Administrator's Guide for the V Series

Version 9.0.6

March 2010 Edition
3725-24475-003/A
Version 9.0.6

POLYCOM®

Trademark Information

Polycom®, the Polycom logo design, and VSX® are registered trademarks of Polycom, Inc. Global Management System™, MGC™, People+Content™, Polycom PathNavigator™, Polycom V500™, StereoSurround™, and V^{2}IU™ are trademarks of Polycom, Inc. in the United States and various other countries. All other trademarks are the property of their respective owners.

Patent Information

The accompanying product is protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

Polycom Inc.
4750 Willow Road
Pleasanton, CA 94588-2708
USA

About this Guide

The *Administrator's Guide for the V Series* is for administrators who need to configure, customize, manage, and troubleshoot V series systems. This guide covers the Polycom® V500™ and V700 systems.

Please read the V Series documentation before you install or operate the system. The following related documents for V Series systems are available at www.polycom.com/videodocumentation:

- *Setting Up the System*, which describes how to set up the hardware
- *Getting Started Guide for the V Series*, which describes how to perform video conferencing tasks
- Setup Sheets, which describe how to install optional hardware
- Release Notes

For support or service, please contact your Polycom distributor or go to Polycom Support at www.polycom.com/support.

Polycom recommends that you record the serial number and option key of your system here for future reference. The serial number for the system is printed on the unit.

System Serial Number: _____

Option Key: _____

Contents

1 Introducing the V Series 1-1

V Series Models 1-1
V500 Set-top System 1-1
V700 Desktop System 1-2
Setting Up Your System Hardware 1-2
Positioning the System 1-3
Positioning the V500 System 1-3
Positioning the V700 System 1-3
Powering On the System 1-4
Powering On the V500 System 1-5
Powering On the V700 System 1-5
Configuring with the Setup Wizard 1-5

2 Networks 2-1

Getting the Network Ready 2-1
Connecting to the LAN 2-1
Configuring LAN Properties 2-2
Configuring IP Settings 2-4
Specifying H.323 Settings 2-4
Configuring the System to Use a Gatekeeper 2-4
Configuring Integration with Avaya Networks 2-6
Configuring the System to Use a Gateway 2-7
Specifying SIP Settings 2-8
Specifying Quality of Service 2-10
Configuring the System for Use with a Firewall or NAT 2-11
Firewall Settings 2-11
H.460 NAT Firewall Traversal 2-13
Connecting to the ISDN BRI Network 2-14
Configuring ISDN Settings 2-15
Configuring Call Preferences 2-16
Configuring Dialing Order Settings 2-18

3 Monitors and Cameras 3-1

Connecting the Monitor 3-1
Using a V700 System as the Monitor for a Computer 3-1

Configuring Monitor Settings 3-2
Using Dual Monitor Emulation 3-3
Examples of Dual Monitor Emulation 3-3
Using Dual Monitor Emulation in a Call 3-4
Adjusting the Monitor's Color Balance, Sharpness, and Brightness 3-4
Preventing Monitor Burn-In 3-5
Configuring Camera Settings 3-6

4 Microphones and Speakers 4-1
Connecting Speakers or Headphones 4-1
Configuring Audio Settings 4-1
V500 System 4-1
V700 System 4-2

5 Content and Closed Captions 5-1
Configuring Content Display with People+Content IP 5-1
Configuring Closed Captioning 5-2
Via the System's Web Interface 5-3
Via a Telnet Session 5-3

6 Calling and Answering 6-1
Configuring Call Settings 6-1
Setting the Call Answering Mode 6-2
Configuring Directory Settings 6-3
Creating a Localized System Name with the System's Web Interface 6-3
Managing Directories with the System's Web Interface 6-4
Configuring the Global Directory 6-5
Configuring Streaming Calls 6-6

7 System Location, Appearance, and Tones 7-1
Setting Date, Time, and Location 7-1
Designing the Home Screen 7-3
Customizing the Home Screen 7-3
Displaying Contacts on the Home Screen 7-5
Adding Marquee Text 7-6
Changing System Appearance 7-6
Applying the Video Overlay 7-7
Setting Ring Tones and Alert Tones 7-8
Screen Savers 7-8
Adding Screen Saver Text 7-8
Adding a Screen Saver News Feed 7-9
Adding a Screen Saver Logo 7-10
Configuring the Screen Saver Wait Time 7-10

8 Security 8-1
Screens that Require the Room Password for Access 8-1
Configuring Security Options 8-2
Setting the Room and Remote Access Passwords 8-4
Managing User Access to Settings and Features 8-5
Enabling AES Encryption 8-6

9 Managing the System Remotely 9-1
Using the System's Web Interface 9-1
Accessing the System's Web Interface 9-1
Monitoring a Room or Call with the System's Web Interface 9-2
Managing System Profiles with the System's Web Interface 9-3
Sending a Message 9-4
Configuring Global Services 9-4
Viewing the Management Servers List 9-5
Requiring an Account Number for Calls 9-5
Adding Information for the Global Management System Administrator 9-6
Requesting Technical Support from the Global Management System Administrator . 9-6
Setting Up SNMP 9-7
Downloading MIBs 9-7
Configuring for SNMP Management 9-7
Keeping Your Software Current 9-8

10 Control Devices 10-1
Configuring Remote Control Behavior 10-1

11 Statistics and Diagnostics 11-1
Diagnostic Screens 11-1
System Status 11-2
Call Statistics 11-3
Network 11-4
Video 11-4
Audio 11-5
Restart System 11-5
Recent Calls 11-6
Call Detail Report (CDR) 11-6
Information in the CDR 11-7
Call Detail Report Archives 11-10

12 Troubleshooting 12-1
Placing a Test Call 12-1
Enabling Basic Mode 12-2
General Troubleshooting 12-2

Power and Start-up 12-3
Controls 12-4
Access to Screens and Systems 12-5
Calling 12-6
Display 12-9
Audio 12-12
Error Indications 12-13
How to Contact Technical Support 12-14

A System Back Panel Views A-1

V500 System Back Panel A-1
V700 System Connector Panel A-2

B Port Usage B-1

C Cables C-1

LAN Cable C-2
Composite Video Cable C-2

D PathNavigator Error Codes and Q.850 Cause Codes D-1

PathNavigator Error Codes D-1
Q.850 Cause Codes D-4

Regulatory Notices . . . . . Regulatory Notices-1

Index Index-1

1

Introducing the V Series

Your Polycom video conferencing system is a state-of-the-art visual collaboration tool. With crisp, clean video and crystal-clear sound, your V Series system provides the essential tools your home or small business needs for video conferencing over broadband networks.

V Series Models

For technical specifications and detailed descriptions of features available for the V Series systems, please refer to the product literature at www.polycom.com.

V500 Set-top System

The V500 system delivers high-quality, face-to-face video communication in a sleek package that includes the camera and microphone. Two models of the V500 system are available: IP only, and IP with ISDN.

V700 Desktop System

The V700 system delivers high-quality, video communication in an all-in-one appliance that includes the camera, LCD screen, speakers, and microphone. Save space in your office by using the VGA cable to connect your computer to the system's 17" high-resolution XGA display.

Setting Up Your System Hardware

This manual provides information to supplement the setup sheet provided with your system. A printed copy of the system setup sheet is provided with each V Series system. PDF versions of the system setup sheets are available at www.polycom.com/videodocumentation.

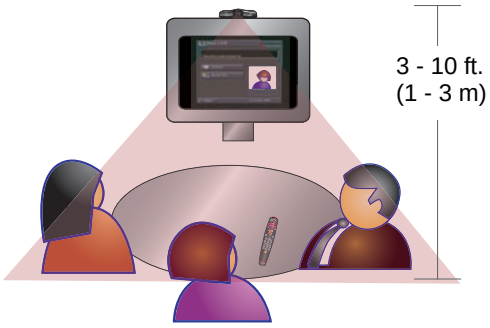
Positioning the System

Position the system so that the camera does not face toward a window or other source of bright light.

Positioning the V500 System

To position the V500 system:

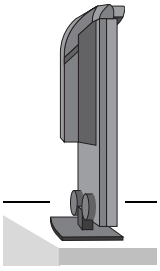
- Place the V500 system on top of your TV monitor. For optimal audio and video performance, locate the monitor within 5 to 10 feet (1.5 to 3 meters) away from the people in the call.



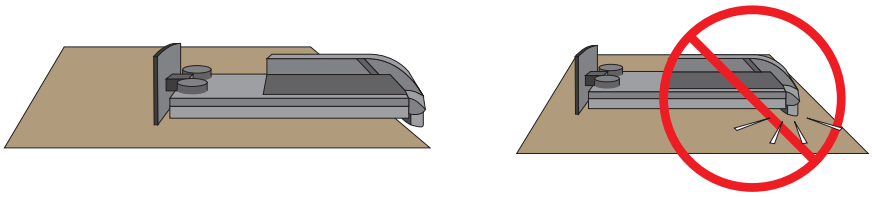
Positioning the V700 System

To position the V700 system:

- Place the V700 system on your desktop or on a table in a small conference room, leaving enough space so that you can connect the cables easily.



If you need to place the system face-down to connect the cables, make sure that the camera does not touch the work surface. The weight of the system can damage the camera mount.



Powering On the System

Connect power and power on the system after you have connected the rest of the equipment that you will use with it. Make sure that the system is powered off before you connect devices to it.

Do not use a power supply other than the one supplied with your system. Using the wrong power supply will void the warranty and may damage your system.

The status lights on the front of the system provide this information:

Status Light	System Status
Off	System is powered off
Steady green light	System is awake and not in a call
Blinking green light (once)	System received an IR signal while awake and not in a call
Blinking green light (on 1 sec, off 2 sec)	System is asleep, not in a call
Steady amber light	System is in a call
Blinking amber light (once)	System received an IR signal while in a call
Steady red light	Microphone is muted

Powering On the V500 System

The V500 system has an external power supply.

To power on the V500 system:

1. Make sure you have connected all equipment to the system, and then connect the power cord to a wall outlet.
2. Power on the monitor.
3. Press the power switch located at the back of the system.

Powering On the V700 System

The V700 system has three power switches.

To power on the V700 system:

1. Press the power switch near the connectors on the back of the system.
2. Press the power switch on the lower back corner of the monitor.
3. Press the power button on the front of the monitor.

Configuring with the Setup Wizard

When you power on the system for the first time, the setup wizard detects your system's IP and ISDN connections, and leads you through the minimum configuration steps required to place a call.

The setup wizard allows you to set a room password, which allows you to limit access to the Admin Settings. The default room password is the 14-digit system serial number from the System Information screen, the bottom of the system, or the back of the system.

Make sure you can recall the room password if you set one. If you forget the password, you will have to reset the system, delete the system files, and run the setup wizard again to access the Admin Settings and reset the password.

You can run the setup wizard or view the configuration screens in either of these two ways:

- In the room with the system — Use the remote control to navigate the screens and enter information.
- **From a remote location** — Use a web browser to access the system's web interface.

2

Networks

This chapter provides information on network types used worldwide. Please note that not all network types are available in all countries.

The ISDN network information only applies to the V500 system with the ISDN option. The IP network information applies to both versions of the V500 system and to the V700 system.

Getting the Network Ready

Before you begin configuring the network options, you must make sure your network is ready for video conferencing.

To begin, refer to the *Preparing Your Network for Collaboration* document, available at www.polycom.com/videodocumentation. This document contains information you need to get your network ready, such as worksheets that will help you order ISDN.

Connecting to the LAN

You must connect the system to a LAN to:

- Make IP or SIP calls
- Use the Global Directory Server
- Access the system's web interface
- Use People+Content IP
- Update system software using the Polycom Softupdate program

Configuring LAN Properties

To configure LAN properties:

1. Go to **System > Admin Settings > LAN Properties.**
2. Configure these settings:

Setting	Description
Connect to my LAN	Specifies whether the system is part of the LAN. Changing this setting causes the system to restart.
Host Name	Specifies the system's DNS name. Changing this setting causes the system to restart.
IP Address	Specifies how the system obtains an IP address. • **Obtain IP address automatically** — Select if the system gets an IP address from the DHCP server on the LAN. • **Enter IP address manually** — Select if the IP address will not be assigned automatically. Changing this setting causes the system to restart.
Your IP Address is or **Use the Following IP Address**	If the system obtains its IP address automatically, this area displays the IP address currently assigned to the system. If you selected **Enter IP Address Manually**, enter the IP address here. Changing the IP address causes the system to restart.
Domain Name	Displays the domain name currently assigned to the system if the system is a member of a domain within an organization. If the system does not automatically obtain a domain name, enter one here if needed for your organization's network.

3. Select  and configure these settings:

Setting	Description
DNS Servers	Displays the DNS servers currently assigned to the system. If the system does not automatically obtain a DNS server address, enter up to four DNS servers here. Changing this setting causes the system to restart.
Default Gateway	Displays the gateway currently assigned to the system. If you are using a router for Internet access, the Default Gateway will be the router's internal address. If the system does not automatically obtain a gateway IP address, enter one here. Changing this setting causes the system to restart.
Subnet Mask	Displays the subnet mask currently assigned to the system. If the system does not automatically obtain a subnet mask, enter one here. Changing this setting causes the system to restart.
WINS Server	Displays the WINS server currently assigned to the system. If the system does not automatically obtain a WINS server IP address, enter one here. Changing this setting causes the system to restart.
WINS Resolution	Sends a request to the WINS server for WINS name resolution.
LAN Speed	Specifies the LAN speed to use. Note that the speed you choose must be supported by the switch. Choose **Auto** to have the network switch negotiate the speed automatically. If you choose **10 Mbps** or **100 Mbps**, you must also select a duplex mode. **Note**: Polycom does not support **Auto** for the V Series system only or the switch only; the setting for both must be the same. Changing this setting causes the system to restart.
Duplex Mode	Specifies the Duplex mode to use. Note that the Duplex mode you choose must be supported by the switch. Choose **Auto** to have the network switch negotiate the Duplex mode automatically. Polycom recommends setting both the switch and the system to negotiate both speed and duplex automatically. **Note:** Polycom does not support Auto for the V Series system only or the switch only; the settings for both must be the same. Changing this setting causes the system to restart.

Configuring IP Settings

Specifying H.323 Settings

If your network uses a gatekeeper, the system can automatically register its H.323 name and extension. This allows others to call the system by entering the H.323 name or extension instead of the IP address.

