POLYCOM®

ViaVideo Technical Reference

June 2001 Edition

Introduction

Audio Connection

Network Connection

1

Introduction

Welcome

Although ViaVideo is a simple tool to use, some aspects of its setup and configuration deserve a more in-depth discussion than can be provided in the context of the online help. For this reason, this *ViaVideo Technical Reference* is provided.

This technical reference discusses the following topics:

- Audio Connection (page 3)
- Network Connection (page 7).

Other Resources

There are many other resources you might find useful when exploring the world of broadband communications. We've listed some of them here for your convenience.

ViaVideo Technical Support Website

The ViaVideo technical support website has a wealth of information to help you set up and troubleshoot your ViaVideo installation. Resources include:

- Frequently asked questions about ViaVideo
- Network connection guidelines for setting up ViaVideo in a small office/home office (SOHO) environment
- ViaVideo Knowledge Base contains plenty of tips to make setting up and ViaVideo easier, including troubleshooting information.

The ViaVideo technical support website address is:

http://esupport.polycom.com/support/viavideo_support.html

DSL Reports Website

The DSL Reports website has a wealth on information on broadband access providers, as well as diagnostic tools for testing bandwidth throughput, packet loss testing and IP address directories (see the **Tests** link).

The DSL Reports website address is:

http://www.dslreports.com

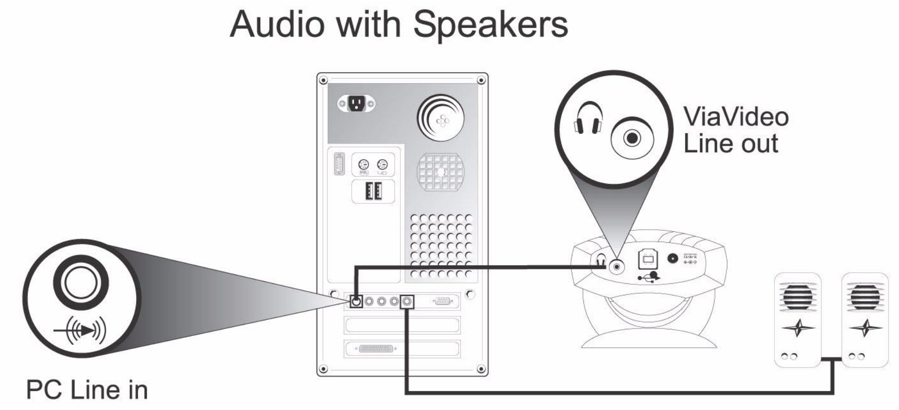
2

Audio Connection

Because of the multiple possibilities for audio connection with the ViaVideo camera unit, the following information is provided to help you correctly install your audio connection.

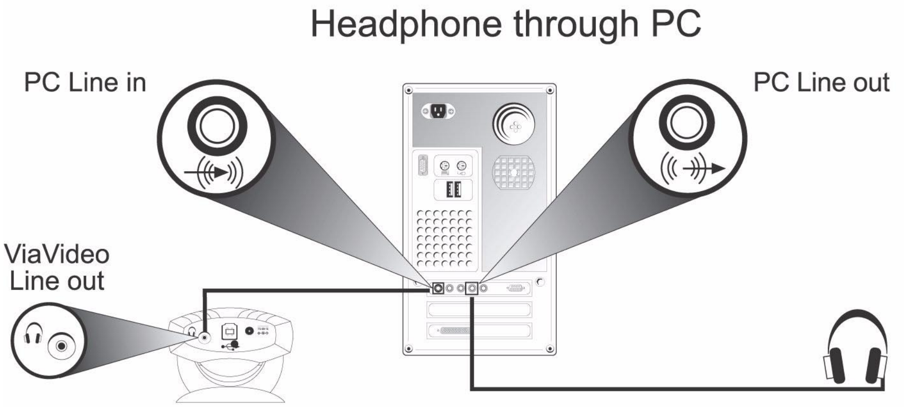
PC with Speakers

This diagram shows the correct connection from the ViaVideo audio line out to the PC line in when using speakers. Select **Headphones or Speakers** in the **Audio** screen (*System Information>Setup> Audio*) when using this type of audio connection.



PC with Headphones

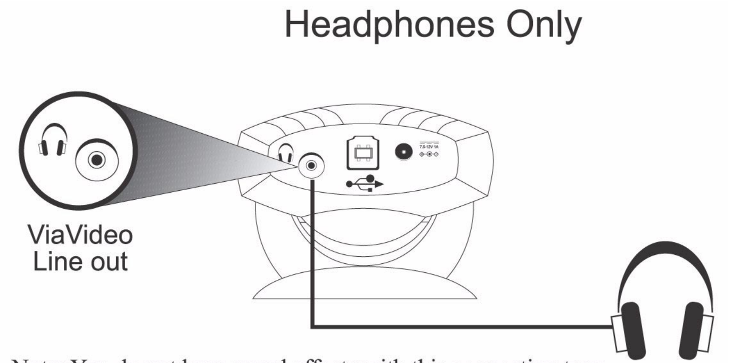
This diagram shows the correct connection from the ViaVideo audio line out to the PC line in when using headphones. Select **Headphones or Speakers** in the **Audio** screen (*System Information>Setup>Audio*) when using this type of audio connection.



