Internet and Intranet Calling with Polycom PVX 8.0.1

An Application Note

Polycom PVX™ is an advanced conferencing software application that delivers Polycom's premium quality audio, video, and content sharing to your PC and standard USB camera.

PVX brings unprecedented video conferencing technology to your desktop PC with the first software application ever offered by the industry leader. Using the industry's highest quality audio/video algorithms, PVX is the only PC application to offer both secure communications and People+Content™.

PVX supports most standard web cams, eliminating the need for a separate video camera. When used in conjunction with a laptop and portable USB camera, PVX provides the ultimate in portability.

PVX 8.0.1 features added flexibility for configuring to a wide variety of network connections, including support for Universal Plug and Play (UPnP), multiple network adapters, and Session Initiation Protocol (SIP).

This application note explains how to configure PVX for the broadband connection in your office, home office, or small business. This document also describes system settings that will maximize video conferencing performance without compromising your network security.

This document contains the following sections:

- Before You Begin
- Configuring Your Connection Using the Setup Wizard
- Configuring Your Connection Using the PVX Application
- Testing and Troubleshooting
- Advanced Router Setup
- Where to Get the Latest Product Information
- Copyright Information
- Disclaimer
- Trademark Information

December 2005
Edition: 3725-23299-001/A

Before You Begin

System Requirements

Please make sure that your PC meets the minimum system requirements for using Polycom PVX. You can find the latest information about system requirements in the *Release Notes for Polycom PVX*, available at www.polycom.com/videosoftware. If your PC does not meet the requirements, you will not be able to make PVX calls.

If you are running on a laptop PC, be sure to have the AC power plugged in before starting Windows to ensure the CPU is running in full power mode.

Downloading Free Demonstration Software

To get a free copy of the Polycom PVX software, go to www.polycom.com/pvxtrial. You can use this software for an unlimited number of calls lasting 5 minutes or less. You can upgrade the demonstration version to the full version by purchasing a license key and activating the software as described in this document.

Installing Polycom PVX Software

The first time you start PVX, a wizard guides you through the initial setup. You can set up your network connection with the help of the wizard, or you can set up your network using the application's setup screens. This document provides information about both methods.

For instructions on installing PVX, see the software CD packaging. For the latest information about Polycom PVX, also refer to the PVX Release Notes, available at www.polycom.com/videosoftware.

Activating Your PVX Software

When you start PVX, the application prompts you to activate your software. You can either enter the activation codes or simply click **Continue** if you prefer to use the evaluation version. The evaluation version allows you to make unlimited five-minute conferences.

PVX will prompt you to activate your software every time it starts until a valid activation key is entered. If you would like to obtain an activation code, please contact a Polycom reseller or go to www.polycom.com.

Configuring Your Connection Using the Setup Wizard

This section provides additional information you will need on some of the wizard pages to enable calling on the following types of connections:

- Within an Intranet
- Within a Virtual Private Network (VPN)
- Through a DSL or cable modem (no router)
- Through a network router

Refer to the appropriate section for your particular connection.

If you need to change your connection setup after you have finished the setup wizard, you can do so through the PVX application. For more information, refer to *Configuring Your Connection from the PVX Application* in this application note.

Setup for Calling Within an Intranet

An Intranet is a private network within a company or organization. Intranet calls remain inside the firewall, so you can communicate with anyone in your office network without security issues.

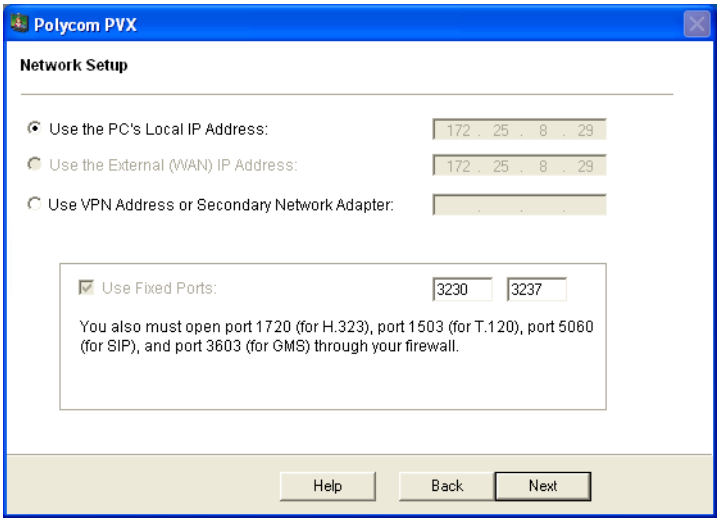
Enter this information in the setup wizard screens if you are setting up PVX for calling within your company network:

- **NAT Detected dialog box**: If the wizard asks whether to use the external WAN address, click **No**.
- **Select Your IP Address** dialog box: If the wizard detects multiple addresses and asks you to choose the recommended address, click **OK**.
- **Network Setup** dialog box: Select **Use the PC's Local IP Address** to make Intranet calls. The first time you start PVX, a wizard guides you through the initial setup.

If you need to use PVX to make external calls outside of your Intranet, please check with your network administrator. Calls outside of your Intranet require changes in the firewall settings to allow video through specific ports. Network administrators oversee firewall configurations for enabling calls to and from the Internet.

Setup for Calling Within a Virtual Private Network (VPN)

VPN is a private network that uses the public network (the Internet) for secured communication. Many offices use a virtual private network (VPN) to connect multiple locations, such as home offices and remote branch offices. With a VPN connection, users have



full access to their company network, whether they are located remotely or at the central offices.

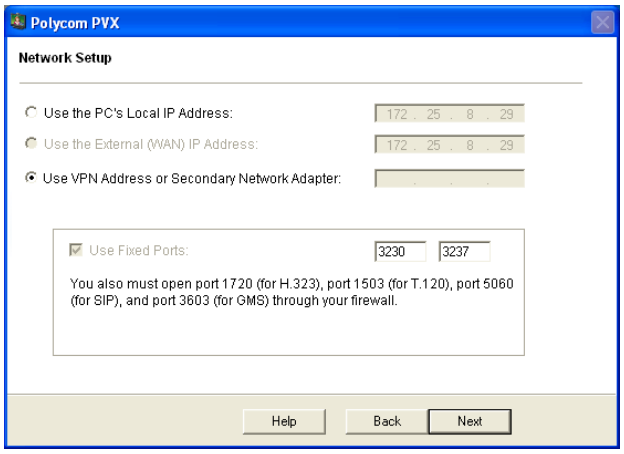
Calls within your company VPN remain within the firewall, so you can communicate with anyone in your office network without configuring PVX for connecting externally to the Internet. This way, users can make calls using the directory and all other communication equipment they have in the office.

Calls outside of your VPN require changes in the firewall settings to allow video through specific ports. See the section *Setup for Calling Through a Network Router* in this document for port information. Contact your network administrator assistance.

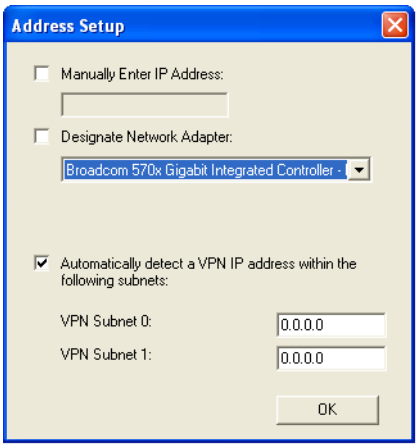
Start your VPN client and establish a connection before starting PVX. Enter this information in the setup wizard screens:

- **NAT Detected dialog box**: If the wizard asks whether to use the external WAN address, click **No**.
- **Select Your IP Address dialog box**: If the wizard detects multiple addresses and asks you to choose the recommended address, click **OK**.

- **Network Setup dialog box**: Select **Use VPN Address or Secondary Network Adapter**.



- **Address Setup dialog box:** Select your VPN connection from the **Designate Network Adapter** list. Click **OK** in Address Setup box and **OK** in Network Setup.



When you connect to your VPN, your company's network assigns you an address. This is different from the address assigned by your router. To make calls through your VPN, you must choose the VPN as your network adapter.

If your VPN is not listed in the network adapter list, please refer to the user manual for your VPN client to find out how to get the address manually.