To specify H.323 settings:

1. Go to **System > Admin Settings > Network > IP > H.323 Settings**.
2. Configure these settings on the H.323 Settings screen:

Setting	Description
Display H.323 Extension	Lets users placing a gateway call enter the H.323 extension separately from the gateway ID. If you do not check this box, you can make gateway calls by entering the call information in this format: gateway ID + ## + extension
H.323 Name	Specifies the name that gatekeepers and gateways can use to identify this system. You can make point-to-point calls using H.323 names if both systems are registered to a gatekeeper. The H.323 Name is the same as the System Name, unless you change it. Your dial plan may define the names you can use.
H.323 Extension (E.164)	Lets users place point-to-point calls using the extension if both systems are registered with a gatekeeper, and specifies the extension that gatekeepers and gateways use to identify the system. The default H.323 Extension can be changed. Your organization's dial plan may define the extensions you can use.

Configuring the System to Use a Gatekeeper

A gatekeeper is a "network administrator" that supervises network traffic and manages functions such as bandwidth control and admission control. The gatekeeper also handles address translation, which allows users to make calls using static aliases instead of IP addresses that may change each day.

To configure the system to use a gatekeeper:

1. Go to **System > Admin Settings > Network > IP > H.323 Settings**.
2. Select  and configure these settings on the Gatekeeper screen:

Setting	Description
Use Gatekeeper	Specifies whether to use a gatekeeper. Gateways and gatekeepers are required for calls between IP and ISDN. • **Off** — Calls do not use a gatekeeper. • **Auto** — System automatically finds an available gatekeeper. • **Specify** — Calls use the specified gatekeeper. Enter the gatekeeper's IP address or name (for example, gatekeeper.companyname.usa.com, or 10.11.12.13). • **Specify with PIN** — Calls use the specified E.164 address and require an **Authentication PIN**. This setting is available only when the Avaya® option key is installed.
H.323 Name	Specifies the name that gatekeepers use to identify this system. You can make point-to-point calls using H.323 names if both systems are registered to a gatekeeper. The H.323 Name is the same as the System Name, unless you change it. Your organization's dial plan may define the names you can use.
H.323 Extension (E.164)	Lets users place point-to-point calls using the extension if both systems are registered with a gatekeeper, and specifies the extension that gatekeepers and gateways use to identify this system. The default H.323 Extension is based on the system serial number, but it can be changed. Your organization's dial plan may define the extensions you can use.
Primary Gatekeeper IP Address	If you chose to use an automatically selected gatekeeper, this area displays the gatekeeper that was discovered in the network. If you chose to specify a gatekeeper, enter the IP address of the primary gatekeeper.
Authentication PIN V500	Specifies the password PIN to use for authentication with the Avaya COMMUNICATIONS MANAGER®. This setting is available when **Use Gatekeeper** is set to **Specify with PIN**.
Use PathNavigator for Multipoint Calls	Lets you specify whether to use the Conference on Demand feature available with Polycom PathNavigator™, ReadiManager SE200, or Polycom CMA system. This feature is available only if the system is registered with one of these gatekeepers.

3. Select  to view the IP addresses for the current gatekeeper, the primary gatekeeper, and any alternate gatekeepers.

Points to note about PathNavigator's Conference on Demand feature:

If your organization uses Polycom's PathNavigator, you can use PathNavigator's Conference on Demand feature to place multipoint calls.

To place calls using PathNavigator, you need to:

- Register your V Series system with PathNavigator.
- Configure your V Series system to use PathNavigator for multipoint calls (see Configuring the System to Use a Gatekeeper on page 2-4).
- Create a multi-site entry in the directory (recommended).

When using PathNavigator's Conference on Demand:

- Once the call begins, users cannot add another site to the call — even if the site was in the call originally.

Configuring Integration with Avaya Networks

V500 systems with an Avaya option key can use the following features on an Avaya telephony network:

- Call forwarding (all, busy, no answer)—Configured by the Avaya COMMUNICATIONS MANAGER (ACM) administrator and implemented by the user
- Call coverage—Configured by the ACM administrator
- Transfer—Implemented via flash hook and dialing digits
- Audio conference—Implemented via flash hook and dialing digits
- Call park
- Answer back
- DTMF tones for Avaya functions

Refer to the Avaya documentation and *Getting Started Guide for the V Series* for information about these features.

To install the Avaya option key:

1. Obtain a license number from Avaya, then enter that online on the Polycom web site at www.polycom.com/support/video, along with your V500 system serial number. This returns a key code for the Avaya option.
2. On the V500 system, go to **System > Admin Settings > General Settings > Options** and enter the key code for the Avaya option.

To configure the V500 system to use Avaya network features:

1. Go to **System > Admin Settings > Network > IP > H.323 Settings > Next**.

   Set **Use Gatekeeper** to **Specify with PIN**.

   Enter the **H.323 Extension (E.164)** provided by the ACM administrator.

   Enter the ACM IP address for **Gatekeeper IP Address**.

   Enter the **Authentication PIN** provided by the ACM administrator.

2. Go to **System > Admin Settings > Network > IP > Call Preference**.

   Verify that **Enable H.239** is enabled.

3. Go to **System > Admin Settings > General Settings > System Settings > Call Settings**.

   Set **Auto Answer Point-to-Point Video** to **No**.

Configuring the System to Use a Gateway

A gateway performs code and protocol conversion between H.323 (IP) and H.320 (ISDN), so that users on different networks can call one another. If the system is configured to use a gateway, you must also configure it to use a gatekeeper.

To configure the system to use a gateway:

1. Go to **System > Admin Settings > Network > IP > H.323 Settings.**
2. Select  three times and configure these settings:

Setting	Description
Country Code	Specifies the country code for the system's location.
Area Code	Specifies the area or city code for the system's location.
Number	Specifies the gateway's number.
H.323 Extension (E.164)	Specifies the extension that identifies this system for incoming gateway calls. The default H.323 Extension can be changed.
Gateway Number Type	Specifies the number type users enter to call this system: • **Direct Inward Dial** — Users enter an internal extension to call this system directly. **Note**: If you choose this setting, you must also register the number with the gatekeeper as an E.164 alias. • **Number + Extension** — Users enter the gateway number and the system's extension to call this system.

Setting	Description
Number of Digits in DID Number	Specifies the number of digits in the DID number. The national or regional dialing plan for your location determines the standard number of digits. For instance, the US standard is 7 digits. This setting is only available when **Gateway Number Type** is set to **Direct Inward Dial**.
Number of Digits in Extension	Specifies the number of digits in the extension. Your organization's dial plan determines this number. This setting is only available when **Gateway Number Type** is set to **Direct Inward Dial**.

3. Select  and enter a prefix or suffix for each bandwidth you want to allow for gateway calls.

   Associating prefixes and suffixes with particular bandwidths on your gateway can optimize the use of bandwidth by your organization. Be sure the gateway is configured to use the same prefixes and suffixes you define for the system.

Specifying SIP Settings

If your network supports Session Initiation Protocol (SIP), you can use SIP to connect IP calls.

To specify SIP settings:

1. Go to **System > Admin Settings > Network > IP > SIP Settings**.
2. Configure these settings on the SIP Settings screen:

Setting	Description
Transport Protocol	Indicates the protocol the system uses for SIP signaling. The SIP network infrastructure in which your V Series system is operating determines which protocol is required. For example, if your V Series system is operating in a Microsoft Live Communication Server (LCS) SIP network, choose **TCP**. If your V Series system is operating in a Nortel Multimedia Communication Server (MCS) SIP network, choose **UDP**.
Authentication Name	Specifies the name to use for authentication when registering with a SIP Registrar Server. If you leave this field blank, the User Name is used for authentication.
User Name	Specifies the system's SIP name. If you leave this field blank, the system's IP address is the SIP user name.

Setting	Description
Password	Specifies the password that authenticates the system to the Registrar Server.
Registrar Server	Specifies the name or IP address of the SIP Registrar Server. By default, the SIP signaling is sent to port 5060 on the registrar server. To specify a different port, add it to the address as shown here: 10.11.12.13:5070
Proxy Server	Specifies the DNS name or IP address of the SIP Proxy Server. If you leave this field blank, no proxy server is used. By default, the SIP signaling is sent to port 5060 on the proxy server. To specify a different port, add it to the address as shown here: 10.11.12.13:5070
PCAS	Specifies whether to register to the PCAS (Polycom Conferencing Application Server). • **Auto** — System automatically finds the PCAS. • **Specify** — Calls use the specified PCAS. Enter the PCAS IP address or name, for example pcas.companyname.xxxx, or 10.11.12.13. • **Off** — Calls do not use the PCAS. **Notes:** For integrations involving Lotus® Sametime®, Lotus Notes®, or both Lotus Sametime and Lotus Notes, set **PCAS** to **Off**. For information about V Series system support for SIP sites using Lotus Sametime or Lotus Notes in audio and video calls with instant meetings, scheduled meetings, and Click2Call via the RAS200I PCAS, refer to the Lotus Sametime or Lotus Notes Integrated Video Conferencing Deployment Guide or User Guide.
PCAS Server Address	Enter the PCAS IP address or name when **PCAS** is set to **Specify**. If **PCAS** is set to **Auto**, the system displays the server address in this field. When a **PCAS Server Address** is configured, **Registrar Server** and **Proxy Server** are set automatically. **Note:** For information about V Series system support for SIP sites using Lotus Sametime or Lotus Notes in audio and video calls with instant meetings, scheduled meetings, and Click2Call via the RAS200I PCAS, refer to the Lotus Sametime or Lotus Notes Integrated Video Conferencing Deployment Guide or User Guide.

Points to note about SIP:

Because some advanced video conferencing capabilities are not yet standardized, and many capabilities depend on the SIP server, the following features are not supported using SIP.

Examples of features that are not supported using SIP are:

- Polycom Video and Audio Error Concealment
- Encryption
- People and Content (H.239 and Polycom People+Content™)

Specifying Quality of Service

Set the Quality of Service options for the way your network handles IP packets during video calls.

To specify Quality of Service:

1. Go to **System > Admin Settings > Network > IP > Quality of Service**.
2. Configure these settings on the Quality of Service screen:

Setting	Description
Type of Service	Specifies your service type and lets you choose how to set the priority of IP packets sent to the system for video, audio, and far-end camera control: • **IP Precedence** — Represents the priority of IP packets sent to the system. The value can be between 0 and 5. If this setting is selected, enter the value in the **Type of Service Value** field. • **DiffServ** — Represents a priority level between 0 and 63. If this setting is selected, enter the value in the Type of Service Value field.
Type of Service Value	Specifies the IP Precedence or Diffserv value for Video, Audio, and Far End Camera Control.
Maximum Transmission Unit Size	Specifies the Maximum Transmission Unit (MTU) size used in IP calls. If the video becomes blocky or network errors occur, packets may be too large; decrease the MTU. If the network is burdened with unnecessary overhead, packets may be too small; increase the MTU. • **Auto** — Allows the system to select the MTU size.

Setting	Description
Enable PVEC	Allows the system to use PVEC (Polycom Video Error Concealment) if packet loss occurs.
Enable RSVP	Allows the system to use Resource Reservation Setup Protocol (RSVP) to request that routers reserve bandwidth along an IP connection path. Both the near site and far site must support RSVP in order for reservation requests to be made to routers on the connection path.

3. Select  and configure these settings on the Bandwidth screen:

Setting	Description
Dynamic Bandwidth	Specifies whether to let the system automatically find the optimum line speed for a call.
Maximum Transmit Bandwidth	Specifies the maximum transmit line speed between 48 kbps and 768 kbps.
Maximum Receive Bandwidth	Specifies the maximum receive line speed between 48 kbps and 768 kbps.

Configuring the System for Use with a Firewall or NAT

A firewall protects an organization's IP network by controlling data traffic from outside the network. Unless the firewall is designed to work with H.323 video conferencing equipment, you must configure the system and the firewall to allow video conferencing traffic to pass in and out of the network.

Firewall Settings

Network Address Translation (NAT) network environments use private internal IP addresses for devices within the network, while using one external IP address to allow devices on the LAN to communicate with other devices outside the LAN. If your system is connected to a LAN that uses a NAT, you will need to enter the NAT Public (WAN) Address so that your system can communicate outside the LAN.

To set up the system to work with a firewall and NAT:

1. Go to **System > Admin Settings > Network > IP > Firewall**.
2. Configure these settings on the Firewall screen:

Setting	Description
Fixed Ports	Lets you specify whether to define the TCP and UDP ports. • If the firewall is not H.323 compatible, enable this setting. The V Series system assigns a range of ports starting with the TCP and UDP ports you specify. The system defaults to a range beginning with port 3230 for both TCP and UDP. **Note**: You must open the corresponding ports in the firewall. You must also open the firewall's TCP port 1720 to allow H.323 traffic. • If the firewall is H.323 compatible or if the system is not behind a firewall, you may not need to enable this option.
TCP Ports **UDP Ports**	Lets you specify the beginning value for the range of TCP and UDP ports used by the system. The system automatically sets the range of ports based on the beginning value you set. **Note:** You must open the firewall's TCP port 1720 to allow H.323 traffic.

3. Select  and configure these settings:

Setting	Description
Enable H.460 Firewall Traversal	Allows the system to use H.460-based firewall traversal. For more information, refer to H.460 NAT Firewall Traversal on page 2-13.
NAT Configuration	Lets you specify whether the system should attempt to determine the NAT Public WAN Address automatically. • If the system is behind a NAT that allows HTTP traffic, select **Auto**. • If the system is behind a NAT that does not allow HTTP traffic, select **Manual**. • If the system is not behind a NAT or is connected to the IP network through a Virtual Private Network (VPN), select **Off**. • If the system is behind a firewalled NAT router that is UPnP™ (Universal Plug and Play) certified, select **UPnP**. Many routers used in homes and small businesses support UPnP NAT traversal. If this is your situation, try selecting **UPnP** first. If this selection does not work for your router, select **Auto** or **Manual**.
NAT Public (WAN) Address	Displays the address that callers from outside the LAN use to call your system. If you chose to configure the NAT manually, enter the NAT Public WAN Address here.

