

# PRODUCT SUPPORT

## Intel® ProShare® Video System 500 Product Support

- ✳ [Using the Telesync\\* TS-256 SW56/ISDN Adapter](#)  
(This product is not sold by PictureTel)
- ✳ [Dashboard like Utility](#)
- ✳ [Troubleshooting Issues](#)
- ✳ [Miscellaneous How-to Information](#)
- ✳ [ProShare® Video products and Firewalls](#)
- ✳ [What is H.323?](#)
- ✳ [Using H.323 ProShare® Conferencing Products Across Firewalls](#)
- ✳ [Aliasing and PBX Hints and Tips](#)
- ✳ [Programming the Definity G2 & G3 PBX](#)
- ✳ [VIN1 and VIN2 Video Input Connector Pinouts](#)



---

Copyright © 1998 PictureTel Corporation  
All rights reserved.

## **Intel® ProShare® Video System 500**

### Using the Telesync\* TS-256 SW56/ISDN Adapter

To configure Intel® ProShare® Video System 500 systems to use the TS-256 adapter, follow these steps:

1. Right click on Network Neighborhood.
2. Select Properties.
3. Highlight 'ProShare ISDN'.
4. Select Properties.
5. Set the protocol to 'National ISDN 1'.
6. Select Numbers.
7. Enter in the first number. Use 10 digits (area code and the number) with no spaces or hyphens.
8. Enter the same number in the SPID box.
9. Make sure the second number box and the second SPID box are both blank, and then select OK.
10. Select OK at this screen. Then select OK again.
11. The system will ask you to reboot. Select YES to reboot.
12. When the system has finish rebooting, it is ready to place and receive calls.

#### **Remember:**

When you dial out, you will need to add the # sign after the first number. When you receive a call, the caller must dial BOTH of your numbers to connect both channels.

#### **NOTE:**

PictureTel does not sell these adapters but will assist in trying to resolve the problem. If a replacement unit is needed, please visit [Telesync's](#) web site for further assistance.

# Intel® ProShare® Video System 500

## Dashboard like Utility

The Dashboard utility is designed to keep track of the status of both B (bearer) channels on your ISDN line during a ProShare® Video System 500 connection. The Dashboard like utility puts an icon in the systray in Windows\* 95 and Windows NT\*, to graphically monitor the B channels. The icon has 2 columns, each column has 4 color bars. The columns represents each of the B channels, and the bars represent the progress of the connection.

### How to use the Dashboard like utility

Watch the lights on the icon. On the first column, you should see row 1 and 2 go yellow, then rows 1,2,3,4 go green. You may see row 4 go red or row 3 go blue, briefly. This is normal. If this stays red or blue, then there is a problem. Then you should see the second column repeat the process.

#### Description:

Establish a connection

#### Dashboard displays (after Succeeding):

(First and Second row turns Yellow)



MultiFrame Alignment  
(Aligning communications)

(First, Second, Third and fourth turns Green)



If there are CRC that continue to occur, the Fourth row will turn red (Rows 1, 2, and 3 will all be green) This indicates a problem on the ISDN line.



If there are transmit errors (we receive notification from the other side, that they received an error in the transmission), the third row will light up with blue.



When both lines are established, and with no errors, the icon should look like:



### Frequently Asked Questions on the Dashboard utility

#### Only one of the columns has any lights on it. Why?

This is because there is only 1 b channel connected. The other hasn't dialed yet, or the channel was closed for some reason. Some of the most common causes for channels being closed: The second channel line is busy.

There are 2 numbers for the machine you are calling, but you only dialed 1. You should separate the 2 numbers with a colon (:).

Example:

15552251111:15552251112

Too many CRC/Transmit errors on the first channel (the top bar will be red). This will prevent the second channel from being initialized.

You are placing a voice call. Voice calls only use 1 b channel.

**One column has 4 green lights, but the second column has a steady red on the fourth row.**

This is because the second channel has lots of errors on them. Common Causes for them are: The connection is going over a 56K trunk. You can specify that Intel Business Video Conferencing uses 56K channels instead of 64K channels, by appending a # sign at the end of the first number.

Example:

15552251111#:15552251112

The ISDN line has a problem. Contact your local phone company to test your line.

**I get 2 lights on the first channel, but then the call disconnects. Why?**

This means that you are not able to align the packets. This can be caused by the drivers on the ITK board not responding correctly, hardware conflict, or a problem with the ISDN line. Please look at the troubleshooting section at the [\*\*ProShare Video System 500 support site\*\*](#) for more information.

# Intel® ProShare® Video System 500

## Troubleshooting

### **Troubleshooting Installation Issues**

Document covers issues when system reboots during installation and setup cannot find Intel ISDN/Audio/video capture board.

### **Errors Encountered During Launching**

Troubleshooting steps for issues when launching Conference Manager or Calibration that include error messages, video window disappearing, and system lock ups.

### **Issues Connecting Over LAN/WAN**

Some programs install Winsock 2 into Windows\* 95, but Intel® ProShare® Video System 500 can not use Winsock 2 in Windows\* 95.

### **Issues Connecting Over ISDN**

### **Adjusting/Resolving Resource Conflicts**

Detailed troubleshooting steps on resolving a resource conflict with the Intel ISDN/Audio/video capture board and resources required for Intel ProShare Video System 500 Conferencing.

### **Troubleshooting Miscellaneous Issues**

Troubleshooting steps for issues including garbled characters in the dial list, selecting the Business Card icon or accessing the Business Card in the Tools/Preference box causes PC to freeze, and unable to view the online manual after installing the software.

## Intel® ProShare® Video System 500

### Troubleshooting Installation Issues

- **System reboots during installation**
- **Setup cannot find Intel ISDN/Audio/video capture board**

#### System reboots during installation

**Operating System:** Windows\* 95

**Symptom:**

While installing Intel® ProShare® Video System 500, when Windows 95 is in the middle of building device driver list, system reboots and runs scandisk on restart.

**Problem:**

The BIOS is not initializing the Intel ISDN/Audio/video capture card properly.

**Solution:**

To resolve this:

1. Restart the computer.
2. Go into the computer setup (BIOS settings).
3. Find a setting about Plug and Play OS, and set it to NO.
4. Save the settings.
5. When Windows 95 starts, restart the setup of Intel ProShare Video System 500.

#### Setup cannot find Intel ISDN/Audio/video capture board

**Operating System:** Windows 95

**Symptom:**

When I try to install Intel ProShare Video System 500, I get an error that Setup cannot find the ISDN/Audio/video capture card.

This can be caused by a few different problems:

- The Intel ISDN/Audio/video capture card is in an end PCI slot
  1. Power down the computer.
  2. Put the ISDN/Audio/video capture card in a middle PCI slot.
  3. Power up the computer.
  4. Rerun Setup.
- The Plug and Play setting in the BIOS is not set correctly
  1. Reboot the computer.
  2. Go into Setup (BIOS settings).
  3. Find a setting that is: "Plug and Play OS". Change it to the opposite of what it is currently set to.
  4. Save the changes.
  5. Restart the installation.
- Some other device in the system is preventing our detection method from finding the ISDN/Audio/video capture card.
  1. Power down the system.
  2. Pull the device.
  3. Power up the system.
  4. Rerun install.
  - 5.** Once the software and drivers are loaded, replace the device that was pulled.

## Intel® ProShare® Video System 500

### Errors Encountered During Launching

- **When I open Conference Manager, the video window disappears after a few seconds, and only the Conference Manager remains**
- **Error message: "Unable to start platform for driver c:/realtime /system/iaspox32.drv"**
- **Error message: "AVVIEW Caused a General Protection Fault in Quartz.DLL"**
- **When I launch Calibration, my system locks**

When I open Conference manager, the video window disappears after a few seconds, and only the conference manager remains

**Operating System:**Windows\* 95

**Symptom:**

When I open Conference manager, the video window disappears after a few seconds, and only the conference manager remains.

**Problem:**

Video capture drivers not installed correctly

**Solution:**

To correct the video capture installation, remove the video capture device, then uninstall and re-install Intel ProShare Video Systems 500 software:

NOTE: See the document **How to Install/Uninstall** if you need assistance **uninstalling** and **installing** the software.

1. Select Start, Settings, Control Panel.
2. Double click on the "Multimedia Icon".
3. Select the Advance tab.
4. Click on the '+' sign next to Video Capture devices.
5. If you see a "blazer.dll" as one of the capture devices, click on it (to highlight the device), press the properties button, and then press the remove button. You will get a confirmation dialog box, select "yes" you want to remove this device.
6. Select OK.
7. Close the control panel window.
8. Uninstall the Intel® ProShare® Video System 500 software.
9. Install Intel ProShare Video System 500 software.
10. Check the Video Capture devices (see above for instructions), and make sure the video capture device is "video driver".
11. Launch Intel ProShare Video System 500.

**Error message: "Unable to start platform for driver c:/realtime /system/iaspox32.drv"**

**Operating System:** Windows\* 95

**Symptom:**

When I launch Intel ProShare Video Systems 500 Application, I get an error message:

"Unable to start platform for driver c:/realtime /system/iaspox32.drv"

**Solution:**

This symptom is usually caused by a hardware conflict with a soundcard.

- If the soundcard is built on the motherboard of the computer, try to disable it in the computer Setup (BIOS settings).
- If the soundcard is an add-in board, try pulling the soundcard.

- If removing the soundcard resolves the problem, then put the soundcard back in and adjust the resources for the soundcard until the error goes away.

Another cause, is that Active Movie\* is not fully initialized. (Client Access software used to log into an IBM AS400 is known to cause this symptom.)

To check this,

1. Restart Windows 95
2. When you are at your desktop,  
Select Start, Run, type in: C:\windows\system\actmovie.exe /check
3. Then select OK.
4. Launch Intel ProShare Video Systems 500. If the problem goes away, add this to your startup group.

To create a shortcut for active movie check do the following:

1. Right click the desktop and choose 'new shortcut'
2. Under 'Command line' type in 'C:\windows\system\actmovie /check'
3. Click 'next' to continue
4. Leave the default name and click 'finish'
5. To place the shortcut in the startup menu do the following.
6. Go to 'start', 'setting' and go to 'task bar'
7. Go to the Start Menu Programs
8. Click the 'Advance' button
9. Find the 'StartUp' group and drag the shortcut to the startup folder.

### **Error message: "AVVIEW Caused a General Protection Fault in Quartz.DLL"**

**Operating System:** Windows 95

**Symptom:**

When I launch Intel ProShare Video Systems 500, and get an error message;

AVVIEW Caused a General Protection Fault in Quartz.DLL

**Solution:**

This can be caused by couple of different issues:

- Resource conflict between the Intel ISDN/Audio/video capture card and some other device in the system:  
There may be a memory conflict between the Video display card and the Intel ISDN/Audio/video capture card. See the document titled [Adjusting/Resolving Resource Conflicts](#).
- Older Video drivers  
Download the latest Video drivers from the Video cards manufacturer and install them.
- Video Compression drivers are not installed completely. To fix this, you will need your Windows\* 95 CD. Remove Windows\* 95 video compression and reinstall.

To do this:

1. Select Start, settings, control panel
2. Double click on the "add/remove programs" icon
3. Click on the "Windows Setup" tab
4. Double click on the Multimedia selection (you may need to scroll down to see it)
5. Uncheck the box next to Video Compression (you may need to scroll down to see this also)
6. Select OK. This will uninstall it.
7. Restart the computer
8. Select Start, Settings, Control Panel
9. Double click on the "add/remove programs" icon

10. Click on the "Windows Setup" tab
11. Double click on the Multimedia selection (you may need to scroll down to see it)
12. Check the box next to Video Compression (you may need to scroll down to see this also)
13. Select OK. This will install it. (You will be prompted for the Windows 95 CD)
14. Restart the computer after it is installed.

### **When I launch Calibration, my system locks**

**Operating System:** Windows 95

**Symptom:**

When I launch Calibration, my system locks.

**Solution:**

This can be caused by a couple of different problems:

- Hardware conflict with the Intel ISDN/Audio/video capture card.  
See the document titled **Adjusting/Resolving Resource Conflicts**.
- The Intel ISDN/Audio/video capture card is in an End PCI slot.  
Move the Intel ISDN/Audio/video capture card to a middle slot.
- Video card drivers are not installed correctly, or are old drivers.  
Download the latest drivers from the video card manufacturer's web site, and reinstall the drivers.

## Intel® ProShare® Video System 500

### How to Install/Uninstall on Windows\* 95

- How to properly install the Intel® ProShare® Video System 500 system.
- How to save the system's original configuration files.
- How to uninstall the Intel ProShare Video System 500 system.

### How to properly install the Intel® ProShare® Video System 500 system

#### Operating System: Windows\* 95

1. Power off the computer.
2. Make sure that you are wearing your grounded wrist-band.
3. Open the computer cover to access its PCI slots.
4. Place the Intel ISDN/Audio/video-capture board in a middle PCI slot.
5. Replace the computer cover.
6. Connect the camera, audio and ISDN cables to the Intel ISDN/Audio/video capture board.
7. Power on the computer.
8. While Windows 95 boots, you will get a message indicating that new hardware has been found.
9. If you are using Windows 95 OSR2, select Cancel. Otherwise, select "Do not install a driver."  
**Note:** Running the Setup program will install the proper drivers.
10. If you are prompted to log into a network, select Cancel.
11. Place the Intel ProShare Video System 500 CD-ROM in the CD-ROM drive.
12. This should launch the Setup program automatically. If not, select the Start button->Run. Then, enter "D:\SETUP"  
**Note:** "D" is the drive letter of your CD-ROM.  
Alternatively, you can double-click on the "My Computer" icon; then, double-click on the CD-ROM icon.
13. Follow the Setup program's install instructions. If you are prompted whether to replace files, replace them.
14. When Setup is finished, you will be prompted to restart the computer. Select OK.
15. While Windows 95 launches, it will detect the new hardware and install the proper drivers.
16. When installation is complete, you will be prompted to reboot the computer.
17. To finish, select Cancel. Then, select Start->Shut Down->Shut Down the computer.
18. When you are prompted that "It's now safe to turn off your computer", power off the computer.
19. Power on the computer. You are now ready to use Intel ProShare Video System 500 system.

### How to save the system's original configuration files

#### Operating System: Windows\* 95

When installing the Intel ProShare Video System 500 software, the Setup program first saves the system's registry and the SYSTEM.INI files before starting the installation process. The Uninstall program **does not** save these files, so it is highly recommended that you manually save these files in order to save your system's original configuration. Since the installation program overwrites the existing copies, you will need to save these files after the **first** install only. If you have not installed multiple times and wish to save your system's original configuration, perform the following steps to manually save these files:

1. Select Start->Programs->MS-DOS\* Prompt.
2. Rename these files using the REN command:  
SYSTEM.BVC (system's original SYSTEM.INI file)  
SYSTEM.BV1 (system's original Registry file: SYSTEM.DAT)
3. For example, type in:  
REN SYSTEM.BVC SYSTEM.ORI <Enter>  
REN SYSTEM.BV1 SYSTEM.ORR <Enter>
4. Close the MS-DOS Prompt window and return to Windows by typing: EXIT <Enter>

### How to uninstall the Intel ProShare Video System 500 system

#### Operating System: Windows\* 95

1. Close the Intel ProShare Video System 500 application.
2. Close any open programs for the computer will need to be restarted during the uninstall process.
3. Select Start->Programs->Intel ProShare Video System 500->Uninstall Intel ProShare Video System 500.
4. When prompted to restart the computer, click on the "Restart" button.
5. If you are prompted to log into a network while Windows 95 boots up, select Cancel.
6. The Uninstall process will automatically launch and will prompt you with a list of items to uninstall.
7. Put a checkmark in the "Microsoft NetMeeting(TM)" and the "ISDN Software" checkboxes.  
**Note:** If you do not wish to uninstall the Business Cards, uncheck the "All Business Cards" checkbox.
8. Click on the OK button.
9. If you are prompted whether to remove a shared file, click on the "Yes to All" button.  
**Note:** If you are re-installing because the installation failed, it is extremely important to remove all shared files.  
When prompted next to confirm the choice, select the "Yes" button.
10. The Uninstall process will then finish removing the software.
11. When the Uninstall program is complete, you will be prompted to Shut Down or Exit to Windows. Select "Shut Down", then power off the computer.
12. If you are removing the software permanently, physically remove the Intel ISDN/Audio/video capture board from the computer. Otherwise, power on the computer.  
**Note:** Remember to select Cancel when Windows 95 detects the boards and prompts you for drivers.