Headphones Only

This diagram shows the correct connection from the ViaVideo audio line out to the PC line in when using headphones. Select the **Headphones or Speakers** option in the **Audio** screen (*System Information>Setup>Audio*) when using this type of audio connection.

To connect headphones directly to the ViaVideo line out port, your headphones must have a single 3.5 mm stereo connector or adapter.



Note: You do not hear sound effects with this connection type.

With this type of connection, you will be able to hear all sounds generated by the ViaVideo camera unit processor:

- In-call audio
- Keypad tones
- Audio test tone.

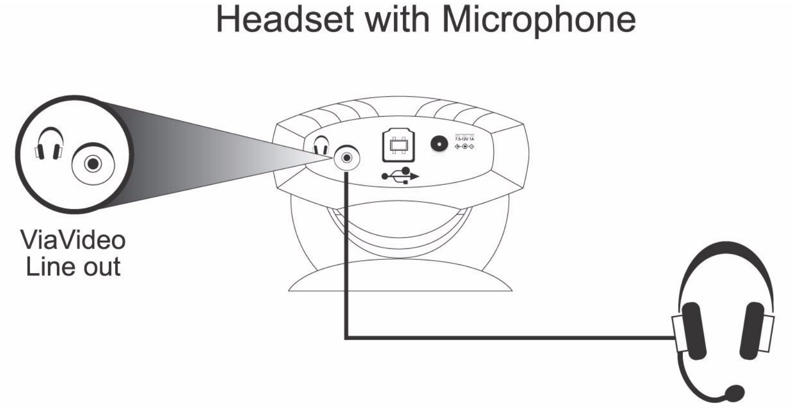
You will not be able to hear sounds generated by the ViaVideo application on your PC:

- Far and near site ring tones
- Splash screen sound effects
- Busy signals
- ViaVideo sound effects.

Headset with Attached Microphone

This diagram shows the correct connection from the ViaVideo audio line out to a headset with attached microphone. Select the **Headset with Microphone** option in the **Audio** screen (*System Information>Setup>Audio*) when using this type of audio connection.

Headsets with attached microphones have a 2.5 mm phono connection. Note that this type of connection requires the use of a 2.5 mm female to 3.5 mm male stereo phono adapter to fit the 3.5 mm **Line Out** port.



With this type of connection, you will be able to hear all sounds generated by the ViaVideo camera unit processor:

- In-call audio
- Keypad tones
- Audio test tone.

You will not be able to hear sounds generated by the ViaVideo application on your PC:

- Far and near site ring tones
- Splash screen sound effects
- Busy signals
- ViaVideo sound effects.

3

Network Connection

Although connecting any networked device can be a confusing task, we at Polycom are all for simplifying this process for you as much as possible. When you start the ViaVideo application for the first time, ViaVideo's setup wizard leads you through a series of configuration steps that set up ViaVideo's network connection configuration settings so you can begin using ViaVideo immediately.

If you need to change your network connection, or are using ViaVideo in more than one network environment, you may need to change your network configuration settings. This is best accomplished by having your network administrator perform these tasks for you.

If you don't have a network administrator to take care of the configuration for you, we've got you covered. Read the information in this document and you will be ready to go in no time.

If you *are* a network administrator, go ahead and read the document anyway. Your secret's safe with us!

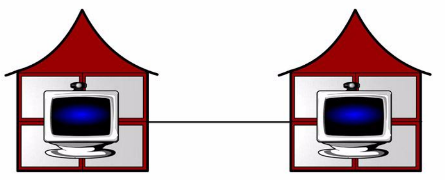
This document contains the following sections:

- Pick Your Connection Type (page 7)
- Configure Your Connection (page 9)
- What's a Firewall? (page 17)
- What's a DMZ? (page 19)
- What's a NAT? (page 19)
- Multiple IP Addresses (page 21)
- Network Configuration Screens (page 23).

Pick Your Connection Type

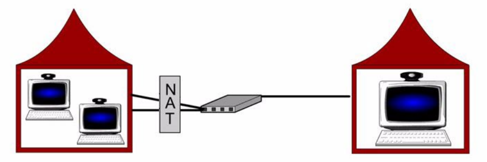
As simple as we can make it - just pick out your connection type from those shown below, perform the tasks in the appropriate section, and you're ready to communicate ViaVideo!

Simple Connection - Just a Modem, Thanks



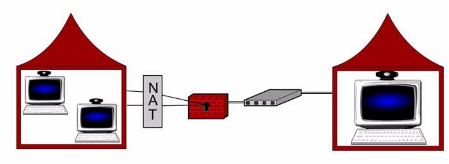
If you are using a direct connection to the internet, such as a cable modem or DSL modem, use the configuration instructions on page 9.