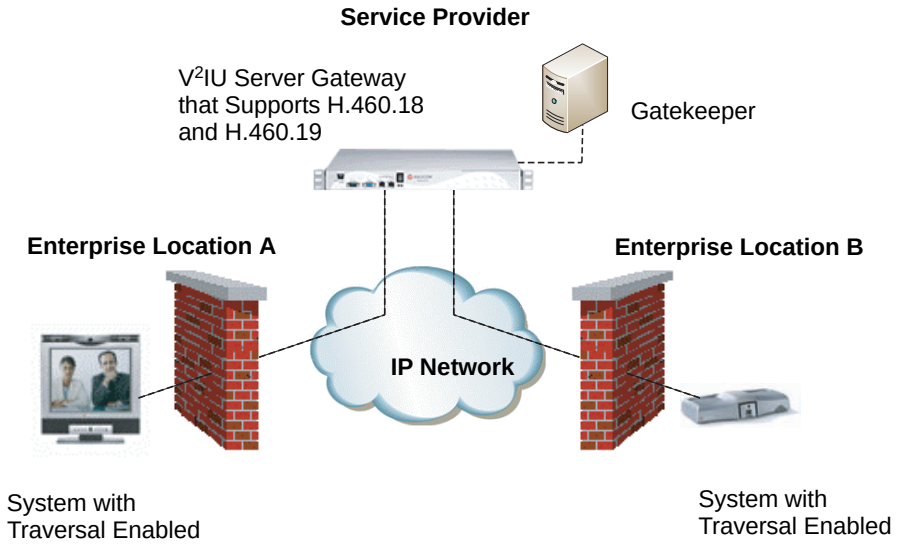
Setting	Description
NAT is H.323 Compatible	Specifies that the system is behind a NAT that is capable of translating H.323 traffic.
Address Displayed in Global Directory	Lets you choose whether to display this system's public or private address in the global directory.

Visit the Polycom Security Center at www.polycom.com for timely security information. Systems deployed outside a firewall are potentially vulnerable to unauthorized access. You can also register to receive periodic email updates and advisories.

H.460 NAT Firewall Traversal

You can configure V Series systems to use standards-based H.460.18 and H.460.19 firewall traversal, which allows video systems to more easily establish IP connections across firewalls.

The following illustration shows how a service provider might provide H.460 firewall traversal between two enterprise locations. In this example the V²IU™ traversal server gateway is on the edge of the service provider network and facilitates IP calls between systems behind different firewalls.



To use this traversal, V Series systems and firewalls must be configured as follows:

- Enable firewall traversal on the V Series system.
- Register the V Series system to an external V²IU Traversal Server Gateway that supports the H.460.18 and H.460.19 standards.

- Make sure that firewalls being traversed allow V Series systems behind them to open outbound TCP and UDP connections.
  - Firewalls with a stricter rule set should allow V Series systems to open at least the following outbound TCP and UDP ports: 1720 (TCP), 14085-15084 (TCP) and 1719(UDP), 16386-25386 (UDP).
  - Firewalls should permit inbound traffic to TCP and UDP ports that have been opened earlier in the outbound direction.
- For best interoperability, make sure that H.323 protocol-aware features are disabled on firewalls being traversed.

To enable firewall traversal on a V Series system:

1. Go to **System > Admin Settings > Network > IP > Firewall > Next**.
2. Select **Enable H.460 Firewall Traversal**.

Connecting to the ISDN BRI Network

The V500 IP with ISDN system includes an ISDN BRI network interface, which allows you to make ISDN calls.

If your site does not use an internal telephone system (PBX), you may need an NT-1 device to connect to the ISDN BRI network. A PBX or NT-1 device provides the S/T interface that the system's BRI network interface requires.

To connect the V500 IP with ISDN system to the ISDN BRI network:

1. Make sure the system is powered off.
2. Connect the BRI cable from the BRI connector on the back of the system to the ISDN or to your NT-1 device, as appropriate.
3. If you are using an NT-1 device, connect it to the ISDN.

The BRI network interface lights are located on the back of the system near the BRI connector.

When the BRI network interface...	It means...
Indicators are off	• No power to the system, or • The system is not connected to the network, or • The system is not receiving a clock signal from the network, or • The system is restarting.
Green indicator is on	The system is receiving a clock signal from the network.
Yellow indicator is on	The system is able to make a call.
Green and yellow indicators are on	• The system is receiving a software update, or • The system is operating normally.

Configuring ISDN Settings

If you have the ISDN option, you can connect your V500 system through ISDN as well as through one of the IP network connections described earlier in this chapter.

To configure the ISDN network interface settings:

1. Go to **System > Admin Settings > Network > ISDN**.
2. Configure these settings:

Setting	Description
Enable ISDN H.320	Allows this system to make H.320 (ISDN) calls.
Outside Line Dialing Prefix	Specifies the ISDN dialing prefix used to call outside the network.
ISDN Switch Protocol	Specifies the protocol used by your network's switch.
Numbering Plan	Specifies the appropriate numbering plan for your location, if it differs from the default.
ISDN Voice Algorithm	Specifies which voice algorithm (**aLaw** or **uLaw**) is used for ISDN voice calls. Do not change this setting unless you experience audio issues in all ISDN voice calls.
Auto BRI Configuration	Allows the NI-1 switch to automatically configure the directory numbers and SPIDs. This setting is only available if you have selected the NI-1 switch protocol.

3. Select and configure these settings:

Setting	Description
Area Code	Specifies the area code for this system's location.
Directory Numbers	Specifies the numbers assigned to the B1 and B2 channels for the BRI line. The two numbers for a line may be the same or different, depending on the switch protocol in use.
Enable	Specifies whether to enable the ISDN line. If you selected Standard ETSI Euro-ISDN protocol, you must enable the BRI line.

4. If you have configured the ISDN switch protocol to be AT&T 5ESS Multipoint, NI-1, or Nortel DMS-100, select and enter the ISDN BRI SPIDs provided by your service provider.

   After you enter the SPIDs, the system verifies them. If the system is unable to verify the SPIDs, make sure the system is connected and that the ISDN numbers you entered are correct.

   If you do not have the SPIDs from your service provider, you can click **Start** to Auto-Detect SPIDs.

Configuring Call Preferences

Call preferences help you manage the network bandwidth used for calls. You can specify the default and optional call settings for outgoing calls. You can also limit the call speeds for incoming calls.

To configure call preferences:

1. Go to **System > Admin Settings > Network > Call Preference**.
2. Configure these settings on the Call Preference screen:

Setting	Description
Enable Basic Mode	Enables a limited operating mode that uses H.261 for video and G.711 for audio. This mode provides administrators with a workaround for interoperability issues that cannot be solved using other methods. The Basic Mode setting stays in effect until you change it. Basic Mode disables many system features such as content sharing, far end camera control, and advanced audio and video algorithms. Use Basic Mode only when calling systems that fail to operate properly with these advanced features.

Setting	Description
Enable H.239	Specifies standards-based People+Content data collaboration. This setting is enabled by default.
Enable IP H.323	Allows the system to make IP calls.
Enable SIP	Allows the system to use SIP when connecting IP calls.
Enable ISDN H.320 V500	Allows the system to make ISDN calls. This selection is only available when the system has ISDN networking capability.
Enable Voice Over ISDN V500	If you have the ISDN option, this allows the system to make voice-only calls to phones connected to an ISDN network, such as an organization's PBX.
Enable ISDN Gateway	Allows users to choose whether to place IP-to-ISDN calls through a gateway.

To make the enabled call types available on the Place a Call screen, you must enable the **Call Quality** setting described on page 7-4.

3. Select  and configure these settings on the Network Dialing screen:

Setting	Description
Preferred Dialing Method	Specifies the preferred method for dialing various call types. If set to **Auto**, calls use the configured Dialing Order. If set to **Manual**, the system prompts the user to select the call type from a list when placing a call.
Dialing Order	Specifies how the system places calls to directory entries that have both IP and ISDN numbers. It also specifies how the system places calls dialed manually, when the call type selection is either unavailable on the home screen or set to **Auto**. If a call attempt does not connect, the system tries to place the call using the next call type in the Dialing Order. This setting is available only when **Preferred Dialing Method** is set to **Auto**. For more information, see Configuring Dialing Order Settings on page 2-18.

4. Select to go to the Preferred Speeds screens and configure these settings:

Setting	Description
Preferred Speed for Placing Calls	Determines the speeds that will be used for calls from this system in either of these cases: • Call Quality is set to **Auto** on the home screen and **Directory** screen. • The **Call Quality** setting is not available for users. If the far-site system does not support the selected speed, the system automatically negotiates a lower speed.
Maximum Speed for Receiving Calls	Allows you to restrict the bandwidth used when receiving calls. If the far site attempts to call the system at a higher speed than selected here, the call is re-negotiated at the speed specified in this field.

5. Select to go to the Call Speeds screen and specify the call speeds to make available to users, if you are allowing them to choose speeds on a call-by-call basis.

Configuring Dialing Order Settings

If the call type on the home screen is set to a specific call type, the system does not attempt to place the call using a different call type, even if other types are listed in the Dialing Order.

You can configure the V Series system so that users can choose to place IP-to-ISDN or ISDN-to-IP calls through a gateway.

To allow users to place an IP-to-ISDN call through a gateway:

1. Make sure the system is registered with a gatekeeper.
2. Go to **System > Admin Settings > Network > Call Preference** and select **Enable ISDN Gateway**.
3. If you want to allow users to place IP-to-ISDN calls through a gateway when calling from the directory, do one of the following:
   - On the Network Dialing screen, set **Preferred Dialing Method** to **Auto** and select **ISDN Gateway** as the first choice under **Dialing Order**. With this configuration, calls placed from the directory will be placed through a gateway first if an ISDN number exists.
   - On the Network Dialing screen, set **Preferred Dialing Method** to **Manual**. With this configuration, users can select **ISDN Gateway** from the list of call types that appears when placing a call from the directory.

To allow users to place an ISDN-to-IP call through a gateway (V500 Only):

1. If you want to allow users to place ISDN-to-IP calls through a gateway when dialing manually:

   a. Make sure **Call Quality** is enabled on the Home Screen Settings screen. This setting displays the Call Type selection on the Place a Call screen.

   b. On the Network Dialing screen, select **IP Gateway** next to **ISDN** in the **Dialing Order**.

   With this configuration, users can enter the gateway address in the dialing field, along with an extension in extension field, and select **IP H.323** in the call type list.

2. If you want to allow users to place ISDN-to-IP calls through a gateway when calling from the directory, do one of the following:

   - On the Network Dialing screen, set **Preferred Dialing Method** to **Auto** and select **IP Gateway** next to **ISDN** under **Dialing Order**. With this configuration, calls placed from the directory will be placed through a gateway first if a gateway address is present in the ISDN number field and an extension is present in the Extension field.
   - On the Network Dialing screen, set **Preferred Dialing Method** to **Manual**. With this configuration, users can select **IP Gateway** from the list of call types that appears when placing a call from the directory.

3

Monitors and Cameras

Connecting the Monitor

You must connect a TV monitor to the V500 system. You can use either an NTSC or PAL monitor, depending on your system. Make sure that the system is powered off before you connect devices.

You must use the same type of video connector on the V500 system as on the monitor. For example, if you use the S-video connector on the system, use the S-video connector on the monitor.

Polycom recommends using S-video because it provides superior video quality.

Using a V700 System as the Monitor for a Computer

You can use the V700 system as a high-resolution XGA display for your computer, as shown on the system setup sheet.

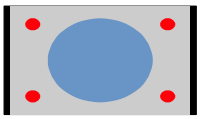
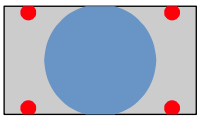
To use the V700 system as the monitor for a computer:

1. Connect the VGA cable from the VGA connector on the back of the V700 system to the VGA connector on your computer.
2. To use the system's built-in speakers for your computer's audio, connect an audio cable from your computer to the audio input connector on the left side of the V700 system.

Configuring Monitor Settings

To configure the monitor:

1. Go to **System > Admin Settings > Monitor**.
2. Configure these settings:

Setting	Description
Monitor (V500 only)	Specifies the monitor's aspect ratio: • **4:3** — Select if you are using a regular TV monitor. • **16:9** — Select if you are using a wide-screen monitor. **Note**: If you select **16:9** for the V500, you will also need to set up the monitor for full-screen display. In the monitor's setup menu, choose the setting that stretches the picture uniformly without clipping the edges, which is usually called Full, Widescreen, or 16x9. Use this setting:  Not this setting: 
PIP	Specifies PIP (Picture-in-Picture) behavior: • **On** — The PIP window stays on for the duration of the call. • **Off** — The PIP window is not displayed during the call. • **Auto** — The PIP window is displayed when a user picks up the remote. **Note:** PIP settings are also available in the User Settings screen. Users can turn the PIP on or off and change its location on the screen by pressing **PIP** on the remote control.
Display Icons in a Call	Specifies whether to display all on-screen graphics, including icons and help text, during calls.
Snapshot Timeout	Lets you choose whether to have snapshots time out after a period of four minutes. If you want to return to live video before four minutes have elapsed, press the **Near** button on the remote control twice.
Dual Monitor Emulation	Specifies whether the system can show multiple views on a single display. If content is being viewed, different views can be displayed by pressing **PIP** on the remote control.

Setting	Description
Quality Preference	Specifies the bandwidth split for People and Content video. • **Both**—50% Content, 50% People • **Content**—90% Content, 10% People • **People**—10% Content, 90% People **Notes:** When you participate in a multipoint call, the system hosting the call determines the People and Content video rates, not the system sending the content.
Output upon Screen Saver Activation (V500 only)	Specifies whether black video or no signal is sent to the monitor when the system goes to sleep and the screen saver activates. Select **Black** if you want to display screen saver text or a screen saver news feed. This is the recommended setting to prevent burn-in for TV monitors.

Using Dual Monitor Emulation

Dual Monitor Emulation is designed for rooms or offices with one monitor only. Users see both near and far sites on one monitor in two different views. During presentations, users see content and the near and far sites. What you see during a call can depend on factors such as the number of sites in the call, and whether content is being shared.

Examples of Dual Monitor Emulation

Far site Near site

Call connects

Near and far site are the same size and appear side by side.

Near site presses PIP

Size of far site window increases.

Near site presents to far site

Content, near site, and far site are displayed with Dual Monitor Emulation.

Using Dual Monitor Emulation in a Call

During calls using Dual Monitor Emulation without content, users can press the PIP button on the remote control to scroll through the following screen layouts:

1. Near and far sites, same size, side by side
2. Far site big, near site small
3. Near site big, far site small
4. Near site, full screen
5. Far site, full screen

The last layout viewed is used for the next call.

Adjusting the Monitor's Color Balance, Sharpness, and Brightness

In most cases, the monitor you connect to your system may be set to a configuration that is appropriate for video conferencing applications. Depending on your environment and model of monitor, however, the video may exhibit one of these problems:

- Picture is too dark or too bright
- Colors appear faded
- Picture has too much of one color — for example, the picture may appear greenish
- Picture has blocky or softened edge detail

If you notice any of these problems, adjust the monitor until the display seems acceptable. Use the video diagnostics test as described in the following steps, or purchase a calibration program DVD tool to help you fine-tune the display settings.

