burst Tolerance Max Cell Rate Max Burst Rate Sustainable Cell Rate	These settings allow you to give priority to data that is sent over the network. Important! You must make arrangements with your ADSL provider to use anything except UBR (Unspecified Bit Rate) in the Traffic Class setting. Your service provider will also supply you with the Cell, Burst, and Tolerance Rates.

Setting	Description
RIP	<p>RIP is an Internet protocol that you can set up to share routing table information with:</p> <ul style="list-style-type: none"> ➤ LAN devices that support RIP ➤ Remote networks connected via the ADSL line ➤ Your ISP's location <p>Most small home or office networks do not need to use RIP since they have only one router and one path to an ISP. In these cases there is no need to share routes because all Internet data from the network is sent to the same ISP gateway.</p> <p>You may want to configure RIP if any of the following circumstances apply to your network:</p> <ul style="list-style-type: none"> ➤ Your home network setup includes an additional router or RIP-enabled PC or device. These routers will need to communicate via RIP to share their routing table information. ➤ Your network connects via the ADSL line to a remote network, such as a corporate network. In order for your modem to learn the routes used within your corporate network, they should both be configured with RIP. ➤ Your ISP requests that you run RIP for communication with devices on their network
Accept V1	Accept Version 1 of the RIP protocol.
Accept V2	Accept Version 2 of the RIP protocol.

Setting	Description
Sent V1	Send Version 1: Send RIP information to other RIP-enabled devices.
Sent V2	Send Version 2: Send RIP Information to other RIP-enabled devices.

Using the Ethernet Configuration Settings

Do I need to change my Ethernet settings?

The **Ethernet Configuration** page contains information about the Ethernet ports on your ADSL modem. Typically you should not need to change these settings. However, if you are having problems establishing your Ethernet connection, you may need to change the **Speed/Duplex** value to match that of the Ethernet NIC in your computer. Here is a picture of the **Ethernet Configuration** page:

Ethernet Configuration

Port	Configuration	Linked	Speed/Duplex
#1	100/Full	✓	100/Full
#2	AutoNego	✗	Autonego
#3	AutoNego	✗	Autonego
#4	AutoNego	✗	Autonego

Save Changes

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

Write Settings to Flash

The following table describes the Ethernet Configuration settings. If you change any of the settings, click **Save Changes**, and then **Write Settings to Flash**.

Setting	Description
Port	The Ethernet Ports 1-4 on the back of your modem.
Configuration	Shows how your Ethernet ports are set up.
Linked	A check mark indicates that the Ethernet port is connected.
Speed/Duplex	If you are having problems establishing your Ethernet connection, try setting the Speed/Duplex value to match that of the Ethernet NIC in your computer.

Setting Up a Static Routing Table

Do I need static routing?

Most users do not need to set up static routes. The default route used in your modem will forward all packets correctly. However, if you set up your network with different subnets, you can use static routing to ensure your packets are handled correctly.

You can manually create a static route to tell the modem how to reach a specific IP network. The route entry specifies a destination network (or single host), together with a mask to indicate what range of addresses the network covers, and a next-hop gateway address or interface. If there is a choice of routes for a destination, the route with the most specific mask is chosen.

To route to a destination that is not on any local network, a route may be added via a gateway, for instance another router. The gateway IP address must be on the same subnet as one of the router's interfaces.

Here is a picture of the **Static Routes** page:

The following table describes Routing Table settings. If you change any of the settings, click **Add**, and then **Write Settings to Flash**.

Setting	Description
Existing Routes	This table shows the existing Static routes set up on your ADSL Modem.
Destination	Enter the Subnet IP address of the destination.
Gateway	Enter the Gateway IP address of your destination's subnet. The HOP gateway must be on the same subnet as the modem.
Mask	Enter the subnet mask (range of IP addresses) of the destination IP addresses based on the above subnet IP address of the destination.
Metric	The number of hops. This should usually be left at 1.
Advertise	Enable this if you want to advertise this route.

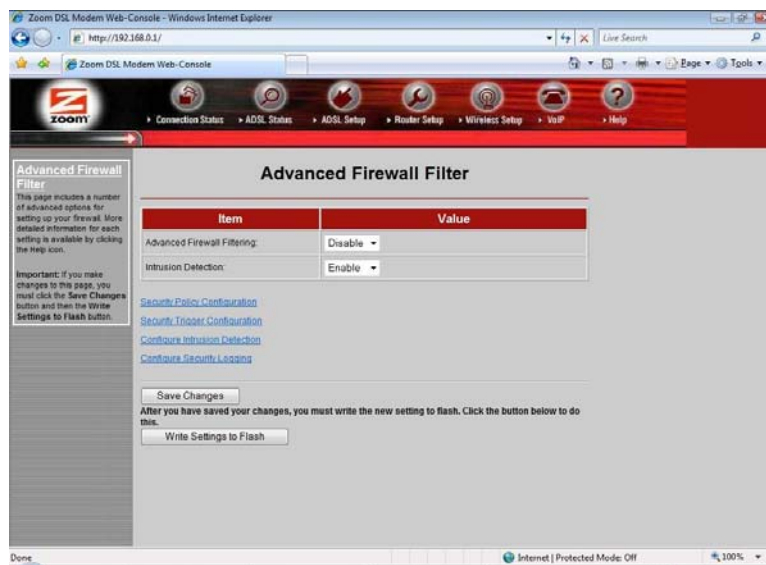
Adding Extra Security with Advanced Firewall Filtering

Do I need extra security?

Setting up advanced firewall security provides an additional layer of security. For example, if you create a DMZ interface for gaming using the **Virtual Server/DMZ** page, you can enable the firewall filtering and add a security policy that blocks IP addresses, ports, aliases, and certain protocols from reaching the DMZ machine.

When you use the **Advanced Firewall Filtering** feature, you will move through multiple screens. Follow the steps below to set up this feature.

- 1 Open the **Advanced Firewall Filter** page by clicking **Advanced Firewall Filter** on the **Router Setup** page.



Important! Do not enable **Advanced Firewall Filtering** on the **Advanced Firewall Filter** page until you create your security policy. Otherwise, if you enable **Advanced Firewall Filtering** before you create your policy, you will block all outgoing and incoming traffic.

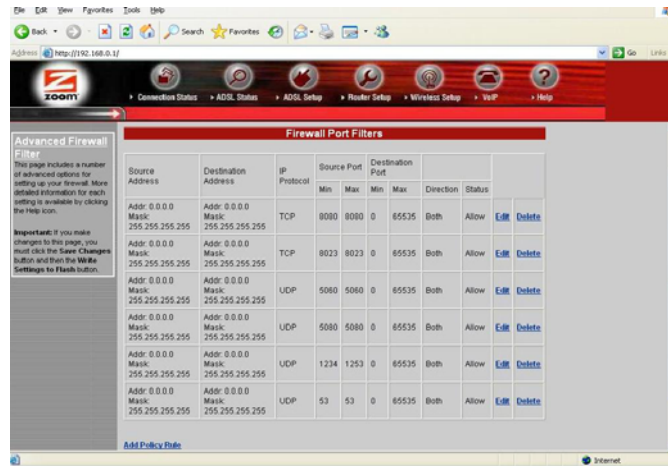
- 2 Click the link to **Security Policy Configuration** on the **Advanced Firewall Filter** page to open the page where you will select the type of policy that you intend to change.



- 3 Choose the **Policy Type** that you want, then click the **Policy Rules...** link. You can set one of three **Policy Types**:
 - Choose the **External – Internal Filter Rules** policy to allow or block what is sent from the WAN to the LAN.
 - Choose the **External –DMZ Filter Rules** policy to allow or block what is sent from the WAN to the DMZ machine or the Virtual Server.
 - Choose the **DMZ-Internal Filter Rules** policy to allow or block what is sent from a DMZ machine to your LAN.

- When the page that corresponds to the selected policy type opens, view the current rules, then **Edit** or **Delete** the current rule or **Add** a new rule, using the links on the page.

For example, if you selected the **External – Internal Filter Rules** policy, and you have a VoIP setup, the Configuration Manager would display a page similar to this:



Important! If your setup includes VoIP services, do **not** edit the default settings that are listed in the above figure.

- To add a new policy, click the **Add Policy Rule** link. The **Add Firewall Policy Rule** page opens.



You use the settings on the **Add Firewall Policy Rule** page to configure your firewall security. In setting your criteria or rules, it is important to know whether you want to block traffic or allow traffic into your network. This is controlled by the **Traffic Inbound** and **Traffic Outbound** settings where you choose **Allow** or **Block**. After you determine what you want to do, you then fill in the other settings to specify what it is that you want to block or allow.

Suppose you enter **Allow** in the **Traffic Inbound** and **Outbound** settings and **Any** in the **Src Address** setting. This sets the firewall to allow any traffic into your network. Conversely, suppose you choose **Block** for **Traffic Inbound**, choose **Assign** for **Src Address** and specify a **range of IP addresses**. This sets the firewall to block all traffic that has the IP addresses you specified.