## Intel® ProShare® Video System 500

### Issues Connecting Over a LAN/WAN

**Operating System:** Windows\* 95

**Symptom:** When I try to connect over my LAN/WAN, I get no audio or video. When I connect over ISDN, I work fine.

**Problem:** You may have Winsock 2.0 installed. Some programs install Winsock 2 into Windows\* 95, but Intel® ProShare® Video System 500 can not use Winsock 2 in Windows\* 95.

**Solution:** Use MS-DOS\* to rename the file that installs Winsock 2. **NOTE: DO NOT USE WINDOWS 95 EXPLORER TO RENAME the FILE.**

To find if you have Winsock 2 installed, search for WS2\_32.dll:

1. Select Start, Find, Files or Folders,
2. Type in WS2\_32.dll
3. Verify the "Look in" box is set to C: (where Windows is installed)
4. Verify the "Include Subfolders" is checked
5. Click on the "Find Now" button

If there are any occurrences, write down where they are located. Normally, the file will be in C:\windows\system.

To remove them:

1. Select Start, Shutdown, Restart the computer in MS-DOS mode
2. Change the directory (CD) to where you found the file, then rename (REN) the file to some other name.

**NOTE: DO NOT USE WINDOWS 95 EXPLORER TO RENAME THE FILE.**

Example:

Type in:

CD \windows\system <enter> (or where you found the files)

Ren WS2\_32.DLL \*.old

Make sure there are no errors when you rename the file.

3. Restart the computer, Winsock 1.1 should now be active, and your LAN/WAN connection should work.

## **Intel® ProShare® Video System 500**

### **Issues Connecting Over ISDN**

#### **Symptom:**

I have a line monitor utility in my Systray. What does it mean?

#### **Solution:**

This is a utility to show the status of the ISDN connection. For Information on what the lights mean, see the **Dashboard like Utility** document.

## Intel® ProShare® Video System 500

### Adjusting/Resolving Resource Conflicts

- Resolving a resource conflict with the Intel® ISDN/Audio/video capture card
- Resources required for Intel® ProShare® Video System 500

#### Resolving a resource conflict with the Intel ISDN/Audio/video capture card

**Solution:** The Intel ISDN/Audio/video capture card is a PCI device. The interrupt (IRQ) can be shared with other PCI devices. If the IRQ needs to be changed, it can only be adjusted in the BIOS settings, since the resources are assigned when the system boots. (Windows\* 95, OSR2 does give an ability to adjust PCI resources. Contact Microsoft as to how to accomplish this.) You can, however, adjust the memory range.

To resolve a memory address conflict, manually assign a memory address to the computer's video card that is not conflicting with another device's memory address:

1. Click on Start -> Settings -> Control Panel.
2. Double-click on the System icon.
3. Select the Device Manager tab.
4. Click on the '+' by the Sound, Video and Game controllers.
5. Double-click on the "Intel ProShare Video".
6. Click on the Resources tab.
7. Uncheck the "Use Automatic Settings" checkbox.
8. Double-click on "Memory Range".
9. Change the conflicting memory address to a range that does not conflict with another device.
10. Select OK. You will be prompted with a confirming dialog boxes. Select Yes.
11. Select OK to close the system window.
12. Shut down, and power down the computer.

To See what memory is being used:

1. Click on Start -> Settings -> Control Panel.
2. Double-click on the System icon.
3. Select the Device Manager tab.
4. Double click on Computer (this should be the first Item in the list).
5. Click on Memory.

This will give you the list of all the memory ranges currently in use. It is not uncommon to have video cards overlap their assigned memory areas, so be careful to make sure there is memory spaces between the Intel AV card's memory assignment and any other device. The Memory ranges are reported in Hexadecimal numbering system (0 - F). The Intel ISDN/Audio/video capture card uses 4095 bytes memory (Hexadecimal: FFF).

#### Resources required for Intel ProShare Video System 500

##### Solution:

- ISDN/Audio/video capture card:
  - One sharable PCI Interrupt Request (IRQ)
  - 4095 bytes of free Memory address

## Intel® ProShare® Video System 500

### Troubleshooting Miscellaneous Issues

- **Garbled characters in the dial list**
- **Selecting the Business Card icon or accessing the Business Card in the Tools/Preference box, causes PC to freeze**
- **Cannot view the online manual after I have installed the software**

#### Garbled characters in the dial list

**Operating System:** Windows \* 95

**Symptom:** Garbled characters in the dial list.

**Solution:** Add a reference for TimesNewRoman to the WIN.INI file. Perform the following steps:

1. Open the WIN.INI file.
2. Find the heading, [FontSubstitutes]
3. Add a line after [FontSubstitutes] by pressing the ENTER key
4. Type the following text:

TimesNewRoman=Times New Roman

5. Save the WIN.INI file.
6. Restart Microsoft Windows\* for the change to take effect.

#### Selecting the Business Card icon or accessing the Business Card in the Tools/Preference box, causes PC to freeze

**Operation System:** Windows 95

**Symptom:** When I click on the Business Card icon or when I try to access the Business Card in the Tools/Preference box, my PC freezes.

**Solution:** Some program has entered in a Toll List in the TELEPHON.INI file. This causes a problem with the business card. To workaround this, remove the toll prefix by editing the Location0 line in the TELEPHON.INI file. For example, if the following was the Location0 line in the TELEPHON.INI file:

```
Location0=0,"Default Location",",",",", "619",1,0,0,1,"467",0," "
```

where the toll prefix is "467". Modify the line by removing the toll prefix so that it reads as follows:

```
Location0=0,"Default Location",",",",", "619",1,0,0,1,"",0," "
```

#### Cannot view the online manual after I have installed the software

**Operating System:** Windows 95

**Symptom:** I cannot view the online manual after I have installed the software.

**Solution:** Go to a DOS\* system and reregister the ENVOCX.OCX.

1. Select Start, Programs, MSDOS Prompt.
2. Type in: CD \progra~1\bizvideo\Manual [Enter].  
Regserv envocx.ocx [Enter].
3. Exit [Enter].

## Intel® ProShare® Video System 500

### Miscellaneous How-to Information

- **Start Intel®ProShare® Video System 500 in Listen Mode**
- **Force an ISDN call at 56K per channel**
- **Maximum video cable length and availability of video extension cables**

#### **Start Intel ProShare Video System 500 in Listen Mode.**

**Solution:** Create a shortcut to start the Intel ProShare Video System 500 application in Listen Mode. Follow these steps to create the shortcut:

1. Close all applications.
2. Right click the workspace > New > Shortcut.
3. Click the Browse button and locate CVIEW.EXE in the directory where the Intel ProShare Video System 500 software was installed.
4. Double-click CVIEW.EXE.
5. In the command line, type /LISTENING (outside the quotation marks). Be sure to leave a space after the quotation mark before typing the text string.
6. Click Next and type the name for the shortcut.
7. Click Finish.

Below are some things to check if the Listening Mode shortcut is not working:

- Verify that /LISTENING is added outside of the quotation marks.
- Verify that there is a space after the end quote mark before /LISTENING.
- Verify that a forward slash "/" is used before LISTENING, not a back-slash "\".

#### **Force an ISDN call at 56K per channel.**

**Problem:**Some public telephone company switches can only handle 56K per B channel. This can cause problems when trying to call out at 64K per channel.

**Solution:**To make a video call at 56k (112k) instead of the normal 64k (128k), dial the number while appending a '#' as follows: 15032641367#

#### **Maximum video cable length and availability of video extension cables.**

**Solution:** Extension video cables are not available from Intel. The maximum length of the video cable will depend on two external factors:

- The quality and grade of the cable itself, which will affect the attenuation of the composite video signal.
- Any environmental forces acting upon the cable which can cause interference (add noise) to the composite video signal.

## Intel® ProShare® Video System 500

### ProShare® Video products and Firewalls

- **Which ports can I open, to let the ProShare® Video System 500 traffic through my firewall?**  
Since H.323 uses dynamic ports, the ports you would have to open is 1024-65535. Since this would defeat the purpose, you might implement an H.323 Proxy.
- **According to my firewall vendor, I have an H.323 proxy built into my firewall. Microsoft's NetMeeting\* works fine through it. ProShare seems to connect, but there is no audio or video.**  
The H.323 proxy is probably H.323 capable, not compliant. These were designed for Microsoft's NetMeeting\* operation through the firewall. Generally, they filter the traffic, based on a byte string within the packet. This does not work properly with H.323 compliant products, such as ProShare® Video System 500.
- **Is the H.323 proxy already included on my Firewall?**  
Generally, Firewalls do not implement H.323 compliant proxies. This is generally a separate computer that can establish the connection internally and externally, and convert between the two.

## What is H.323?

- ✱ Technical Overview
- ✱ Frequently Asked Questions
- ✱ Building Blocks
- ✱ Benefits
- ✱ Deployment Scenarios
- ✱ Choosing H.323 Solutions



## H.323 Technical Overview

H.323 is designed for network compatibility and works over and across existing infrastructures — LAN/WANs, the Internet, ISDN, and POTS. H.323 can be deployed wherever Internet Protocol (IP) is supported, regardless of physical network topology or protocol — ATM, FDDI, Ethernet, T1, etc. The H.323 standard is both hardware and operating system independent, which means products can be manufactured by many different vendors for use in a variety of environments.

H.323 defines four major components and how they interact with each other, as well as how they interact with a circuit-switched network (e.g. H.320 conferencing systems). These four components are: endpoints, gatekeepers, gateways, and multipoint control units (MCUs). H.323 also defines two modes for conferencing: point-to-point and multipoint.

### Endpoints

Endpoints are the clients in an H.323 network. They are typically video conferencing, audio conferencing, or other multimedia systems implemented by end users to communicate in real time. The H.323 standard requires that every endpoint support certain functions and codecs that have been previously defined by the ITU. Endpoints are required to support the following:

**G.711** - An ITU standard for speech compression

**H.245** - A protocol for controlling media between H.323 endpoints

**Q.931** - A signaling protocol for establishing and terminating calls

**Registration/Admissions/Status (RAS) Channel** - A data stream used to communicate with a gatekeeper (not used if a gatekeeper is not present)

**Real-Time Protocol/Real-Time Control Protocol (RTP/RTCP)** - IETF application-level protocol for carrying packetized real-time media on IP networks

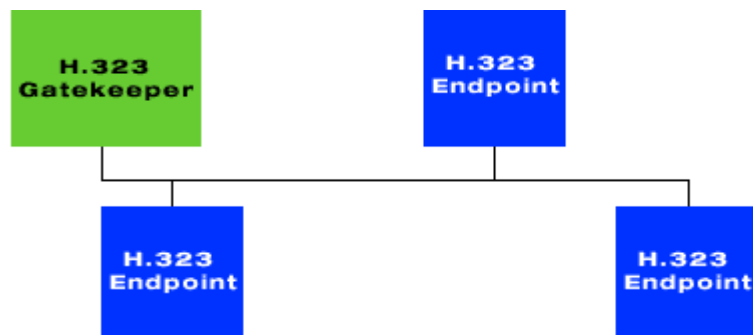
Optionally, H.323 endpoints may also support video, additional audio codecs, T.120 data conferencing, multicast, and Quality of Service (QoS). If an endpoint supports video, the standard requires a minimum of H.261 QCIF (Quarter Common Interchange Format - 176 x 144 pixels) support. Support for other video formats is optional.

The fact that there are many optional features for an endpoint creates significant challenges for H.323 interoperability. For example, an H.323 endpoint that supports only the basic requirements is "standards compliant;" however, when connecting with another compliant endpoint that supports optional video and data sharing, the conference will be limited to basic H.323 functionality. To the end user, the conference will be limited to G.711 audio and no video or data. In other words, they are limited to the same functionality as a standard telephone call.

### Gatekeepers

A gatekeeper provides call authorization for both accepting and placing calls in its "zone." A zone consists of H.323 endpoints, H.323-to-H.320 gateways, H.323 proxies and H.323 multipoint units that are configured to be under the gatekeeper's control. A gatekeeper also allocates bandwidth and provides address translation between aliases and IP addresses. Each zone can have only one active gatekeeper, but there can be many zones, and therefore many gatekeepers within an organization. Gatekeeper support on an H.323 network is optional; however, if a gatekeeper is used, all endpoints on the network are required to make use of it. Gatekeepers are not required but may support bandwidth allocation during a call or other supplemental services like call accounting, routing, and network management.

Gatekeeper Diagram



## H.323 Frequently Asked Questions

Standards

H.323

Endpoints

Gatekeepers

Gateways

MCUs

Firewalls

Miscellaneous

### Standards

#### Q: What video conferencing standards exist today?

**A:** There are four "umbrella" standards for video conferencing today:

**H.320 for ISDN video conferencing** describes standards for both multipoint and point-to-point video conferences over circuit-switched networks (CSNs), such as ISDN and Switched-56. H.320 governs the basic concepts of audio and video communication by:

- Specifying requirements for processing audio and video information
- Providing common formats for compatible audio and video inputs and outputs
- Defining protocols for multimedia endpoints to use the communication links and synchronization of audio and video signals

**T.120 for data conferencing** specifies how to distribute files and graphical information efficiently and reliably in real time during a multimedia multipoint conference, including conferences using network bridging products and services. The T.120 objective is to:

- Ensure transparent interoperability among unlike endpoints
- Permit data sharing among participants in a multimedia conference connecting through ISDN, PSDN, CSN, or TCP/IP and IPX LAN
- Specify infrastructure protocols for data conferencing applications

**H.323 for LAN and intranet conferencing** describes standards for both multipoint and point-to-point video conferences over packet-switched, IP networks.

**H.324 for POTS multimedia conferencing** describes high-quality video and audio compression over POTS modem connections. This recommendation specifies a common method for sharing audio, video, and data simultaneously using high-speed (V.34) modem connections over a single analog (POTS) telephone line.

#### Q: What standards organizations exist today?

**A:** The major organizations responsible for defining and promoting conferencing standards are the ITU-T, the IMTC, and the IETF:

**The International Telecommunications Union - Telecommunications (ITU-T)** is a United Nations organization of international governments and the private sector that coordinates standards for global telecommunication networks and services. The Telecommunication Standardization Sector — the second T in ITU-T — develops telephony standards. While companies are welcome to join and participate in ITU discussions and proposals, the voting members are not companies but countries. For more information, check out the International Telecommunications Union web page at <http://www.itu.ch/>.

**The International Multimedia Teleconferencing Consortium (IMTC)** is a non-profit organization whose purpose is to promote and facilitate the development and implementation of standards-based, interoperable products and services for multimedia conferencing. The IMTC is comprised of individuals from organizations that develop and supply multimedia conferencing products and services around the world. While IMTC members are encouraged to participate in the ITU, their primary concerns are the validation and promotion of standards and interoperability. The IMTC concentrates its attention on the adoption of ITU multimedia conferencing standards and market education. The IMTC has become the leader in coordination and promotion of conferencing-related, standards-based interoperability events.

**The Internet Engineering Task Force (IETF)** is a parallel standards committee that focuses on lower layer network protocols used by many conferencing applications.

### H.323

#### Q: What is H.323?

**A:** H.323 is a multimedia protocol for real-time conferencing over a packet-based network (LAN). It is a collection of multimedia communication standards established by the International Telecommunications Union (ITU). H.323 borrows from a compatible set of H.320 (ISDN) audio/video codec recommendations so new H.323 endpoints can still communicate with older, ISDN-based desktop and room video conferencing systems. H.323 also incorporates the T.120 data conferencing standard. Microsoft's NetMeeting\* (an H.323 application) also supports the T.120 protocol.