To adjust the monitor for natural color:

1. Go to **System > Diagnostics > Video**.
2. Select the color bars icon to display the color bar test screen.
3. Adjust the color using the monitor's controls for color, contrast, and brightness. Your monitor may also have controls for tint and temperature.

   The colors from left to right should be white, yellow, cyan, green, magenta, red, and blue. Make sure that the white is not tinted red, green, or blue, and that the red is not tinted pink or orange.

4. When the colors look right on the test screen, press **Near** on the remote control to stop the color bars test and show video of the room.
5. If the color appears natural, you do not need to make further adjustments.

   If the color still needs adjustment, use the monitor's controls to make small adjustments until the picture appears natural.

Preventing Monitor Burn-In

Monitors and V Series systems provide display settings to help prevent image burn-in. Plasma televisions can be particularly vulnerable to this problem. Refer to your monitor's documentation or manufacturer for specific recommendations and instructions. The following guidelines help prevent image burn-in:

- Set **Output upon Screen Saver Activation** to **Black**.
- Use the monitor's burn-in prevention features, if available.
- Ensure that static images are not displayed for long periods.
- Set the **Screen Saver Wait Time** to 3 minutes or less.
- To keep the screen clear of static images during a call, disable the following settings:
  - **Display Icons in a Call** described on page 3-2
  - **Display Time in Call** described on page 6-1
  - **Far Site Name Display Time** described on page 6-2
- Be aware that meetings that last more than an hour can have the same effect as a static image.
- Consider decreasing the monitor's sharpness, brightness, and contrast settings if they are set to their maximum values.

Configuring Camera Settings

To configure camera settings:

1. Go to **System > Admin Settings > Camera**.
2. Configure these settings:

Setting	Description
Backlight Compensation	Specifies whether to have the camera automatically adjust for a light background. Backlight compensation is best used in situations where the subject appears darker than the background.
Camera Brightness	Specifies how much light is let into the camera's iris. A low number allows in less light; a high number allows in more light.
Power Frequency	Specifies the frequency of the electrical power used for the system. This helps to eliminate video flicker. Typically, the default setting is correct for your system and location. • **50 Hz** — Select if you have a PAL system. • **60 Hz** — Select if you have an NTSC system.

4

Microphones and Speakers

Connecting Speakers or Headphones

You can connect desktop speakers to provide better audio for the V700 system if you place it in a large room, or you can connect headphones to listen to calls privately. The system's speaker connector is on the system's right side panel, and the headphone connector is on the front of the system.

Refer to your system's setup sheet for connection details. Make sure that the system is powered off before you connect devices to it.

Configuring Audio Settings

V500 System

To configure general audio settings on a V500 system:

1. Go to **System > Admin Settings > Audio.**
2. Configure these settings:

Setting	Description
Master Audio Volume	Sets the volume level for audio from the far site.
Sound Effects Volume	Sets the volume level of the ring tone and user alert tones.
Incoming Video Call	Specifies the ring tone used for incoming calls.
User Alert Tones	Specifies the tone used for user alerts.
Bass	Sets the volume level for the lower frequencies without changing the master audio volume.

Setting	Description
Treble	Sets the volume level for the higher frequencies without changing the master audio volume.
Mute Auto-Answer Calls	Specifies whether to mute incoming calls. Incoming calls are muted by default until you press the **Mute** button on the remote control.
Enable Internal Ringer	Specifies an additional ring tone when receiving an incoming call. The internal ringer is built into the system and alerts you to incoming calls.

V700 System

To configure general audio settings on a V700 system:

1. Go to **System > Admin Settings > Audio.**
2. Configure these settings:

Setting	Description
Sound Effects Volume	Sets the volume level of the ring tone and user alert tones.
Incoming Video Call	Specifies the ring tone used for incoming calls.
User Alert Tones	Specifies the tone used for user alerts.
Mute Auto-Answer Calls	Specifies whether to mute incoming calls. Incoming calls are muted by default until you press the **Mute** button on the remote control.
Enable Internal Ringer	Specifies an additional ring tone when receiving an incoming call. The internal ringer is built into the system and alerts you to incoming calls.
Enable Live Music Mode	Specifies whether the system transmits audio using a configuration that best produces live music picked up by microphones. **Note**: Noise suppression and automatic gain control are disabled when this setting is enabled.
Enable Polycom StereoSurround	Specifies that Polycom StereoSurround™ is used for all calls.
Enable Polycom Microphones	Specifies whether integrated V700 system microphones are enabled.

3. Select  and configure these settings:

Setting	Description
Master Audio Volume	Sets the volume level for audio from the far site.
Bass	Sets the volume level for the lower frequencies without changing the master audio volume.
Treble	Sets the volume level for the higher frequencies without changing the master audio volume.

5

Content and Closed Captions

Configuring Content Display with People+Content IP

People+Content IP is optional for the V Series system. It enables a presenter to show content from a computer to other sites in a video conference using only an IP network connection.

The presenter can show PowerPoint® slides, web pages, spreadsheets, or any other type of content that runs from a computer. Supported resolutions include 640x480, 800x600, 1024x768, and 1280x1024.

Before a presenter can use a computer to show content with People+Content IP, you need to:

- Enable People+Content IP on the V Series system.

  When you purchase this option, you receive a software activation key. This key allows you to enable People+Content IP on a V Series system.

- Download the People+Content IP software application from the Polycom web site to the computer(s) that the presenter will use to show content.

  You don't need to change the computer resolutions and you don't need special cables or hardware, but the computer(s) must meet these requirements:

  – Operating System: Windows 2000, Windows XP Home, or Windows XP Professional

  – Minimum computer: 500 MHz Pentium® III (or equivalent); 256 MB memory
  Recommended computer: 1 GHz Pentium III (or equivalent); 512 MB memory

  Note that, although you can use the license key on only one V Series system, you can install the presenter software on an unlimited number of computers.

- Connect the computer(s) to the IP network.

For information about purchasing the People+Content IP option, please contact your Polycom distributor.

To enable People+Content IP on a V Series system:

1. On a computer, open a web browser and go to the Polycom web site at http://www.polycom.com/support/video.
2. Enter your user login information to enter the web site, or click **New User** to create a new account, if needed.
3. Enter the license key you received when you purchased the People+Content IP option.
4. Enter the serial number of the V Series system onto which you want to install People+Content IP. You will then receive a People+Content IP software activation key.
5. Go to **System > Admin Settings > General Settings > Options** on the V Series system.
6. Enter the People+Content IP software activation key.

To install the People+Content IP application on a computer:

1. On a computer with Windows XP or Windows 2000, open a web browser and go to the Polycom web site at www.polycom.com.
2. Select **Downloads & Documentation** from the Quick Links menu.
3. Under Downloads, select **Video** as the Category, and select the appropriate V Series system under Products.
4. Download and install the People+Content IP software.

For information about showing content using People+Content IP, refer to the *Getting Started Guide for the V Series* at www.polycom.com/videodocumentation.

Configuring Closed Captioning

You can provide real-time text transcriptions or language translations of the video conference by displaying closed captions on your system. When you provide captions for a conference, the captioner may be present, or may use a telephone or web browser to listen to the conference audio. When the captioner sends a unit of text, all sites see it on the main monitor for 15 seconds. The text then disappears automatically.

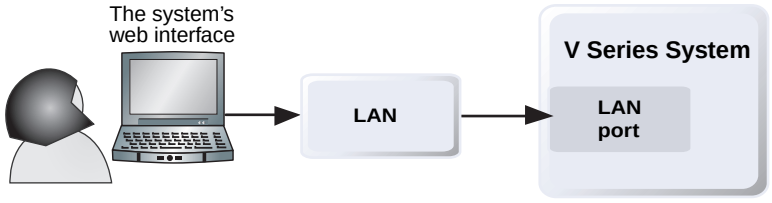
Captions can be provided in any language that uses the Latin alphabet.

The captioner can enter caption text in one of these ways:

- In the room or remotely, using the system's web interface
- In the room or remotely, using a Telnet session

Via the System's Web Interface

Closed captioners can provide captions from inside the conference room, or from a remote location, by entering the captions directly into the system's web interface, as shown in the following diagram.

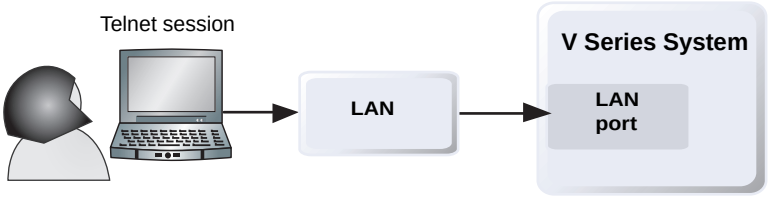


To supply closed captions for a conference using the system's web interface:

1. On a computer, open a web browser.
2. In the browser address line, enter the IP address of the system, for example, `http://10.11.12.13`) to go to the system's web interface.
3. Go to **Utilities > Closed Caption**.
4. Log in using this information:
   - **User Name:** Your name.
   - **Password:** Meeting password defined for your video conferencing system.
5. In the Closed Caption screen, type the caption text into the text field. Text wraps to the next line after 32 characters.
6. Press **Enter** to send the text to the sites in the conference.

Via a Telnet Session

Closed captioners can provide captions from inside the conference room, or from a remote location, by entering captions via a Telnet session, as shown in the following diagram.



To supply closed captions for a conference using a Telnet session:

1. On a computer, open a command line interface.
2. Start a Telnet session using the V Series system IP address and port 24, for example, `telnet 10.11.12.13 24`.
3. Enter the command `cc` to start captioning.
4. Press **Enter** to send the text.
5. To stop sending closed captions, press **Ctrl-Z**.

6

Calling and Answering

Configuring Call Settings

The Call Settings screens provide access to high-level options for the entire system. For convenience, some of the User Settings options are repeated on these screens.

To configure call settings:

1. Go to **System > Admin Settings > General Settings > System Settings > Call Settings**.
2. Configure these settings:

Setting	Description
Maximum Time in Call	Enter the maximum number of minutes allowed for call length. When that time has expired, you see a message asking you if you want to hang up or stay in the call. If you do not answer within one minute, the call automatically disconnects. If you choose to stay in the call at this time, you will not be prompted again. Choosing 0 removes any limit.
Auto Answer Point-to-Point Video	Specifies whether to answer incoming point-to-point calls automatically.
Display Time in Call	Specifies whether to display the elapsed time or the local time during a call. You can also choose not to display the time.

Setting	Description
Call Detail Report	Specifies whether to collect call data for the Call Detail Report and Recent Calls list. When selected, information about calls can be viewed through the system's web interface and downloaded as a .csv file. **Note:** If this setting is disabled, the Call Detail Report (CDR) will stop recording new entries for any calls placed or received. As a result, applications that retrieve the CDR, such as the CDR synchronization feature of the Polycom Global Management System will no longer reflect new call activity.
Recent Calls	Specifies whether to display the **Recent Calls** button on the home screen. The Recent Calls screen lists the site number or name, the date and time, and whether the call was incoming or outgoing. **Note:** If the Call Detail Report option is not selected, the Recent Calls option is not available.
Far Site Name Display Time	Turns the far site name display on or off, or specifies the time period the far-site name appears on screen when calls first connect.

Setting the Call Answering Mode

To set the call answering mode:

1. Go to **System > Admin Settings > General Settings > System Settings > Call Settings**.
2. Select **Auto Answer Point-to-Point Video**.
3. Select one of the following:
   - **Yes** – Answers calls automatically.
   - **No** – Enables you to answer calls manually.
   - **Do Not Disturb** – Refuses incoming calls automatically. The caller receives a message that the site is unavailable.

   If you have a V700 system that you are using as your computer monitor, Polycom recommends that you set up the system so that you have to answer calls manually. If you receive a call while using the system as a computer, you hear a ringing sound and you can switch to video to answer the call manually. Alternatively, you can ignore the call and it will not connect, thereby preventing the caller from seeing or hearing you at your desk.

Configuring Directory Settings

To configure system settings:

1. Go to **System > Admin Settings > General Settings > System Settings > Directory**.
2. Configure these settings:

Setting	Description
System Name	Enter or change the system name in this field. This name appears on the screen for the far site when you are making calls.
Localized System Name	Displays the localized system name, if you have entered one. You can enter a **Localized System Name** for Simplified Chinese on this screen using the Chinese Virtual Keyboard. You must use the system's web interface to enter localized system names for other languages. The localized system name is sent to the far site and displayed as the caller ID by V Series systems running version 8.0 or later, when the user interface is set to that language. However, the English/Pinyin name is the name used by the Global Directory Server and the gatekeeper, and it is also the name that shows up in the Recent Calls list.
Allow Directory Changes	Specifies whether users can save changes they make to the directory.
Confirm Directory Additions Upon Call Disconnect	Specifies whether users are prompted to confirm new directory entries when saving the information for the last site called.
Confirm Directory Deletions	Specifies whether users are prompted to confirm deletions of directory entries.

Creating a Localized System Name with the System's Web Interface

Localized system names are sent to the far site and displayed as the caller ID by V Series systems using version 8.0 or later. When you enter a localized system name, it is also entered in English/Pinyin. The English/Pinyin name is the name used by the Global Directory Server, the gatekeeper, and other systems that do not support this feature, and it is also the name that shows up in the Recent Calls list.

To create a localized system name using the system's web interface:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address, for example, `http://10.11.12.13`, to go to the system's web interface.
3. Go to **Admin Settings > General Settings > System Settings**.
4. Enter the localized system name in the appropriate language field.

Managing Directories with the System's Web Interface

The system's web interface import/export directory feature allows you to efficiently maintain consistency of system directories. It is particularly useful if you are managing multiple systems that call the same locations. You can:

- Transfer existing directory entries between systems
- Develop directory entries on one system, save them to your computer, and then distribute them to other systems
- Create localized directory entries

Only local directories can be downloaded. The directory file is in .csv format.

To export a V Series system directory to your computer:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address, for example, `http://10.11.12.13,` to go to the system's web interface.
3. Go to **Utilities > Import/Export Directory**.
4. Click **V500 -> PC or V700 -> PC** to export the .csv file to the computer.
5. Save the file to a location on your computer.

To import V Series system directory entries to the V Series system:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address, for example, `http://10.11.12.13`, to go to the system's web interface.
3. Go to **Utilities > Import/Export Directory**.
4. Click **PC -> V500** or **PC -> V700**.
5. Click **Browse** and browse to the location of the .csv file on your computer.
6. Import the .csv file to the V Series system.