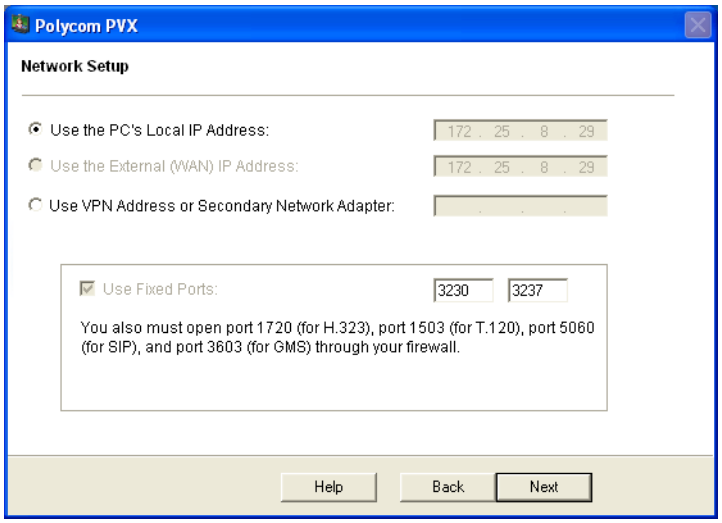
Setup for Calling Through a DSL or Cable Modem

Use the following instructions for setting up PVX on a computer that accesses the Internet directly through a DSL or cable modem with no network router.

Calls across the public Internet typically pass through a firewall that protects the computer from unsolicited traffic from the outside. Computers connected directly to a broadband modem often use a software-based firewall. If you have firewall software installed on your computer, you may need to disable or configure the software to allow PVX traffic. See the *Testing and Troubleshooting* section of this document for more information.

Enter this information in the setup wizard screens:

- **NAT Detected dialog box**: If the wizard asks whether to use the external WAN address, click **No**.
- **Select Your IP Address dialog box**: If the wizard detects multiple addresses and asks you to choose the recommended address, click **OK**.
- **Network Setup dialog box**: Select **Use the PC's Local IP Address**.



Setup for Calling Through a Network Router

Network routers enable multiple computer resources to share a high-speed Internet connection such as Digital Subscriber Lines (DSL) or cable. Most routers for Small Office Home Office (SOHO) networks include a firewall to protect the network by controlling unsolicited traffic from outside the network. To allow video conferencing traffic to pass in and out of your local network, you must open ports in the firewall or your router will block the request.

Routers also provide Network Address Translation (NAT). NAT uses private internal IP addresses for the devices within the network while using a single external IP address to

communicate outside the network. NAT adds an extra level of security by effectively masking the internal network behind a single external IP address.

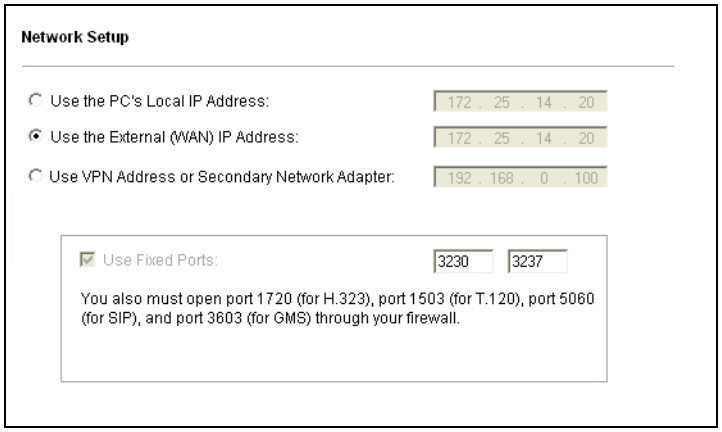
PVX supports video calls behind a firewall. In order to run PVX through a network router and firewall, you must open specific ports for video conferencing. You assign the open ports to the internal IP address (as defined by NAT) of the computer running PVX. This process is known as port forwarding or pinholing. This application note provides procedures for port forwarding on the most common routers.

If you have firewall software installed on your computer in addition to the router firewall, you may need to disable or configure the software. See the *Testing and Troubleshooting* section of this document for more information.