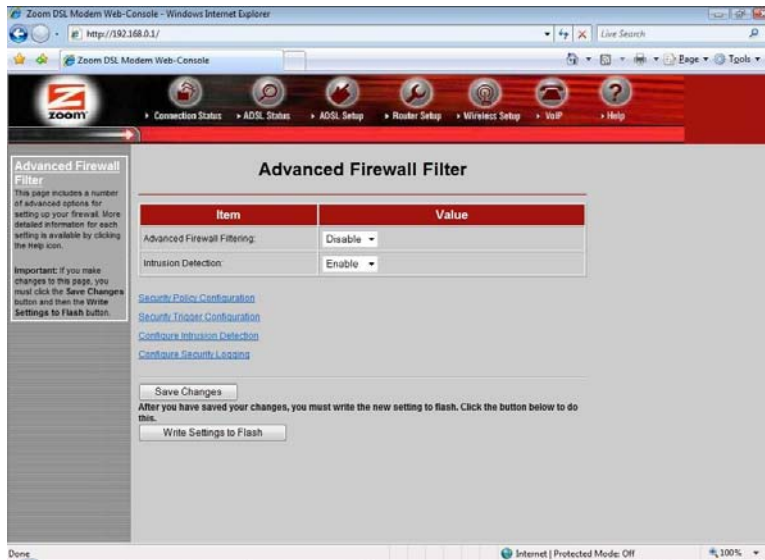
The following table shows you the criteria that you can enter:

Setting	Description
Source Address	Lets you specify Any for all IP addresses or a specific range of IP addresses from a particular source to be blocked or allowed.
Destination Address	Lets you specify Any for all IP addresses or a specific range of IP addresses of a destination to be blocked or allowed.
IP Protocol	Lets you specify a protocol to be blocked or allowed. eq is equals and neq is not equal. For example, eq TCP will allow only TCP. neq TCP will allow everything including TCP.
Source Port	Lets you block or allow traffic from a particular port.
Destination Port	Lets you block or allow traffic going to a destination port.

Setting	Description
Direction	Lets you block or allow inbound/outbound traffic based on the rules you set up in the policy.
Status	Specifies if the filter will Allow traffic.

6 Click **Save Changes** then **Write Settings to Flash**.

7 Return to the **Advanced Firewall Filter** page and select **Enable** as the value for **Advanced Firewall Filtering**. Then click **Write Settings to Flash**.



Setting Security Logging

What is security logging?

Security logging is a list of events (computer activity and user activity) that alerts you to potential security issues. Based on the **Level** selected, you can record all or some of these events. It also lets you examine the effectiveness of your blocking and intrusion detection. You can set the level of importance of the logged event and receive alerts if particular IP addresses are trying to gain access to your network.

To set security logging on, follow these steps:

- 1 Click **Advanced Firewall Filter** on the **Router Setup** page. Then, click the link to **Configure Security Logging**. The **Security Logging Configuration** page opens:

Logging Type	Status	State	Level	Output to:
Session Logging	Enabled Level: notice Output to Event Log	Enable	notice	Event Log
Blocking Logging	Enabled Level: notice Output to Event Log	Enable	notice emergency alert critical error warning notice informational debug	Event Log
Intrusion Logging	Enabled Level: notice Output to Event Log	Enable		Event Log

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

Write Settings to Flash

- 2 Enable the **Logging Types** that you want and set the **Level**. You can also print (**Output to**) the information to your console or to a file (**Event Log**).

Configuring Intrusion Detection

What is intrusion detection?

Intrusion detection protects your network from hackers who use the Internet to damage your network. Your modem's default **Intrusion Detection** setting should work fine for most hacker attacks, but there is additional functionality that you can set up. Your modem offers protection from various Denial of Service (DOS) attacks; prevents users from scanning your ports to try to access your computer; and can blacklist any host trying to damage your network.

Follow these steps to enable additional intrusion detection:

From the **Router Setup** page, click **Firewall**. Then click the link to **Configure Intrusion Detection**. The **Configuration** page opens:

Item	Value
Use Blacklist	false ▾
Use Victim Protection	false ▾
Victim Protection Block Duration	600 seconds
DOS Attack Block Duration	1800 seconds
Scan Attack Block Duration	86400 seconds
Maximum TCP Open Handshaking Count	5 per second
Maximum Ping Count	15 per second
Maximum ICMP Count	100 per second

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

The following table shows you the values you can enter:

Setting	Description
Use Blacklist	Blacklisting denies an external host access to your computer/network if an intrusion from a host has been detected. Access to the network is denied for ten minutes.
Victim Protection Block Duration	The length of time that packets destined for the victim of a spoofing attack are blocked.
Use Victim Protection	Protection for your system against broadcast pings. An attacker sends out a ping with a broadcast destination address and a spoofed source address. Packets destined for the victim of a spoofing attack are blocked for a specified duration.
DOS Attack Block Duration	The duration that hosts are blocked once a Denial of Service (DOS) attack is detected.
Scan Attack Block Duration	The length of time that traffic from IP addresses doing the port scan are blocked once a port scan is detected. Port scans are used to determine if you have any open ports that can be accessed.
Maximum TCP Open Handshaking Count	Sets the maximum number of TCP open session requests allowed per second before a SYN flood attack is detected. SYN Flood is a specific type of DOS attack.

Setting	Description
Maximum Ping Count	Sets the maximum number of pings per second before an Echo Storm is detected. Echo Storm is a DOS attack where the attacker sends oversized ICMP datagrams to the network using the ping command.
Maximum ICMP Count	Sets the maximum number of ICMP packets per second before an ICMP Flood is detected. ICMP Flood is a DOS attack where the attacker tries to flood the network with ICMP packets in order to prevent legitimate network traffic.

Adding a DNS Server Name

Do I need to add a DNS server name?

Typically you should not need to enter a DNS server name as it is assigned automatically when your connection is established. However, your ISP may instruct you to enter an **IP address** for a **DNS server name**. Here is a picture of the DNS page where you add the **IP address**:

DNS

DNS server list

DNS server IP address	Delete
-----------------------	--------

Add new DNS server

New DNS server IP address: Add

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

Write Settings to Flash

Note: If a **DNS server IP address** is currently assigned, it will be displayed on the page. You must delete it before adding the new IP address.

The following table shows you the values to enter. After you enter the value, click **Add**, then **Write Settings to Flash**.

Setting	Description
DNS Server List	Shows the list of currently configured DNS servers.
New DNS Server IP Address	Enter the IP address of the DNS server that your ISP instructed you to enter.

Creating a Virtual Server or a DMZ

Do I need to create a virtual server or DMZ?

By default, your modem uses NAT to hide your computers from users on the Internet; however, there may be times when you want to allow access by outside users to a computer on your network. For instance, you would want to allow access if a computer in your network is hosting Internet games or running a web server. For more information about the **Virtual Server/DMZ** feature and the differences between a virtual server and a DMZ, see page 77. For information about setting up a Virtual Server or DMZ for gaming, see [Setting Up the X6v for Online Gaming](#) on page 73.

Here is a picture of the **Virtual Server/DMZ** page:

Enable	Internal IP Address	Protocol	Start Port	End Port	Delete?
--------	---------------------	----------	------------	----------	---------

[Add Virtual Server/DMZ](#)

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

Click the **Add Virtual Server/DMZ** link to open the **Add Virtual Server/DMZ** page:

Internal IP Address	Protocol	Start Port	End Port
<input type="text"/>	icmp	<input type="text" value="0"/>	<input type="text" value="0"/>

The following table shows you the values you can enter. After you enter the value, click **Save Changes**, then **Write Settings to Flash**.

Setting	Description
Internal IP Address	<p>The IP address of the computer where you will set up the virtual server or DMZ.</p> <p>Note: You should use fixed IP mapping to ensure that the computer you are setting up as the virtual server or DMZ is always assigned the same IP address by your modem's DHCP server. To assign a fixed IP map, see Step 1: Choosing an IP Address for Gaming on page 73.</p>
Protocol	<p>Select the protocol that you want to allow through to the computer. Select DMZ if you want to allow all protocols and all ports to be open on the computer.</p>
Start Port	<p>If you selected TCP or UDP, you must specify the port(s) where you want to allow access. If you need to open a range of ports, enter the first port number here. If you need to open only one port, enter the port you wish to open as both the Start Port and End Port.</p>
End Port	<p>If you selected TCP or UDP, you must specify the port(s) where you want to allow access. If you need to open a range of ports, enter the first port number here. If you need to open only one port, enter the port you wish to open as both the Start Port and End Port.</p>

Using the ADSL Settings

Do I need to change my ADSL settings?

Typically you should not need to change your ADSL settings; however, you may be instructed to do so by your service provider. Or, if you are having problems establishing a physical layer connection, you may want to change a couple of the settings on the **ADSL Configuration** page.

Here is a picture of the **ADSL Configuration** page where you change your settings:

The screenshot shows the 'ADSL Configuration' page. It features a table with two columns: 'Item' and 'Value'. The table contains the following rows:

Item	Value
BitSwap	Disable
BitSwapUp	Disable
Standard	ADSL2PlusAuto
EC/FDM Mode	EC
Activate Line	None

Below the table is a 'Save Changes' button. Underneath that is a note: 'After you have saved your changes, you must write the new setting to flash. Click the button below to do this.' Below the note is a 'Write Settings to Flash' button.

The following table shows you the values to enter. After you enter the values, click **Save Changes**, then **Write Settings to Flash**.

Setting	Description
BitSwap	Enables or disables bit swapping in both upstream and downstream directions. If you experience frequent connection drops, it may help to change the bit swap settings.
BitSwapUp	Enables or disables upstream bit swapping.

Setting	Description
Standard	If you are having problems establishing the physical layer connection, you can try selecting different settings to see if this helps you connect. (If the INTERNET light on the modem is flashing then the physical layer connection is down; if the INTERNET light is steady on, then the problem is elsewhere.) The default is ADSL2PlusAuto .
EC/FDM Mode	If you are having problems establishing the physical layer connection, you can try changing this value to EC .
Activate Line	Select None if there are no changes to the current mode. Select Abort if you want to stop the modem from connecting. The status will show up as idle on the ADSL Status page. Select Start to restart the connection.

Changing Your LAN Settings

When would I need to change my LAN settings?