To create a localized directory entry using the system's web interface:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address, for example, `http://10.11.12.13`, to go to the system's web interface.
3. Go to **Place a Call > Directory**.

   Edit an entry to enter a localized directory entry name in the **Localized Name** field, and specify the language for the localized directory entry.

Configuring the Global Directory

The global directory provides a list of other systems that are registered with the Global Directory Server and are available for calls. The other systems appear in the directory, allowing you to place calls to other users by selecting their names.

To configure the Directory Server settings:

1. Go to **System > Admin Settings > Global Services > Directory Servers**.
2. Configure these settings:

Setting	Description
Global Directory (GDS)	Specifies the IP address or DNS address of the Global Directory Server. If you specify a Polycom CMA system here, the system cannot register to other servers. If you specify another Global Directory Server, you can enter up to five addresses.
Password	Lets you enter the global directory password, if there is one.
Register	Registers this system with the Global Directory Server.
Display Global Addresses	Displays other registered systems in the global directory.
Display Name in Global Directory	Specifies whether to display the system's name in the global directories of other registered systems.

Setting	Description
Save Global Directory to System	Copies the global directory to this local system. When this setting is enabled: • Polycom V700 systems that are registered to a Polycom CMA system can display up to 5000 global directory entries. • Polycom V700 systems that are registered to other Global Directory Servers can display up to 4000 global directory entries. • Polycom V500 systems can display no more than 1000 entries. When this setting is disabled: • Polycom V700 systems can display no more than 1000 entries. • Polycom V500 systems can display no more than 1000 entries.
Group Name	Specifies the group name used for global directory entries in the local directory. In the directory, entries from Global Directory Servers are listed in the **Polycom GDS** group.

Configuring Streaming Calls

You can configure the V700 system to allow users to stream audio and video from one to many viewers. Viewers watch the conference (people video only) from their computers, as the meeting is taking place. You can start streaming before or during a call.

Points to note about streaming on the V700 system:

- If a password is set on the system, streaming participants must enter it before receiving the stream.
- Participants must have the Apple QuickTime player installed on their computer to view the stream.
- To send a stream across a subnet, multicasting must be enabled on the network or you must unicast to a particular IP address, which will forward the stream to that IP address regardless of the location destination.
- The number of viewers is limited only by your network topology.
- For security reasons, you cannot start streaming from the system's web interface.
- Streaming provides video at a reduced frame rate.

To configure the V700 system for a streaming call:

1. Go to **System > Admin Settings > Network > IP > Streaming**.
2. Configure these settings:

Setting	Description
Allow Streaming	Specifies whether users can start streaming from the system by making the Start Streaming option available on the Utilities screen.
Enable Streaming Announcement	Specifies whether the names of users logged on to the streaming system are displayed on screen.
Speed	Specifies the speed used for the streaming call.
Number of Router Hops (TTL)	Specifies the number of routers the data can traverse before it is no longer passed on. For example, when set to 1, the data stays within a subnet.
Audio Port	Specifies the fixed port used for audio. This can be changed if you need to go through a firewall.
Video Port	Specifies the fixed port used for video. This can be changed if you need to go through a firewall.
IP Multicast Address	Specifies the multicast address used for the stream. The default address is based on your system serial number but can be changed, if required. This could be the unicast location of your streaming server.

To stream a conference from the V700 system:

1. Go to **System > Utilities > Web Streaming**.
2. Select the **Start Streaming** option to begin streaming.
3. Place the video call to other participants.

You can start streaming before or during a call.

To stop streaming a conference from the V700 system:

1. Go to **System > Utilities> Web Streaming**.
2. Clear the **Start Streaming** selection.

To view a streamed conference on the V700 system:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address, for example, `http://10.11.12.13`, to go to the system's web interface.
3. Click **Utilities > View a Meeting**.
4. If prompted, enter the user name and password.

   The stream starts automatically.

Participants must have the QuickTime player installed on their system to view the stream.

To stop viewing the streamed conference on the V700 system:

- Close the web browser.

  This stops the stream but does not end the call.

7

System Location, Appearance, and Tones

Setting Date, Time, and Location

You can update the system with regional settings, including the location-specific language and calling parameters.

To set the date, time, and location:

1. Go to **System > Admin Settings > General Settings > Location.**
2. Configure these settings on the Location screen:

Setting	Description
Country	Specifies the country where the system is located. Changing the country automatically adjusts the country code associated with your system number.
Language	Sets the language for the user interface.
Country Code	Specifies the country code for the system location.
Area Code Required	Specifies if an area code is required to place ISDN calls in the specified country.
ISDN International Access	Specifies the international code required for placing ISDN calls from the system location to another country.

Setting	Description
Room Telephone Number	Indicates the telephone number of the room where the system is located.
Always Dial Area Code	Specifies that calls to sites in the same area code must include the area code.
Dial 1+ for all USA calls	Specifies that calls to systems in the United States must include a "1" before the area code. **Note:** Even if you have this setting enabled, you may need to dial 1 and the area code when calling long distance over ISDN within your same area code.

3. Select  and configure these settings:

Setting	Description
Date Format and Time Format	Specifies your format preference for the date and time display and lets you enter your local date and time.
Display Time in Call	Specifies the time display in a call: • **Elapsed Time** – Displays the amount of time in the call. • **Local Time** – Displays the local time on the screen during a call. • **Off** – Time is not displayed.

4. Select  and configure these settings:

Setting	Description
Auto Adjust for Daylight Saving Time	Specifies the daylight savings time setting. When you enable this setting, the system clock automatically changes for daylight saving time.
Time Zone	Specifies the time difference between GMT (Greenwich Mean Time) and your location.
Time Server	Specifies connection to a time server for automatic system time settings.

Customizing the Home Screen

Designing the Home Screen

Customize according to users' needs, skill levels, and environments.

Infrequent Users (Kiosk Mode)

Provide a simple workspace so no training is needed:

- Let users make calls to pre-defined numbers with one button click.
- Include instructions on screen.

Include a short list of specific items for users to select

Use the marquee to add instructions

New Users

Provide more options but keep it simple:

- Dialing entry field
- Directory numbers
- Recent Calls

Add features for users as needed

Advanced Users

Provide additional options for advanced video conferencing users:

- Call Quality (bandwidth and call type)
- User Settings, Diagnostics, and System Information
- Speed Dial list of frequently called sites
- Alerts

Add more features as users gain experience

To design the home screen:

1. Go to **System > Admin Settings > General Settings > Home Screen Settings**.
2. Configure these settings:

Setting	Description
Dialing Display	Specifies which dialing option to display: • **Dialing entry field** — Allows users to enter numbers manually. • **Display marquee** — Displays text in the dialing entry field. Can be used to display user instructions. Users cannot enter numbers manually when this option is selected. • **None** — Removes the dialing entry field from the screen.
Contact List	Specifies whether to display the contact list home screen.
Call Quality	Allows users to select the bandwidth for calls, as well as the call type, from the Place a Call screen. For information about enabling call types, see Configuring Call Preferences on page 2-16.
H.323 Extension (E.164)	Allows users to enter extensions on the home screen.
Directory	Allows users to access the directory.
System	Allows users to access the System screen, which includes User Settings, Diagnostics, and System Information. If you remove the **System** button, you can still access the System screen by navigating to the home screen, pressing ? on the remote, and selecting **System**.

3. Select  and configure these settings:

Setting	Description
System Name	Specifies whether to display the name of the system on the home screen above the PIP window.
IP or ISDN Information	Specifies whether to display the system's IP address, ISDN number, or both on the home screen.
Local Date and Time	Specifies whether to display the local date and time on the home screen.

Setting	Description
Do Not Disturb Icon	Allows users to set the system to automatically accept or ignore incoming calls using the **Do Not Disturb** button on the home screen.
Call Detail Report	Specifies whether to generate a report of all calls made with the system. When selected, all calls can be viewed through the system's web interface and downloaded as a .csv file. **Note:** If this setting is disabled, applications such as the Polycom Global Management System will not be able to retrieve Call Detail Report (CDR) records.
Recent Calls	Specifies whether to display the **Recent Calls** button on the home screen. The Recent Calls screen lists the site number or name, the date and time, and whether the call was incoming or outgoing. **Note:** If the Call Detail Report option is not selected, the Recent Calls option is not available.

4. Select  and configure these settings:

Setting	Description
Sites	Allows users to access any pre-defined sites from a My Contacts/Speed Dial list on the home screen.
Last Number Dialed	Specifies whether to display the last number dialed or clear the dialing field on the home screen.

Displaying Contacts on the Home Screen

Sites configured for speed dial are displayed on the home screen. You can also display them on the contact list home screen.

To configure speed dial sites:

1. Make sure that the site information is entered in the directory.
2. Go to **System > Admin Settings > General Settings > Home Screen Settings**.
3. Select  two times and enable **Sites**.
4. Select  to access the Sites screen.
5. Select **Add** and choose the sites to add from the directory.
6. Select either **Speed Dial** or **Contacts** as the name you want to appear on the button.

To display the contact list home screen:

1. Go to **System > Admin Settings > General > Home Screen Settings**.
2. Select **Contact List**.

Adding Marquee Text

You can create marquee text to display in the dialing entry field on the home screen. You can create context-specific instructions or, if the home screen has Site buttons, the marquee text can provide information that helps users choose which site to call.

To enter marquee text using the system's web interface:

1. Go to **System > Admin Settings > General Settings > Home Screen Settings**.
2. In **Dialing Display**, select **Display Marquee** and enter the text.

You can also add marquee text through the system's web interface. For some languages such as Russian, Korean, Japanese, Simplified Chinese, and Traditional Chinese, you must use the system's web interface to add marquee text.

To enter marquee text using the system's web interface:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address, for example, `http://10.11.12.13`, to go to the system's web interface.
3. Enter the user name and remote access password, if a password has been established.
4. Click **Admin Settings > General Settings > Home Screen Settings** and enter.
   - **Dialing Display** — Set to Display marquee.
   - **Enter Marquee Text** — Type the text to display on the home screen.
5. Click **Update**.

Changing System Appearance

Different user interface color schemes are available, allowing you to coordinate the system interface with the room décor.

To change the system appearance:

1. Go to **System > Admin Settings > General Settings > System Settings > Appearance.**
2. Configure the color scheme.

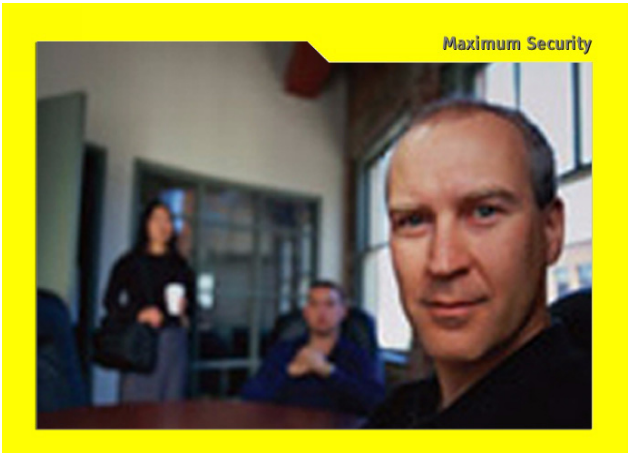
The color scheme may change to Steel Gray after upgrading a 64 MB system (V500) to software version 8.7 or later. In this case, you must change the color scheme manually to select a different color scheme.

On 64 MB systems, software version 8.7 or later provides only four choices for color schemes (Steel Gray, Ocean Blue, Midnight Gray, and ViewStation Classic).

You can allow users to change color schemes by allowing user access to the User Settings screen.

Applying the Video Overlay

You can apply a video overlay that borders the screen at the near site and that provides information for the user. To customize the video overlay, you can choose the color of the border and can enter text to display. For example, you could apply a yellow video overlay with the text, "Maximum Security," to indicate a system that you have designated as highly secure.



Whether the V Series system is or is not in a call, the video overlay and customized text both appear on the monitor displaying the near-site video, and the customized text alone appears on the screens in the user interface of the near-site system. The far site cannot see the video overlay and customized text on your system.

To apply the video overlay:

1. Go to **System > Admin Settings > General Settings > System Settings > Appearance**.
2. Enter up to 20 English-only characters in the **Overlay Name** field.
3. Configure the color of the video overlay with the **Overlay Theme** setting. The default setting is **None**.

Because the video overlay is displayed on top of the monitor image, portions of video or content might be obscured.

Setting Ring Tones and Alert Tones

To set ring tones and alert tones:

1. Go to **System > Admin Settings > Audio**.
2. Select a tone, as desired.

To set the V700 system internal ringer:

1. Go to **System > Admin Settings > Audio.**
2. Select **Enable Internal Ringer** to specify an additional ring tone when receiving an incoming call. The ringer is built into the system and will alert you to incoming calls.

Screen Savers

Adding Screen Saver Text

You can customize the V Series system to display text when the system is in sleep mode. For instance, you can display on-screen instructions to assist users with what steps they should take next.

Output upon Screen Saver Activation on the Monitors screen must be set to **Black** if you want to display screen saver text.

The screen saver text is only displayed on Monitor 1.

To enter screen saver text:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address, for example, `http://10.11.12.13`, to go to the system's web interface.
3. Enter your user name and remote access password, if a password has been established.
4. Click **Utilities > Screen Saver** and enter:
   - **Screen Saver Text** — Appears as scrolling text when the system is in sleep mode. You can use this scrolling text to provide instructions or next steps for users of the system.
   - **Logo Screen Text** — Appears underneath the logo before the system goes into sleep mode.
5. Click **Update**.

Adding a Screen Saver News Feed

You can customize the V Series system to display a news feed when the system is in sleep mode.

Output upon Screen Saver Activation on the Monitors screen must be set to **Black** if you want to display a screen saver news feed.

The screen saver news feed is only displayed on Monitor 1.

To configure a screen saver news feed:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address, for example, `http://10.11.12.13`, to go to the system's web interface.
3. Enter the user name and remote access password, if a password has been established.
4. Click **Utilities > Screen Saver**, and paste a feed URL into the **News Feed** field.
5. Click **Update**.

Adding a Screen Saver Logo

You can customize the V Series system to display your own logo instead of the Polycom logo.

The screen saver logo is only displayed on Monitor 1.

To upload a screen saver logo:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address, for example, `http://10.11.12.13`, to go to the system's web interface.
3. Enter the user name and remote access password, if a password has been established.
4. Click **Utilities > Screen Saver**, click **Next**, and follow the onscreen instructions for uploading a logo file.