Router With NAT, No Firewall



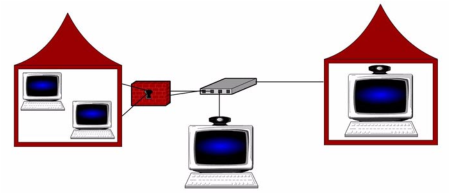
If your network connection is through a router with a Network Address Translator (NAT), but no firewall, use the configuration instructions on page 10. For more information about NATs, refer to “What’s a NAT?” on page 19.

Router With Firewall



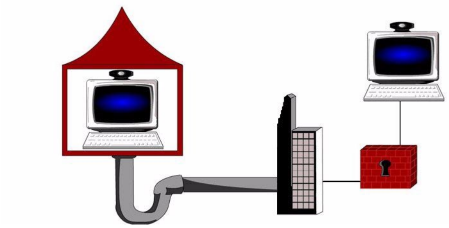
If your network connection is through a router with a firewall, use the configuration instructions on page 11. For more information about firewalls, refer to “What’s a Firewall?” on page 17.

Router With Firewall, Using a DMZ



If your network connection is through a router with a firewall, and you want to set up your PC with ViaVideo in a “Demilitarized Zone” (DMZ) use the configuration instructions on page 14. For more information about DMZs, refer to “What’s a DMZ?” on page 19.

Through a Virtual Private Network

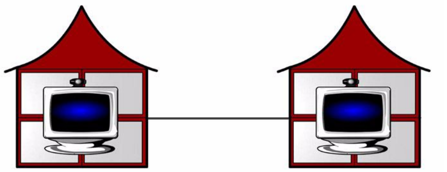


If your network connection is through a Virtual Private Network (VPN), use the configuration instructions on page 15.

Configure Your Connection

And you’re ready to communicate ViaVideo!

Simple Connection - Just a Modem, Thanks

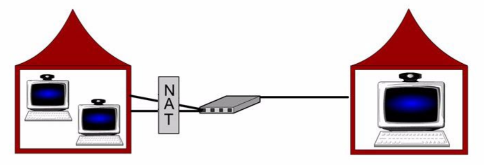


If you are using a direct connection to the internet, such as a cable modem or DSL modem, configure your ViaVideo by performing the following steps:

1. Select the **Direct Connection to Network** option on the **Firewall/Lan Connection** screen (*System Info>Setup>Lan&Internet>Firewall/LAN Connection*).
2. Enter your PC's external IP address in the **External IP Address** field.
   You can enter the address manually, or let ViaVideo enter it automatically by selecting the **Auto Discover IP Address** option. When you select **Auto Discover IP Address**, ViaVideo automatically discovers your external IP address and enters it in the **External IP Address** field.

Because of the limited bandwidth available with DSL and cable networks, it is recommended that you select a lower line speed, such as 128, for most calls. Select line speeds in the **Dialing Speeds** screen (*System Info>Setup>H.323>Dialing Speeds*).

Router With NAT, No Firewall



If you are using a router with Network Address Translator (NAT) software, you need to configure ViaVideo to use the external IP address provided by your NAT. For more information on NATs, see "What's a NAT?" on page 19.

To configure ViaVideo to use your router's NAT:

1. Go to the **Firewall/Lan Connection** screen (*System Info>Setup>Lan&Internet>Firewall/LAN Connection*).
2. Select the **Using a NAT** option.

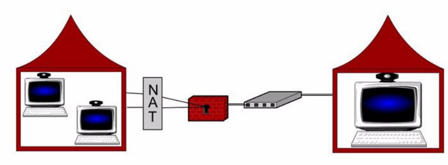
Note When you select the **Using a NAT** option, you will not be able to make video calls from the PC running ViaVideo to other PCs in your local area network. To make calls to other PCs in your local area network, de-select the **Using a NAT** option. You can re-select this option at any time to re-enable exterior video calling.

3. Enter your NAT's external IP address in the **External IP Address** field.

You can enter the address manually, or let ViaVideo enter it automatically by selecting the **Auto Discover IP Address** option. When you select **Auto Discover IP Address**, ViaVideo automatically discovers your external IP address and enters it in the **External IP Address** field.

If your network uses a proxy server, the **Auto Discover IP Address** option may not work correctly. Enter your NAT's external IP address manually in this case.

Router With Firewall



If you are using a firewall, you need to perform the following tasks:

- Configure ViaVideo to work with your firewall's Network Address Translator (NAT)
- Open and assign ports in the firewall to the PC running ViaVideo.

Configure your ViaVideo for NAT

To configure ViaVideo to use your router's Network Address Translator (NAT):

1. Go to the **Firewall/Lan Connection** screen (*System Info>Setup>Lan&Internet>Firewall/LAN Connection*).
2. Select the **Using a NAT** option.

Note When you select the **Using a NAT** option, you will not be able to make video calls from the PC running ViaVideo to other PCs in your local area network. To make calls to other PCs in your local area network, de-select the **Using a NAT** option. You can re-select this option at any time to re-enable exterior video calling.