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) is a protocol that enables your modem to manage the assignment of IP addresses to computers and devices on your Ethernet (LAN) network, as well as to the internal VoIP system on the X6v. Enabling DHCP on your modem allows it to assign temporary IP addresses to your computers whenever they connect to your network. You can control the amount of time that elapses before a new address is issued or renewed. You can extend the range of IP addresses that are assigned to your network devices should you add new devices to your network. You can also change the default LAN IP address for your modem.

NOTE: If you change your modem's IP Address, you must first change the IP Address settings of your VoIP System.

Here is a picture of the **LAN Configuration** page:

Item	Value
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	
Status	Enable
Maximum Lease Time	86400 seconds
Default Lease Time	86400 seconds
Start IP address	192.168.0.4
End IP address	192.168.0.24

Save Changes

Existing DHCP server fixed host

Add DHCP fixed host

The following table shows you the values to enter. After you enter the values, click **Save Changes**, then **Write Settings to Flash**.

Setting	Description
IP Address	The LAN IP address of your modem. This is the IP Address at which PCs and other devices in your network will contact your modem.*
Subnet Mask	The modem's subnet mask address.
Status	You should leave this setting on Enable. Disable would require you to set up fixed IP addresses for all of the devices in your network.
Maximum Lease Time	The maximum amount of time, in seconds, that a device in your network will have the temporary IP address before a new one is issued by the modem's DHCP server. (86,400 seconds equals 24 hours)

Setting	Description
Default Lease Time	The Default amount of time that your modem's DHCP server will assign an IP address.
Start IP Address	The first IP address of a range that you specify using the Start and End IP Address settings. Your modem's DHCP server will assign the IP addresses in this range at random to the computers and devices in your network. Note that the Start and End IP Addresses must both be in the same subnet as the IP Address, above.
End IP Address	The last IP address of a range that you specify using the Start and End IP Address settings. Your modem's DHCP server will assign numbers from this range at random to the computers and devices in your network. By default the DHCP server has 21 addresses available to assign. If you plan on attaching more than 21 devices to your network, change the ending IP address to allow for more devices. Note that the Start and End IP Addresses must both be in the same subnet as the IP Address, above.

Creating a Fixed (Static) IP Address

How do I create a fixed IP address?

You create a fixed IP Address for a computer on your network using the **DHCP Server Fixed Host** page. The link to this page is found on the **LAN Configuration** page. (This is not strictly speaking a static IP Address, since it is served via DHCP.

However, the effect is the same. You are uniquely assigning a particular IP Address to a particular device on your network.)

You will want to create a fixed IP Address if you are setting up a computer, Xbox, or PlayStation for gaming.

To create a fixed IP address, see steps 2 through 6 in **Step 1: Choosing an IP Address for Gaming** on page 73.

Assigning a Half Bridge Device

When would I assign a half bridge device?

Assigning a **PPP Half Bridge** gives a public IP address to a computer that you choose so you can bypass the modem's NAT feature and open up all ports on your computer. You may want to do this if you are using an application that requires multiple ports on a computer in your network. Some examples are video conferencing applications, gaming applications, and instant messaging.

Here is a picture of the **Half Bridge Configuration** page:

Name	Value
PPP Half Bridge Status	Disable
Choose which computer will use the public IP address:	None

[Advanced PPP Half Bridge](#)

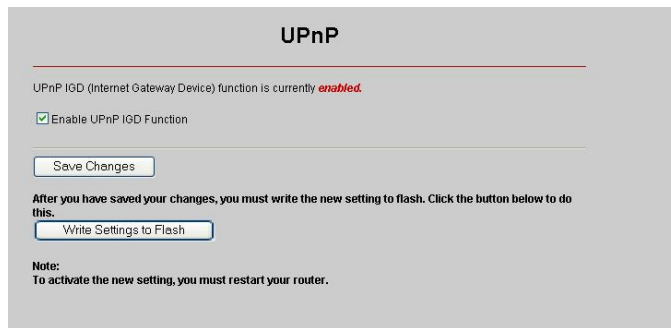
After you have saved your changes, you must write the new setting to flash. Click the button below to do this.

To configure a half bridge, set the Half Bridge status to **Enable**. From the drop-down list, choose the computer that you want to share the public IP address. This default setup for the PPP Half Bridge works for most applications. You should not need to make additional changes using the **Advanced PPP Half Bridge**.

Enabling or Disabling UPnP

Universal Plug and Play (UPnP) with Internet Gateway Device (IGD) protocol is installed in X6v units when they are shipped by Zoom. Change this setting only if you have a good reason to do so.

To change the status of Universal Plug and Play, on the **Router Setup** page click **UPnP**:



UPnP

UPnP IGD (Internet Gateway Device) function is currently *enabled*.

Enable UPnP IGD Function

Save Changes

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

Write Settings to Flash

Note:
To activate the new setting, you must restart your router.

Setting	Description
Enable UPnP IGD Function	Select this check box to enable or disable Universal Plug and Play with Internet Gateway Device (IGD) protocol. By default UPnP is enabled.

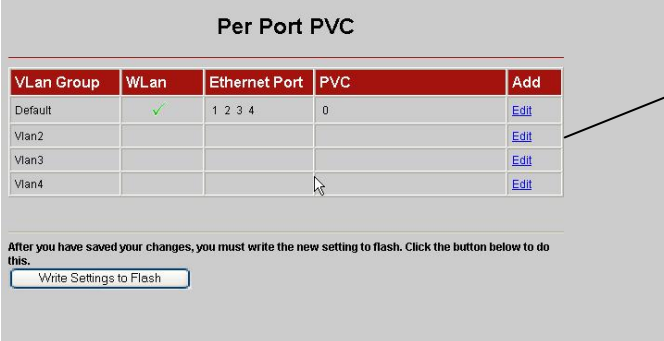
Click **Save Changes** and then **Write Settings to Flash** to save your UPnP setting to permanent memory.

Assigning Ports to a PVC

Normally you should not change Per Port PVC (Permanent Virtual Circuit) settings unless your ISP tells you to do so.

If you have more than one PVC set up, you can use this feature to assign Ethernet ports to the additional PVC(s). Per Port PVC is typically used to assign different video streams to particular Ethernet ports.

To assign ports to a PVC, on the **Router Setup** page click **Per Port PVC**:

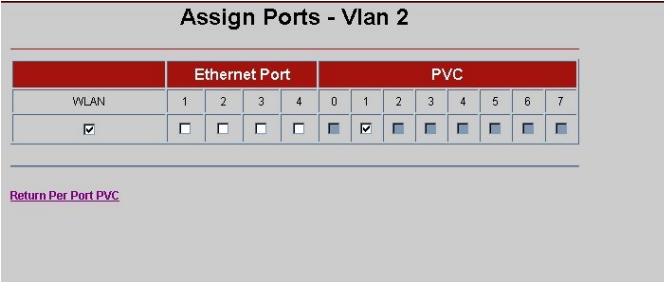


VLAN Group	WLAN	Ethernet Port	PVC	Add
Default	✓	1 2 3 4	0	Edit
Vlan2				Edit
Vlan3				Edit
Vlan4				Edit

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

Click **Edit** to assign a port or ports to Vlan Group 2.

To assign a port to PVC 1, in the **Add** column for **Vlan2** (see above) click **Edit** to display the **Assign Ports** screen:



WLAN	Ethernet Port				PVC							
	1	2	3	4	0	1	2	3	4	5	6	7
✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Return Per Port PVC](#)

Setting	Description
WLAN	If you are assigning a wireless device – for example, a wireless set-top box for your television set – to an additional PVC, select this check box to assign PVC 1 to the X6v’s wireless port. This port will no longer be assigned to PVC 0.
Ethernet Port	If you are assigning a wired device to PVC 1, select the ETHERNET port or ports. These ports will no longer be assigned to PVC 0.
PVC	Select the PVC number. Note: While you can create up to eight separate PVCs (0 to 7) by assigning different VPI and VCI settings (see page 16) only four can be used for Per Port PVC..
Return to Per Port PVC screen	Click this link to return to the main Per Port PVC screen.

If you assigned Ethernet (LAN) ports 3 and 4 to PVC 1, note that those ports are no longer available to PVC 0:

Per Port PVC

Vlan Group	WLAN	Ethernet Port	PVC	Add
Default	✓	1 2	0	Edit
Vlan2		3 4	1	Edit
Vlan3				Edit
Vlan4				Edit

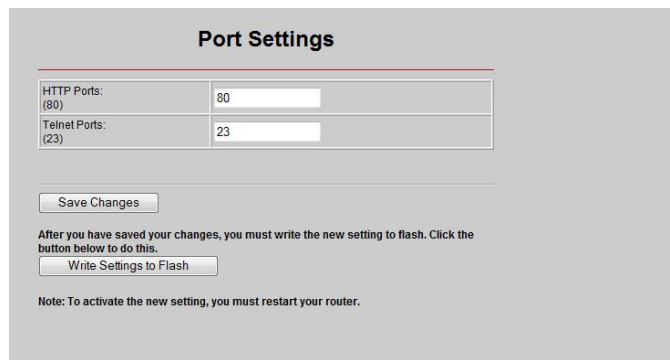
After you have saved your changes, you must write the new setting to flash. Click the button below to do this.

Click **Write Settings to Flash** to save your PVC port settings to permanent memory.

Changing HTTP and Telnet Ports

This feature lets you change the default X6v ports for Internet and Telnet traffic. If, for example, you are running another Internet server on the network and that server is using Port 80, you need to assign a different port to the X6v to avoid a conflict.

To assign Internet (HTTP) or Telnet ports, on the **Router Setup** page click **Port Settings**:



Setting	Description
HTTP Port	Enter a port number. (The default is 80.)
Telnet Port	Enter a port number. (The default is 23.)

Click **Save Changes** and then **Write Settings to Flash** to save the new port settings to permanent memory. Reboot your PC to make the settings active.