Entering settings in the setup wizard

Enter this information in the setup wizard screens:

- **NAT Detected dialog box**: If the wizard asks whether to use the external WAN address, click **Yes**.
- **Select Your IP Address dialog box**: If the wizard detects multiple addresses and asks you to choose the recommended address, click **OK**.
- **Network Setup dialog box:** Select **Use External (WAN) IP Address** and select **Use Fixed Ports (3230 and 3235)**.



Verify that the External (WAN) IP Address is the correct number provided by your ISP. Most routers list the external IP address on a router status page. If you need to change the IP address, finish the wizard, start PVX, and click **Setup > Network** to open the Network tab. Enter the correct External (WAN) IP Address and click OK.

Configuring PVX port forwarding

After you complete the wizard, you must configure ports in your router before you can make calls with PVX.

If your network is behind a fully aware H.323 firewall, you do not have to configure port forwarding. Your firewall can detect H.323 video traffic and open ports as necessary. Please contact your network administrator and refer to *Configuring Your Connection from the PVX Application*.

Using a router that does not support Universal Plug and Play (UPnP)

If your router supports Universal Plug and Play, please continue to the next section. If your router does not support Universal Plug and Play, proceed to the section *Configuring Your Router's Port Forwarding*.

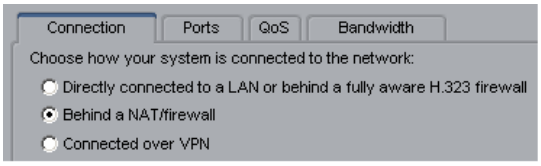
Using a router that supports Universal Plug and Play (UPnP)

Many new routers use UPnP technology that automatically detects network devices, assigns IP adresses, and enables communication. If your router has UPnP capability, you do not have to manually configure router ports to open for PVX traffic. PVX 8.0.1 can use UPnP to automatically open the ports required during your call and close the ports after use.

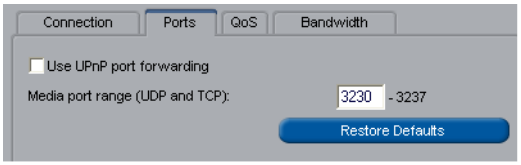
If your network security policies prohibit you from using UPnP, you can manually configure port forwarding. Refer to the next section, *Configuring Your Router's Port Forwarding*.

To use UPnP port forwarding:

1. In PVX, click **Setup > Network** to open the Network tab.
2. On the Network Setup page, click the Connection tab.
3. Select **Behind a NAT/firewall**.



4. Click **Apply**.
5. Click the Ports tab.
6. Select **Use UPnP port forwarding**.



If PVX has not detected a UPnP-enabled router, you cannot select this field.

7. Click **Apply**.

Configuring your router's port forwarding

This section provides instructions for opening and assigning ports in the most common routers from NetGear, Linksys, and D-Link. Most other routers require similar procedures.

Before you can change your router configuration, you must have the following:

- ❑ The IP address of your router.

  Consult your router's user documentation for the IP address. (Note that many routers use the default address 192.168.0.1.)

- ❑ Your router's administrator name and password.

  Consult your router's user documentation for the user name and password. (Note that many routers use the default user name admin and password blank or password.)

- ❑ The IP address that the NAT has assigned to your computer.

  To obtain the IP address that a NAT has assigned to a specific Windows XP computer, click **Start > Settings > Network Connection > LAN** and select the **Support** tab. The **Details** window shows the IP address. PVX also lists the local IP address in the main window.

With any router brand or model, you will need to open the ports listed in the following table.

Table 1: Router ports to open for PVX use

Port	Function	Type
1720	H.323 call setup	TCP
5060	SIP call setup	TCP and UDP
3230-3237	Siognalling and control for audio, call, video, and data/FECC	TCP and UDP
1503 (optional)	T.120 data collaboration	TCP

NetGear Routers

The following procedure applies to NetGear MR814v2 and RP614v2 routers. The screens and settings may vary slightly for different NetGear models. The procedures assume that your router is correctly configured and connected to the Internet and that your network is operational. Follow these steps to configure your NetGear router:

1. In a browser such as Internet Explorer, type the IP address of your router. Consult your NetGear user documentation for the IP address.