Configuring the Screen Saver Wait Time

To change the screen saver wait time:

1. Go to **System > Admin Settings > General Settings > System Settings > Appearance**.
2. Configure the screen saver wait time to specify how long the system remains awake during periods of inactivity. The default is 3 minutes. Setting this option to **Off** prevents the system from going to sleep.

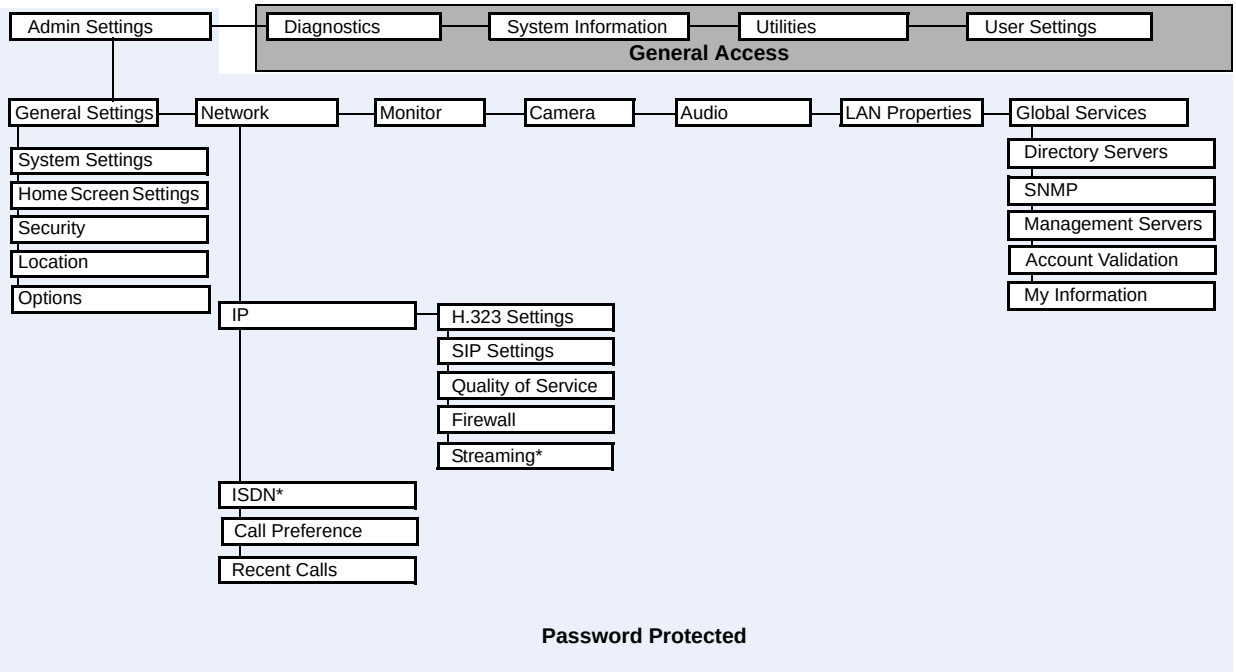
   After the specified number of minutes, the monitor displays the signal specified for the **Output upon Screen Saver Activation** setting (V500 only) described on page 3-3.

8

Security

Screens that Require the Room Password for Access

The following illustration shows which screens require the room password.



* May not be present for all system types

Configuring Security Options

To set passwords and security options:

1. Go to **System > Admin Settings > General Settings > Security.**
2. Configure these settings on the Security screen:

Setting	Description
Use Room Password for Remote Access	Specifies whether the room password and remote access password are the same.
Room Password	Enter or change the room password. When the room password is set, you must enter it to configure the system Admin Settings using the remote control. The room password must not contain spaces.
Meeting Password	Stores a password required by another system that this system calls. If a password is stored in this field, you do not need to enter it at the time of the call; the V Series system supplies it to the system that requires it. The meeting password must not contain spaces.
Remote Access Password	Enter or change the remote access password. When the remote access password is set, you must enter it to upgrade the software using Softupdate or to manage the system from a computer. The remote access password must not contain spaces.

3. Select  and configure these settings:

Setting	Description
Enable Remote Access	Specifies whether to allow remote access to the system by: • FTP • Web • Telnet • SNMP You may select any of these, or any combination of them. **Note:** The system restarts if you change the remote access settings. This setting does not deactivate the associated port, only the application. Use **Web Access Port** to disable the port.
AES Encryption	Specifies how to encrypt calls with other sites that support AES encryption. • Off—AES Encryption is disabled. • When Available—AES Encryption is used with any endpoint that supports it, even if the other endpoints in the call don't support it. This setting is available only for V700 systems. • Required for Video Calls Only—AES Encryption is used for all video endpoints in the call. Analog phone and voice over ISDN connections are allowed. Video endpoints must support AES Encryption to participate in the call. This setting is available only for 128 MB systems.
Allow Access to User Settings	Specifies whether the User Settings screen is accessible to users via the System screen. Select this option if you want to allow users to change limited environmental settings.
Allow Video Display on Web	Specifies whether to allow viewing of the room where the system is located, or video of calls in which the system participates, using the system's web interface. **Note:** This feature activates both near site and far site video displays in Web Director.
Web Access Port (http:)	Specifies the port to use when accessing the system using the system's web interface. If you change this from the default (port 80), specify a port number of 1025 or higher, and make sure the port is not already in use. You will need to include the port number with the IP address when you use the system's web interface to access the system. This makes unauthorized access more difficult. **Note:** The system restarts if you change the web access port.

Setting the Room and Remote Access Passwords

You can set the room password to restrict who can configure system Admin Settings using the remote control. You can set the remote access password to restrict who can upgrade the V Series system software using Softupdate or to restrict who can perform other remote management from a computer.

To set or change the room password:

1. Go to **System > Admin Settings > General Settings > Security.**
2. Enter or change the password.

The default room password is the 14-digit system serial number.

To set or change the remote access password:

1. Go to **System > Admin Settings > General Settings > Security.**
2. Clear the **Use Room Password for Remote Access** setting if it is selected. By default, the remote access password is the same as the room password.
3. Enter a **Remote Access** password.

To access Admin Settings using the system's web interface when a remote access password is set, enter "admin" for the user name.

To use the same password for both local and remote access:

1. Go to **System > Admin Settings > General Settings > Security**.
2. Select **Use Room Password for Remote Access**.

To reset a forgotten password:

1. Get the system's serial number from the system or from the System Information screen.
2. Go to **System >Diagnostics > Reset System.**
3. Enter the system's serial number and select **Delete System Settings.**
4. Select **Reset System.**

After the system resets, it leads you through the setup wizard. You can enter a new password when you set up the system.

Managing User Access to Settings and Features

You can manage user access to settings and features by using passwords and by configuring the system to show only those options you want your users to see.

To maintain this security level:	You can allow users to:
High (Kiosk mode)	Call only the numbers you specify on the home screen. See Designing the Home Screen on page 7-3.
Medium	Place calls using the restrictions you specify for length of call, type of call, and use of the directory.
Low	Configure user settings.
Very low	Configure all system settings.

You can allow users to change common user preferences by providing access to the User Settings screen.

To allow users to customize the workspace:

1. Go to **System > Admin Settings > General Settings > Security**.
2. Select the **Allow Access to User Settings** option to make the **User Settings** button available to users on the System screen.

User Settings contains the following options, which are also available to administrators on the Admin Settings screens:

- Backlight Compensation
- Camera Brightness
- Meeting Password
- Auto Answer Point-to-Point
- Mute Auto Answer Calls
- PIP
- Keypad Audio Confirmation
- Color Scheme
- Video Overlay
- Far Site Name Display Time
- Dual Monitor Emulation
- Allow Video Display on Web

Enabling AES Encryption

AES encryption is a standard feature on all V Series systems. When it is enabled, the system automatically encrypts calls to other systems that have AES encryption enabled.

Whenever AES Encryption is enabled, the system continually displays an icon. The icon behavior is as follows:

A lock icon in the user interface indicates whether the call is encrypted.

- In a multipoint call, the host system displays  if all connections in the call are encrypted.
- In a multipoint call, the host system displays  if one or more connections in the call are not encrypted.
- Far-end systems that are connected with encryption display  .
- Far-end systems that are connected without encryption display  .

Some connections might be encrypted while others are not. To avoid security risks, Polycom recommends that all participants communicate the state of their encryption icon verbally at the beginning of a call.

Points to note about AES Encryption:

- You cannot enable AES encryption during a call.
- AES Encryption can be configured for Required for Video Calls Only on V700 systems only.
- If you enable Security Mode before upgrading the system to version 9.0.6, this setting is automatically set to When Available but can be changed.
- If you enable Security Mode after installing version 9.0.6 the system uses Required for Video Calls Only for AES Encryption.
- AES Encryption is not supported for systems registered to an Avaya H.323 gatekeeper.

To enable AES encryption:

➢ Go to **System > Admin Settings > General Settings > Security** and set **AES Encryption**.

9

Managing the System Remotely

You can configure, manage, and monitor the system from a computer using the system's web interface. You can also use the Polycom Global Management System or SNMP.

- The system's web interface requires only a web browser.
- Polycom Global Management System requires the Global Management System application to be installed on your network.
- SNMP requires network management software on your network management station.

Using the System's Web Interface

You can use the system's web interface to perform most of the calling and configuration tasks you can perform on the local system.

Accessing the System's Web Interface

To configure your browser to use the system's web interface:

1. Be sure that you use Microsoft Internet Explorer 6 or later as your web browser and that you have Java 1.2 or later installed.
2. Configure these settings:
   - Allow cookies: Enabled
   - Force pages to reload on every visit to a page: Enabled

To access the system using the system's web interface:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address, for example, `http://10.11.12.13`, to go to the system's web interface.
3. If prompted, enter `admin` as the user name, and enter the remote access password.

You can use the system's web interface to configure all of the system settings except the remote management settings. For security reasons, these settings must be configured on the local system by an administrator.

Monitoring a Room or Call with the System's Web Interface

The monitoring feature within the system's web interface allows administrators of V Series systems to view a call or the room where the system is installed. For security reasons, this feature can only be enabled on the local system by an administrator.

To enable room and call monitoring:

1. Go to **System > Admin Settings > General Settings > Security**.
2. Select  and enable **Allow Video Display on Web** to allow the room or call to be viewed remotely.

To view a room or call:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address, for example, `http://10.11.12.13`, to go to the system's web interface.
3. Go to **Utilities > Web Director**.
4. Perform any of the following tasks:
   - Place or end a call
   - View near and far sites
   - Change PIP properties
   - Adjust system volume settings
   - Mute and unmute the microphone

You can view near and far sites without opening Web Director by selecting **Tools > Remote Monitoring**.

Managing System Profiles with the System's Web Interface

Administrators managing systems that support multiple applications can change system settings quickly and easily using profiles. You can store a V Series system profile on a computer as a .csv file using the system's web interface. There is no limit to the number of profiles you can save.

The following settings are included in a profile:

- Home screen settings
- User access levels
- Icon selections
- Option keys
- System behaviors

Passwords are not included when you store a profile.

Polycom recommends using profiles only as a way to back up system settings. Attempting to edit a stored profile or upload it to more than one system on the network can result in instability or unexpected problems.

To store a profile:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address, for example, `http://10.11.12.13`, to go to the system's web interface.
3. Go to **Utilities > Profile Center**.
4. Click **V500 —> PC** or **V700 —> PC** to download the .csv file from the V Series system.
5. Save the file to a location on your computer.

To upload a profile:

1. Reset the V Series system to restore default settings.
2. On a computer, open a web browser.
3. In the browser address line, enter the system's IP address, for example, `http://10.11.12.13`, to go to the system's web interface.
4. Go to **Utilities > Profile Center**.
5. Click **Browse** and browse to the location of the .csv file on your computer.
6. Click **PC —> V500** or **PC —> V700** to upload the .csv file to your system.

You should only apply a .csv file to a system with recently erased system flash memory.

Sending a Message

If you are experiencing difficulties with connectivity or audio, you may want to send a message to the system that you are managing.

Only the near site can see the message; it is not broadcast to the far site in the call.

To send a message via the system's web interface:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address, for example, `http://10.11.12.13`, to go to the system's web interface.
3. If prompted, enter `admin` as the user name, and enter the remote access password.
4. Go to **Diagnostics > Send a Message**.
5. In the Send a Message page, enter a message (up to 100 characters in length), then click **Send Message**.

   The message is displayed for 15 seconds on the screen of the system that you are managing.

Configuring Global Services

If your organization uses the Polycom Global Management System, you can configure, manage, and monitor the V Series system using the Global Management System server. The Global Management System is a web-based client/server software tool that allows administrators to manage a network of video conferencing systems.

Viewing the Management Servers List

On networks managed by the Global Management System, several Global Servers may be configured to manage this system remotely. The system also has a primary Global Management System server that performs account validation. You can view information about these servers, but this information can only be changed by the Global Management System Administrator.

To view the management servers list:

- Go to **System > Admin Settings > Global Services > Management Servers.**

Requiring an Account Number for Calls

If your system is set up for use with the Global Management System, the system can prompt the user to enter an account number before placing a call. The account number is added to the Global Management System's Call Detail Record (CDR) and the system's local CDR file (`localcdr.csv`), and this information can be used for call tracking and billing purposes.

If you do not configure the system to validate account numbers, calls are completed and the entered account number is recorded on the CDR. If you configure the system to validate account numbers, calls are completed only when placed using a valid account number. Account numbers are set up in Global Management System by the Global Management System administrator.

For more information about account validation, please contact your Global Management System administrator.

To require an account number for calls:

1. Go to **System > Admin Settings > Global Services > Account Validation**.
2. Specify whether to require an account number for placing calls and whether that number should be validated by the Global Management System server.

Adding Information for the Global Management System Administrator

If your system is managed by the Global Management System, you can configure the V Series system so that users can request help from the Global Management System administrator.

To configure Global Management System contact information:

1. Go to **System > Admin Settings > Global Services > My Information**.
2. Enter the contact information for the Global Management System administrator for technical support.

Valid entries for the Contact Number and Contact Fax fields in the user interface include numbers 0—9, the period (.), the asterisk (*), and the number sign (#).

To configure Global Management contact information from the system's web interface:

1. On a computer, open a web browser.
2. In the browser address line, enter the IP address of the system, for example, `http://10.11.12.13`, to go to the system's web interface.
3. If prompted, enter `admin` as the user name, and enter the remote access password.
4. Go to **Admin Settings > Global Services > My Information**.