3. Enter your NAT's external IP address in the **External IP Address** field.
   You can enter the address manually, or let ViaVideo enter it automatically by selecting the **Auto Discover IP Address**

option. When you select **Auto Discover IP AddressAuto Discover IP Address**, ViaVideo automatically discovers your external IP address and enters it in the **External IP Address** field.

If your network uses a proxy server, the **Auto Discover IP Address** option may not work correctly. You should de-select **Auto Discover IP Address** and enter your NAT's external IP address manually in this case.

Open and Assign Ports in the Firewall

To configure your ViaVideo to operate with a firewall, perform the following tasks. For more information on the steps to configure specific routers and firewalls, see the small office configuration information on Polycom's support website: http://www.polycom.com/products/video/viavideo/NetConnect/.

Before you Begin

Before you start, determine the internal IP address of the PC running ViaVideo. To do so, start the ViaVideo application and look in the **System Information** screen.

In Your Firewall

You will need to open and assign ports to the PC running ViaVideo in your router's firewall interface software so that ViaVideo can listen for incoming calls and make outgoing calls. The exact steps and terms involved may be different in your firewall interface, but the concepts are the same.

For example, opening and assigning ports to the PC running ViaVideo is referred to in the Linksys firewall interface software as "Forwarding," while the Cisco firewall software refers to the same task as "Port to Application Mapping." However your firewall interface describes it, the concepts and tasks remain the same.

1. Open a range of ports in your firewall. We recommend that you open the default ports: 3230-3235 for TCP and UDP for ViaVideo.
   Open port 1720 in your firewall. You must open this port for your ViaVideo to receive incoming calls, as specified by the International Telecommunications Union standards.
   Open port 1503 to NetMeeting to allow data sharing.

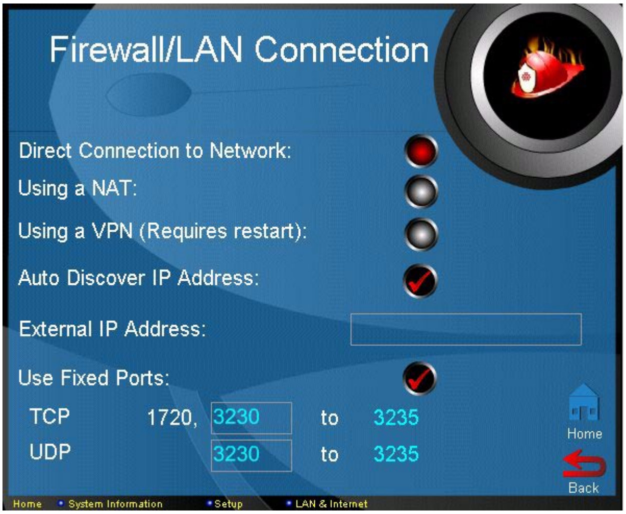
Note When you assign port 1720 to the PC running ViaVideo, this routes all incoming H.323 calls to that PC. This has the effect that no other devices in your local area network can receive incoming video or voice over IP calls (this includes IP phones).

2. Assign the port range to the PC running ViaVideo.
   In some firewall interfaces, opening and assigning port numbers is performed in one step.
   In some firewall interfaces, you assign the ports to an IP address, while in others you assign the ports to an application, in this case ViaVideo. Either way works fine.

In ViaVideo

Now you need to point ViaVideo at the right port numbers.

1. Go to the **Firewall/Lan Connection** screen (*System Info>Setup>Lan&Internet>Firewall/LAN Connection*).



Firewall/LAN Connection

Direct Connection to Network: ●

Using a NAT: ○

Using a VPN (Requires restart): ○

Auto Discover IP Address: ☑

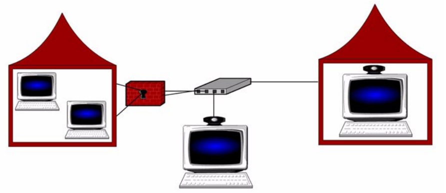
External IP Address:

Use Fixed Ports: ☑

TCP	1720,	3230	to	3235
UDP		3230	to	3235

2. Select the **Use Fixed Ports** option.
3. If you used the default port range when assigning the ports in your firewall interface, you don’t need to change anything. ViaVideo automatically enters this range. If you are using a different range, enter the port numbers for that range here.
4. You should have already performed your NAT configuration. if not, see “Configure Your ViaVideo for NAT” on page 14, and follow the instructions listed there.

Router With Firewall, Using a DMZ



If you are using a router with a firewall, and want to place the PC running ViaVideo outside the firewall, you need to perform the following tasks:

- Configure ViaVideo to work with your firewall's Network Address Translator
- Assign your ViaVideo to the DMZ.

Configure Your ViaVideo for NAT

In addition to assigning your PC running ViaVideo to the DMZ, you also need to configure your ViaVideo to use your router's NAT.