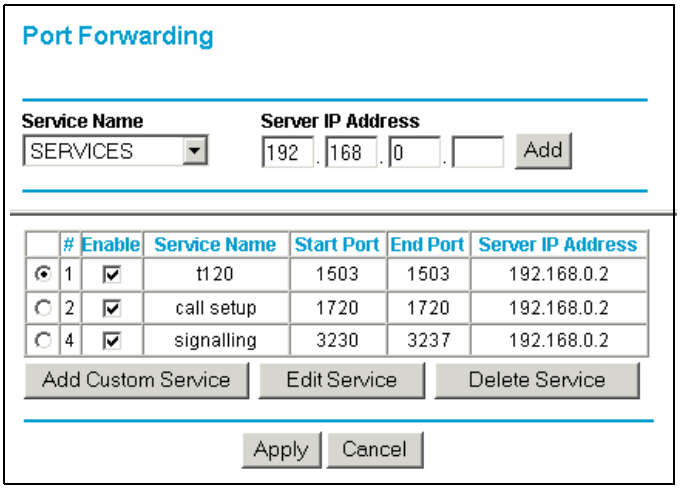
2. Log in to your router setup. Consult your NetGear user documentation for the user name and password.

3. From the Advanced menu on the left of the page, select **Port Forwarding**.
4. On the Port Forwarding page, select **Add Custom Service**.
5. On the Ports-Custom Services page, enter the following information for the first port in Table 1.

In this field...	Enter this information...
Service Name	Any unique identifier such as “H.323 call setup”
Starting Point	Port or the starting value of the range listed in Table 1
Ending Point	Port or the ending value of the range listed in Table 1
Server IP Address	IP address that the NAT has assigned to your computer

NetGear routers automatically pass TCP and UDP traffic through the same port. You do not have to designate TCP or UDP when you open ports.

6. Click **Apply**.
7. Repeat steps 4-6 of this procedure for the remaining ports in Table 1.
8. When you have opened and assigned all of the ports in Table 1, review the Port Forwarding page. Check that all of the ports are correct, enabled, and assigned to the correct Server IP (internal) Address.



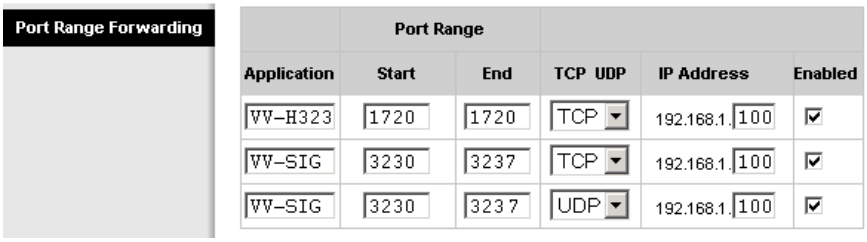
Linksys Routers

The following procedure applies to the Linksys BEFSX41 router. The screens and settings may vary slightly for different Linksys models. Follow these steps to configure your Linksys router:

1. In a browser such as Internet Explorer, type the IP address of your router. Consult your Linksys user documentation for the IP address.
2. Log in to your router setup. Consult your Linksys user documentation for the user name and password.
3. Locate the Port Range Forwarding page. (Depending on your router model, Port Range Forwarding may be listed in the Advanced or the Applications and Gaming menu.)
4. On the Port Range Forwarding page, enter the following information for the first port in Table 1.

In this field...	Enter this information...
Application	Any unique identifier such as “H.323 call setup”
Start	Port or the starting value of the range listed in Table 1
End	Port or the ending value of the range listed in Table 1
TCP/UDP	Port type listed in Table 1. Where Table 1 lists both TCP and UDP, enter the Application twice-once as TCP and once as UDP.
IP Address	Internal IP address that the NAT has assigned to your computer
Enabled	Click this box.

5. Repeat step 4 of this procedure for the remaining ports in Table 1.
6. When you have opened and assigned all of the ports listed in Table 2, review the Port Range Forwarding list. Check that all of the ports are correct, enabled, and assigned to the correct IP (internal) Address as shown in the following figure.