Valid entries for the Contact Number and Contact Fax fields in the system's web interface include spaces, numbers 0—9, the period (.), the asterisk (*), and the number sign (#).

The following section illustrates the interaction between the Global Management System and the system you are configuring.

Requesting Technical Support from the Global Management System Administrator

If you need to contact the Global Management System administrator, press  on the remote control from the home screen, select **Support** and press  . The administrator receives an alert to call you at the number you specified on the My Information screen.

Setting Up SNMP

The V Series system sends SNMP (Simple Network Management Protocol) reports to indicate conditions, including the following:

- All alert conditions found on the V Series system alert page
- Details of jitter, latency, and packet loss
- Low battery power is detected in the remote control
- A system powers on
- Administrator logon is successful or unsuccessful
- A call fails for a reason other than a busy line
- A user requests help
- A telephone or video call connects or disconnects

V Series systems are compatible with SNMP version 1 and version 2c (v2c).

Downloading MIBs

To allow your SNMP management console application to resolve SNMP traps and display human-readable text descriptions for those traps, you need to install Polycom MIBs (Management Information Bases) on the computer you intend to use as your network management station.

The MIBs are available for download from the system's web interface.

To download the Polycom MIBs:

1. On a computer, open a web browser.
2. In the browser address line, enter the IP address of the system, for example, `http://10.11.12.13`, to go to the system's web interface.
3. Go to **Admin Settings > Global Services > SNMP**.
4. Click **Download MIB** and follow the onscreen instructions.

Configuring for SNMP Management

To configure the V Series system for SNMP management:

1. Access the SNMP configuration screen either in the system's web interface or on the V Series system:
   - In the system's web interface, go to **Admin Settings > Global Services > SNMP**.

– On the V Series system, go to **System > Admin Settings > Global Services > SNMP**.

2. Configure these settings:

Setting	Description
Enable SNMP	Allows administrators to manage the system remotely using SNMP.
Trap Version	Specifies the trap protocol that the system uses. • **v2c** — System uses the v2c trap. • **v1** — System uses the v1 trap.
Read-Only Community	Specifies the read-only SNMP management community in which you want to enable this system. This community is also used for traps. The default community is **public**. **Note:** Polycom does not support SNMP write operations on the V Series system.
Contact Name	Specifies the name of the person responsible for remote management of this system.
Location Name	Specifies the location of the system.
System Description	Specifies the type of video conferencing device.
Console IP Address	Specifies the IP address of the computer you intend to use as your network management station and to which SNMP traps will be sent.

Keeping Your Software Current

If you have Internet access and a software key, you can use the web-based Softupdate application to upgrade the V Series system software. If you do not have Internet access, your reseller can supply you with the V Series system software update on CD-ROM. Alternatively, you can update your software via ISDN.

Do not power off the system during the software upgrade process. If the upgrade is interrupted, the system may become unusable.

To update your software via the Internet:

1. Using a web browser, go to www.polycom.com/support/video.

2. Navigate to your product software.

   Refer to the *Release Notes* for information about the latest software version. Refer to *Updating Polycom Video Software* for detailed information about obtaining software key codes and using the Softupdate program.

3. Download the V Series system software update file in .zip format.

4. Double-click the software .zip file to extract the file.

5. Double-click **Softupdate.exe** to run the update program.

10

Control Devices

Configuring Remote Control Behavior

You can customize the behavior of the remote control to support the users' environment.

To configure remote control behavior:

1. Go to **System > Admin Settings > General Settings > System Settings > Remote Control**.
2. Configure these settings:

Setting	Description
Keypad Audio Confirmation	Specifies whether to play a voice confirmation of numbers selected with the remote control.
Remote Control Keypad	Specifies whether pressing remote control keypad buttons moves the camera to presets or generates DTMF tones. If this is set to **Presets**, users can generate DTMF tones by pressing # on the remote control while on a video screen.
Chinese Virtual Keyboard	Specifies the type of onscreen keyboard to display for Simplified Chinese. This setting is only available when the system's Language is set to Simplified Chinese.
Snap Button Option V700	Specifies alternative uses for the **Snap** button on the remote control. Choose from **Mute Speakers**, **Calendar**, **Recent Calls**, **System Info**, **Call Statistics**, or **Off**.
Use Non-Polycom Remote	Configures the system to accept input from a programmable, non-Polycom remote control. In most cases the Polycom remote works as designed, even when this feature is enabled. However, try disabling this feature if you experience difficulty with the Polycom remote.

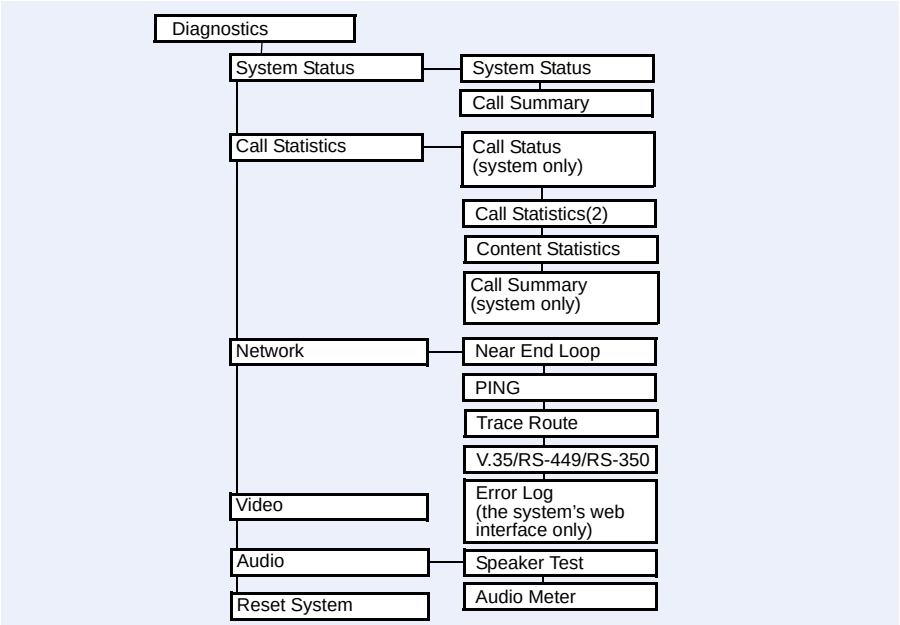
11

Statistics and Diagnostics

The V Series system provides various screens that allow you to review information about calls made by the system and to review network usage and performance.

Diagnostic Screens

The following Diagnostics screens are available on the system and in the web interface.



To access the Diagnostics screens on the system:

➢ Go to **System > Diagnostics.**

To access the Diagnostics screens from the system's web interface:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address, for example, `http://10.11.12.13`, to go to the system's web interface.
3. If prompted, enter `admin` as the user name, and enter the remote access password.
4. Click **Diagnostics** from any page in the system's web interface.

System Status

Diagnostic Screen	Description
System Status	Displays system status information, including auto-answer point to point, remote control battery, time server, global directory, IP network, gatekeeper, and ISDN BRI line. For an explanation of any of the status items, select the item and press ? on the remote. When there is a change in system status that is a potential problem, you see an alert at the bottom of the Place a Call screen.

Call Statistics

Diagnostic Screen	Description
Call Status (system only)	Displays call type, data speed, and number dialed for the current call. You can highlight the spheres on this screen to see the number dialed, the relevant status code, and details of any errors. In ISDN calls, this screen also displays connection status for each channel. Selecting a channel call progress indicator displays its ISDN number.
Call Statistics	Displays call speed, audio and video protocols, annexes, and error count for the call in progress. View Call Statistics during a call by pressing **Help** on the remote control. Call Statistics (1) • Call speed (transmit and receive) • Video protocol, annexes, and format in use (transmit and receive); the video protocol is shown in green if the system is currently using error concealment • Audio protocol in use (transmit and receive) • Number of packets lost and percentage packet loss (transmit and receive) in IP calls • Encryption type, key exchange algorithm type, and key exchange check code (if the encryption option is enabled and the call is encrypted) • Far site details and call type Call Statistics (2) • Audio and video data rates specified (transmit and receive) • Video data rate and frame rate in use (transmit and receive) • Video packet loss and jitter in IP calls • Audio packet loss and jitter in IP calls • Far site details and call type Content Statistics The Content Statistics screen shows statistics for content shared during a call, including transmit statistics for People+Content IP.
Call Summary	The Call Summary screen provides details about the calls placed by the system, including: • Duration of the last call • Total number of calls placed and received • Number, total time, and percentage of IP calls • Number, total time, and percentage of ISDN calls

Network

Diagnostic Screen	Description
Near End Loop	Tests the system's audio and video circuitry, camera and monitor. The monitor displays the video and plays the audio that would be sent to the far site in a call. This test is not available when you are in a call.
PING	Tests whether the system can establish contact with a far-site IP address that you specify. If the test is successful, the V Series system displays a message indicating that the IP address under test is available.
Trace Route	Tests the routing path between the local system and the IP address entered. If the test is successful, the V Series system lists the hops between the system and the IP address you entered.

Video

Diagnostic Screen	Description
Video Diagnostics	Tests the color settings of your monitor for optimum picture quality. If the color bars generated during the test are not clear, or the colors do not look correct, the monitor needs to be adjusted.

Audio

Diagnostic Screen	Description
Speaker Test	Tests the audio cable connections. A 473 Hz audio tone indicates that the local audio connections are correct. If you run the test from the system during a call, the far site will also hear the tone. If you run the test from the system's web interface during a call, the people at the site you are testing will hear the tone, but you will not.
Audio Meter	Measures the strength of audio signals from the system's microphone. • To check the microphone, speak into the microphone. • To check far-site audio, ask a participant at the far site to speak or call a phone in the far-site room to hear it ring. The audio meter should register between 0 and 15 dB.

Restart System

Diagnostic Screen	Description
Restart System	Cycles power to the system. When you reset the system using the remote control, the system's user interface allows you to: • Keep your system settings (such as system name and network configuration) or restore factory settings. • Keep or delete the directory stored on the system. You may wish to download the CDR and CDR archive before you reset the system. See Call Detail Report (CDR) on page 11-6.

Recent Calls

When the **Call Detail Report** setting is enabled, Recent Calls shows a list of up to 99 calls made by the system. It includes the following information:

- Site name or number
- Date and time
- Call in or out

The Recent Calls list shows incoming and outgoing calls that connect, as well as outgoing calls that do not connect.

If Do Not Disturb has been enabled, any incoming calls attempted by other sites will not be listed.

The home screen can be configured to include Recent Calls. For more information about including the Recent Calls list on the home screen, see Designing the Home Screen on page 7-3.

To view the Recent Calls screen:

➢ Go to **System > Admin Settings > Network > Recent Calls.**

You can see more detail about any call by highlighting an entry and pressing **Help** on the remote control. Information includes the far site's number and name, and the type, speed (bandwidth), and duration of the call.

If you need even more detail about calls, you can download the Call Detail Report (CDR) from the system's web interface. For more information about the CDR, see Call Detail Report (CDR).

Call Detail Report (CDR)

When enabled, the Call Detail Report (CDR) provides the system's call history. You can view the CDR from the system's web interface. Within 5 minutes of the end of the call, the CDR is written to memory and then you can download the data in CSV format for sorting and formatting. CSV (Comma Separated Value) files can be imported into spreadsheet and database programs.

Every call that connects is added to the CDR, whether it is a call that you make or that you receive. If a call does not connect, the report shows the reason.

The CDR does not include incoming calls that the V Series system does not answer, so if calls were missed while Do Not Disturb was enabled, details will not be included in the CDR.

To view and download the CDR via the system's web interface:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address (for example, `http://10.11.12.13`) to go to the system's web interface.
3. Enter `admin` as the user name, and the remote access password, if a password has been established.
4. Click **Utilities > Call Detail Report** to view the details of the file.
5. Click **Save** and then specify a location on your computer to save the file.

As an added security feature, downloading the CDR file with the format xxx.xxx.xxx.xxx/localcdr.csv requires a user name and password in VSX® system software version 8.5.2 and later.

The CDR format includes quotation marks in version 8.7 and later; this change allows the use of commas and other special characters in the data fields and helps to retain the integrity of the CDR data.

Information in the CDR

The following table describes the data fields in the CDR.

Data	Description
Row ID	Each call is logged on the first available row. A call is a connection to a single site, so there may be more than one call in a conference.
Start Date	The call start date, in the format dd-mm-yyyy.
Start Time	The call start time, in the 24-hour format hh:mm:ss.
End Date	The call end date.
End Time	The call end time.
Call Duration	The length of the call.
Account Number	If Require Account Number to Dial is enabled on the system, the value entered by the user is displayed in this field.
Remote System Name	The far site's system name.
Call Field Number 1	The number dialed from the first call field, not necessarily the transport address. For incoming calls — The caller ID information from the first number received from a far site.

Data	Description
Call Field Number 2 (If applicable for call)	For outgoing calls — The number dialed from the second call field, not necessarily the transport address. For incoming calls — The caller ID information from the second number received from a far site.
Transport Type	The type of call — Either H.320 (ISDN) or H.323 (IP).
Call Rate	The bandwidth negotiated with the far site.
System Manufacturer	The name of the system manufacturer, model, and software version, if they can be determined.
Call Direction	In — For calls received. Out — For calls placed from the system.
Conference ID	A number given to each conference. A conference can include more than one far site, so there may be more than one row with the same conference ID.
Call ID	Identifies individual calls within the same conference.
Total H.320 Channels Used	The total number of ISDN B channels used in the call. For example, a 384K call would use six B channels.
Endpoint Alias	The alias of the far site.
Endpoint Additional Alias	An additional alias of the far site.
Endpoint Type	Terminal, gateway, or bridge.
Endpoint Transport Address	The actual address of the far site (not necessarily the address dialed).
Audio Protocol (Tx)	The audio protocol transmitted to the far site, such as G.728 or G.722.1.
Audio Protocol (Rx)	The audio protocol received from the far site, such as G.728 or G.722.
Video Protocol (Tx)	The video protocol transmitted to the far site, such as H.263 or H.264.
Video Protocol (Rx)	The video protocol received from the far site, such as H.261 or H.263.
Video Format (Tx)	The video format transmitted to the far site, such as CIF or SIF.
Video Format (Rx)	The video format received from the far site, such as CIF or SIF.
Disconnect Reason	The description of the Q.850 (ISDN) cause code showing how the call ended.
Q.850 Cause Code	The Q.850 cause code showing how the call ended.