To configure your ViaVideo to use your router's NAT:

1. Go to the **Firewall/Lan Connection** screen (*System Info>Setup>Lan&Internet>Firewall/LAN Connection*).
2. Select the **Using a NAT** option.
3. Enter your NAT's external IP address in the **External IP Address** field.
   You can enter the address manually, or let ViaVideo enter it automatically by selecting the **Auto Discover IP Address** option. When you select **Auto Discover IP Address**, ViaVideo automatically discovers your external IP address and enters it in the **External IP Address** field.

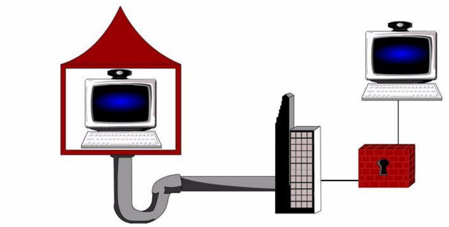
   If your network uses a proxy server, the **Auto Discover IP Address** option may not work correctly. You should de-select **Auto Discover IP Address** and enter your NAT's external IP address manually in this case.

Assign your ViaVideo to the DMZ

If your router's firewall software provides a "Demilitarized Zone" or DMZ, simply follow your firewall's instructions to assign the internal IP address of the PC running VIaVideo to the DMZ. This allows full (unrestricted) external access for the PC running ViaVideo, while the other devices in your internal network are protected by the firewall.

Note This solution does not provide protection for the PC running ViaVideo in the DMZ. For more information about DMZs, see “What’s a DMZ?” on page 19.

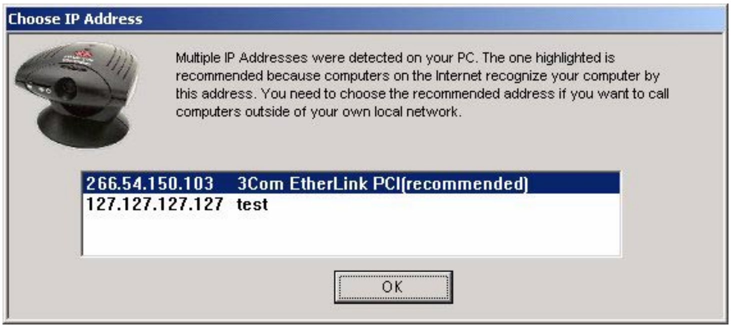
Through a Virtual Private Network



To configure your ViaVideo to operate through a Virtual Private Network (VPN) you first need to configure your VPN (in Windows’ *Settings>Control Panel>Network>Configuration*). Select the VPN connection as your network connection before launching the ViaVideo application.

Note Whenever you select, or de-select the **Using a VPN** option, you must re-start ViaVideo for your configuration change to take effect.

When you start ViaVideo, it detects the presence of multiple IP addresses assigned to your machine, and asks you which one you want to choose.



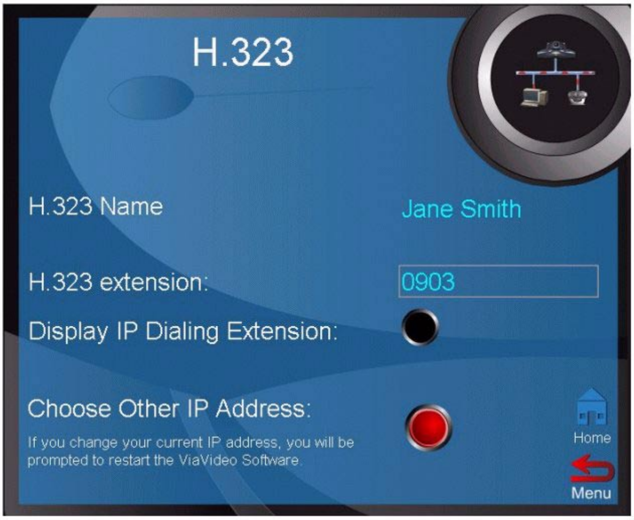
Choose IP Address

Multiple IP Addresses were detected on your PC. The one highlighted is recommended because computers on the Internet recognize your computer by this address. You need to choose the recommended address if you want to call computers outside of your own local network.

266.54.150.103 3Com EtherLink PCI(recommended)
127.127.127.127 test

Select the IP address of your VPN connection. ViaVideo displays this address in the **System Information** screen, in the bottom of the application window, and in your address book user information.

If you want to change IP addresses once ViaVideo is already running, go to the **H.323** screen (*System Info>Setup>H.323 Setup>H.323)* and click **Choose Other IP Address**.



H.323

H.323 Name Jane Smith

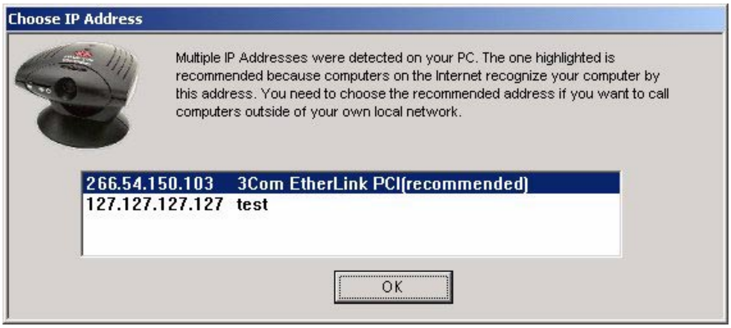
H.323 extension: 0903

Display IP Dialing Extension: ●

Choose Other IP Address: ●

If you change your current IP address, you will be prompted to restart the ViaVideo Software.