D-Link Routers

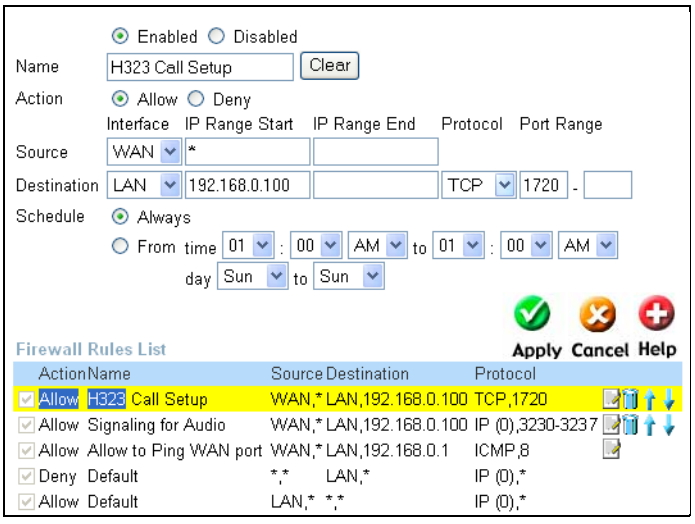
The following procedure applies to the D-Link DI-604 router. The screens and settings may vary slightly for different D-Link models. Follow these steps to configure your D-Link router:

1. In a browser such as Internet Explorer, type the IP address of your router. Consult your D-Link user documentation for the IP address.
2. Log in to your router setup. Consult your D-Link user documentation for the user name and password.

3. Select the Advanced tab.
4. Click the **Firewall** button.
5. On the Firewall page, enter the following information for each port in Table 1.

In this field...	Do this...
Enabled	Click this radio button.
Name	Enter any unique identifier such as “H.323 call setup”.
Action	Select **Allow**.
Source	Enter the following: Interface: WAN IP Range Start: * IP Range End: (blank).
Destination	Enter the following: Interface: LAN IP Range Start: The internal IP address that the NAT has assigned to your computer. IP Range End: (blank) Protocol: TCP, UDP, or * for both Port Range: The Port or the starting and ending value of the range listed in Table 1.
Schedule	Select **Always** or select a time for the port to be open.

6. When you have opened and assigned all of the ports listed in Table 1, review the Firewall Rules list. Check that all of the ports are correct, enabled, and assigned to the correct IP (internal) Address as shown in the following figure.



Setting up a DMZ

Some users may prefer to set up a PVX computer in a demilitarized zone (DMZ). A DMZ can be a quick way to configure PVX without opening specific ports individually.

DMZ is a firewall configuration that opens all of the ports through the router to a specific computer and places the computer outside of the firewall. Other devices within the network remain within the protection of the firewall. By isolating the computer with open ports, DMZ protects the rest of the network from exposure. If outside users penetrated the security of the DMZ computer, they could not gain access to any other computers on the network.

However, PVX requires only a limited number of open ports, so the advantage of opening all ports by running in a DMZ is minimal. If you choose to set up a DMZ, please refer to your router's user manual for instructions.

Setup for Multiple Network Adapters

Many PVX users have computers with more than one connection to a network. For example, a laptop user may connect most of the time via an ethernet cable at an office desk. The same user may connect the laptop less often via a wireless connection from other locations in the workplace, and least frequently by VPN from home.

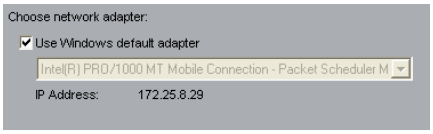
The Microsoft Windows Control Panel lists your connections in the order in which they are accessed by network services. These settings are available in the Advanced Settings in the Network and Dial-Up Connections.

By default, PVX 8.0.1 will use the Windows order of preference when attempting to connect. If the first adapter is unavailable, PVX will try the next adapter and continue through the list until an adapter is available. The Windows order of preference is convenient for most users.

However, if you want PVX to access a specific connection first, you can select the connection you want to be used. For example, if your network has a dedicated connection for video traffic, you can configure PVX to use the video adapter. If the specified adapter is unavailable, PVX will try the next adapter.