When the new port settings are saved, network users who want to access the X6v via the Internet must add a colon [:] plus the new port number after the X6v's IP address. For example, in their browser's address bar, users would enter **192.168.0.1:61101**, where 61101 is the new Internet port.

To access the X6v via Telnet, users would type **telnet[space]192.168.0.1[space]61102**, where 61102 is the new port.

Filtering Out MAC Addresses

Most users will not need this feature.

However, if there is a PC or other device on the X6v network that you don't want using the Internet, you can use MAC address filtering to deny the device Internet access. (That computer or device will still be able to communicate with other devices on the LAN, such as printers.)

To block Internet access, on the **Router Setup** page click **MAC Filtering**:

MAC Filtering

Name	Value
Status	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Name	<input type="text"/> <input type="button" value="Clear"/>
MAC Address	<input type="text"/>

MAC Filters List

Name	MAC Address	Status	Edit/Delete
------	-------------	--------	-------------

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

Setting	Description
Status	Select Enabled to deny Internet access to the specified MAC address. The default is Disabled .
Name	Enter the name associated with the MAC address.
MAC Address	Enter the 12-digit address without separators.
Save Changes	Click this button to display the MAC address information in the MAC Filters List (see next page).
Reset	Before you click Save Changes , you can click this button to clear all entries.

MAC Filtering

Name	Value
Status	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Name	<input type="text"/> <input type="button" value="Clear"/>
MAC Address	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>

MAC Filters List

Name	MAC Address	Status	Edit/Delete
test	00:20:e0:6d:68:a4	Enabled	Edit/Delete

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

Click this link to display the associated MAC address information in the top half of the screen, where you can edit it or delete it from the **MAC Filters List**.

MAC Filters List	
<u>Edit/Delete</u>	Click this link to edit or delete the associated MAC address information. To delete, click the Reset button in the top half of the screen.

Click **Save Changes** and then **Write Settings to Flash** to save the **MAC Filters List** to permanent memory.

Managing Access to Services

To change access settings, on the **Router Setup** page click **Management Control** to open the **Management Control** page.



Setting	Description
LAN Access	If a check box is selected, the associated service is enabled for local network users. The default for all services is Enabled .
WAN Access	Select a check box to enable the associated service for remote network users. By default, all the services are Disabled for remote users.

Click **Save Changes** and then **Write Settings to Flash** to save the service availability configuration to permanent memory.

Configuring Quality of Service

Quality of Service (QoS) helps guarantee upstream bandwidth for applications that require fast and dependable throughput. For example, QoS can slow down a photo upload so a phone call can proceed without garbling, and/or a gamer can enjoy faster response time.

With QoS you can assign VoIP, each of the four ETHERNET ports, and the Wireless port a priority of High, Medium, or Standard. High priority ports together share a guaranteed percentage of upstream bandwidth, typically 70%. Medium priority ports share a lower guaranteed percentage, typically 20%. Standard priority ports share the remaining upstream bandwidth that is guaranteed to them. If ports aren't using their guaranteed bandwidth, the excess bandwidth becomes available to other ports in order of priority.

For VoIP, you normally assign a High Priority QoS port. For a game console, you may want to assign a High or Medium priority. For ports used for Web browsing, normally you use Standard priority.

Windows users normally set up QoS by using the **Install Assistant** CD that comes with the X6v. To configure Quality of Service using Router Setup instead, click **QoS** on the **Router Setup** page. For a help message, select the [Click here](#) link in the first paragraph of the page.

Quality of Service(QoS)

With Quality of Service (QoS) you can assign each port a priority of High, Medium, or Standard. There are 5 ports - the 4 Ethernet LAN Ports and the Wireless port - and QoS lets you set their guaranteed upstream bandwidth. To learn more about QoS, [click here](#).

Do you want to turn on QoS, so some devices and ports have priority in sending information to the internet? YES NO

Setting the priority of QoS ports

Which ports should be High Priority?
Please pick one to three ports. VoIP 1 2 3 4 Wireless

Which ports should be Medium Priority?
Please pick one to three ports. VoIP 1 2 3 4 Wireless

All other ports are Standard Priority.

[Advanced QoS page](#)

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

Note:
To activate the new setting, you must restart your router.

Note that on the QoS screen, Port 1 is the Ethernet port labeled ETHERNET 1 on the X6v back panel. Port 2 is ETHERNET 2, and so forth.

Setting	Description
Do you want to turn on QoS?	If you click YES to assign priorities to the X6v's VoIP, ETHERNET and wireless ports, by default VoIP and ETHERNET port 1 are set to High Priority, ETHERNET port 2 is set to Medium Priority, and ETHERNET ports 3 and 4 as well as the wireless port are set to Standard priority. These default settings can be changed. The default is NO .
Which ports should be High Priority?	Select one to three ports. By default, these ports will together share 70% of the upstream bandwidth. You can configure a different percentage on the Advanced QoS page. (See page 127.)

Setting	Description
Which ports should be Medium Priority?	Select one to three ports. By default, these ports will together share 20% of the upstream bandwidth. You can configure a different percentage on the Advanced QoS page, shown below.
<u>Advanced QoS page</u>	Click this link to specify a different upstream bandwidth percentage for High, Medium and Standard priorities.

Advanced Quality of Service(QoS)

With Quality of Service (QoS) you can assign each port a priority of High, Medium, or Standard. High priority ports all share a certain guaranteed percentage of upstream bandwidth, typically 70%. Medium priority ports all share a lower guaranteed percentage of upstream bandwidth, typically 20%. Standard priority ports share the remaining upstream bandwidth that is guaranteed to them. If ports aren't using their guaranteed bandwidth, it becomes available to other ports in order of priority.

What guaranteed bandwidth should the High Priority Ports share? You can choose between %
50% and 90%. 70% is typical.

What guaranteed bandwidth should the Medium Priority Ports share? You can choose between %
10% and 45%. 20% is typical.

Your selections above establish the follow guaranteed bandwidths:

VoIP - %
Port 1 - %
Port 2 - %
Port 3 - %
Port 4 - %
Wireless - %

[Return to Main QoS Page](#)

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

Note:
To activate the new setting, you must restart your router.

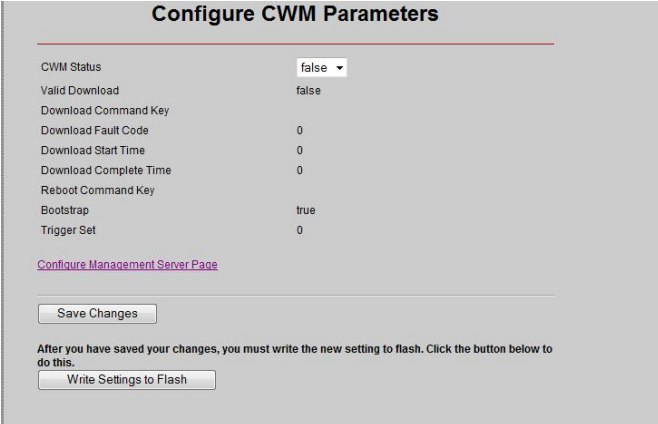
Setting	Description
What guaranteed bandwidth should High Priority Ports share?	The default is 70%. You can enter a different whole number percent. The High Priority and Medium Priority percentages together must be less than 100. Note: Standard Priority ports must have at least 1% of the upstream bandwidth.
What guaranteed bandwidth should Medium Priority Ports share?	The default is 20%. You can enter a different whole number percent. The Medium Priority and High Priority percentages together must be < 100. Note: Standard Priority ports must have at least 1% of the upstream bandwidth.
<u>Return Main QoS page</u>	Click to return to the main QoS page.

After you make your selections, click **Save Changes**, then **Write Settings to Flash**.

TR-069

The TR-069 option opens the **Configure CWM Parameters** page, where you can allow an **Access Control Server (ACS)** to control and configure your X6v. CWM stands for the **CPE WAN Management** protocol.

This feature must be supported by your service provider and should be used only if the provider instructs you to enable it.



Configure CWM Parameters

CWM Status	false ▾
Valid Download	false
Download Command Key	
Download Fault Code	0
Download Start Time	0
Download Complete Time	0
Reboot Command Key	
Bootstrap	true
Trigger Set	0

[Configure Management Server Page](#)

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

Setting	Description
CWM Status	When set to true , enables the CWM protocol. When set to false (the default), disables CWM.
Configure Management Server Page	Opens the page where you set parameters for the ACS server you are connecting to.

After you make changes on the **Configure Management Server Page**, click **Save Changes**, then **Write Settings to Flash**.

Configure Management Server

Item	Value
URL	<input type="text"/>
Username	<input type="text" value="acs"/>
Password	<input type="password" value="....."/>
Periodic Inform Enable	false ▾
Periodic Inform Interval(in seconds)	<input type="text" value="86400"/>
Periodic Inform Time	Date : 01 Jan ▾ 0001 Time: 00 : 00 : 00
Connection Request URL	<input type="text" value="/cwm/CRN.html"/>
Connection Request Username	<input type="text" value="admin"/>
Connection Request Password	<input type="password" value="....."/>
Upgrades Managed	false

[Return to Configure CWM Parameters Page](#)

Make the following entries:

Setting	Description
URL	URL of the Access Control Server (ACS) the X6v will communicate with.
Username	ACS server user name
Password	ACS server password
Periodic Inform Enable	Specifies whether or not (true or false) the X6v must periodically send information to the ACS server.
Periodic Inform Interval (in seconds)	Specifies the time interval between X6v information calls to the ACS.
Periodic Inform Time	Specifies the reference time, plus or minus an integer multiple of the Inform Interval, of the Inform call.
Connection Request URL	Specifies the X6v URL to be used by the ACS server. The default is /cwm/CRN.html .