ViaVideo presents the **Multiple IP Addresses** screen.



Choose IP Address

Multiple IP Addresses were detected on your PC. The one highlighted is recommended because computers on the Internet recognize your computer by this address. You need to choose the recommended address if you want to call computers outside of your own local network.

```
266.54.150.103    3Com EtherLink PCI(recommended)
127.127.127.127  test
```

Chose the IP address of your VPN connection and click **OK**. ViaVideo uses the IP address you specified. This address is displayed in the **System Information** screen, at the bottom of the application window, and in your address book user information.

If you are using a VPN for other purposes (such as logging in to a server at work), and do not want to use the VPN for your ViaVideo connection, make sure **Using a VPN** is *not* selected, and configure ViaVideo for the type of connection you want to use. When ViaVideo detects multiple IP addresses at startup, simply choose the non-VPN IP address.

What's a Firewall?

A firewall acts as a security barrier between one network and another. Usually the barrier is erected between an interior network, such as a Small Office Home Office (SOHO) network, and an exterior network, such as the internet.

Firewall services are provided as part of the configuration software with most SOHO - quality routers, such as Linksys® and Cisco®. You can also run a firewall independent of your router by using one of the popular software-only firewall packages, such as Black Ice, Norton® Firewall, and McAfee® Firewall.

With either type of firewall, setting up a video communications connection with the outside world runs into the same problem: firewalls provide security for your network by putting up a barrier to packet traffic, limiting outside access to your internal network. This is a good thing, but you wouldn't be reading this if you didn't want to communicate with the outside world, so there are two solutions: opening ports in the firewall, and setting up a DMZ.

Opening Ports

This solution consists of opening ports in the firewall and assigning these ports to the PC running ViaVideo. This allows ViaVideo to freely accept and receive calls with the outside world, while maintaining protection for your PC and network.

For both router-based and software-only types of firewalls, the procedure is the same. Router-based firewalls usually ask you to specify the IP address of the PC running VIaVideo, and software-only firewalls ask you to assign the ports to the ViaVideo application. Either way, the result is the same - your internal network is protected, and you have video communications access to the outside world.

For information on opening and assigning ports in the firewall, see “Router With Firewall” on page 11.

Port Number Assignation

ViaVideo has applied with the Internet Assigned Numbers Authority (IANA) for the default range of 6 ports: 3230 - 3235. You must also assign port 1720 to ViaVideo so you can receive incoming calls.

We recommend that you use the default range of ports for both TCP and UDP packet transfer. If you wish to assign a different range of ports, you can specify any registered, non-assigned ports in a 6-port range to ViaVideo. For a list of registered, non-assigned ports, go to: http://www.isi.edu/in-notes/iana/assignments/port-numbers.

When you assign the ports to the ViaVideo application, the router reserves the assigned ports for use by ViaVideo.

Is it Safe?

The short answer is: “Safe enough.” Like any other defense, there’s no such thing as a perfect firewall. Whenever you are connected to the outside world, there is always some risk that someone could gain unauthorized access. The need for protection must be balanced against the need to communicate with the outside world. This is why most security solutions focus on minimizing the risk until it reaches an acceptable level.

Opening ports in the firewall might seem at first like an unnecessary security risk. However, there are in reality so many ports (65535) that simply discovering which port might be open is difficult enough. In addition to the sheer number of ports, protections written into the operating system make it very difficult to gain unauthorized access to your network, even if those ports are open. Finally, only port 1720 is open to receive incoming requests. The range of six ports is only open in your PC during a call.

If “safe enough” isn’t secure enough for you, then setting your ViaVideo up in a DMZ is safer option. For more information about DMZs, see the next section.

What’s a DMZ?

Most firewalls provide DMZ configuration as a way to allow high availability access for web servers and video communications servers (that’s your PC running ViaVideo) while providing firewall access for the other devices in the network. A DMZ is not a physical location, but is instead a way to configure your network so that the devices that are “in” the DMZ are served by the router, but are outside the protection of the firewall. Devices in the DMZ then communicate with the other devices in the internal network through the firewall.

This solution creates a “safe zone” within your internal network by effectively placing the video communications server outside of the firewall’s protection. In this way, no unauthorized connections are allowed within the firewall-protected zone, and the video communications server is allowed free access to the internet. Note that this configuration leaves the video communications server without protection from external sources.

Setting up your ViaVideo’s computer in a DMZ is the quickest way to configure your ViaVideo to run while using a firewall. For more information about configuring your video communications server in a DMZ, see “Router With Firewall, Using a DMZ” on page 14.