To use the Windows default adapter:

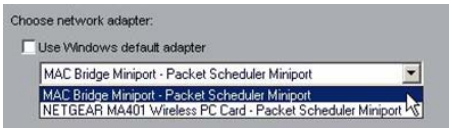
1. In PVX, click  **Setup > Network** to open the **Network** tab.
2. On the Network Setup page, click the Connection tab.
3. Select **Use Windows default adapter.**



4. Click **Apply**.

To select a default adapter:

1. In PVX, click **Setup > Network** to open the Network tab.
2. On the Network Setup page, click the Connection tab.
3. Clear the checkbox for **Use Windows default adapter**.



4. In the dropdown list, select the adapter you want to use.
5. Click **Apply**.

Configuring Your Connection from the PVX Application

If you need to change your connection settings after you finish the setup wizard, you can do so through the PVX application.

To change your connection settings:

1. In PVX, click **Setup > Network** to open the Network tab.
2. On the Network Setup page, select the Connection tab.
3. Configure the selections for your connection as follows.

For this connection type...	Do this...
Intranet	1. Select **Directly connected to a LAN or behind a fully aware firewall**. 2. Click **Apply**.
VPN	1. Select **Connected over VPN**. 2. Do one of the following: - If you are already logged in to VPN, select **Use virtual network adapter for VPN** and select your connection from the list. - If you arenot already logged in to VPN, select **Do not use virtual network adapter for VPN**. Choose whether to let PVX automatically detect a VPN IP address within a subnet or manually specify the VPN IP address obtained from your VPN client. 3. Click **Apply**.

For this connection type...	Do this...
DSL or cable modem	1. Select **Directly connected to a LAN or behind a fully aware firewall**. 2. Click **Apply**.
Network router	1. Select **Behind a NAT/firewall**. 2. Choose whether to let PVX automatically detect an IP address or manually specify your external (WAN) IP address. Your external IP address is the number provided by your ISP. Most routers list the external IP address on a router status page. 3. Click **Apply**. 4. Reboot your router.

Testing and Troubleshooting

Please refer to the *Release Notes for Polycom PVX* (available at www.polycom.com/videosoftware) for troubleshooting information including audio, video, camera, and calling issues.

If your call connects but users cannot view the incoming video (black screen), please follow these steps:

1. If you cannot see another user, verify that his or her camera is working.
2. If other users cannot see you, verify that your camera is working.
3. Verify that you have correctly followed the setup instructions.
4. Refer to this section for possible causes.

Software Firewalls

Many systems run software-only firewall packages from Microsoft or other products such as Zone Labs, Black Ice, Norton® Firewall, and McAfee® Firewall. Firewalls may interfere with video communications connection.

Windows XP Internet Connection Firewall

Users with the Windows XP operating system will not be able to place or receive video calls if the Internet Connection Firewall is enabled. To correct this:

1. Right-click **My Network Connections**.
2. Select **Network Properties**.
3. In Local Area Connection Properties, select **Advanced**.

4. Clear the **Internet Connection Firewall** option.

Windows XP Service Pack 2

Users running Windows XP Service Pack 2 may experience difficulty establishing a connection to incoming calls through a firewall. If this occurs, do the following:

1. Click **Start** and then choose **Settings > Control Panel**.
2. Select **Windows Firewall**.
3. Select **Exceptions**.
4. Confirm that the **vvsys.exe** and **Windows NetMeeting** check boxes are selected.

Zone Labs

If you are using the free downloadable version of Zone Labs firewall and virus protection, turn the software off while using PVX. If you are using other Zone Labs products, refer to the user documentation for blocking and unblocking ports.

Calling Speed and Bandwidth

Bandwidth rate is the connection speed, or the number of bits per second of data that can travel through a system or line. PVX is capable of up to 2 mbps. However, PVX requires 64 kbps minimum to connect a call.

It is important to note that high-speed DSL and cable services advertise bandwidth rates "up to" a specific speed. When a DSL or cable service claims connections up to 1.5 mbps, for example, this connection speed is a maximum and is not guaranteed.

Moreover, most ISPs do not provide bi-directional bandwidth, in which the upload rate is the same as the download rate. With most DSL and cable services, downloading is much faster than uploading. Downloading speed may be up to 1.5 mbps, but uploading speed is typically in the order of 384 kbps for DSL and 256 kbps for cable.