Setting	Description
Connection Request Username	Specifies the X6v User name that will authenticate an ACS making a connection request to the X6v. The default is user .
Connection Request Password	Specifies the X6v password that will authenticate an ACS making a connection request to the X6v. The default is welcome .
Upgrades Managed	If set to true , specifies that the ACS server will manage upgrades for the X6v.

After you make your entries, click **Save Changes** and then click **Return to Configure CWM Parameters Page**.

Monitoring ADSL, Wireless, and Ethernet Status

How should I use the ADSL, Wireless, and Ethernet Status Reports?

These reports are useful tools for evaluating your system and for troubleshooting. Should a problem arise, a Technical Support Representative may ask you for the information that is contained in the reports.

Wireless Status Report

Here is a picture of a typical **Wireless Status** Report:

Item	Status
Link Speed	540000
SSID	zoom
Default Channel	10
Encryption	None
Mac address	00:0c:20:00:77:1f

Rx Packets	96308	Tx Packets	707
------------	-------	------------	-----

The **Wireless Status** Report shows you the modem speed (**Link Speed**), the **SSID**, your **Default Channel**, the **Mac address** of the modem, and the number of packets that are being received and transmitted (**Rx** and **Tx Packets**). You can also tell if your modem has wireless encryption enabled. (To encrypt your information, click the **Wireless** icon in the **Zoom Configuration Manager**).

ADSL Status Report

Here is a picture of the **ADSL Status Report**:

ADSL Status				
Item	Status			
ADSL Line State:	HandShake			
Mode:	Multimode			
Transmit Power:	0.0 dB			

	Downstream		Upstream	
Bit Rate	0 Kbps		0 Kbps	
Cell Rate	0		0	
SNR Margin	0.0 dB		0 dB	
Line Attenuation	0.0 dB		0.0 dB	
	Fast	Interleaved	Fast	Interleaved
CRC Errors	0	0	0	0
FEC Errors	0	0	0	0
HEC Errors	0	0	0	0
NCD Errors	0	0	0	0

The **ADSL Line State** tells you where your modem is in the connection process. The three states are **Training**, **Handshake**, and **ShowTime**. A line state of **ShowTime** shows that your modem has established a physical connection to the DSLAM (DSL Access Multiplexer – a device used in the process of connecting your computers, and/or network to the Internet). **Training** is at the beginning of the connection and **Handshake** is right after **Training**.

The **Downstream** and **Upstream** values tell you the speed at which information is being downloaded from the Internet (**Downstream**) and uploaded to the Internet (**Upstream**).

Ethernet Status Report

Here is a picture of the **Ethernet Status** Report:

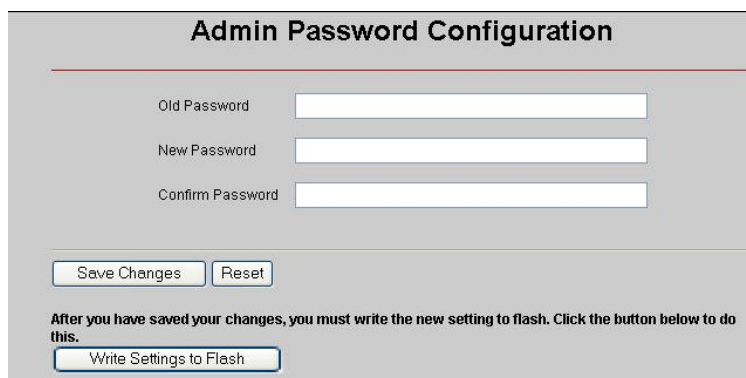
Ethernet Status			
Rx Packets	695	Tx Packets	1017
Rx Bad Packets	0	Tx Bad Packets	0
Rx CRC Packets	0	Tx Collisions	0
Rx Overlong Packets	0	Tx Excessive Collisions	0
Rx Short Packets	0		

The **Ethernet Status** Report gives you information about the receive (**Rx**) and transmission (**Tx**) rates of packets.

Changing Your Password

When should I change my password?

For added protection of your X6v settings, you should change the **admin** login password (**zoomadsl**) after you have logged into the **Zoom Configuration Manager**. Here is a picture of the page where you enter your **Old Password** and **New Password**:



Admin Password Configuration

Old Password

New Password

Confirm Password

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

Enter a new password with a minimum of 8 characters (upper- and lower-case letters A through Z, numbers 0 through 9).

Be sure to write your new settings to Flash, and to remember your new password.

CAUTION: If you change the password and then forget it, you will be unable to log onto the **Configuration Manager**. You will need to restore the modem to the original factory settings and will lose any changed configuration data. You can later restore changed configuration data, assuming that you backed it up previously. See [Backing Up and Restoring Your Configurations](#) on page 137 for instructions.

If you forget your password, reset the modem by inserting the tip of a paper clip into the **Reset** pinhole in the modem's back panel and pressing it for at least 3 seconds.

Reboot/Restore Factory Settings

How do I restore my modem's factory settings?

You can restore your modem to its original factory settings. This will restore the original **admin/zoomadsl** (user name/password) to the **Zoom Configuration Manager** on your computer. You can then log in using the **admin/zoomadsl** login.

Here is a picture of the **Reboot/Restore Router** page:



Click the **Check to Restore Factory Settings** check box, click **Reboot**, then follow the instructions to reset your ADSL modem to its original firmware. Please see **Backing Up and Restoring Your Configurations** on page 137 for information about restoring a stored X6v configuration.

Backing Up and Restoring Your Configurations

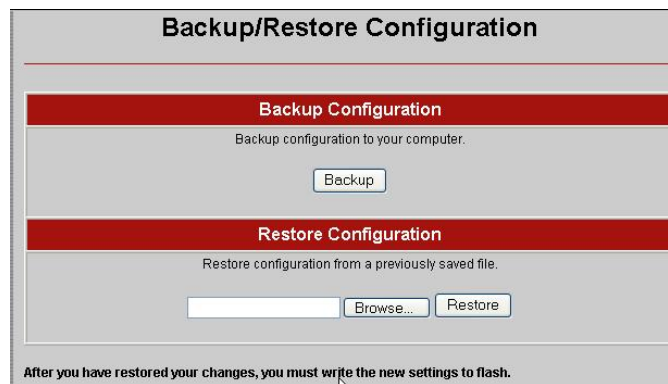
When would I need to back up and restore my configuration settings?

It is a good idea to back up your configuration settings after you set up the X6v, and also before you upload new firmware. Then if the update overwrites your configurations, you can put them back using the **Backup/Restore Config** option. You may also want to back up your configurations so you can use them to set up the same configurations in other modems.

To back up and restore your configuration:

- 1 Click **Backup/Restore Config** in the **Administration** section of the **Router Setup** page.

The **Backup/Restore Configuration** page opens.



Backup/Restore Configuration

Backup Configuration
Backup configuration to your computer.
Backup

Restore Configuration
Restore configuration from a previously saved file.
Browse... Restore

After you have restored your changes, you must write the new settings to flash.

- 2 Follow the instructions on the page to back up or restore your configuration settings.

Updating Your Firmware

How do I update my firmware?

Periodically you may want to update the firmware on your X6v modem. To do this, you download the Image file from the Zoom Web Site to your computer. You then use the **Firmware Update** option to upload the file to your modem.

Important! It is recommended that you backup your modem's configurations before you upload the firmware. (See **Backing Up and Restoring Your Configurations** on page 137). Also, **do not** turn off the modem or unplug it while the upload is in progress.

Here is a picture of the **Firmware Update** page:



The screenshot shows a web page titled "Firmware Update". At the top, there is a red banner with the text "Select Image Upload to start a Firmware Update." Below this, there is a form with a label "New Firmware Image" and a text input field. To the right of the input field is a "Browse..." button. Below the form, there is a warning message: "Please Backup your settings before uploading new firmware. Important - do not turn off the modem or unplug it while upload is in process." At the bottom of the form area, there is an "Image Upload" button.

Click **Browse** to go to the firmware update file. Then click **Image Upload**.

Appendix A:

ADSL Internet Settings Tables

Below are two tables, one for the USA and one for other countries. These tables are for customers whose service providers do not supply them with ADSL settings. Many ADSL providers use different settings depending on the region where they are operating. This is why there may be more than one setting for your service provider. If you refer to the tables and there is more than one listing for your service provider, the most common is labeled (1), the next (2), and so on. We recommend that you try them in order, starting with 1.

We post updated tables on our Web site. If your service provider or country is not listed in the tables below, please consult www.zoom.com.

Note to USA customers:

If your ADSL service provider is not shown below, use the settings for **Service Provider Not Shown** at the bottom of the table. If those settings do not work, use the settings for the company that provides local telephone service in your area.