What’s a NAT?

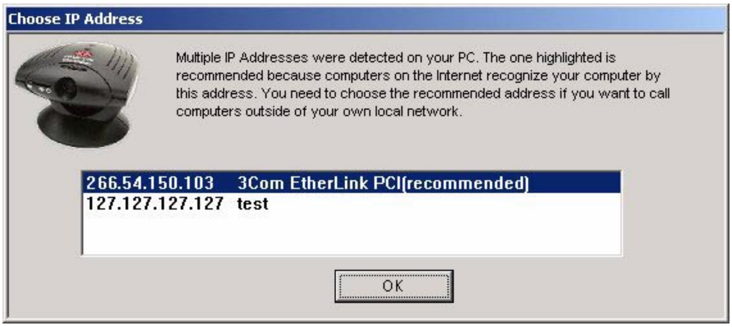
A Network Address Translator (NAT) is a set of services on the router that allow you to operate a local network of devices, each with its own locally unique IP address, while communicating to the Internet through a router which presents a single, globally unique IP address to the outside world. Most small business and home office (SOHO) routers provide NAT services.

The NAT ensures that outgoing packets have a globally valid IP address, and that incoming packets go to the right device by translating between the internal IP address and the external IP address, owned by the router. This also adds an extra level of security by effectively masking the internal network behind a single external IP address.

A simplified explanation of how this translation takes place is that when an internal device sends an outgoing packet to the router, the NAT service either notes the internal IP address or the port number of the device, and attaches an identifier to the external IP address of the outgoing packet, substituting the router's globally unique IP address for the device's internal IP address. When the answering packet comes back, the NAT notes the indentifier, re-assigns the packet to the device's internal IP address, and sends it on its merry way.

Multiple IP Addresses

If you are set up to use multiple IP addresses, ViaVideo detects the presence of these addresses. The first time you start up the ViaVideo application, ViaVideo presents the **Multiple IP Addresses** screen.



Choose IP Address

Multiple IP Addresses were detected on your PC. The one highlighted is recommended because computers on the Internet recognize your computer by this address. You need to choose the recommended address if you want to call computers outside of your own local network.

266.54.150.103 3Com EtherLink PCI(recommended)
127.127.127.127 test

You can select the IP address you want to use and click **OK**.

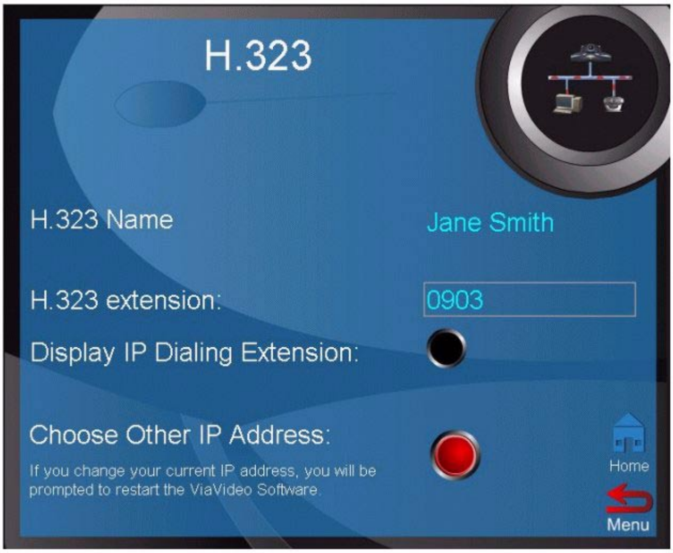
ViaVideo detects more than one IP address when:

- There is more than one LAN card in your PC.
- You are using a docking station and a PCMCIA network card.
- You are connected to your network using a Virtual Private Network (VPN).

If you want to change IP addresses once ViaVideo is already running, go to the **H.323** screen (*System Info>Setup>H.323 Setup>H.323)* and click **Choose Other IP Address**.

Note **Choose Other IP Address** is displayed in the **H.323** screen only when ViaVideo detects the presence of more than one IP address at startup. If you add another IP address while

ViaVideo is running, you must restart the application so that ViaVideo can detect the new IP address.



H.323

H.323 Name Jane Smith

H.323 extension: 0903

Display IP Dialing Extension: ●

Choose Other IP Address: ●

If you change your current IP address, you will be prompted to restart the ViaVideo Software.