#### Q: What is included in the H.323 standard?

**A:** H.323 defines four major components that interact on a packet network. Included in this definition are:

- H.323 endpoints that conduct an audio, video and data conferencing call
- An interworking device (gateway) for operation with a circuit-switched network
- An optional gatekeeper to provide the connectivity between ISDN endpoints calling into the LAN to reach an H.323 endpoint and perform network management
- Multipoint Control Units (MCUs) for conducting multipoint conference calls on the LAN

The H.323 standard defines:

- How endpoints make and receive calls
- How endpoints negotiate to a common set of audio, video and data capabilities
- How audio and video information is formatted and sent over the network
- How audio and video are synchronized (lipsync)
- How endpoints communicate with their respective gatekeepers, which permits calls to go through based on well-defined policies like bandwidth utilization

Only one form of audio (G.711) is mandatory. All video and data capabilities are optional. That is why H.323 is known as THE standard for IP Telephony. Fortunately, the standard defines a wide variety of optional capabilities, including video, data and other audio options to permit more robust, multimedia-based, video conferencing to occur.

#### Q: Why use H.323? What are the benefits?

**A:** H.323 allows flexible, high-quality video conferencing over a LAN or WAN, leveraging existing network infrastructures. If you have invested in ISDN, H.323-based video conferencing can reduce your overall costs while providing the same connectivity benefits of ISDN. Instead of having to deploy ISDN to every desktop, you could deploy H.323 instead, using one or more H.320 gateways, shared by all users, to make calls to remote H.320 endpoints. Since fewer ISDN lines are required, you save on ISDN access and usage charges. The cost of the H.320 gateway can be recovered quickly, and you avoid the complexities of setting up ISDN.

H.323 also allows voice calls over LANs and WANs, even the Internet, saving long distance charges. H.323-based voice-over IP technology requires hardware that converts packet-based audio into Time-Division Multiplexed (TDM) audio used by the switched circuit network. This type of gateway, often called an IP Telephony Server, is offered by a number of companies. Cisco recently announced its MC3810 Multi-service Access Concentrator that offers the ability to make H.323-based voice calls, along with many other features.

H.323, using the gatekeeper component, gives companies the ability to control conferencing usage (bandwidth) and to track and bill conferencing usage based on services end users use.

**Q: What components are typically needed for H.323-based video conferencing?**

**A:** A typical end-to-end H.323 solution could include a combination of the following components:

- A TCP/IP network
- H.323 and T.120 standards-compliant video conferencing endpoints
- H.323 gatekeeper
- H.320 gateway
- H.323 Multipoint Control Unit
- H.323 firewall/proxy

H.323 uses the Internet Protocol (IP) for operation, so you will need a network that can support TCP/IP. You will also need an H.323-based video conferencing endpoint, which is either a desktop or a group conferencing system. There are very few H.323-based group conferencing systems on the market. Intel offers the only H.320 and H.323-based systems.

If you want to manage the amount of video conferencing traffic on your LAN or WAN, you will need a gatekeeper. A gatekeeper is also useful when trying to make a call if you do not know the IP address of the endpoint you want to call. Most gatekeepers will complete your call by providing an IP address if you supply an email address.

If your H.323 endpoint needs to call an ISDN-based H.320 endpoint, you will need an H.323-to-H.320 gateway. This eliminates the need to install ISDN to every desktop.

For in-house multipoint calls, you will need an H.323 MCU. For more information, visit Intel's Web site at: <http://www.intel.com/proshare/conferencing/h323/>

**Q: Is H.323 video conferencing limited to calls over local area networks?**

**A:** H.323 works wherever the Internet Protocol is supported and in fact is the standard for Internet telephony. H.323 operates across packet-based networks, including ATM local area networks and the Internet. H.323 was designed to work with the global switched telephone network. H.323 promotes interoperability of many devices through its flexibility to negotiate capabilities.

**Q: Why purchase a product based on a standard like H.323?**

**A:** Standards make it possible for people all over the world to communicate using hardware and software developed and distributed by different vendors. When products interoperate, consumers can choose from a vast selection of multimedia teleconferencing products without the fear of being tied to one vendor. And these products can then work together as seamlessly as telephones and fax machines.

**Q: What is a codec?**

**A:** A codec is an algorithm implemented in hardware or software for Compressing and Decompressing audio or video stream of information.

**Q: What video codecs are supported in H.323?**

**A:** Video codecs in H.323 are optional. If video capability is provided, the H.261 QCIF must be supported. Optionally, an endpoint may be capable of supporting H.261 (CIF mode) or H.263 (QCIF mode). If H.263 CIF mode is supported, then H.261 CIF must also be supported. CIF stands for Common Interchange Format, representing a video image 352 x 288 pixels in size. QCIF stands for Quarter CIF, representing a video image 176 x 144 pixels in size, containing one fourth the information contained in a CIF image.

**Q: What audio codecs are supported in H.323?**

**A:** Every H.323 endpoint must support an audio codec. At minimum, an H.323 endpoint must support G.711, both A-law and M-law. Optionally, endpoints can support G.722, G.728, G.729, MPEG1 audio and G.723.1. An endpoint should be capable of sending one audio codec while receiving another, provided it supports both.

**Q: What types of multipoint conferences are supported by H.323?**

**A:** H.323 defines two types of multipoint conferencing - centralized and decentralized. Centralized multipoint, commonly used today, involves an H.320 MCU (multipoint control unit), where all endpoints either call into, or are called from, the MCU. For H.323, the MCU resides on the network and can be either hardware or software implementations.

De-centralized multipoint is multipoint on the network without an MCU present. As defined in H.323, one endpoint is responsible for call setup and management and is otherwise known as a multipoint controller (MC). All the endpoints are multipoint processors (MPs), meaning they can locally switch video or mix audio. Each endpoint supports multicast and can selectively choose what they broadcast or receive. For example, an endpoint may choose to listen to audio from only the endpoint that is currently "talking." Or it could listen to audio from all endpoints, mixing them and producing audio from all participants. De-centralized multipoint requires powerful endpoints to perform audio mixing and is not currently available.

**Q: How is LAN bandwidth utilization controlled under H.323?**

**A:** Some endpoints permit an upper bound for bandwidth utilization to be specified in the endpoint. In most instances, bandwidth is controlled by an H.323 gatekeeper. The gatekeeper controls conferencing traffic by implementing a set of policies defined by the network administrator. These policies may mandate that endpoints can use no more than 128kbps bandwidth on the LAN, similar to an ISDN call. H.323 bandwidth is usually specified for local H.323 calls and for external calls to and from other gatekeeper zones.

**Q: What is H.323 Revision 2?**

**A:** Over time, standards are modified to encompass more functionality or to clarify past specifications. For H.323, Revision 2 represents the second revision of the standard, having received final approval in January 1998. Revision 2 is fully backward-compatible with Revision 1. Revision 2 covers additional functionality including:

- H.263+ (video codec improvements)
- Fast connect
- RSVP/QoS negotiation
- H.235 security (user authentication, call tracking, billing)
- Supplementary telephony support (call transfer, forward, etc.)
- IP over ATM
- Improved addressing (DNS, email)

**Endpoints**

**Q: How do you call another endpoint on the LAN?**

**A:** Another endpoint can be called by referencing its IP address. However, many products (through their user interfaces) permit mappings to the IP address, such as an alias, an extension, or a DNS name. Examples include: Call 211.211.10.1 (IP Address); Call chuck\_smith (alias), Call 1234 (extension) or Call chuck.smith@intel.com (DNS name).

Be careful using aliases, since some gatekeepers may attach special significance to them. For example, each Cisco gatekeeper is assigned a gatekeeper ID string and a numeric prefix. For inter-zone calls, if an endpoint calls another endpoint using an alias string, the alias string must include the gatekeeper ID of the called endpoint's gatekeeper. An alias string such as "@othergatekeeperID" would have to be appended. Also with Cisco gatekeepers, if an endpoint calls an endpoint in another zone using a numeric extension, it must begin with the prefix of the gatekeeper the called endpoint registers to.

**Q: Does Intel® Business Video Conferencing, ProShare® Video System 500 or the TeamStation™ system support RSVP?**

**A:** Not currently. RSVP support, however, is planned for a future release. RSVP will be used primarily to signal that Quality of Service (QoS) is desired. Network manufacturers will likely deliver QoS end-to-end without using RSVP, since management of RSVP requests can likely exceed available router memory, especially in large deployments of RSVP.

**Q: What Intel H.323 desktop products are available today?**

**A:** Intel is currently shipping two desktop products that support both ISDN (H.320) and LAN (H.323) in a single system. These include:

- Intel® ProShare® Video System 500
- Intel® Business Video Conferencing System

**Q: What Intel H.323-based room systems are available today?**

**A:** Intel currently offers the Intel® TeamStation™ system, one of the only group systems that supports both H.323 and ISDN (H.320) in the same system.

### Gatekeepers

**Q: What is a gatekeeper?**

**A:** A gatekeeper is software that primarily provides two functions: call control and address translation. If a gatekeeper is present on the network, an endpoint must contact the gatekeeper and ask permission to make a call. Following policies established by the LAN administrator, the gatekeeper will permit the call to go through. The gatekeeper also provides address lookup and translation services. To make a connection, an endpoint must reference the IP address of the remote endpoint it is calling, whether on a LAN or at the other end of a gateway. The gatekeeper will resolve an IP address for all endpoints under its control, given an email address or an "alias" string or an extension, such as a phone extension. This information is normally configured in the calling endpoint at setup.

**Q: Explain the process of an H.323 endpoint registering with a gatekeeper.**

**A:** Every H.323 endpoint has an IP address, either a permanent one assigned to a particular network card, or a temporary one that is assigned at network login, via Dynamic Handshake Control Protocol (DHCP). Once the H.323 video conferencing application is invoked, it immediately looks for an H.323 gatekeeper on the network. If the gatekeeper is found, the H.323 endpoint sends its IP address, extension or alias (provided by the user in the endpoint H.323 software application) to the gatekeeper, registering itself. If a gatekeeper is present on the network, an endpoint must be registered with the gatekeeper before calls are permitted between that endpoint and another endpoint for both initiating and receiving calls. If no gatekeeper is present, the H.323 endpoint is permitted to make calls without permission from a gatekeeper.

**Q: How does a DNS server get involved when an H.323 call is made?**

**A:** To make an H.323 call, the user will supply the IP address, extension, or alias (such as an email address) of the user they are calling. If an extension or alias is supplied, the DNS server is first contacted during a call to determine if the supplied string is a DNS name. If the DNS server does not have knowledge of the extension or alias, the H.323 endpoint then passes the extension or alias on to the gatekeeper for resolution. If necessary, a gatekeeper will poll other gatekeepers in other zones to resolve an IP address. How this process occurs varies by vendor.

**Q: What is a gatekeeper zone?**

**A:** A gatekeeper zone is the collection of H.323 endpoints, gateways, MCUs and proxies that are collectively managed by a gatekeeper. If a gatekeeper is present on the network, all the H.323 components must register with the gatekeeper before they are able to make or accept calls. Otherwise, the H.323 standard allows the H.323 endpoints to make calls without any restrictions. Once registered, the gatekeeper dynamically keeps track of all components in its zone, and when a call comes in from another zone, or gateway, the gatekeeper can translate the requested extension into the appropriate IP address of the endpoint on the LAN. Without the LAN-based endpoint registering first, the external call could not be completed.

**Q: What H.323 gatekeepers are available today?**

**A:** Companies currently offering H.323 gatekeepers, either standalone or included with another product sold by the same company, that have been tested on a limited basis for use with Intel video conferencing endpoints include Intel® LANDesk® Conference Manager, VideoServer's Encounter NetGate\*, and RADVision's OnLAN\* L2W 323 gateway.

**Gateways**

**Q: What is a gateway?**

**A:** A gateway is a hardware device that acts as a "bridge" between the packet-based network and the public-switched circuit world. It transcodes, or converts, the audio, video and data as necessary between the two networks. Depending on vendor offerings, gateways can support ISDN (H.320), Plain Old Telephone System (H.324) and voice call connections to and from the LAN and can often assist in other telephony-like services such as call forwarding, call transferring, hold, etc.

**Q: What is an H.320 gateway?**

**A:** An H.320 gateway is a hardware device that acts as a "bridge" between the packet-based network and the public-switched circuit world, specifically enabling calls between a LAN endpoint and an H.320 (ISDN) endpoint.

By having an H.320 gateway on the network supporting multiple 128K ISDN (BRI) adapters, ISDN no longer needs to be installed on every desktop. All the network users can share the ISDN ports on the gateway, to the extent that ports are available. ISDN costs, including installation charges, ISDN access charges and ISDN usage charges, are reduced, since charges only need to be incurred supporting the gateway.

**Q: How do I call H.320 users if I am using H.323?**

**A:** H.323 users can call H.320 endpoints through an H.320 gateway. The gateway resides on the LAN and provides the connection between the H.323 endpoint and a remote H.320 endpoint. The gateway takes packet-based audio, video and data information from the LAN and processes it for transmission over the Publicly Switched Telephone Network (PSTN) to an ISDN, H.320-based endpoint. Since H.323 supports the same audio and video codecs as H.320, little transcoding or conversion of the audio/video information from one format to another is required.

**Q: How do you make an inbound call through a gateway?**

**A:** Inbound calls are very user interface-dependent. From Intel's perspective, when making an inbound call from an ISDN endpoint through the gateway to an H.323 endpoint, you dial the ISDN phone number of the gateway and include a caret ^ followed by the extension of the endpoint or MCU you are calling. An example would be 98885551212^123456. The 9 is dialed for an outside line, the 888 for area code, the 5551212 for the number, and 123456 as the extension configured in the endpoint or MCU that was registered with the gatekeeper.

**Q: How do you make an outbound call through a gateway?**

**A:** Outbound calls are also very user interface-dependent. From Intel's perspective, the gateway is referenced on the LAN using a prefix. Each gateway will have a different prefix, and there may even be a different prefix based on the type of service the gateway offers. For example, the prefix 80 may mean a 128K ISDN call, but the prefix 90 may mean a voice call through the gateway. When an H.323 endpoint on the LAN makes an outbound call to an ISDN endpoint, it dials 80 followed by the ISDN number for the remote endpoint. If two ISDN numbers are required, each must be preceded by the prefix 80 and separated by a colon. For example,

80918885551212:80918885551213

where 80 is the gateway prefix, 91 gets an outside line through the PBX, and the 8885551212 and 8885551213 are the two ISDN numbers being called. Depending on implementation, some vendors may require a special character to separate the prefix from the ISDN number, such as the pound sign (#). You should check with your gateway vendor to be certain.

**Q: What vendors provide H.320 gateways today?**

**A:** A number of vendors offer H.323/H.320 gateways. Intel has conducted limited testing with gateways from VideoServer Inc. and RADVision.

**MCUs**

**Q: What is an H.323 MCU?**

**A:** An H.323 multipoint control unit (MCU) is a device, either hardware or software, that mixes audio and switches video between two or more endpoints. The number of simultaneous conferences and endpoints supported by an MCU varies by implementation. A hardware-based MCU can generally support more simultaneous users by dedicating a digital signal processor on a card to each user, often called a port. A software-based MCU typically runs on a network server, and is performance-bound by the speed of that server. A software-based MCU, however, generally costs much less than a hardware-based MCU.

**Q: What vendors provide H.323 MCUs today?**

**A:** A number of vendors offer H.323 MCUs. VideoServer is currently shipping a hardware-based H.323 MCU (Encounter NetServer\*), while WhitePine Software is shipping a software-based MCU (MeetingPoint\*). Other vendors with H.323 MCUs include Accord, Lucent, Outreach, and PictureTel.

**Firewalls**

**Q: Which firewall vendors support H.323 today?**

**A:** Checkpoint Software and Cisco Corporation support H.323 via filter- or state-based firewall implementation. Secure Computing and Trusted Information Systems offer H.323 proxy-based firewalls, based on proxy code licensed from Intel Corporation.

**Miscellaneous**

**Q: Is there a LAN latency limit specified in H.323?**

**A:** H.323 defines a number of timer values related to the control flow of messages. Due to the varied environments in which IP can be deployed, response times are given as guidelines only. Timeouts and retries are specified to allow compatibility between different products. For real-time media streams, the Real-Time Control Protocol (RTCP) may provide some latency indications. Latency is greatly affected by transient network loading and specific local implementation choices.