Table A: USA

Service Provider	VPI	VCI	Encapsulation
AllTel (1)	0	35	PPPoE LLC
AllTel (2)	0	35	1483 Bridged IP LLC
AT&T (1)	0	35	PPPoE LLC
AT&T (2)	0	35	1483 Bridged IP LLC
AT&T (3)	8	35	1483 Bridged IP LLC
August.net (1)	0	35	1483 Bridged IP LLC
August.net (2)	8	35	1483 Bridged IP LLC
BellSouth	8	35	PPPoE LLC
Casstel.net	0	96	1483 Bridged IP LLC
CenturyTel (1)	8	35	PPPoE LLC
CenturyTel (2)	8	35	1483 Bridged IP LLC
Covad	0	35	PPPoE LLC

Service Provider	VPI	VCI	Encapsulation
Earthlink (1)	0	35	PPPoE LLC
Earthlink (2)	8	35	PPPoE LLC
Eastex	0	100	PPPoA LLC
Embarq (Sprint) (1)	0	35	PPPoA LLC
Embarq (Sprint) (2)	8	35	PPPoE LLC
GWI	0	35	1483 Bridged IP LLC
Hotwire	0	35	1483 Bridged IP LLC
Internet Junction	0	35	1483 Bridged IP LLC
Qwest (1)	0	32	PPPoA LLC
Qwest (2)	0	32	PPPoA VC-MUX
SBC (1)	0	35	PPPoE LLC
SBC (2)	0	35	1483 Bridged IP LLC
SBC (3)	8	35	1483 Bridged IP LLC
Socket (1)	8	35	1483 Bridged IP LLC
Socket (2)	0	35	1483 Bridged IP LLC
Socket (3)	0	35	PPPoE LLC
Sonic	0	35	1483 Bridged IP LLC
Sprint (Embarq) (1)	0	35	PPPoA LLC
Sprint (Embarq) (2)	8	35	PPPoE LLC
Uniserve	0	33	1483 Bridged IP LLC
Verizon (1)	0	35	PPPoE LLC
Verizon (2)	0	35	1483 Bridged IP LLC
Service Provider Not Shown	0	35	PPPoE LLC

Table B: Countries Other Than the USA

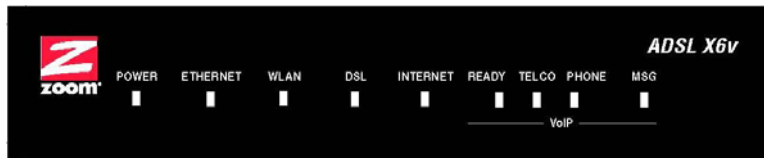
Service Provider	VPI	VCI	Encapsulation
Australia-Telstra	8	35	PPPoA LLC
Argentina-Telecom	0	33	PPPoE LLC
Argentina-Telefonica	8	35	PPPoE LLC
Belgium-ADSL Office	8	35	1483 Routed IP LLC
Belgium-Turboline	8	35	PPPoA LLC
Bermuda (1)	0	35	PPPoA LLC
Bermuda (2)	0	35	PPPoE LLC

Service Provider	VPI	VCI	Encapsulation
Bolivia (1)	0	34	1483 Routed IP LLC
Bolivia (2)	0	35	PPPoE LLC
Brazil- 3 Corp (1)	8	35	PPPoE LLC
Brazil- 3 Corp (2)	8	35	Classical IP over ATM
Brazil-Brasil Telecom	0	35	PPPoE LLC
Brazil-Telefonica	8	35	PPPoE LLC
Brazil-Telmar	0	33	PPPoE LLC
Brazil-South Region	1	32	PPPoE LLC
Colombia-EMCALI	0	33	PPPoA VC-MUX
Costa Rica	1	50	PPPoA LLC
Denmark-Cybercity, Tiscali	0	35	PPPoA VC-MUX
France (1)	8	35	PPPoE LLC
France (2)	8	67	PPPoA LLC
France (3)	8	35	PPPoA VC-MUX
France (4)	0	35	1483 Bridged LLC
France (5)	8	35	1483 Bridged LLC
Germany	1	32	PPPoE LLC
Greece	8	35	PPPoA VC-MUX
Hungary	1	32	PPPoE LLC
Hungary-Sci-Network	0	35	PPPoE LLC
Iceland-Islandssimi	0	35	PPPoA VC-MUX
Iceland-Siminn	8	48	PPPoA VC-MUX
Israel	8	48	PPPoA VC-MUX
Italy	8	35	PPPoA VC-MUX
Jamaica (1)	8	35	PPPoA VC-MUX
Jamaica (2)	0	35	PPPoA VC-MUX
Jamaica (3)	8	35	1483 Bridged IP LLC SNAP
Jamaica (4)	0	35	1483 Bridged IP LLC SNAP
Kazakhstan	0	33	PPPoA VC-MUX
Mexico	8	35	PPPoE LLC
Netherlands-Baby XL	0	34	1483 Bridged IP LLC
Netherlands-BBNED	0	35	PPPoA VC-MUX

Service Provider	VPI	VCI	Encapsulation
Netherlands-BBNED-Bridged	0	35	1483 Bridged IP LLC
Netherlands-MX Stream	8	48	PPPoA VC-MUX
Portugal	0	35	PPPoE LLC
Saudi Arabia (1)	0	33	PPPoE LLC
Saudi Arabia (2)	0	35	PPPoE LLC
Saudi Arabia (3)	0	33	1483 Bridged IP LLC
Saudi Arabia (4)	0	33	1483 Routed IP LLC
Saudi Arabia (5)	0	35	1483 Bridged IP LLC
Saudi Arabia (6)	0	35	1483 Routed IP LLC
Spain- Albura, Tiscali	1	32	PPPoA VC-MUX
Spain- Colt Telecom, Ola Internet	0	35	PPPoA VC-MUX
Spain -EresMas, Retevision	8	35	PPPoA VC-MUX
Spain-Knet Comunicaciones S.L.	8	32	PPPoA VC-MUX
Spain- Servidores Voz	0	33	PPPoA VC-MUX
Spain-Telefonica (1)	8	32	PPPoE LLC
Spain-Telefonica (2), Terra	8	32	1483 Routed IP LLC
Spain- Wanadoo (1)	8	35	PPPoA VC-MUX
Spain- Wanadoo (2)	8	32	PPPoE LLC
Spain- Wanadoo (3)	8	32	1483 Routed IP LLC
Sweden-Telenordia	8	35	PPPoE
Sweden-Telia	8	35	1483 Bridged IP LLC
Switzerland	8	35	PPPoE LLC
Turkey (1)	8	35	PPPoE LLC
Turkey (2)	8	35	PPPoA VC-MUX
UK (1)	0	38	PPPoA VC-MUX
UK (2)	0	38	PPPoE LLC
Venezuela-CANTV	0	33	1483 Routed IP LLC
Vietnam	0	35	PPPoE LLC

Appendix B: Front and Back Panels

The X6v Front Panel

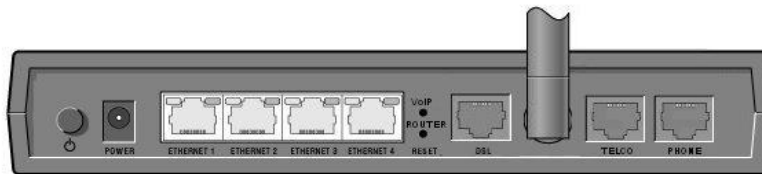



The following table describes each LED on the X6v's front panel.

LED	Description
POWER	Green when the X6v is plugged into a power source. Red when a self-test error is found.
ETHERNET	Lights if any Ethernet port of the X6v is plugged into the Ethernet port of a powered-up device. Flashes when data is sent. Additional lights for each Ethernet port are on the back of the X6v.
WLAN	Lights when the Wireless Local Area Network is running and enabled. Flashes when data is sent.
DSL	Flashes when the X6v is performing its startup sequence. Steady on when the unit has synched up with its DSL connection. Note: If the light fails to switch from flashing to steady after a minute or two, check with your DSL provider that the DSL connection is activated, or refer to Appendix D, Troubleshooting on page 153.

LED	Description
INTERNET	Steady green when an Internet connection is established. Flashes green to indicate data activity. Red when the X6v cannot access the Internet. Off when the X6v is in Bridge mode, or if there is no DSL connection.
READY	Steady on when the X6v is ready to place a VoIP call.
TELCO	Flashes during an outgoing or incoming call over your standard telephone line, or when the X6v is bridging a call.
PHONE	Flashes whenever the telephone connected to the PHONE port is in use – for either a VoIP or a standard landline call.
MSG	Flashes when a recorded VoIP message is waiting. Steady on if the X6v cannot communicate with the VoIP update server.

X6v Back Panel Connectors



Port or Button	Description
	Turns the X6v on or off.
POWER	Port to connect the unit to the X6v's power cube.

Port or Button	Description
ETHERNET 1 ETHERNET 2 ETHERNET 3 ETHERNET 4	Ethernet ports that can connect the unit to an access point, a network hub, or the Ethernet port of a computer. The X6v has four Ethernet ports. Each port has a yellow and a green light above it. The yellow light turns on when the port is connected to a 100 megabit per second Ethernet port. The green light flashes when there is activity on that particular Ethernet line.
RESET VoIP	Returns the VoIP configuration to the previous settings. To reset, insert a paper clip and hold it down for 5 seconds. To force the X6v to download the latest settings from the VoIP server, wait 2 minutes after the reset, insert the paper clip again and hold it down for 5 more seconds.
RESET ROUTER	Resets the modem to its factory settings. To reset, insert a paper clip and press the button three times.
DSL	Connects the modem to the ADSL-enabled telephone wall jack.
TELCO	(TELEphone COmpany connection) Connects the modem to a standard telephone line so you can switch between Internet and landline calls.
PHONE	Lets you connect a telephone for making calls via your VoIP service – or your standard phone service, if you have connected the X6v to the TELCO port.

Appendix C:

TCP/IP Network Settings

If you are using a Macintosh or Linux computer, you **must** ensure that your computer's TCP/IP network settings are configured properly. Otherwise you will not be able to connect to the Internet.

Note: If you are using a Windows computer, you do not have to configure the TCP/IP settings. This is because your Windows computer will automatically configure them for you. Only Windows users who are troubleshooting the X6v will need to verify the TCP/IP settings.

Depending on your operating system, follow the steps in the appropriate section to ensure your TCP/IP settings are correct.

- If you are using Macintosh, see [Macintosh TCP/IP Settings](#) on page 147.
- If you are using Linux, see [Linux TCP/IP Settings](#) on page 149.
- If you are using Windows, see [Windows TCP/IP Settings](#) on page 150.