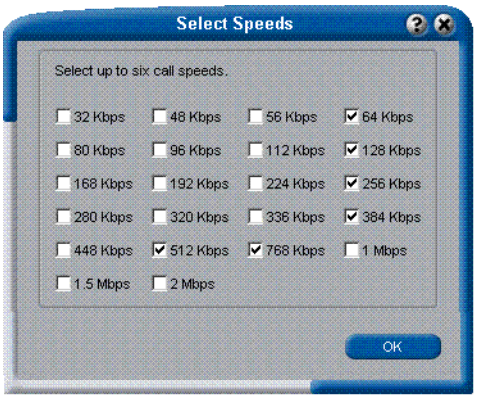
When you specify a dialing speed for PVX to use on your system, PVX uses the same specified rate for both upload and download. If any computer in the videoconference cannot upload at the speed you specified, your calls may suffer from poor video quality or you may not be able to view video at all (black screen).

For best results, ask your Internet Service Provider for their upstream speed, or their guaranteed bandwidth rate for uploading. Start by setting the PVX dialing speed to the minimum rate claimed by your ISP and test your connection with faster settings.

To change your PVX call speed:

1. In PVX, click  **Setup >Network**.
2. Select the Bandwidth tab.

3. Select a Default Call Rate that matches your ISP upstream speed (128 kbps recommended).
4. Click the **Call Speeds** button and make sure that the default rate you selected is also checked.



Network Issues

If your router ports are forwarded correctly but you still cannot view video, try setting up your router and PVX in the following order:

1. Configure port forwarding on your router.
2. Configure the PVX network setup.
3. Reboot the router.
4. Start PVX.

PVX may not function properly if more than one network connection is used simultaneously.

Test Call

Polycom offers customers global access to a variety of video conferencing equipment. Feel free to utilize these numbers to conduct testing of your video conferencing units.

www.polycom.com/videotest

Uninstall PVX

If you need to uninstall PVX, click Start and then choose Settings>Control Panel>Add or Remove Programs. Choose Polycom>PVX, and remove the program.

Advanced Router Setup

The following ports are for advanced PVX features.

GMS Ports:

Port	Feature
21 (FTP)	Software updates and provisioning
80 (HTTP)	Pulling ViewStation/VS4000 information
3601 (Data Traffic) (Proprietary)	GAB data
3603	TCP - Pulling Video inf (since might be non-web server PC)
389	LDAP and ILS
1002	ILS

GMS listens for connections on ports 80 and 3601 (GAB) and in the future will listen on port 3604 (ViaVideo) and other potentials later.

H.323 Ports:

Port	Feature
80	Static TCP - HTTP Interface (optional)
389	Static TCP - ILS Registration (LDAP)
1503	Static TCP - T.120
1718	Static UDP - Gatekeeper discovery (Must be bidirectional)
1719	Static UDP - Gatekeeper RAS (Must be bidirectional)
1024-65535	Dynamic TCP H245
1024-65535	Dynamic UDP - RTP (Video data)
1024-65535	Dynamic UDP - RTP (Audio data)
1024-65535	Dynamic UDP - RTCP (Control information)
3604	GMS Server Discovery - Used by ViaVideo (Broadcast)

MGC (Accord), Polycom Network Systems Additional Ports:

Port	Feature
5001	Static TCP - MGC Manager (5003 can be chosen instead within MGC)
21	Static TCP - FTP (retrieve MGC configuration files, etc.)

RADVision Additional:

Port	Feature
1828	Gateway signaling/call setup
2720	MCU signaling/call setup

Where to Get the Latest Product Information

To view the latest Polycom product documentation, visit the Documentation section of our website at www.polycom.com/videodocumentation.

Warranty and Registration

The Polycom PVX includes a 90-day software warranty. For the first year, software updates (bug fixes and maintenance releases) and software upgrades (feature releases) are also included.

Complete the one-time product registration form on the Polycom Resource Center website at http://extranet.polycom.com to access software downloads. Using the information provided as part of product registration, Polycom will make every effort to send you electronic notification of software releases as and when available.

Copyright Information

Disclaimer

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and fitness for purpose.

Trademark Information