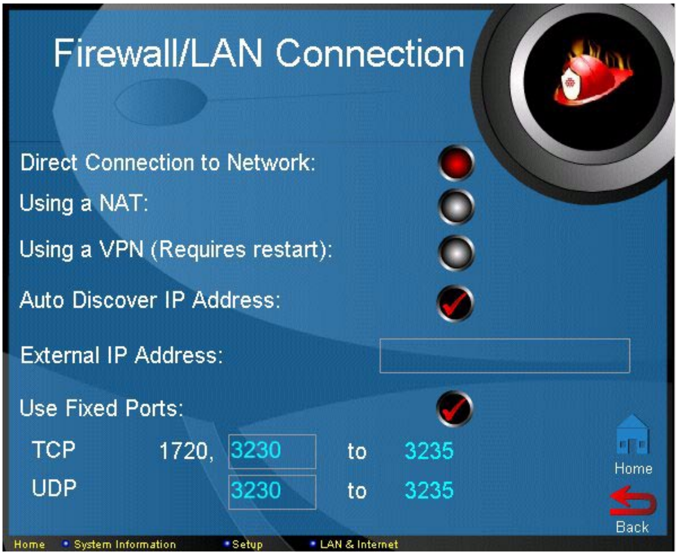
ViaVideo presents the **Multiple IP Addresses** screen, and you can choose which IP address you want to use.

Once you restart the ViaVideo application, ViaVideo uses the IP address you specified. This address is displayed in the **System Information** screen, at the bottom of the application window, and in your address book listing.

Network Configuration Screens

Firewall / LAN Connection

In this screen, you can configure ViaVideo’s Network Address Translator (NAT), Virtual Private Network (VPN), and firewall options.



Firewall/LAN Connection

Direct Connection to Network: ●

Using a NAT: ○

Using a VPN (Requires restart): ○

Auto Discover IP Address: ✓

External IP Address:

Use Fixed Ports: ✓

TCP	1720,	3230	to	3235
UDP		3230	to	3235

Using a NAT

Alerts ViaVideo to use the IP address that appears in the **External IP Address** field as its external IP address.

Using a VPN

Alerts ViaVideo to use a VPN connection.
To use a VPN with ViaVideo, select the **Using a VPN** option, turn on your VPN, and restart the ViaVideo application. When ViaVideo restarts, it presents a dialog so you can select the VPN IP address.
When switching to and from the **Using a VPN** option, you must restart the ViaVideo application.

Auto Discover IP Address

Activates ViaVideo's automatic external IP address feature, which discovers your NAT's external IP address and automatically enters it in the **External IP Address** field.

If you have entered an IP address manually in the **External IP Address** field, selecting **Auto discover IP Address** replaces whatever was in that field with the auto discovered IP address value.

In most cases, ViaVideo discovers the correct external IP address. Some VPN configurations confuse the auto discover feature. If you are using a VPN, be sure and check the VPN client application to make sure you are using the correct IP address.

External IP Address Enter the correct external IP address for your system here. If you chose the **Auto discover IP Address** option, ViaVideo selects your external IP address for you.

Use Fixed Ports Configures ViaVideo to use the fixed ports you specify in the TCP and UDP addresses fields. The firewall must be configured to assign these ports to ViaVideo.

When operating behind a firewall, you must open and assign a range of 6 ports to ViaVideo, as well as port 1720.

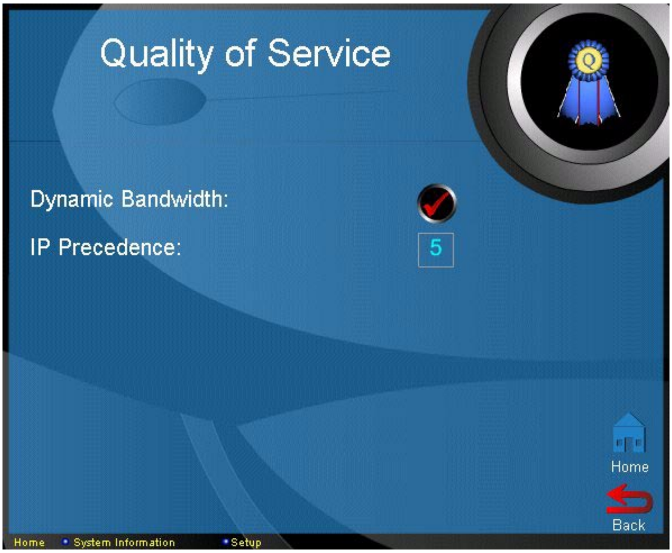
If you are using NetMeeting, you must also assign port 1503 to NetMeeting.

TCP Addresses Specify the TCP ports you will assign to ViaVideo in your firewall.

UDP Addresses Specify the UDP ports you will assign to ViaVideo in your firewall. These can be the same as the TCP ports.

QOS

In this screen, you can configure ViaVideo’s IP precedence and dynamic bandwidth options.



Quality of Service

Dynamic Bandwidth: ✓

IP Precedence: 5

IP Precedence

Specifies the priority given IP packages sent by ViaVideo. The default value for IP precedence is 5.

Dynamic Bandwidth

Specifies use of dynamic bandwidth allocation. ViaVideo’s dynamic bandwidth function automatically finds the optimum line speed for a call.

If you experience excessive packet loss while in a call, the dynamic bandwidth function incrementally lowers the line speed until there is no more packet loss. After some time with no packet loss, the dynamic bandwidth function incrementally increases line speed until packet loss occurs. At this point, the dynamic bandwidth function lowers the line speed one increment to ensure minimal packet loss with maximum throughput.