Macintosh TCP/IP Settings

How you configure your Macintosh computer's network settings differs, depending on your Mac OS. For OS X, follow the instructions below. Otherwise go to page 148.

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 Ensure that **Automatic** is selected from the **Location** list box.
- 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 Continue with [Establishing Communication](#) on page 15.

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**.
- 3 Under **Configure:**, select **Using DHCP Server**. Do not enter anything in the **DHCP Client ID** field.
- 4 Close the **TCP/IP** Window. You will be asked if you want to save the changes. Click **Save**.
- 5 Continue with [Establishing Communication](#) on page 15.

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.

Once you have followed the instructions for your Linux system, continue with [Establishing Communication](#) on page 15.

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

RedHat

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

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

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="dhcpcient"
```

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

Debian

Add this line to the file `/etc/network/interfaces`:

```
iface eth0 inet dhcp
```

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

Windows TCP/IP Settings

How you configure your Windows computer's network settings differs, depending on your operating system. Go to the section that corresponds to your Windows operating system.

Note: If you are using a Windows computer, you do not have to configure the TCP/IP settings. This is because your Windows computer will automatically configure them for you. Only Windows users who are troubleshooting the X6v will need to verify the TCP/IP settings.

Windows XP

- 1 To open the **Internet Protocol (TCP/IP) Properties** dialog box, follow these steps:
 - a From the desktop, click the **Start** button, point to **Control Panel**, and then click **Network and Internet Connections**.
 - b Right-click the **Local Area Connection** icon, and select **Properties**.
 - c Select your NIC card's TCP/IP entry (it should include TCP/IP in it, but not AOL, Dial-up, or Adapter) and click the **Properties** button.
- 2 Ensure the following is selected, depending on whether you are using dynamic (DHCP) or static IP addressing:
 - a If you are using DHCP (most users): Ensure that **Obtain an IP address automatically** is selected and that either **Obtain a DNS server address automatically** or **Enable DNS** is selected. All fields should be blank.
 - b If you are using a static IP address: Ensure that **Use the following IP address** and **Use the following DNS server addresses** are selected and that the correct IP address, Subnet mask, Default gateway, and Preferred DNS server values appear.

Windows 2000

- 1 To open the **Internet Protocol (TCP/IP) Properties** dialog box, follow these steps:
 - a From the desktop, click the **Start** button, point to **Settings**, then **Network and Dial-up Connections**.
 - b Right-click the **Local Area Connection** icon, and select **Properties**.
 - c Select your NIC card's TCP/IP entry (it should include TCP/IP in it, but not AOL, Dial-up, or Adapter) and click the Properties button.
- 2 Ensure the following is selected, depending on whether you are using dynamic (DHCP) or static IP addressing:
 - If you are using DHCP (most users): Ensure that Obtain an IP address automatically is selected and that either Obtain a DNS server address automatically or Enable DNS is selected. All fields should be blank.
 - If you are using a static IP address: Ensure that Use the following IP address and Use the following DNS server addresses are selected and that the correct IP address, Subnet mask, Default gateway, and **Preferred DNS server** values appear.

Windows 98/Me

- 1 To open the **Internet Protocol (TCP/IP) Properties** dialog box, follow these steps:
 - a From the desktop, click the **Start** button, point to **Settings**, then **Control Panel**.
 - b Double-click the **Network** icon to display the **Network** dialog box.
 - c Select your NIC card's TCP/IP entry (it should include TCP/IP in it, but not AOL, Dial-up, or Adapter) and click the **Properties** button and then click **OK**.
- 2 Ensure the following is selected, depending on whether you are using dynamic (DHCP) or static IP addressing:
 - If you are using DHCP (most users): Ensure that **Obtain an IP address automatically** is selected and that either **Obtain a DNS server address automatically** or **Enable DNS** is selected. All fields should be blank.
 - If you are using a static IP address: Ensure that **Specify an IP address** is selected and that the correct IP Address and Subnet Mask values appear. On the **DNS Configuration** tab, ensure that **Enable DNS** is selected and that something appears in the **Host** box. (If not, enter any name, word, or combination of letters and numbers.) Ensure that the **DNS Server Search Order** box contains either **192.168.0.1** or **192.168.0.2**.

Appendix D:

Troubleshooting

The following are some problems you might experience and some possible solutions to remedy the situation.

Problem

My X6v's **DSL** light is steady on, but I cannot connect to the Internet.

Solution

First, perform a power cycle on your computer and the X6v. Take the following steps in the order given:

- 1 Turn off the computer.
- 2 Turn off your X6v and wait a few seconds.
- 3 Turn the X6v back on.
- 4 Turn on the computer.

If that doesn't work, check these items:

- Ensure that you are using the correct **VPI**, **VCI**, and **Encapsulation** settings. See Appendix A on page 139.
- If your **Encapsulation** begins with **PPP**, ensure that you have typed your DSL Username and Password correctly. (Note that this is NOT the username and password you used to log into the **Zoom Configuration Manager** on page 15.)
 - a If you had the modem automatically configure its settings, open the **ADSL Setup** page, and ensure that **MANUAL** is selected, and then select **7** from the **Virtual Circuit** drop-down list. When the screen changes to show the automatic configuration settings, select **MANUAL** again, then enter the correct **Username** and **Password**

in the boxes provided. Click **Save Changes** and **Write Settings to Flash**.

- b If you manually configured your modem, open the **ADSL Setup** page, ensure that **MANUAL** is selected, and then enter the correct **Username** and **Password** in the boxes provided. Click **Save Changes** and **Write Settings to Flash**.
- Verify that your service provider's DSL connection is functioning properly. (Place a call to your service provider's customer support department to verify this.)
- **Windows users only:** Verify that the Web browser on the computer on which you installed the software is configured for a **network connection** (this might be called a **Local Area Network** or **broadband** connection). If you need help configuring your Web browser, refer to **Appendix E: Configuring Your Web Browser** on page 158.
- Verify that your TCP/IP network settings are properly configured on your computer. To do this, refer to the appropriate section.
 - If you are using Macintosh, see Macintosh TCP/IP Settings on page 147.
 - If you are using Linux, see Linux TCP/IP Settings on page 149.
 - If you are using Windows, see Windows TCP/IP Settings on page 150

Problem

My X6v's **DSL** light continually flashes and does not stay solidly lit.

Solution

There are several issues that could cause this problem. Check these items:

- Ensure that the phone cord is firmly plugged into the wall jack and the **DSL** jack on the back of the X6v (not the **PHONE** jack on the back of the modem).

- Verify that the jack the phone cord is connected to is enabled for DSL service. Check with your service provider.
- Your phone cord may be defective. Replace the phone cord with a known good one.
- Check that you have phone filters on all the phones and fax machines using the same ADSL line as the X6v. These devices can produce noise and interfere with your ADSL connection when they are off-hook.

Problem

I cannot log into the **Zoom Configuration Manager**. I have typed **http://192.168.0.1**, but I am not prompted for a User Name and Password.

Solution

There are several issues that could cause this problem. Check these items:

- If you are using a Macintosh or Linux computer, your TCP/IP settings may not be properly configured. See page 146 for more information.
- If you are using Mac OS X 10.3 and above, renew your **IP address: Point to System Preferences**, then choose **Network**. Click the **Configure** button and then the **Renew DHCP Lease** button.
- If you are using a Windows computer, perform a **Release/Renew** operation:
- **Windows 2000/XP:** From the desktop, click the **Start** button, then point to **Programs**, point to **Accessories**, and then select **Command Prompt**. Type **ipconfig /all** and press the **Enter** key on your keyboard. In the subsequent dialog box, make sure the **NIC adapter** is highlighted in the drop-down list, click **Renew**, and then click **Release**. Then type **192.168.0.1** into your browser's address bar, and the **Authentication** box should display.
- **For Windows 95/98/Me:** From the desktop, click the **Start** button and the point to **Run**. Type **winipcfg**, and click **OK**. In the subsequent dialog box, make sure the NIC adapter is highlighted in the drop-down list, click **Renew**, and then click

Release. Then type **http://192.168.0.1** into your browser's address bar, and the **Authentication** box should display.

Problem

The computer on which I installed the X6v software is connected to the Web, but one or more of the additional computers I have connected directly to the modem cannot access the Internet.

Solution

There are several issues that could cause this problem. Check these items:

- Check that there's a good connection between an X6v ETHERNET port and the computer that can't access the Internet.
- Try rebooting the computer that can't access the Internet. This will allow for the computer to release and renew its IP address.
- Try the following for any computer that can't access the Internet: Ensure that the computer is connected using its Ethernet port and one of the X6v modem's ETHERNET ports. Run the installation CD (as explained in **Installing the Software** on page 12), reboot the computer, and then try to connect to a familiar Web address to ensure that the Internet connection is made.

Problem

The computer on which I installed the X6v software is connected to the Web, but the computers connected through my network device (such as a wireless access point, router, hub, or switch) cannot access the Internet.

Solution

The problem is most likely with your network device (such as a wireless access point, router, hub, or switch). Check these items:

- Try rebooting each computer on your network. For example, if you are using a router, reboot each computer that is connected to the router. This will allow for the computers to release and renew their IP addresses.