**Q: How secure is H.323?**

**A:** Concurrent with the completion of H.323 Revision 2 was the associated security framework H.235. It provides security services including authentication, privacy and integrity. These may be supplied using passwords or digital certificates. Another mode of operation uses the framework of Transport Layer Security (TLS) or IP Security (IPSec). Finally, H.235 allows negotiation of specific security parameters required by local or national policy.

**Q: Does H.323 guarantee performance?**

**A:** H.323 can guarantee performance only to the extent that the underlying network can guarantee performance. H.323 may be operated in an environment such as ATM which can provide consistent and guaranteed performance through the use of virtual circuits. Specific implementations may monitor and regulate the number and types of media that are exchanged depending on the network performance. H.323 does provide control signaling to take advantage of demand type performance where the interfaces are given by the underlying transport.

**Q: Will H.323 replace H.324?**

**A:** H.323 has demonstrated the ability to adapt to many different environments due to the leveraging of existing underlying technologies. H.323 will be used in many situations that now use H.324 when it becomes efficient and effective to use IP for direct point-point connections (or to simplify everything by always using IP).

**Q: What is multicast?**

**A:** Multicast is an IP-level mechanism for distributing data (or media streams) efficiently to many listeners. Rather than repeatedly sending the data to individual recipients, the sender can broadcast the information to a specific channel to which all the recipients are tuned.

**Q: Does Intel support multicast?**

**A:** Intel's current products do not support multicast; however, multicast support is being considered for future releases. Since Intel's video conferencing products are based on PC technology, multicast-based products such as Cisco's IPTV can run as a separate application on the same PC, enabling both applications to be available on the same system.

**Q: Can I have a multipoint call on the LAN without an MCU?**

**A:** The H.323 standard specifies this capability; however, no currently available commercial products offer this capability. An endpoint must support distributed multipoint operation and there must be what is known as a Multipoint Controller (MC) in the conference.

**Q: In a large company, how realistic is it to complete an H.323 call?**

**A:** The size of the company or network is irrelevant to call completion. The ability to control and manage the network for bandwidth and loading are the important factors. RSVP or other QoS protocols can help manage the segment-by-segment performance.

In general, the likelihood of completing an H.323-based call in a large company is very good. The ability to complete a call, however, can be limited by internal firewalls and routers that are not enabled for H.323-based video conferencing. How gatekeeper zones are established and how LAN administrators establish policies governing video conferencing activity also influence call completion.

**Q: Can Intel's video conferencing products make calls over the Internet?**

**A:** Intel's H.323-based products will operate on any IP network (either Internet or Extranet) which is supported by the underlying platform. However, Internet performance cannot be guaranteed due to unpredictable network loading.

**Q: Are Intel's video conferencing products compatible with other (non-Intel) H.323 systems?**

**A:** Intel's video conferencing products are standards-compatible and therefore, should interoperate with other products compatible with the same standards. Standards, however, are subject to interpretation, and the only way full compatibility can be guaranteed is through extensive testing. Intel tests interoperability in two ways — by participating in public testing events such as those sponsored by the IMTC, and through independent joint testing with other vendors' products.

**Q: Are Intel® TeamStation™ System and ProShare® Video System 500 products compatible with Intel® Create & Share™ Camera Pack?**

**A:** Intel® Video Phone Version 3.1 (shipping with Create & Share Camera Pack 2.0) will interoperate with Intel TeamStation™ systems versions 4.0 and 4.0a, Intel® Business Video Conferencing 4.02, and Intel ProShare® Video System 500 version 5.0.

**Q: Can Intel products be managed remotely?**

**A:** Intel® TeamStation™ Manager offers the ability to remotely control the TeamStation system, including remote diagnosis and troubleshooting, remote software upgrades, remote call initiation and the capability to monitor system "health" such as determining if a camera is disconnected.

## H.323 Building Blocks

H.323 defines four major components, or building blocks, and how they interact with each other, as well as how they interact with a circuit-switched network (for example, with H.320 conferencing systems). When purchasing these components, there are certain things you should look for and certain things you should avoid:

### **"Endpoints"**

What to look for in a video and data conferencing endpoint. Discover which audio codecs are important to your business.

### **"Gatekeepers"**

Features to look for in a gatekeeper. Discover additional gatekeeper functionalities which will impact your deployment.

### **"Gateways"**

Interfaces your gateway should support. Discover how using a gateway can decrease your organization's ISDN costs.

### **"Multipoint Control Units (MCUs)"**

What to look for in an MCU. Discover how T.120 support is critical when implementing an MCU on your network.

## H.323 Endpoints

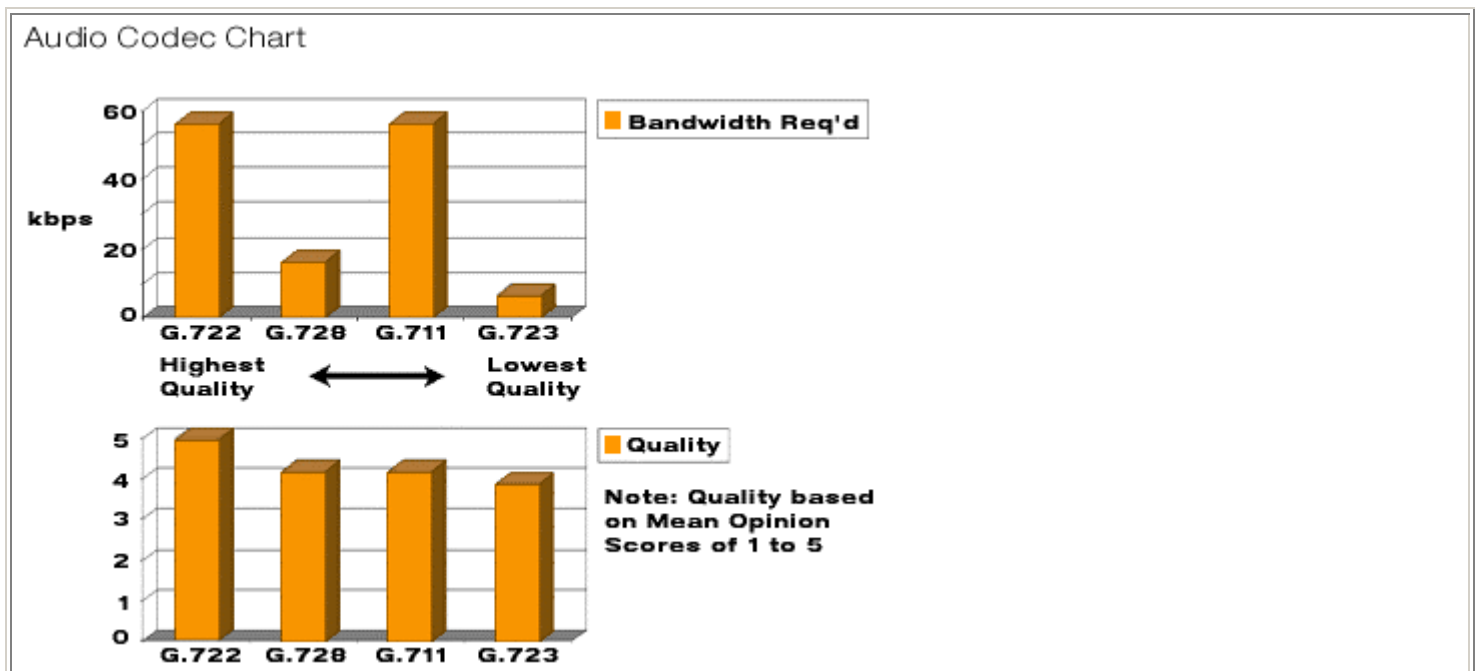
### What Should I Look for in an Endpoint?

Remember, an endpoint can be H.323-compliant if it runs over a packet network, such as IP, and supports only audio. Support for video and data sharing capabilities by an endpoint should be investigated if that is important to you.

If you require video, the type of video supported by the H.323 endpoint is important. H.261 video — used in ISDN video conferencing — is required by the standard for basic interoperability with both H.323 and H.320 endpoints. Two optional video codecs — H.263 and H.263+ (extensions to H.263) — are more efficient than H.261, delivering better video quality when there is less bandwidth. The efficiency becomes even more important if connectivity is desired over POTS or BRI lines. (See audio below.)

For data conferencing, the ITU has incorporated the T.120 data conferencing standard as an optional component of H.323. Microsoft NetMeeting\*, which supports T.120, has become the de-facto standard for data sharing. When evaluating an H.323 endpoint, check to see if the endpoint supports NetMeeting, and make sure it is cleanly integrated with the video conferencing application.

Additional audio codecs are available to enhance endpoint audio, depending on what sort of network bandwidth is available. These codecs are G.722, G.723, G.728, and G.729. If you are considering a group system, you will likely want support for the wideband kHz audio codec, G.722, providing higher fidelity sound. G.722 requires 48-56Kbps of bandwidth and, as a result, is more commonly found with group systems using 384Kbps ISDN. G.722 ensures that enough bandwidth remains to deliver high video quality.



G.723, defined as the low-bit-rate codec for H.323, is a very efficient codec, requiring only 5.3 to 6.3Kbps of bandwidth, and therefore is well suited for modem-based video conferencing where bandwidth is at a premium. There is a tradeoff, however, since G.723 delivers slightly less than toll (telephone) quality.

G.728 delivers telephone quality audio and requires only 16Kbps of bandwidth, making it a very practical codec to support. Its only drawback is that it takes a lot of computational power for compression/decompression and usually requires a DSP for processing, or a fast microprocessor if G.728 is host-based.

G.729 is similar to the G.723 audio codec, requiring little bandwidth, and is primarily used for voice-over IP applications, delivering almost-telephone quality. G.729 is more compatible with the public switched circuit networks and is therefore preferred for use in voice gateways. To date, almost no video conferencing endpoints support G.729.

Regarding endpoint manageability, LAN administrators should not have to manually configure each H.323 endpoint with the IP address of the gatekeeper managing its calls. The endpoint should support auto-discovery of a gatekeeper when the conferencing application is initiated.

If you will be deploying H.323 alongside your current H.320 network, choose an endpoint that supports both H.320 and H.323. A system that supports both standards permits video conferencing with older ISDN-based systems while easing the transition to IP-based video conferencing systems.

### **What to Watch for in an Endpoint**

Vendors may claim H.323 compliance but additionally support proprietary codecs, particularly audio, to achieve higher-quality conferencing. These codecs are useful only when you are connected to endpoints offering the same capability. Since they are non-standard, the endpoints usually have to be from the same vendor. They will not interoperate in this mode with other standards-based video conferencing products, reducing their value for most companies.

Beware of endpoints that take shortcuts in implementing H.323. These endpoints may not support some of the bandwidth-scalable features of H.323, such as H.263 video and G.723 audio, having implemented only the ISDN-based, H.261 video codec and the G.711 audio codec.

An endpoint claiming support for H.323 should also register with the H.323 gatekeeper on the network. This configuration provides some manageability for the LAN administrator. Microsoft NetMeeting\*, used standalone as a consumer-based video conferencing product, does not recognize an H.323 gatekeeper. Despite this, it is bundled with H.323 endpoints because of its T.120 compatibility, with the H.323 endpoints providing the necessary gatekeeper operation.

Finally, beware of systems that claim H.320 and H.323 support but do not seamlessly integrate the two transports in a single product. Intel products are designed to support both H.320 and H.323. You can place ISDN or LAN calls simply by referencing the appropriate phone number or IP address. Other vendors require that you buy two separate systems or run two different applications on the same hardware. As an example, if you are running an H.323 video conferencing application or system, you cannot answer an incoming ISDN call unless you have a truly integrated H.323 and H.320 product.

### **H.323 Endpoints You Can Deploy Today**

<b>Product</b>
Intel® ProShare® Video System 500
Intel® TeamStation™ System

## H.323 Gatekeeper

### What Should I Look for in a Gatekeeper?

An H.323 gatekeeper is a software application. It is sold standalone or bundled with H.323 hardware, such as an H.323-to-H.320 gateway, an H.323 multipoint control unit, or even a network router. A standalone gatekeeper will obviously cost less when you do not have to purchase hardware. Before you purchase a gatekeeper, make sure your H.323 endpoints will properly register with it and that it is compatible with the gateway or multipoint control unit you are considering.

Gatekeepers bundled with gateways or multipoint control units are typically customized for these products and can offer capabilities not otherwise available. Discuss these additional capabilities with your vendor(s) and determine if they are sufficient to warrant buying the bundled product.

H.323 equipment is configured as part of a "zone" and is subsequently managed by the gatekeeper for that zone. How zones are defined and how equipment is mapped to a zone varies by vendor. When considering a gatekeeper, investigate how easy it is to configure and update zones.

Some gatekeepers offer the ability to log all calls. Make sure your gatekeeper can differentiate between different service levels, such as 128Kbps BRI ISDN calls, 384Kbps ISDN, or voice calls. This information can be used to bill back usage to each department. Also, investigate whether or not a billing package is available that works with the gatekeeper.

### What to Watch for in a Gatekeeper

Be careful when mixing and matching gatekeepers or gateways from different vendors. Vendor A's gatekeeper may not work with Vendor B's gateway and, if they do, they may not support all available gateway features. Long term, this problem will be addressed by all vendors.

A gateway may support multiple services such as voice calls, 128Kbps, or 384Kbps ISDN calls. When more than one of these services are offered in the same gateway, the gatekeeper that manages that gateway may not be able to recognize all these unique services. Instead, it may route requests of only one type, such as 128Kbps ISDN calls, to the gateway while ignoring 384Kbps ISDN calls, even though the gateway is equipped to handle a 384Kbps ISDN call. This is generally not a problem when the gateway and gatekeeper are made by the same vendor. In the future, vendors will enable their gatekeepers to recognize unique gateway services, even those offered by other vendors.

## H.323 Gatekeepers You Can Deploy Today

Product
PictureTel LiveManager

## H.323 Gateways

### What Should I Look for in a Gateway?

The H.323 standard does not specify what types of interfaces a gateway should support. Therefore, you should make sure the gateway supports the type of interface(s) that you require for video conferencing. Gateway interfaces may be ISDN BRI (Basic Rate Interface), ISDN PRI (Primary Rate Interface), V.35, or others. And, since gateways can provide support for H.324, H.320, or analog telephones, make sure the gateway you choose supports the types of calls you want.

If you currently have ISDN deployed at your company, you should consider deploying a gateway as part of your H.323 deployment. Instead of running ISDN to every desktop or group system, you can incorporate a gateway with a limited number of shared ports. An analysis of your corporate ISDN usage should help you determine how many ISDN lines, on average, are used at any given time. You should then purchase a gateway that supports the number of ports (or concurrent sessions) that you will require at any one time. If you cannot find a gateway with enough ports, you will have to deploy more than one on your network. Analyze existing or planned usage of 384Kbps ISDN or voice calls over IP in a similar manner to purchase the correct number of gateways. Since gateways can support multiple types of calls at the same time, you should determine how many calls of each type — audio/video, audio/video/data, or voice-only calls — it can handle concurrently, with or without transcoding. This will also affect how many gateways you may have to deploy.

Explore how the gateway supports incoming H.320 calls. Some gateways are configured to work with the newest H.320 endpoints that support H.323 gateway calling, permitting direct dialing through the gateway to a network endpoint (commonly referred to as supporting TCS-4 in the gateway). Using TCS-4, a user will specify the H.323 endpoint's IP address, e-mail address, or some other alias, or Domain Name System (DNS) when calling the gateway. For older, legacy H.320 systems, the gateway must support some method for the H.320 endpoint to specify how to reach the H.323 endpoint on the network. A common approach is to support DTMF. The user calls the gateway, and the gateway then prompts the user to enter an extension for the user using the dial pad. Assuming an extension has been defined in each endpoint and shared with the gatekeeper, the gateway will then complete the connection.