- If you are using a wireless access point or a router, verify that the device is using Dynamic Host Configuration Protocol (DHCP). This is also known as dynamic IP addressing. Depending on your device, this may be controlled by an **Obtain an IP address automatically** option. If you need help, refer to the documentation that came with your network device or contact its manufacturer.
- Refer to the documentation provided with your network device or contact its manufacturer for assistance.

Appendix E: Configuring Your Web Browser

Important!

This section is for Windows computers only. If you are using a Macintosh or Linux computer, your browser is already configured properly. However, you must ensure that your computer's TCP/IP settings are configured properly. See [Macintosh TCP/IP Settings](#) on page 147 or [Linux TCP/IP Settings](#) on page 149 for instructions on how to do this.

When using a Windows computer, the software that you use to make an Internet connection must be set for a **network connection**, not a **dial-up connection**. This configuration should have been done automatically when you installed the software.

If you find that you need to configure your Web browser, this section includes instructions for recent versions of two popular Web browsers: Internet Explorer Version 6.0 (or later) and Mozilla Firefox Version 2.0 (or later). The configuration is done on the same computer on which you installed the X6v software.

Depending on the browser you have on your Windows computer, follow the corresponding instructions in this section.

Tip:

If you are using an earlier version of one of these browsers, the configuration may be slightly different from below. In those cases—or if you are using another browser altogether—configure the browser to use a **network connection** (this might be called a **Local Area Network** or **broadband** connection).

Configuring Internet Explorer

The following instructions are for Internet Explorer Version 6.0 or later. (If you do not have this version, you can get a free upgrade from Microsoft Corp. If you are not sure what version you have, open Internet Explorer and from the **Help** menu, choose **About Internet Explorer**. The version number is directly below the Microsoft Internet Explorer logo. You can ignore all the numbers after the period following the first digit.)

- 1 On the desktop, right-click the **Internet Explorer** icon, and select **Properties**.

Tip:

If you cannot access Internet Explorer in this way, open your computer's **Control Panel** (click the **Start** button and then, depending on your computer, either click **Control Panel**, or click **Settings** and then **Control Panel**). In the **Control Panel**, double-click the **Internet Options** icon. If this icon does not appear, double-click the **Network and Internet Options** icon and then double-click the **Internet Options** icon.

- 2 On the **Internet Properties** dialog box, select the **Connections** tab, then click the **Setup** button.
- 3 The setup process will proceed differently, depending on your operating system. The following table details the process for your Windows computer. The setup process will proceed differently, depending on your operating system. The following subsections detail the process for Windows computers.

Windows Vista:

- a On the **Connect to the Internet** dialog, click **Broadband (PPPoE)**.
- b Enter your ISP **User Name** and **Password**, then click **Connect**.

Windows XP:

- a On the **Welcome to the New Connection Wizard** dialog, click **Next**.

(If you see a **Location Information** dialog box, click **Cancel** and then when asked if you are sure you want to cancel, click **Yes** to return to the **Welcome** dialog.)

- b On the **Network Connection Type** dialog, select **Connect to the Internet**, then click **Next**.
- c On the **Getting Ready** dialog, select **Set up my connection manually**, then click **Next**.
- d On the **Internet Connection** dialog, select **Connect using a broadband connection that requires a user name and password**, then click **Next**.
- e Follow the prompts and enter the requested information on the **New Connection Wizard** dialogs.
- f On the **Completing the New Connection Wizard** dialog, click **Finish**.

Windows 98/Me/2000:

- a On the **Internet Connection Wizard** dialog, select **I want to set up my Internet connection manually**, or **I want to connect through a local area network (LAN)**, then click **Next**.
 - b On the **Setting up your Internet connection** dialog, select **I connect through a local area network (LAN)**, then click **Next**.
 - c On the **Local area network Internet configuration** dialog, uncheck the **Automatic discovery of proxy server** check box then click **Next**.
 - d On the **Set Up Your Internet Mail Account** dialog, select **No**, then click **Next**.
 - e On the **Completing the New Connection Wizard** dialog, uncheck the **To connect to the Internet immediately, select this box...** check box (if it appears) and click **Finish**.
- 4 If you accessed Internet Explorer's settings from the **Control Panel** (as explained in the **Tip** following Step 1), the **Control Panel** window will still be open. Close it now.

Configuring Mozilla Firefox

The following instructions are for Mozilla Firefox Version 2.0. (If you do not have Version 2.0, you can get a free download from Mozilla at <http://www.mozilla.com/en-US/firefox/>. If you are not sure what version you have, open Mozilla Firefox and choose **About Firefox** from the **Help** menu. The version number is at the top of the screen.)

- 1 Double-click the **Mozilla Firefox** icon on your desktop to open the browser.
- 2 From the **Tools** menu, choose **Options...** to open the **Options** page.
- 3 On the **Options** page, click **Advanced**, click the **Network** tab, and then click **Settings**
- 4 On the **Connections Setting** page, select **Direct connection to the Internet**, then click **OK..**

Appendix F: Wireless Channels by Country

For most countries channels 1-13 are normal for private wireless networks. The following table shows countries known to use channels other than 1-13 for private wireless networks.

Country	Channels
France	10-13
Israel	4-9
Japan	1-13 14 (802.11b only)
Taiwan	1-11
USA	1-11

Appendix G:

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.

When operating this unit in the US or Canada, only channels 1~11 can be operated.

Selection of other channels is not permitted under FCC and Industry Canada regulations.

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

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

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

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: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

The Ringer Equivalence Number (REN) for this terminal equipment is identified on the bottom label of the equipment. The REN assigned to each terminal equipment 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 five.

Operation is subject to the following two conditions: (1) This device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

AVIS : Le présent matériel est conforme aux spécifications techniques d'Industrie Canada applicables au matériel terminal. Cette conformité est confirmée par le numéro d'enregistrement. Le sigle IC, placé devant le numéro d'enregistrement, signifie que l'enregistrement s'est effectué conformément à une déclaration de conformité et indique que les spécifications techniques d'Industrie Canada ont été respectées. Il n'implique pas qu'Industrie Canada a approuvé le matériel.

L'indice d'équivalence de la sonnerie (IES) du présent matériel est montré sur l'étiquette inférieure du produit. L'IES assigné à chaque dispositif terminal indique le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas 5.

Electrostatic Discharge Statement: The unit may require resetting after a severe electrostatic discharge event.

Declaration of Conformity



Declaration of Conformity
 Conformiteitsverklaring van de EU
 Konformitätserklärung
 Dichiarazione di conformità
 Declaração de Conformidade
 Konformitätsdeklaration

Overensstemmelseserklæring
 Déclaration de conformité
 Δήλωση Συμμόρφωσης
 Deklaracja zgodności
 Declaración de conformidad
 Cam kết về sự tuân thủ ở Châu Âu

Manufacturer/Producent/Fabrikant/ Constructeur/Hersteller/Κατασκευαστής/ Fabricante/ Fabricante/Tilverkare/Nhà sản xuất	Zoom Technologies, Inc. 207 South Street Boston, MA 02111 USA 617-423-1072 www.zoom.com
Brand/Varemærke/Merk/Marque/Marke/Mάρκα/ Marchio/Marke/Marca/ Thương hiệu	Zoom X6v DSL 2/2+ Wireless-G Modem with built-in VoIP adapter
Type/Typ/Mάρκα/Tipo/Kiểu mẫu	Models 5695, 5697

The manufacturer declares under sole responsibility that this equipment is compliant to Directive 1999/5/EC via the following. This product is CE marked.

Producenten erklærer under eneansvar, at dette udstyr er i overensstemmelse med direktivet 1999/5/EC via følgende. Dette produkt er CE-mærket.

De fabrikant verklaart geheel onder eigen verantwoordelijkheid dat deze apparatuur voldoet aan Richtlijn 1999/5/ EC op grond van het onderstaande. Dit product is voorzien van de CE-markering.

Le constructeur déclare sous son entière responsabilité que ce matériel est conforme à la Directive 1999/5/EC via les documents ci-dessous. Ce produit a reçu le marquage CE.

Hiermit erklärt Zoom die Übereinstimmung des Gerätes modem mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EC. Dieses Produkt ist das gekennzeichnete CE.

Ο κατασκευαστής δηλώνει με αποκλειστική του ευθύνη ότι αυτό το προϊόν συμμορφώνεται με την Οδηγία 1999/5/EC μέσω των παρακάτω. Αυτό το προϊόν φέρει τη Σήμανση CE.

Il fornitore dichiara sotto la sola responsabilità che questa apparecchiatura è compliant a 1999/5/EC direttivo via quanto segue. Questo prodotto è CE contrassegnato.

Producent stwierdza że to urządzenie zostało wyprodukowane zgodnie z Dyrektywą 1999/5/EC. Jest to potwierdzone poprzez umieszczenie znaku CE na urządzeniu.


O fabricante declara sob sua exclusiva responsabilidade que este equipamento está em conformidade com a Directiva 1999/5/EC através do seguinte. Este produto possui Marcação CE.

El fabricante declara bajo su exclusiva responsabilidad que este equipo satisface la Directiva 1999/5/EC por medio de lo siguiente. Este producto tiene marca CE.

Nhà sản xuất cam kết với trách nhiệm của mình là thiết bị này tuân theo Hướng dẫn 1999/5/EC thông qua các mục sau. Sản phẩm này được đánh dấu là CE.

Safety: 2006/95/EC	EN 60950-1: 2001/A11:2004
EMC/RF: 2004/108/EC	EN 301 489-1, V1.5.1: 2004-2011
	EN 301 489-17, V1.2.1: 2002-2008
	EN 300 386, V1.3.2: 2003-2005
1999/5/EC	EN 50371: 2002; EN 50392: 2004
	EN 300 328, V1.7.1: 2006




 Andy Pollock
 12 March, 2009
 1058/TF, Boston, MA, USA

Director, Hardware Engineering/Direktør, Hardware Engineering/Director, Sustaining Engineering /Directeur, ingénierie de soutien/Direktør, Sustaining Engineering /Διευθυντής, Μηχανικής Διατήρησης /Direttore, Hardware Engineering /Dyrektor, Inżynieria ciągła/Director, Engenharia de Manutenção /Director, Ingeniería de apoyo/ Giám Đốc Kỹ thuật Phần cứng

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 2009**

All rights reserved.