### What to Watch for in a Gateway

Be careful when mixing and matching gatekeepers or gateways from different vendors. Vendor A's gatekeeper may not work with Vendor B's gateway and, if they do, they may not support all available gateway features. Long term, this problem will be addressed by all vendors.

A gateway may support multiple services such as voice calls, 128Kbps, or 384Kbps ISDN calls. When more than one of these services are offered in the same gateway, the gatekeeper that manages that gateway may not be able to recognize all these unique services. Instead, it may route requests of only one type, such as 128Kbps ISDN calls, to the gateway while ignoring 384Kbps ISDN calls, even though the gateway is equipped to handle a 384Kbps ISDN call. This is generally not a problem when the gateway and gatekeeper are made by the same vendor. In the future, vendors will enable their gatekeepers to recognize unique gateway services, even those offered by other vendors.

Also consider the codec(s) your gateway will need to support. A good gateway will support all the codecs referenced by the H.323 standard, avoiding the need to transcode or convert among the different codecs, possibly introducing some loss of quality or latency. If the gateway does not support all the common codecs — H.261, H.263, G.711, G.722, G.723, and G.728 — check and see if the gateway provides transcoding for at least the codecs you will commonly use.

Finally, if you will share data during your video conferences, check to see if the gateway fully supports T.120 data. T.120 data support through a gateway should work in both point-to-point mode and multipoint mode to an H.323 multipoint control unit on the network. Some gateways have problems handling T.120 data, so make sure you get a demonstration of this capability before purchasing your unit.

### H.323 Gateway You Can Deploy Today

Product
PictureTel LiveGateway

## H.323 Multipoint Control Unit (MCU)

### What Should I Look for in a Multipoint Control Unit (MCU)?

H.323 MCUs come in two forms: software and hardware. Both provide the same functionality, but they differ in price and performance. Software-based MCUs usually cost less per seat, and the number of simultaneous users they can support is constrained by the performance of the server. Hardware-based MCUs use a PC-like chassis containing cards with DSPs to implement the MCU functionality. Depending on the implementation, one card can support one or more users.

Therefore, the number of cards supported by a chassis limits the number of simultaneous users. You can cascade MCUs to support more users, but most H.323 MCUs do not yet support this functionality.

The first question to ask when considering an MCU is how many simultaneous calls of what type(s) it can handle — voice, data, audio/video, or audio/video/data.

When evaluating an MCU, you will also want to determine what audio and video codecs it supports (preferably the same ones your H.323 endpoint and gateway support).

An MCU should support T.120 data in addition to audio and video, i.e., T.120 data support should be present for all participants joining a conference call — even those participants joining via an H.323-to-H.320 gateway.

To monitor MCU usage, the MCU should provide some form of call-logging. MCU diagnostics should be available for troubleshooting. Large corporations with centralized help desks may want to remotely manage in-house MCUs. Therefore, desirable features are SNMP support and the ability to remotely configure MCUs by modem or LAN. The ability to perform these administrative functions via browser-based interfaces is even better.

### What to Watch for in an MCU

If your MCU doesn't support some audio codecs, the MCU will have to perform transcoding, which may introduce some latency or loss of quality. More importantly, transcoding may require additional MCU resources — either more server MIPS or more DSPs — which may reduce the number of simultaneous users or conferences you can support.

One function of an MCU is to mix audio from all the endpoints. It is important to know which audio codecs your MCU can mix in full-duplex mode; otherwise, audio performance for some attendees will suffer.

MCUs generally come bundled with their own H.323 gatekeeper. Under certain conditions, you may want to be able to disable the bundled gatekeeper and substitute another on the network. Check with your MCU vendor to see if the bundled gatekeeper can be disabled and/or if you lose any MCU functionality as a result.

### H.323 MCUs You Can Deploy Today

Product
PictureTel 330

## **H.323 Benefits**

The H.323 standard is very comprehensive yet flexible. It can be used in developing audio-only solutions or full-fledged video/audio/data conferencing networks. There are many benefits in implementing an H.323 conferencing solution:

- Delivers high-quality, scalable multimedia-based conferencing.
- Permits interoperability between H.320- and H.323-based equipment from different vendors.
- Leverages existing investment in corporate network infrastructure.
- Can be used for long distance voice calls to reduce telephony costs.
- Allows more cost-effective use of ISDN by using H.320 gateways and fewer ISDN lines.
- On a corporate intranet, can provide more reliable connections and reduce support problems.
- Offers more sophisticated manageability of conferencing on the network.
- Hardware- and operating system-independent.

## H.323 Deployment Scenarios

Our H.323 deployment scenarios provide configuration tips, help you understand which H.323 components are typically used and how many components are required. A general understanding of your video conferencing requirements, a knowledge of your existing network infrastructure (including LAN/WAN configurations and performance), and familiarity with H.323 video conferencing components will allow you to gain more from these scenarios. For detailed background on the H.323 basics, refer to the [H.323 - What Is It?](#) section of our site.

H.323 network multimedia solutions are typically deployed in one of three ways:

★ **"Interdepartmental"**

Find out what you need to know to use H.323 solutions between departments.

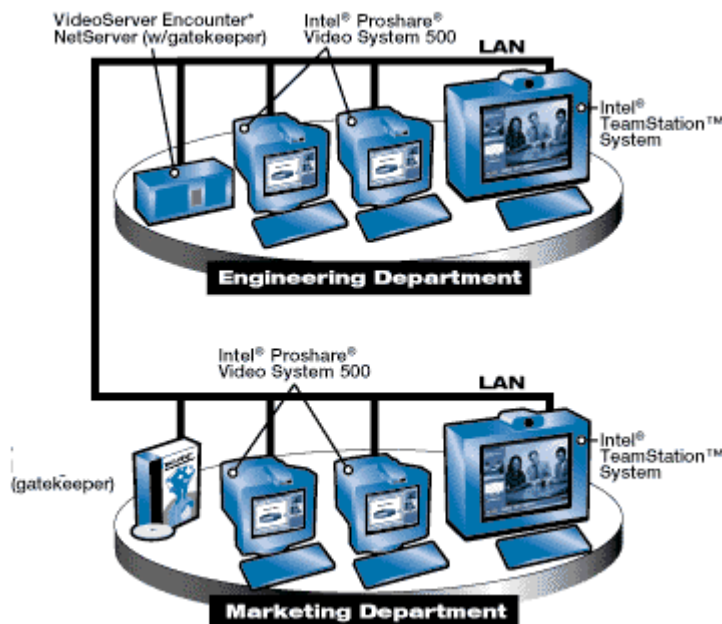
★ **"Site to Site"**

Find out what you need to know to use H.323 solutions between sites.

★ **"Company to company"**

Find out what you need to know to use H.323 solutions between companies.

## H.323 Interdepartmental



### Department-to-Department video conferencing deployment

In deploying H.323-based video conferencing department to department, first determine:

1. How many H.323 endpoints and what types (desktop or group system) need to be deployed.
2. If gatekeepers are needed and if so, how many.
3. If an H.323 Multipoint Control Unit is needed (see [Site-to-Site video conferencing deployment](#)).

The number and types of endpoints needed is a corporate decision based on need, budget, availability of conference rooms for group system deployment, and suitability of PC hardware to accommodate desktop video conferencing. How these endpoints are used influences what additional H.323 components — gatekeepers, gateways, and multipoint control units (MCUs) — will be deployed. The number of endpoints deployed for video conferencing will affect the amount of network bandwidth required, which will in turn influence the decision as to whether or not to install a gatekeeper. If more than two users need to video conference at the same time, you'll need an H.323 MCU.

### Gatekeeper Deployment

An H.323 gatekeeper is software that manages the H.323 network. It performs the following services:

- **Address translation.** Supplies the IP address of the H.323 endpoint using a provided name (alias) or phone number (extension).
- **Zone management.** Defines what endpoints and services it controls and interacts with other gatekeeper zones to connect calls.
- **Admission.** Manages LAN and gateway usage by controlling bandwidth used by an H.323 session in a zone and types of gateway calls and other services (such as multipoint) that a specific user can access.
- **Call routing.** Provides optimal routing of calls to zone services.
- **Other services** depending on the particular gatekeeper.

**Is a gatekeeper needed?** This depends on whether or not 1) your LAN administrator needs to manage the amount of network bandwidth used for video conferencing, 2) you want to use an endpoint's alias (e.g., e-mail address) to make a call, or 3) you want to use H.323 gateways or MCUs.

If the expected usage is a small percentage of available network bandwidth, a gatekeeper is unnecessary. A gatekeeper is not mandatory for H.323 endpoints to work. However, once a gatekeeper is installed on a network, the gatekeeper subsequently controls all H.323 endpoints.

A gatekeeper sets limits regarding how much bandwidth can be used for video conferencing. When an endpoint wishes to make a conference call, it registers with the gatekeeper and requests permission to make the call. If there is sufficient bandwidth available for BOTH endpoints to communicate, permission is granted. The amount of bandwidth required for endpoints to make calls varies by vendor. Intel's endpoints generally prefer somewhere between 200Kbps and 400Kbps each way, although they will still operate if less bandwidth is available.

When you set bandwidth limits, remember that non-switched Ethernet networks operate at an average 30 percent efficiency. You should not allocate more than 20 percent of your total bandwidth for conferencing services. A gatekeeper must be present if an endpoint wants to call another endpoint by a name (alias) or phone number (extension), rather than an IP address. The gatekeeper provides the address translation services needed to do this. The gatekeeper also provides similar services to permit endpoints to connect to MCUs (using conference IDs) and gateways. For outbound H.323 calls, the gatekeeper assists endpoint connections to gateways using prefixes. For inbound calls, the gatekeeper supplies the IP address of the H.323 endpoint being called through a gateway, using an extension supplied by the calling endpoint.

Once you decide you need a gatekeeper, you can determine how many gatekeepers you need.

### Gatekeeper Zone Setup

When deploying gatekeepers, the LAN administrator must establish a zone for each gatekeeper. A zone consists of a group of H.323 endpoints and, if used, gateways and MCUs. The gatekeeper must be configured to know which components are under its control and which ones are not. A database of each component's IP address, alias string or domain name is maintained by the gatekeeper.

The number of zones defined, and the number of gatekeepers required in an organization, is a function of how the LAN administrator prefers to set them up. Typically, zones are established based on:

1. Natural communities of interest or functional workgroups such as an engineering or quality assurance lab
2. One or more departments, or even an entire site
3. Physical topology based on the IP network infrastructure
4. How bandwidth on segments is to be managed
5. Other criteria, such as WAN communication limitations

The number of H.323 endpoints managed by the gatekeeper is typically not a concern, since most gatekeepers can effectively handle hundreds of users.

## **Gatekeeper Locations**

Since gatekeepers are software-based, they can reside in a number of locations such as an application running on a network server, a gateway, an MCU, or a Cisco-based network router. The choice depends on how your H.323 components are deployed. If you want only to manage a collection of H.323 endpoints on a network, a standalone gatekeeper running on an existing network server is the ideal choice. If you need an MCU for multipoint conferencing or a gateway for external ISDN access, it's easier to use the gatekeeper that comes bundled with these products. A bundled gatekeeper is often customized for use with the gateway or MCU it comes with and can offer functionality not available with other gatekeepers.

If you're deploying video conferencing on a Cisco network, you may already have a router that can act as a gatekeeper. Cisco's 2600, 3600 and 5300 Series of routers can be converted for use as gatekeepers. Cisco's IOS-based MCM (Multimedia Conference Manager) software can be installed on these routers and used as a gatekeeper. Once MCM is installed on a router, it no longer functions as a router but as a gatekeeper.

A standalone gatekeeper offers additional cost advantages. If a gatekeeper comes only bundled with hardware, you have to buy hardware you don't need just to get the gatekeeper.

## **Gatekeeper Setup**

When setting up the gatekeeper, the LAN administrator must define how much bandwidth is dedicated to conferencing. Some gatekeepers differentiate between internal conferencing and external conferencing. Internal conferencing refers to the amount of shared LAN bandwidth that should be allocated for endpoints calling each other within the same zone. External conferencing applies to conference calls between gatekeeper zones. Bandwidth limits can be established on a per-call basis or for all video conferencing combined.

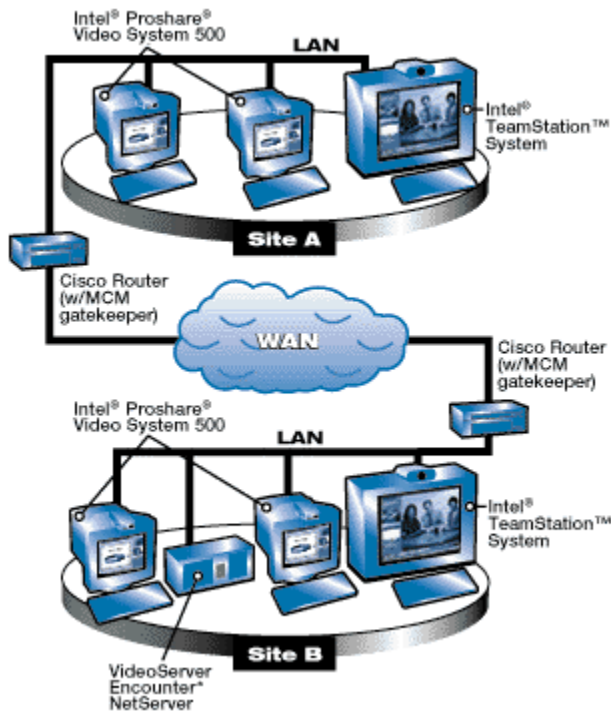
Gatekeepers also provide address translation services. Some H.323 endpoints, such as Intel's business video conferencing products, when launched, automatically attempt to discover a gatekeeper. The endpoint can be configured in advance to look for a specific gatekeeper by its IP address or Domain Name Server (DNS) name, or use any gatekeeper that responds to its discovery request. Once an endpoint links up with a gatekeeper, it registers its IP address, alias string(s), or extension(s) to the gatekeeper. The gatekeeper then uses this information later to translate an address requested by another calling endpoint into the relevant IP address.

Gatekeepers also may have to be configured to allow only endpoints in its zone to register with it, or to allow any endpoint, regardless of its location, to register with it.

How endpoints are specified to be in a gatekeeper's zone varies by vendor implementation. Endpoints can be specified by their IP addresses used, including groups of endpoints based on their sub-net identifiers. A gatekeeper also may use a gatekeeper ID string specified in the endpoint. When an endpoint attempts to discover and register itself with a gatekeeper, the gatekeeper will compare its ID string with that of the endpoint to determine whether or not it is part of its zone.

An endpoint also may be configured to automatically look for any gatekeeper on the network, registering with the first gatekeeper that responds. Optionally, some endpoints can be configured to register with a specific gatekeeper, referencing the gatekeeper's IP address.

## H.323 Site-to-Site Deployment



Video conferencing between two corporate sites or departments is performed over the company's wide area network. Point-to-point or multipoint calls can be made anywhere as long as users have access to the corporate network and are not blocked by departmental firewalls, incompatible router configurations or other secure sub-networks. Intel's video conferencing products support proxies enabling them to work with firewalls supporting H.323 proxies.

### MCU Deployment

Multipoint Control Units (MCUs) can be implemented in hardware or software. Their function is to mix the audio from all the endpoints and switch the video and data as necessary. When a multipoint conference call is established, the MCU will register the conference name with the gatekeeper. End users will refer to the conference name when they wish to join the multipoint conference call. Users may call into a multipoint conference call from any gatekeeper zone representing one or more different departments or sites.

For video conferencing between multiple sites, it's probably more convenient to provide a commonly accessible MCU at one site, permitting multipoint calls to be made between sites. The MCU can be located anywhere on the network, and more MCUs can be added as demand requires.

The number of MCUs required is a function of how many and how frequently multipoint calls are conducted. MCUs generally support 4 to 48 ports, each one used by an endpoint joining a conference call. The type of call coming in often determines the number of ports available per MCU during a conference call. Some MCUs, for example, may support a fixed number of simultaneous audio, video, and data calls, with the remainder of ports supporting standard telephone or POTS (Plain Old Telephone System) calls. If transcoding of audio or video coming in is required for some endpoints, additional ports may be required. Check with your MCU vendor regarding port availability and the factors that reduce the total number available at any one time.

Cascading MCUs can overcome limitations of a single MCU by combining multiple MCUs and their related endpoints into a single conference call. However, cascaded MCUs may add latency, which can degrade conference performance.

How MCUs are administered varies by vendor. A common approach is to use a browser-based interface to configure the MCU and schedule and manage multipoint calls. Depending on the type of endpoints planning to join a conference call, the MCU may have to be configured to provide optimum performance among all users. The MCU will, however, work with all the endpoints to negotiate to a common set of audio and video codecs.

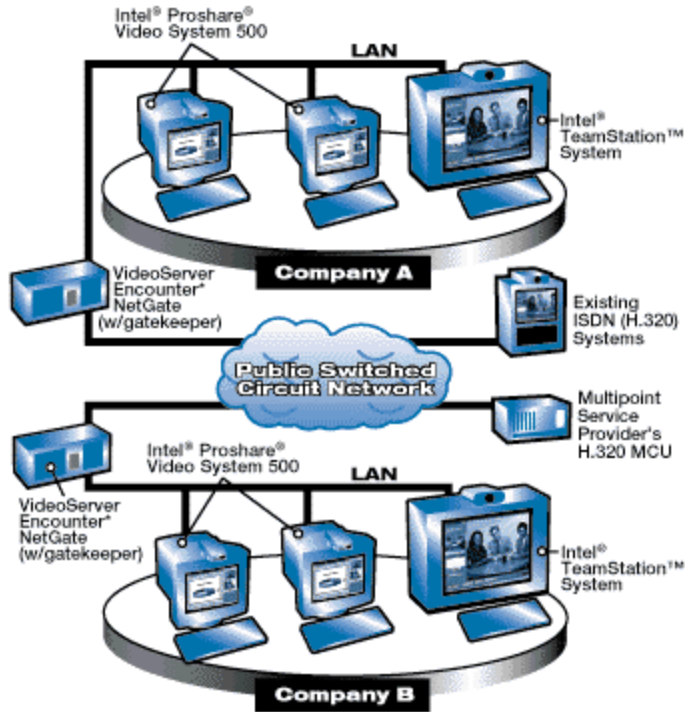
Be aware that maintaining, deploying, and scheduling MCUs requires extra time and staff.

**Network Connections**

Another factor to consider with site-to-site video conferencing is how the sites are networked together. Analyze the bandwidth among sites to determine whether there is enough to handle day-to-day data transfers in addition to the expected amount of video conferencing traffic. If not, you may need to increase the bandwidth of your WAN links or use higher-speed routers and switches to minimize jitter and packet latency . Some routers can prioritize H.323 traffic to deliver maximum audio and video performance.

If you use Cisco routers for WAN communications, you can configure them to deliver Quality of Service among locations. Additional Cisco routers can be installed with Cisco's Multimedia Conference Manager software and used as a gatekeeper/proxy. The MCM software resides in the memory of each router and is compatible with Cisco's IOS operating system.

## H.323 Company to Company



### Company-to-Company Video Conferencing Deployment

For conferencing between companies, you use an H.323-to-H.320 gateway. This gateway provides a bridge between packet-based IP networks and ISDN using the public-switched circuit network. If necessary, the gateway will provide transcoding or conversion among various audio and video codecs used by the various H.323 endpoints.

Gateways permit an H.323 endpoint to make an ISDN call without having ISDN access from the desktop. Multiple ISDN lines can be configured in the gateway and simultaneously shared by a number of users. This eliminates the cost of installing ISDN to every desktop and the subsequent support cost of maintaining and operating those lines. Users must share a limited number of ISDN ports provided in the gateway. Also, a gateway may interject some latency — check with your gateway vendor.

To use the gateway, it is important to evaluate the amount of ISDN-based video conferencing expected among remote sites or companies. This will help you determine how many gateways are necessary to deliver the same quality of video conferencing service that users expect with ISDN direct to their desktop.

#### How many gateways do I need?

The number of gateways you'll need is a function of the number of endpoints using ISDN to communicate to external users and how many simultaneous calls are required. A gateway supporting ISDN can be used instead of supporting ISDN to every desktop. Using a gateway, all users must share a fixed number of ISDN lines. Depending upon the time and amount of usage, some users may receive busy signals.

Gateways vary in terms of available ISDN ports. Some gateways support as few as one ISDN port, others many more. Many gateways typically support four BRI (Basic Rate Interface) ISDN connections or one PRI (Primary Rate Interface) ISDN connection.

**Note:** Some gateways use more ports to transcode audio or video codecs. For example, if a gateway normally supports 8 ISDN ports and the audio/video stream from four users needs to be transcoded, then all 8 ports will be used for the conference call. The more flexible the H.323 endpoints are supporting a larger variety of codecs (which can be negotiated at conference call startup), the less transcoding that will have to take place.

Unless you have collected hard data regarding frequency of ISDN usage, you will need to make a guess about how many gateways to deploy, basing your estimate on the number of available ISDN ports per gateway. Since all ISDN calls can

be directed through a gateway, and most gateways support call logging, you can monitor ISDN usage to more accurately determine the number of gateways required to provide reasonable ISDN call coverage with few busy signals.

### **Gateway Setup**

Like all endpoints, a gateway must be registered with a gatekeeper so the gatekeeper is aware of the gateway's existence to route ISDN calls (or other types of calls, depending on the gateway) to the gateway for connection to the public-switched telephone network.

**Note:** If you use a gatekeeper built into a gateway, or an MCU, they will use the same IP address.

A gateway relies on the gatekeeper to route an inbound call to the appropriate endpoint on the LAN, based on the IP address, extension or alias provided by the external caller to the gateway.

For outbound calls, the gateway must be configured to assign prefixes to the various types of services supported by the gateway. For example, an ISDN port might be assigned the prefix 80, while a POTS call going through the gateway might be assigned the prefix 70. To make an ISDN call through the gateway, an endpoint would precede the ISDN number it normally calls with the prefix 80. A gatekeeper, knowing this service is provided by a gateway and referenced by the prefix 80, would then route the ISDN call to the gateway. LAN administrators who set up the gateway need to communicate these prefix assignments to users.

Supported-gateway communication interfaces vary by vendor offering. The types of interfaces supported, such as ISDN BRI, ISDN PRI, V.35, Ethernet, etc., have to be configured appropriately. Some gateways also offer special services like line hunting, group hunting and call forwarding. Each of these services has to be set up. Contact your gateway vendor for more information regarding product installation and configuration.

## H.323 Solutions

When deploying an end-to-end H.323 solution, it is important to choose components from vendors that have proven to be the "best of breed" in a particular category. Due to the complexities involved in building a comprehensive H.323 system solution, it is difficult for a single company to adequately provide a top-to-bottom solution without making sacrifices in quality or functionality.

Supplying a top-to-bottom solution also requires expertise in a broad range of categories: areas - standards, video conferencing, PC and network architectures, circuit-switched gateway technology, and multipoint control unit (MCU) knowledge.

Since you are unlikely to find a company with this breadth of expertise, we recommend you choose vendors that specialize in particular H.323 components and guarantee interoperability with all the other components you are evaluating. Intel Corporation, for example, is an industry leader in H.323-compliant video conferencing **endpoints**. Since many functions of H.323 are optional, you should spend some time deciding which components are important to you and your business. When building your solution, you can use the descriptions and checklist below to help make these decisions.

### "H.323 Endpoint Checklist"

Print this checklist and use it to compare potential H.323 endpoints. Discover how well the Intel® Business Video Conferencing product family fits your needs.

### "ISDN-Compatible Codecs"

Learn more about ISDN codecs and why they are important. Discover how these codecs help create solutions that interoperate with existing ISDN-only deployments.

### "H.323-Compatible Codecs"

Learn more about H.323 codecs and why they are important. Discover how these codecs take advantage of available LAN bandwidth.

### "Call Support"

Learn why both H.323 and ISDN call support are important. Discover how voice calls over Internet Protocol (IP) can decrease long distance costs for your business.

### "Data-Sharing Support"

Learn why T.120 data-sharing support is important. Discover how web-based document access can save time for conferencing users on your network.

### "Remote Management"

Learn why remote management of endpoints is important. Discover how management can reduce the overall support costs of your solution.

### "Miscellaneous"

Learn about other endpoint features that can enhance the overall effectiveness of your solution. Discover how H.323 Revision 2 compliance can affect your deployment.

### "Selecting an H.323 Gatekeeper"

Learn about additional H.323 gatekeeper features which can improve your deployment.

## H.323 Endpoint Checklist

H.323 Endpoint Functionality	Intel® TeamStation™ System	Intel® ProShare® Video System 500	Vendor A	Vendor B
<b><u>(H.320) ISDN-Compatible Codecs</u></b>				
H.261 Video	Yes	Yes		
G.711 Audio	Yes	Yes		
G.722 Wideband Audio	Yes	No		
G.728 Audio	Yes	Yes		
H.261 Post Filtering	Yes	No		
ISDN 384Kbps Support	Planned	No		
<b><u>(H.323) LAN-Compatible Codecs</u></b>				
H.263 Video	Yes	Yes		
G.723 Audio	Yes	Yes		
H.263 Post Filtering	Yes	No		
Scalable Video (28.8 to 400Kbps)	Yes	Yes		
<b><u>Call Support</u></b>				
ISDN and H.323 Call Support	Yes	Yes		
Voice Calls over IP Networking	Planned	Planned		
<b><u>Data Sharing Support</u></b>				
Microsoft NetMeeting*/T.120 Data Support	Yes	Yes		
Web-Based Document Access	Yes	No		
<b><u>Remote Management</u></b>				
Remote Call Initiation/Monitoring	Yes	No		
Remote Software Upgrades	Yes	No		
Remote Diagnostics/Troubleshooting	Yes	No		
<b><u>Miscellaneous</u></b>				
PC Functionality "Off the Call"	Yes	Yes		
H.323 Revision 2 Compliance	No	No		
<b><u>H.323 Gatekeeper Support</u></b>				
Multicast Discovery	Yes	Yes		
Unicast Discovery	Planned	Planned		
Registration/Authentication	Yes	Yes		

## ISDN Compatible Codecs

### H.261

This is an ITU-T recommendation for transmitting video in all H.320-based video conferencing systems operating over ISDN. Video support in the H.323 standard is optional, but if a video conferencing system supports video, it must support H.261 QCIF.

H.261 defines two picture formats: Common Interchange Format (CIF) and Quarter CIF (QCIF). CIF format represents a displayable video window 352 x 288 pixels in size. QCIF format represents a

displayable video window 176 x 144 pixels in size. A CIF window displays four times the amount of information that a QCIF window does, requiring a more powerful video conferencing system to display CIF video versus QCIF video at the same frame rate. A video conferencing system must support both QCIF and CIF video formats to be considered adequate for business users.

**Why H.261 is important:** H.261 is required for an H.323 video conferencing system to communicate with H.320-based video conferencing systems.

## G.711

This is an ITU-T recommendation for transmitting audio among H.320-based video conferencing systems. The 3.1kHz audio signal is encoded using Pulse Code Modulation (PCM) and either Mu-law (US and Japan) or A-law (Europe).

G.711 needs 64Kbps of bandwidth for transmission, which is fine for transmission over ISDN or LAN but less suitable over a standard telephone line using a modem at 28.8 to 56Kbps rates. A more bandwidth-efficient audio codec like G.728, requiring only 16Kbps of bandwidth, or G.723, requiring 5.3 or 6.3Kbps, is more appropriate when available bandwidth is limited.

**Why G.711 is important:** The H.320 and H.323 standards dictate that G.711 audio must be supported by all compliant video conferencing systems.

## G.722

This is an ITU-T recommendation for transmitting wideband, 7 kHz, audio between H.320-based video conferencing systems. G.722 delivers better video conferencing audio quality, as FM radio audio is superior to AM radio audio.

G.722 needs 48-64Kbps of bandwidth for transmission and, like G.711, is suitable for transmission over ISDN or LAN. Because it delivers more natural sound, G.722 is generally supported by group conferencing systems. These room systems are typically connected over ISDN at 384Kbps, where G.722's appetite for more bandwidth is more easily accommodated.

**Why G.722 is important:** G.722 delivers a richer, more natural sound, generally demanded by groups of users trying to communicate using room-based video conferencing systems.

## G.728

This is an ITU-T recommendation for transmitting audio between H.320-based video conferencing systems. The 3.4 kHz analog audio signal, after encoding and compression, uses 16Kbps of bandwidth.

G.728 audio takes more computational power to process, unlike G.711, which requires much less; but G.728 delivers toll-quality audio over lower bandwidth.

**Why G.728 is important:** G.728 offers telephone audio quality, without requiring a lot of bandwidth, and it can be particularly suited for H.320 or H.323-based video conferencing.

## Host-Based H.261 Post-Filtering

Once H.261 video is received from a remote endpoint, you can perform additional post-processing to improve image quality.

**Why host-based H.261 post-filtering is important:** The post-filtering process occurs after the video is received. Hence the endpoint will see better video quality than when using the standards-based video codecs. However, since H.261 is still in use, post-filtering remains interoperable with all systems transmitting H.261 video. Because the post-filtering process is host-based (i.e., performed on the CPU), software-only upgrades can be used to modify the post-filtering algorithms used, taking advantage of state-of-the-art techniques to improve video quality.

## ISDN 384Kbps Support

ISDN Basic Rate Interface (BRI) operates at a maximum bandwidth of 128Kbps. By combining three BRI ISDN lines together, you can achieve a combined bandwidth of 384Kbps, enabling higher H.261 video quality — up to 30 frames per second — and higher quality audio, such as wideband G.722 audio.

You maximize performance at the expense of cost. The basic ISDN line charges are tripled, not including the cost of additional hardware in the endpoint.

## H.323 Codecs

### H.263

This is an optional video codec for H.323-based video conferencing systems offering video capabilities. The H.323 standard states that if a video conferencing system supports video, it must support H.261 QCIF, not H.263.

Like H.261, H.263 defines two picture formats: CIF and QCIF.

**Why H.263 is important:** H.263 is designed to be scalable, permitting video display under limited bandwidth conditions where H.261 would be unable to do so. It will also produce better video when more bandwidth is available. Good H.263 implementations generally can offer better video quality than H.261 under the same bandwidth conditions.

### G.723

This is an ITU-T recommendation for transmitting audio between H.323-based video conferencing systems.

G.723 is a bandwidth-efficient audio codec requiring either 5.3 or 6.3Kbps, depending upon vendor implementation, and is well suited for video conferencing over connections with limited bandwidth.

**Why G.723 is important:**

Although the H.320 and H.323 standards dictate that G.711 audio must be supported by all compliant video conferencing systems, G.723 audio requires less bandwidth, making more bandwidth available for video or data transmission, while delivering almost telephone-quality audio.

### Host-Based H.263 Post-Filtering

Once H.263 video is received from a remote endpoint, additional post-processing can be performed to improve image quality.

**Why host-based H.263 post-filtering is important:** The post-filtering process occurs after the video is received. Hence the endpoint will see better video quality than when using the standards-based video codecs. However, since H.263 is still in use, post-filtering remains interoperable with all systems transmitting H.263 video. Because the post-filtering process is host-based, software-only upgrades can be used to modify the post-filtering algorithms used, taking advantage of state-of-the-art techniques to improve video quality.

### Scalable Video (28.8 to 400Kbps)

Scalable video refers to an endpoint's ability to deliver reasonable video quality across a wide range of bandwidths. Video quality over a 28.8Kbps modem is not expected to be stellar; however, scalable video can be displayed at a reduced frame rate to improve performance. Scalable video also allows much higher video quality when one-way bandwidths of 400Kbps or more are available, permitting frame rates up to 30 frames per second.

**Why scalable video is important:** On Local Area Networks or the Internet with no guaranteed quality of service, available bandwidth can fluctuate based on network activity. If available bandwidth should fall below a level normally expected by an endpoint, an endpoint without truly scalable video may stop

displaying video, may appear blocky or less sharp, or may lose key frames and display video "artifacts" from previous frames. Support for scalable video can reduce an endpoint's vulnerability to sudden drops in bandwidth, permitting the system to "ride out the storm" more gracefully. Ultimately, scalable video gives users a higher quality conferencing experience.

## **H.323 and ISDN Call Support**

ISDN and H.323 call support refers to the ability of an endpoint to support both ISDN calls to the public-switched circuit network and H.323 calls over IP-based networks in the same product. A user should not have to run two different video conferencing applications on the same product to make both ISDN and H.323 calls. Ideally, ISDN and H.323 call support means needing only an address book to select an individual to call and letting the system do the rest. In the worst case, an ISDN number or an IP address must be entered to reference the remote endpoint.

### **Why ISDN and H.323 call support is important:**

You should have to buy only one system for video conferencing with both your installed base of ISDN video conferencing systems and for conferencing with H.323 and IP network-based video conferencing systems being deployed in the near future.

## **Voice Calls over IP Networks**

Voice calls over IP networks refers to the ability to make a voice call using an H.323-based video conferencing system over an IP network, such as a LAN/WAN or the Internet.

### **Why voice calls over IP networks are important:**

The ability to place voice calls over an IP network allows you to complement your telephone handset with the video conferencing system on your desk. Voice-over IP networks enable you to make long distance calls at a much lower cost. When using your IP network for voice communication, you are also more fully utilizing your existing infrastructure. Eventually, you can simplify management of your communication networks. Instead of supporting two parallel networks, you can eliminate the circuit-switched network and perform all communication over IP-based networks.

## **Netmeeting\* / T.120 Data Support**

T.120 is a data-sharing specification that enables users to share documents during any H.32x video conference. T.120 is actually an umbrella specification encompassing a number of other recommendations (covering file transfer, whiteboard usage and application sharing). Microsoft NetMeeting\* is available free for any Windows\* 9x or NT\* operating system. Due to its widespread availability, NetMeeting has become the de facto standard for T.120 data sharing in video conferencing systems.

### **Why NetMeeting / T.120 data support is important:**

T.120 data support enables two or more H.323 endpoints to share and use documents during a conference call, complementing audio and video interactions that may be occurring at the same time. Many users consider data sharing even more important than video. When configuring H.323 equipment, it is important that T.120 be supported from endpoint to endpoint, whether or not an H.32x gateway or multipoint control unit is involved.

## **Web-based Document Access**

A common problem facing group video conferencing users is how to display information — charts, graphs, or scribbled notes — to the remote endpoint. Document cameras have been used, but they are of limited value when dynamic presentations — like those done in Microsoft PowerPoint\* — are involved.

Users often hook up laptops to monitors in order to make presentations in conference rooms, or they use networked PCs to run PowerPoint presentations.

Web-based document access enables an endpoint to act as a document server on a network. Documents are uploaded from a user's local hard disk to the Web server using a browser interface. Then they are accessed in the conference room by supplying a user ID and password.

#### **Why Web-based document access is important:**

With Web-based document access, a user always has access to documents from a conference room. Physical laptop connections are unnecessary, and the frustration of not having access to a server where your private files are stored is eliminated.

## **H.323 Remote Management**

### **Call Initiation/Monitoring**

Call initiation/monitoring refers to the ability to remotely initiate a conference call or to remotely monitor the operating status of video conferencing equipment.

**Why call initiation/monitoring is important:** With call initiation/monitoring, a corporate help desk can remotely assist users in placing calls. Help-desk technicians can also monitor the active status of all equipment, reacting quickly to equipment problems as they occur.

### **Software Upgrades**

Software upgrades refers to the ability to remotely install or update software in video conferencing equipment.

**Why software upgrades are important:** Software-upgrade capability permits some software to be installed without sending a person to the system's location. At the very least, software-upgrade activity can be centrally administered and controlled by IT management.

### **Diagnostics/Troubleshooting**

When equipment fails or a call will not connect, the first priority is to determine the source of the problem. Diagnostics/troubleshooting software enables the local user — in consultation with remote support staff — to minimize the time needed to get the equipment back up and running. The ability to remotely troubleshoot the equipment by either modem or LAN connection permits the support staff to diagnose the problem without local assistance.

**Why diagnostics/troubleshooting is important:** The ability to execute built-in diagnostics and remotely troubleshoot the equipment failure permits more timely response by support organizations that typically are not locally accessible.

## **H.323 Miscellaneous**

### **PC Functionality "Off the Call"**

Typically when group or room video conferencing equipment is not being used for a video conferencing call, it sits idle. If the video conferencing equipment is based on PC architecture, this equipment (if properly configured) could be used as a PC when "off the call." Groups can use the system to make presentations, access files on the network, or perform research on the Internet.

**Why PC functionality "off the call" is important:** PC functionality enables a company to get a better return on its group video conferencing equipment investment, enabling the system to be used throughout the working day. "Off the call" functionality also permits attendees to always have access to their information, since a network connection would typically be present. During a group meeting, work can happen on the system in real time, instead of being postponed until everyone can return to his or her desktop computer.

## H.323 Revision 2 Compliance

Revision 2 of the H.323 standard was approved in January 1998. Revision 2 clarifies some of the original standard's specifications that were subject to interpretation by participating companies. It also adds some enhancements that improve the H.323 video conferencing experience (such as the H.263+ video codec, which improves video quality). Vendors can claim Revision 2 compliance by simply recompiling their code in a specified manner without adding any new functionality. As a result, vendor claims to be "Revision 2 compliant" may not hold much merit and should be properly evaluated. In particular, explore what specific enhancements from the H.323 Revision 2 standard have been implemented.

**Why H.323 Revision 2 compliance is important:** Revision 2 compliance is important only if a video conferencing product supports some of the enhancements specified as part of Revision 2, specifically:

- Security — the authentication and privacy of endpoints
- H.323 on native ATM (annex C)
- Faster voice call connections
- MCU cascading to support more users on a conference call
- Support for alternate gatekeepers

When a vendor claims compliance with H.323 Revision 2, find out specifically what additional features they support and determine if the supported features have any relevance to your deployment of H.323.

## Selecting an H.323 Gatekeeper

### Multicast/Unicast Discovery

If a gatekeeper is present on a network, all active H.323 video conferencing systems should register with that gatekeeper. Specifically, endpoints will discover and register with a gatekeeper by referencing its specific IP address or by using a Multicast- or Unicast-based gatekeeper request to contact the gatekeeper. Ideally, the gatekeeper should be flexible enough to respond to any of these methods.

**Why Multicast/Unicast discovery is important:** If a gatekeeper can respond to either a Multicast or a Unicast discovery method, LAN administrators do not have to manually configure each video conferencing system to reference the gatekeeper specifically by IP address. If that gatekeeper's IP address should change, the endpoints would not be able to register with it. Therefore, all calls would receive permissions by default, possibly overloading network bandwidth. Multicast discovery of gatekeepers is the most practical method for endpoints to contact gatekeepers; however, some LAN administrators do not like to enable Multicast in their routers, so a gatekeeper behind one of these routers would not be located. To get around Multicast-disabled routers, a Unicast-based discovery message can be sent to the gatekeeper (if it supports Unicast) by specifying its IP address.

### Call Logging

If a gatekeeper keeps a log of all call activity, this log can be used to bill back department usage. At a minimum, the gatekeeper needs to provide some method to export this information to a file where it can be loaded into a spreadsheet for analysis. The amount of information that is recorded is also important — call start date and time, call termination date and time, bandwidth utilized (128Kbps, 384Kbps, etc.), endpoint determination, and call type (audio, video, data). If call successes, failures, or abnormal terminations are also recorded, this information can be supplied to the gateway vendor for service improvement.

**Why call logging is important:** Call logging becomes particularly important for calls through a gateway. A 384Kbps ISDN call is more expensive than a 128Kbps ISDN call, and you want the additional expense charged back to the actual department or individual who used the service.

### **Ease of Zone Setup**

H.323 equipment is organized into zones, which are managed by unique H.323 gatekeepers. How each gatekeeper defines each zone can differ among vendors. Endpoints, gateways, MCUs, etc. can be identified by their IP address (topologically scoped). Aliases and domain names can also be used to uniquely identify H.323 equipment (logically scoped). The larger the zone, the more equipment the gatekeeper has to be aware of. The ease in which H.323 equipment can be partitioned into zones will make a big difference when evaluating gatekeepers.

**Why ease of zone setup is important:** Without an easy way to specify a group of endpoints, the task of individually specifying each endpoint's IP address would be very time-consuming and frustrating.

## Intel® ProShare® Video System 500

### Using H.323 ProShare® Conferencing Products Across Firewalls

One of the problems encountered when trying to use ProShare® Video System 500 or Intel® Business video conferencing over the Internet is firewalls. Firewalls are designed to keep the private network secure from the general public.

#### Basic Understanding of Firewalls

When you connect your private network to the public network (for example, the Internet), you need some way of preventing access from the public network to your private network. This is the purpose of a firewall. Firewalls are intended to stop all traffic, and only allow "safe" traffic through. There are different types of firewall implementation, including Packet Filtering router, Circuit Gateway, Address translation, and Application Proxy.

One of the most common implementations of the firewall is the Packet Filtering Router: This type of firewall implementation will either block or allow the packet through based on the addressing information in the packet. The addressing information in the packet is like an address on an envelope. One of the addressing information items, which is commonly used, is the Port the packet is using. To explain what a Port is, you can use an analogy that Network Traffic is a visitor to an apartment building, and Port address is like an apartment door. When a visitor (Network packet) arrives, he (the network packet) tells the security guard (the Firewall) which apartment he is trying to go to (Port Address). If the security guard was given permission (by the Firewall administrator) to allow the visitor to the apartment (open the Port), the visitor is let in.

Another common firewall implementation, is known as Network Address Translation (NAT). NAT separates the internal IP address from the external, and the firewall is responsible for translating the addresses.

Example of NAT:

Internal network using a 134.134.160.xxx IP number

External network using 192.102.198.xxx IP number

If someone from the Internet wants to get to the system at 134.134.160.118 (which is an internal network number), they must go through the firewall at the external address (somewhere in the 192.102.198.xxx range). The firewall will replace the incoming address (the 192.102.198.xxx) and reroute it back to 134.134.160.118 system.

Most firewalls also implement the Application Proxy. This is generally used in conjunction with the other types of firewall implementations. The Application proxy knows what kind of content is in the packet that is being sent. The proxy looks at the packet, and if it knows that it is one that is allowed though, it passes though. Like other applications, there are different kinds of application proxies. Application Proxy Firewalls are one of the most secure type of firewalls and feature a built-in proxy function, completely separating the external and internal systems.

#### Basic understanding of H.323

H.323 is an International Telecommunication Union's (ITU) recommendation for visual telephone systems and equipment (video conferencing) over packet-based networks, which provide a non-guaranteed quality of service.

In short, H.323 is a set of rules that permit multiple vendors to create video conferencing products that inter-operate together, over a network. This allows you to intermix different vendors equipment and still be able to make them all work together.

For more information on H.323, please refer to the document titled [H.323 What is it?](#).

#### H.323 and Firewalls

So what is so difficult about getting H.323 through firewalls? The short answer is that H.323 is complex, uses dynamic ports, and includes multiple UDP and TCP streams. This causes real problems for the firewall. How does the firewall determine that it is a packet that's ok to let though? The Packet Filtering Router would have to open all the ports from 1024 to 65535 to accommodate the dynamic port assignment of H.323. This would defeat the purpose of the firewall.

To get around the shortcomings of H.323 traffic through the firewall, you can implement an Application Proxy. The application, of course, is H.323. An H.323 Proxy is able to determine that it is OK to allow the packets through, thus giving a connection through the firewall. The way H.323 Proxies goes around the firewall is to actually establish 2 connections. One to the caller, then one from the callee. The call information is transferred from one side to the other, changing whatever information is necessary to make the connection happen. These changes include the UDP port address, TCP address. The H.323 application has to be proxy aware in order for this to work.

Here's an example of how this works:

Chad is on the internal side of his firewall (with an H.323 Proxy running) using an Intel ProShare Video System 500. He wants to call Kim who is on the external side of the firewall.

Chad configures his ProShare system with the proxy address specified under Preferences and now is ready to call. He selects Call, types in Kim's address and hits dial. Now, the ProShare software sends a request to the Proxy (at the address specified under Preferences) with Kim's address in it. The proxy then tries to make a connection with Kim. We will assume that Kim wants to talk to Chad, so now Kim has a connection to the proxy. The proxy then accepts the connection from Chad. Every packet that Chad sends goes to the Proxy, and then the Proxy forwards it on to Kim. The same process happens in the other direction. This prevents any other packets coming into the network, since the proxy knows whom they are connected to, and what port the information is coming in on.

There are different ways to implement H.323 proxies. The problem is that there are "H.323 Capable" proxies and "H.323 compliant" proxies.

Those that are H.323 capable, likely do not support H.323 calls. These types of proxies screen packets based on a byte string in the network packet. If the byte string exists in the packet, the packet is routed through. This type of proxy is just a filter, and does not implement separate connections and is therefore not a true H.323 proxy. This type of proxy will allow programs like Microsoft's NetMeeting\* to pass packets through the firewall, but not allow true H.323 compliant application traffic, such as that transmitted via a ProShare Video System 500. Another difficulty with the H.323 capable proxies, is that they may not handle "H.323 gatekeeper" requirements. A gatekeeper is an H.323 device that controls the bandwidth of Multimedia Video conferencing over the network.

### **More Information**

The information above is a short, simplified explanation of H.323 and firewalls. To get more details and technical information, you can check these links. These links will also have other links to even more information.

**[ProShare® Video products and Firewalls](#)**

**[The Problems and Pitfalls of Getting H.323 Safely Through Firewalls](#)**

**[Cisco's web site](#)** (search on H.323)

**[Ezenia web site](#)** (search on H.323)

## Intel® ProShare® Video System 500

### Aliasing and PBX Hints and Tips

#### ProShare® Video Conferencing Products

- Aliasing
- PBX Hints and Tips

#### Intel Business Video Conferencing with ProShare® Technology

- Aliasing
- Subaddressing
- Calling Party Number Restriction

#### ProShare® Conferencing

##### Aliasing

ProShare® conferencing units that are configured behind a PBX often fail to receive calls from external locations. This problem is almost always due to the fact that the line the ProShare system is attached to has an internal PBX number that is different from the external number. To operate in this environment, ProShare systems have an aliasing function that allows them to answer both the internal and external numbers. Aliasing is configured by running the ISDN configuration utility located in the ProShare Personal Conferencing group under Diagnostics and Utilities.

Use this configuration if you know that people calling your ProShare systems from external sources need to dial a different number than those calling you internally.

1. Open Diagnostics and Utilities, then choose Hardware and ISDN Configuration.
2. In the first screen, choose the ISDN Configuration button.
3. In the next screen, choose the ISDN protocol and switch manufacturer appropriate to the line your ProShare system is attached to.
4. Continue through the configuration until you reach the screen asking you to enter your ISDN phone number(s) and SPID(s). Enter the external number in the phone number box, (this would be the number that you would have external callers use), and then choose the Aliasing button to access the aliasing configuration dialog box.
5. For the aliasing number, enter the <internal> number for your ProShare system. This is the internal PBX number that you will have obtained from your company's telecommunications specialist. It will be different from the one that you entered in the phone number and SPID screen. Note that it doesn't matter whether the internal number or the external number is described as an alias; your ProShare system will consider them to be equally pertinent to any incoming calls.
6. When you've finished entering the alias number, click Add, then click OK to close the dialog box.

##### PBX Hints and Tips

Intel ProShare system PBX compatibility list

Vendor	Model Number	Minimum software rev.	Compatible?
Alcatel	4220 ETSI	v2.0	Yes
	4300M, S - ETSFV60, 1995		Yes
	4300M, S - ETSEExport 410		Yes
	4300L - ETSI		Yes with 1.8Hb

	Export 420		
	4400,M,L	v1.3	See notes. <u>(10)</u>
<b>Ascom</b>	Ascotel BCS64	v4.4	Yes
	BCS64	v4.4	Yes
<b>Ericsson</b>	MD110	BC 7.2	Yes
	MD110	7.2, 8.0	Yes
<b>GPT</b>	iSDX	v5.2	Yes
	iSDX - Micro	v5.2	Yes
	iSDX - S	v5.2	Yes
	iSDX - L	v5.2	Yes
	iSDX - T	v5.2	Yes
	BRAFE Cards		Yes
<b>Hicom</b>	300	v3.3	Yes
<b>Matra</b>	MD6530	v7	Yes
<b>Nortel</b>	DMS-1		Yes
<b>Octopus</b>	8188	v5.4	Yes
<b>Phillips</b>	Sopho iS3010		See notes. <u>(9)</u>
	Sopho iS3030		See notes. <u>(9)</u>
	Sopho iS3050		See notes. <u>(9)</u>
	Sopho iS3070		See notes. <u>(9)</u>
	Sopho iS3010	P300	Yes
	Sopho iS3030	P300	Yes
	Sopho iS3030	P800	Yes
	Sopho iS3050	P800	Yes
	Sopho iS3070	P740	Yes
	Sopho iS3070	P741	Yes
	ISDX (7)	3.0, 8.0 / 8.2	Yes
	CDX (8)	8.x, 80.x	Yes

<b>Siemens</b>	Hicom 3xx	from 3.3	With Patches (1)
	Hicom 125 / 13	from 4.3	Yes
	Hicom 116	from 1.0	Yes
	Hicom 112 / 11	from 2.0	Yes
	8818 (Octopus)	from 5.4	Yes
<b>Teles</b>		v2.64	Yes

(1) Hicom Patches - S20D32 and S20D40 with software version 3.3 S7 S30626 and S30640 with software version 3.3 S8

Footnotes below are country-specific PBX model numbers / names.

(2) in Holland - VOX 5411

(3) in Holland - VOX 5421

(4) in Holland - VOX 5431

(5) in Holland - VOX6200, DE - Octopus-S

(6) in Denmark - Octopus-S

(7) in Denmark - Octopus-K, M, M26, 180i

(8) in Denmark, Holland, Italy, Sweden, Belgium, Spain, New Zealand - Sopho S15, 25, 35

(9) Phillips Sopho iS3010, iS3030, iS3050, iS3070 Due to Phillips PBX not accepting Calling Party Numbers, this PBX will only accept incoming calls if you delete Phone=#xxx in telephon.ini, however then you cannot accept calls. This issue will exist until summer 1996. To accept calls Phillips makes you accept a call with two numbers one for each b channel. You have to use alias for these two channels. For example, if your number is 1234, and Phillips assigns your b-channels as 1,2 then you need to enter 1234 as your main number and create an alias of 1 and for 2.

(10) The Calling Party Number is a provisional item in the Alcatel. The default provisioning is to check the calling party number. This number is often not the same number as the number to actually call. For example 01793403 6666 may be your phone number for someone to call you but the PBX thinks your extension is 1234. You need to enter this 1234 as your number or have the PBX turn off Calling party number checking.

#### **Tech notes for switches not in the compatibility table:**

##### **Siemens Hicom 300 V3.3**

- Release S7 needs two patches
- Release S8 needs two patches
- V3.358 - needs one patch

Details - there are currently following models/software out in the field:

- HICOM 300 Version 3.3 Release S7 ask Customer Support for patches S20D32 and S20D40
- HICOM 300 Version 3.3 Release S8 ask Customer Support for patches S30626 and S30640

##### **Octopus M26**

- Octopus M26 only works with ProShare systems if certain software release levels are reached. The Octopus M26 has 4 B channels. All other versions of the Octopus product line are compatible with ProShare units if the following conditions are fulfilled: The Bus must NOT be configured with a EAZ (EndgeräteAuswahlZiffer). Software release of the PBX should be at least 8.04 s/w rel. of the component group TRQ should be at least 3.1, software release of the component group AUMA should be at least 1.3.

## Telenorma

- None of the Telenorma PABXs is capable of handling DSS1 (Euro-ISDN protocol) internally.
- Telenorma offers two larger and two smaller systems: I33X and I33XE are large systems that can be converted to handling DSS1 externally. That means the PABX can be connected to a Euro-ISDN line. Still internally the protocol for the transmission of calls remains to be 1TR6.
- A ProShare Video System making a call would go through the PABX to the outside world will therefore never be able to successfully place a call.
- The smaller systems I3 and I2H cannot be converted at all and purely 1TR6 systems.
- Result: ProShare Video System users with Telenorma PABX have to have a separate outside line in order to be able to run ProShare Video System.

## Alcatel 4210

- Alcatel 4210, Software release 5M is DSS1 compliant but not ETSI. Cannot bundle 2 B channels together.

## Siemens Hicom V. 3.358

- Siemens Hicom 300 Release 3.358 needs patch VK3080 in order to be able to provide ISDN channel bundling for ProShare conferencing.

## Intel Business Conferencing with ProShare Technology

The next revision of ProShare conferencing functions properly with all the above switches, but the aliasing, subaddressing, and Calling Party Number restrictions are slightly different.

### Aliasing

To get this version of ProShare conferencing to enter an alias, follow these steps:

1. Select settings-> control Panel -> Network -> ITK Ix1-micro v3.0.
2. Enter properties -> numbers -> advanced.  
Where you see additional numbers, you can enter up to four alias's. If the PBX thinks you are 1234 and your full number is 6789543, then you enter 1234 as an additional number.
3. Click OK. You will be prompted to reboot.

### Subaddressing

To enter a Subaddress in the current product you need to go to the ITK/numbers property page. Where the line says phone number one, use the "pipe" character | after your number and assign a user specified subaddress.

For example, if you want to have the subaddress 1357 and your phone number is 5038765432, you would enter 5038765432|1357 for your phone number.

Notes on subaddressing:

- In Europe, only use 4 digits of Subaddressing.
- Ericsson PBX only uses three digits and today only internal subaddress calls will work.
- Siemens Hicom 300 does not use Subaddressing properly. If you call on a line enabled with subaddressing without a subaddress, it will fail.
- Alcatel PBX only passes four digits of subaddress.

### Calling Party Number Restriction

On alcatel 4400, Matra 6450, Phillips PBXs, and Hicom 100, the calling party number is checked. Therefore, the following should be done on each;

On the Alcatel, Hicom and Matra, in the TELEPHON.INI where the ITK provider is, add the following:

### **For Windows\* 95 for version 3.0:**

```
[Provider2]
NumLines=1
NumPhones=0
LineName0=ITK ix1-micro V3.0
NoUseDefaults=1
LineAddr0=0, 0, 1, TEL, FAX, DATA
```

```
Add
ModelType=PBX
```

If you want to have a calling party number to match your PBX, but different than your business card number, add the following to the same location in your TELEPHON.INI;

```
CPN_Value=xxxx
```

Where xxxx is the calling party number expected.

### **For Windows NT\* version 4.0:**

1. In the install directory, double click on the file, PBX\_ON.REG, to disable the calling party number. (For turning the calling party number back on, click on PB\_OFF.REG)
2. If you want to have a calling party number to match your PBX, but different than your business card number, do the following:
  - o Edit CPN.REG between the quotes as below,
  - o [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\ixmicro1\Parameters\Line1]
  - o "Modeltype"="PBX"
  - o "CPN\_VALUE"="12345"

### **For Windows NT version 4.01**

1. Click Start > Settings > Control Panel.
2. Double-click the Network icon.
3. On the Adaptors tab, highlight ITK ix-micro V3.0, and then click Properties.
4. Click Phone Numbers.
5. Click Advanced.
6. Click the "Calling Party Number Disable" box to select it.

### **For Windows 95 version 4.01**

1. Click Start > Settings > Control Panel.
2. Double-click the Network icon.
3. On the Configuration tab, highlight ITK ix-micro V3.0, and then click Properties.
4. Click Numbers.
5. Click Advanced.
6. Click the "Calling Party Number Disable" box to select it.



Manual Line Termination	Misc Trunk Restriction Group 4
Origination	Misc Trunk Restriction Group 5
Outward	Misc Trunk Restriction Group 6
Terminal to Terminal	Misc Trunk Restriction Group 7
Termination	Misc Trunk Restriction Group 8
Toll Restricted	All
WCR Toll Restricted	

Code Restriction Level 0  
 Facility Restriction Level 3

**ISDN Routing: I**

AT&T Mgr IV 2.2                      DEFINITY G2.2

tcm product-admin bearer-capability-cos display  
 This information is retained only in the product

**Bearer Capability Class of Service 49**

**Bearer capability Datarates Facility attributes**

Voice 0	64000 bps? y	Transport
Mode: c		
Model 0	56000 bps? y	Channel
Type: c		
Mode 2 0	19200 bps? n	Async/Sync: a
Mode 3 0	9600 bps? n	Duplex: f
Mode 0 0	4800 bps? n	Clock i
Voice Grade Data 0	2400 bps? n	
Unknown Digital: 0	1200 bps? n	
Unknown Analog: 0	300 bps? n	
Mode 3/2 0	low bps? n	

**Bearer Capability Class of Service 49**

Default attributes

Default Bearer Capability Class: 4      Default Transport Mode c

Default Data Rate (bps): none

Default Channel Type: r

AT&T Mgr IV 2.2

DEFINITY G2.2

tcm product-admin extension display  
You are directly accessing the product.

Extension 35099

Analog? n Hot Line n

**Extension attributes**

Class of Service 3 LWC Destination 0</TD

Auxiliary ANI? n AP No. 0 Audible n

Hunt To Extension AUDIX Machine No.: 0 Bearer Capability COS: 49

Call Pickup Group No. Attd. Controlled Restriction Group:

Call Coverage Group No. NPA-NXX Designator

DSC Message? n Call Fwd Off-Net Toll n

Univ. Code Calling ID:

AT&T Mgr IV 2.2

DEFINITY G2.2

tcm product-admin terminal display  
You are directly accessing the product.

Set Type Encode: 150 Terminal Option: 06 Equip.

Loc.:  
13/0/c/15/00

Origination Preference 2

Termination Preference 0

**Terminal options**

Data Module? y

## Data module feature options

Physical Data Type I  
Terminal Dialing? y

AT&T Mgr IV 2.2

DEFINITY G2.2

tcm product-admin button display  
You are directly accessing the product

Page 1 of 1

Equip. Loc. 13/0/c/15/00  
Button Number 01  
Set Module 0  
Button Type: 6

AT&T Mgr IV 2.2

DEFINITY G2.2

tcm product-admin button display  
You are directly accessing the product

Equip. Loc. 13/0/c/15/00  
Button Number 02  
Set Module 0  
Button Type: 0

AT&T Mgr IV 2.2

DEFINITY G2.2

tcm product-admin button display  
You are directly accessing the product

Equip. Loc. 13/0/c/15/00  
Button Number 03  
Set Module 0  
Button Type: CALL

Extension No. 35099

Call Appearance 01  
Line Type: 4  
Alert Type: I  
Alerting Transfer Encode 0  
Alerting Encode: I  
Orig. Only: 0  
Home Terminal I  
SAC Group Member: 0

AT&T Mgr IV 2.2

DEFINITY G2.2

tcm product-admin button display  
You are directly accessing the product

Equip. Loc. 13/0/c/15/00  
Button Number 04  
Set Module 0  
Button Type: CALL

Extension No. 35099  
Call Appearance 02  
Line Type: 4  
Alert Type: I  
Alerting Transfer Encode 0  
Alerting Encode: I  
Orig. Only: 0  
Home Terminal I  
SAC Group Member: 0

AT&T Mgr IV 2.2

DEFINITY G2.2

tcm product-admin set-type display  
You are directly accessing the product

Set Type Encode: 150

**Terminal Option:**

No. of signed:  
Terminals 20

**Set type parameters**

**Number of buttons**

Equipment Type: 5

Basic Set 4

Data Capability: 5

Display Module

Display Capability:

Feature Module

ISDN Capability: 0

Coverage Module:

AT&T Mgr IV 2.2

DEFINITY  
G2.2

tcm product-admin btn-template display  
You are directly accessing the product.

Set Type Encode 150  
Device Type: 0  
Button Number I  
Button Type: u  
Number of Lamps: 0

Set Type Encode 150  
Device Type: 0  
Button Number 2  
Button Type: u  
Number of Lamps: 0

Set Type Encode 150  
Device Type: 0  
Button Number 3  
Button Type: p  
Number of Lamps: 2

Set Type Encode 150  
Device Type: 0  
Button Number 4  
Button Type: p  
Number of Lamps: 2

## **G3 programming**

Add Data Module 7500 - Data/Video

add data (extension)

### **Data module 1**

Data Extension: (extension)    Type: 7500    Port:

(BRI port)

Name: (persons name)COS: (1 or site choice)    COR: (1 or site)

### **Abbreviated dialing:**

List:

### **Special dialing option:**

### **Circuit switched data attributes**

Default Duplex: full    Default Mode: async    Default Speed: 1200

### **Data module capabilities**

### **Circuit switched data attributes**

Default ITC: restricted    Default Data Application: M2\_A

**Data modlue1**

**BRI link/maintenance parameters153**

XID? y  
Fixed TEI? y  
MIM support? y  
Endpt Init? y  
SPID: (extension) MIM Mtce/Mgt ? y

Optional Voice - Add Station ISDN Set Type

add station (extension)

**Station75**

Extension: (extension)            BCC: 0  
Type: 8510d(or other)            Lock Messages? n            COR: 1  
Port: (Port)                        Security Code:                COS: 1  
Name:(persons name)               Coverage Path:

**Feature options**

LWC Reception: spe                Coverage Msg Retrieval? y  
LWC Activation? y                 Auto Answer: none  
CDR Privacy? n                     Data Restriction? n  
Redirect Notification? y            Idle Appearance Preference? n  
Bridge Call Alerting? n            Restrict Last Appearance? y  
XID? y                                Fixed TEI? n  
MIM support? y                     Endpt Init? y  
SPID: (extension)                 MIM Mtce/mgt?y  
AUDIX Name:  
Messaging Server Name:            Audible Message Waiting? n  
Display Language: english        Disp Client Redir? n

**Station75**

**Site data125**

Room:                                Headset? n  
Jack:                                 Speaker? n  
Cable:                                Mounting: d  
Floor:                                Cord Length: 0  
Building:                             Set Color:

## Abbreviated dialing39

List1:

List2:

List3:

### Button Assignments

1: call-appr 6:

2: call-appr 7:

3: call-appr 8:

4: 9:

5: 10:

### Station75

#### Feature button assignments73

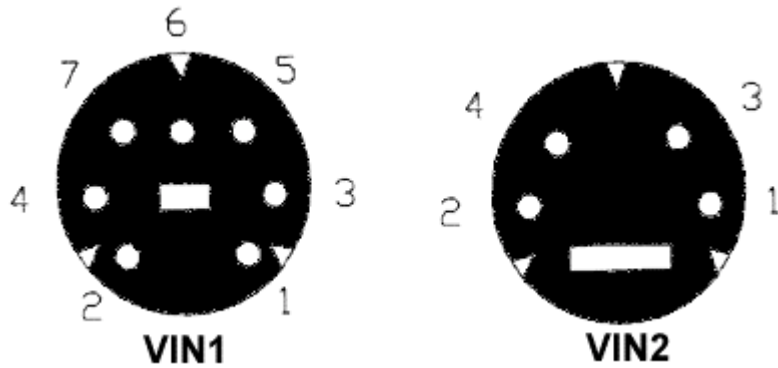
11: normal

## Intel® ProShare® Video System 500

### VIN1 and VIN2 Video Input Connectors' Pinouts

The VIN1 input jack is a proprietary 7-pin mini-DIN input connector.

The VIN2 input jack is a standard S-Video 4-pin mini-DIN input connector.



#### VIN1 Input Connector Pinout

Pin number	Signal
1	+12 VDC 300mA
2	GND
3	GND
4	GND
5	Composite video signal
6	GND
7	GND

#### VIN2 Input Connector Pinout

Pin number	Signal
1	GND
2	GND
3	Y (Luminance video signal)
4	C (Chrominance video signal)