Data	Description
Total H.320 Errors	The number of errors during an H.320 call.
Average Percent of Packet Loss (Tx)	The combined average of the percentage of both audio and video packets transmitted that were lost during the 5 seconds preceding the moment at which a sample was taken. This value does not report a cumulative average for the entire H.323 call. However, it does report an average of the sampled values.
Average Percent of Packet Loss (Rx)	The combined average of the percentage of both audio and video packets received that were lost during the 5 seconds preceding the moment at which a sample was taken. This value does not report a cumulative average for the entire H.323 call. However, it does report an average of the sampled values.
Average Packets Lost (Tx)	The number of packets transmitted that were lost during an H.323 call.
Average Packets Lost (Rx)	The number of packets from the far site that were lost during an H.323 call.
Average Latency (Tx)	The average latency of packets transmitted during an H.323 call based on RTCP, calculated from sample tests done once per minute.
Average Latency (Rx)	The average latency of packets received during an H.323 call based on RTCP, calculated from sample tests done once per minute.
Maximum Latency (Tx)	The maximum latency for packets transmitted during an H.323 call based on RTCP, calculated from sample tests done once per minute.
Maximum Latency (Rx)	The maximum latency for packets received during an H.323 call based on RTCP, calculated from sample tests done once per minute.
Average Jitter (Tx)	The average jitter of packets transmitted during an H.323 call, calculated from sample tests done once per minute.
Average Jitter (Rx)	The average jitter of packets received during an H.323 call, calculated from sample tests done once per minute.
Maximum Jitter (Tx)	The maximum jitter of packets transmitted during an H.323 call, calculated from sample tests done once per minute.
Maximum Jitter (Rx)	The maximum jitter of packets received during an H.323 call, calculated from sample tests done once per minute.

Call Detail Report Archives

Calls are added to the CDR until the file size reaches 50 KB, which is equivalent to about 150 calls. The system then automatically archives the CDR and creates a new CDR file. If an archive is already present, the new archive overwrites it.

The CDR starts with Row 1, but the conference numbers continue from the file most recently archived. Conference numbering restarts at 1 after the system assigns conference number 100,000.

To get an archived CDR:

1. From your computer, open an FTP client.
2. FTP into the V Series system.
3. Enter this FTP command:

   ```
   GET localcdr_archive.csv
   ```

4. Close your FTP session.

12

Troubleshooting

Placing a Test Call

When you finish configuring the system, you can use one of the sample numbers in the directory to test your setup.

To place a test call:

1. On the **Place a Call** screen, select **Directory**.
2. Select **Group**.
3. Select **Sample Sites** and highlight a location.
4. Press **Call** on the remote control.

You can also find a list of worldwide numbers that you can use to test your V Series system at www.polycom.com/videotest.

If you have trouble making video calls:

- Make sure the number you dialed is correct, then try the call again. For example, you may need to dial 9 for an outside line or include a long distance access code or country code.
- To find out if the problem exists in your system, ask the person you were trying to reach to call you instead.
- Find out if the system you are calling has its power turned on and is functioning properly.
- If you can make calls but not receive them, make sure that your system is configured with the correct number.

Enabling Basic Mode

Basic Mode is a limited operating mode that uses H.261 for video and G.711 for audio. It provides administrators with a workaround for interoperability issues that cannot be solved using other methods. The Basic Mode setting stays in effect until you change it. The Call Statistics screen indicates whether the system is operating in Basic Mode

Basic Mode disables many system features such as content sharing, far-site camera control, and advanced audio and video algorithms. Use Basic Mode only when calling systems that fail to operate properly with these advanced features.

To enable Basic Mode using the system's web interface:

1. On a computer, open a web browser.
2. In the browser address line, enter the system's IP address (for example, `http://10.11.12.13`) to go to the system's web interface.
3. Go to **Admin Settings > Network > Call Preference > Call Preference**.
4. Select **Enable Basic Mode**.

To enable Basic Mode in the Polycom V Series system interface:

1. Go to **System > Admin Settings > Network > Call Preferences**.
2. Select **Basic Mode**.

To view the Basic Mode indicator:

1. Go to **System > Diagnostics > Call Statistics**.
2. Select  .
3. View the Call Type field.

   "(Basic Mode)" is appended to the data in the Call Type field when the VSX system or V Series system is operating in Basic Mode.

General Troubleshooting

This section presents problems, likely causes, and corrective actions. It is organized by category to help you troubleshoot any issue.

- Power and Start-up
- Controls
- Access to Screens and Systems

- Calling
- Display
- Audio
- Error Indications

Power and Start-up

Symptom	Problem	Corrective action
The system does not start or respond in any way.	The power switch is off. **Note**: The V700 system has three power switches.	Turn on the power switches for the system and all equipment connected to it.
	The power cord is not connected.	Make sure the power pack is connected to a power outlet, and that its power cords are seated securely.
	The power outlet is not active, or the system's power supply is not operating properly.	If you connect the system's power cord to a power strip, be sure the power strip is connected to a power outlet and its power switch is on. Check the power outlet by unplugging the system and plugging in a lamp, radio, or other small appliance. If it does not operate, the outlet is not active — connect the system to a different outlet. If the outlet is active, the problem could be in the system's power supply. In this case, call Polycom Technical Support and arrange to return the system for service.
The system starts in the software update screen.	The system software is corrupted or not loaded properly.	Load the system software from your computer. For instructions on how to do this, see Keeping Your Software Current on page 9-8.
The system restarts over and over again.	The power plug is not fully seated.	Make sure the power plug is seated securely.
	The socket is corroded.	Unplug and reseat the power plug 5 times.
	The power plug is damaged or the power supply is bad.	Call Polycom Technical Support and arrange to return the system for service.
The system locks up upon restart.	You assigned a a static IP address of xxx.xxx.xxx.255 (for example, 172.26.145.255).	**1.** Disconnect the network cable, power off the system, and restart the system. The system now has a static IP address of 0.0.0.0. **2.** Configure the system to obtain a different static IP address via DHCP. **3.** Reconnect the network cable, and restart the system.

Controls

Symptom	Problem	Corrective action
The system does not respond to the remote control.	No, low, or dead batteries in the remote control.	Install three AAA batteries in the remote control.
	The batteries are installed incorrectly in the remote control.	Insert the batteries in the correct +/- position.
	The room lights operate in the 38 Khz range and interfere with the remote control signals.	Turn off the lights in the room and try the remote control again.
	The infrared sensor is not receiving signals from the remote control.	To check the remote control: Point the remote control directly at the camera and press a button. If the light on the system flashes, the remote control works properly. Make sure the transparent protective strip has been removed from the infrared sensor on the front of the system. Make sure you are pointing the remote control at the infrared sensor on the front of the system or the camera.
The monitor screen remains blank when you pick up the remote control.	The monitor's power cord is not plugged in.	Connect the monitor's power cord and then power on the monitor.
	The monitor is powered off.	Power on the monitor.
	The monitor is not connected correctly to the system.	Verify that the monitor is connected correctly according to the installation procedures in Connecting the Monitor on page 3-1.
	The monitor is not set to use the signal input that is connected to the V500 system.	On the monitor, change the signal input. The image may take a few seconds to synchronize after you select the signal input that is connected to the V500 system.
A change in the Directory is not saved.	If you edit an entry and then press **Home** on the remote, you are prompted to save your change, but the change is not saved.	Choose **Save** first before you press **Home**.

Access to Screens and Systems

Symptom	Problem	Corrective action
Cannot navigate to Admin screens — System button is not displayed.	The home screen is not configured to display the **System** button.	Press the ? button on the remote and select **System** at the end of the help message, or access the system remotely using the system's web interface, FTP, Telnet, or SNMP. From the system's web interface, you can add the **System** button back to the home screen. Click **System Setup** and navigate to **Admin Settings > General Settings > Home Screen Settings**, then select **System**. The change takes effect after you navigate away from the home screen and then back again on the system.
Cannot navigate to Admin screens without a password.	The system administrator has set a password, or The default password was not deleted.	Enter the password. The default password is the system's serial number.
Cannot access the system remotely.	The system does not allow remote access.	On the system, go to **Admin Settings > General Settings > Security >** and enable access.
	The system or your computer is not connected to the LAN.	Check the LAN cable to the LAN port on the rear of the system. Check the LAN cable to your computer.
	The LAN cable to the system or to your computer is bad. To verify this, check the lights on the system. There should be a steady green light indicating a connection to the LAN, and a flashing orange light indicating LAN traffic if the cable is good.	Replace the appropriate LAN cable.
	DHCP Client is ON and no DHCP server is available.	Contact your network administrator.
	There is a firewall between your computer and your system.	Contact your network administrator.
	Your computer is on a different network and there is not connectivity between the networks.	Place your computer and system on the same subnet. If this corrects the problem, check your router configuration. If it does not, contact your network service provider.

Symptom	Problem	Corrective action
Cannot manage the system remotely.	You have not entered the correct password.	Enter the correct user name and remote access password. **Note**: For web access, the user name is **admin**, and the default password is the unit's serial number.
	Too many managers are logged into the system.	Only five system managers are allowed at any one time. To log everyone out, restart your system.
Cannot connect to the Directory Server.	The system does not automatically reconnect to the Directory Server when a network cable is unplugged and reconnected.	Recheck **Register** on the Global Directory Servers screen (**System > Admin Settings > Global Services > Directory Servers**) to manually reconnect to the Directory Server.

Calling

Symptom	Problem	Corrective action
Error message occurs when placing an IP (H.323) call.	The system is not connected to the LAN.	Verify that the LAN cable is connected properly.
	The system's LAN cable is bad.	Replace the system's LAN cable.
	The far site is not connected.	Use the PING test (**System > Diagnostics > Network > PING**) to determine whether the far site is accessible to your system. If the test fails, the far site system is unavailable.
	The system is not configured correctly for the network.	Check your IP configuration.
	The IP Gateway/Gatekeeper is not operating or is not configured correctly.	Contact the gatekeeper/gateway administrator.
	Calls do not connect.	Use the PING test (**System > Diagnostics > Network > PING**) to determine whether the far site is an H.323 device. If it is not an H.323 device and you are sure the IP address is correct, it is likely that address is not on your network. This is especially true with addresses beginning with 10., 168.254, 172.16 through 172.31, or 192.168, which are private networking addresses.
	If you are unable to place calls to known sites on your network, a gatekeeper might be blocking calls from unregistered systems.	Register with the gatekeeper.

Symptom	Problem	Corrective action
ISDN: Line Status icons do not go away so video calls cannot be made.	The system is not connected to an ISDN.	Check the ISDN line connections.
	The ISDN number is entered incorrectly.	Check the ISDN numbers with your service provider.
	The ISDN line is provisioned incorrectly by the ISDN service provider.	Check that your ISDN line is provisioned for Voice/Data.
	The V500 system is in an unknown state.	Power off the system, wait five seconds, and power on the system.
	The BRI network interface is directly connected to a user interface.	Install an NT-1 device between your network interface module and the ISDN connection.
	The BRI network interface is connected to an NT-1 then to a PBX S/T interface.	You do not need an NT-1device when connecting to a PBX S/T interface. Connect the system directly to the PBX S/T connection.
	The system was not able to auto-detect SPIDs, or the SPID numbers are entered incorrectly. **Note**: The AT&T point-to-point protocol does not require SPIDs.	Select the **Clear** icon on the **Auto Detect SPIDs** page, and then select the **Start** icon to automatically detect the new SPIDs. Make sure your ISDN numbers are entered correctly. Check with your ISDN service provider and enter the SPIDs and switch protocol manually. **Note**: The AT&T point-to-point protocol does not require SPIDs.
ISDN: When placing a call, progress indicators do not turn green.	The call does not connect properly.	Try the call again.
	The NT-1 device is not powered on.	Verify power on the NT-1 device.
ISDN: Calls cannot be completed successfully. The green light on the NT-1 device flashes slowly.	There is a problem with the V500 system or between it and the NT-1 device.	Check for other problems listed in this table.
ISDN: Calls cannot be completed successfully. The green light on the NT-1 device flashes rapidly.	There is a problem on the network side of the NT-1 device.	Contact your ISDN service provider.
ISDN: Calls cannot be completed successfully when using the Recent Calls list.	Some ISDN switches add the area code to numbers when calling from the Recent Calls list.	Set the system to dial local numbers without an area code.
Limited call rate in a multipoint video call with at least one audio-only IP system.	The call rate is limited to 64 kbps if the audio-only IP system is called first.	Call all video systems before calling audio-only IP systems.

Symptom	Problem	Corrective action
Error message occurs when placing an ISDN (H.230) call.	An ISDN cause code is received from the ISDN line.	Try the call again. For more information, see Q.850 Cause Codes on page D-4.
	The highest-numbered channel did not connect. The system cannot make a call if this channel does not connect.	Be sure you are calling the correct number. The number may need to include: • A digit for an outside line • A long distance access code • An international access code • A country code • An area code or city code Check that all network cables are properly connected. Power off the system, wait five seconds, and power on the system. Then wait about two minutes to allow the ISDN lines to resynchronize. Ask the person at the far site to call your system.
	The ISDN switch type is not configured correctly on the V500 system.	Check the ISDN configuration and verify with your ISDN service provider that the system is configured correctly.
Cannot complete calls to sites that do not use encryption.	The system displays a message stating that encryption is required.	Your system is configured to require all calls to be encrypted, and encryption is not available at the far site.
Cannot complete Conference on Demand calls to ISDN systems when dialed from an H.323-only system.	The ISDN system numbers provided are not complete.	Provide the full international numbers, including country code, for ISDN systems.
Cannot dial remote system in BONDING calls. (The call progress circles only show blue or yellow.)	Switch protocol issue.	Start by calling the far site at 1x56 K, and progressively try higher speeds, as appropriate. This will verify the primary number. Being able to dial non-bonded but unable to dial bonded to all locations is usually a switch protocol issue. Verify your ISDN provisioning with the telephone service provider.
Dialing a remote site in calls above some particular speed does not work. (The call progress circles do not turn green, or remain blue after the first channel connects.)	The far site may be unable to accept calls above this speed.	Go to the **Call Status** screen. Highlight the circle for the channel dialed. The number dialed for the channel will be displayed as you highlight the circle. Make sure that the far site has entered the number for its ISDN lines correctly.

Symptom	Problem	Corrective action
Cannot select the desired speeds for BONDING calls from the speed selection.	Speeds do not show when selecting the speed icon.	1. Go to **Admin Settings > Network > Call Preference** and select ▶ four times to go to the **Call Speeds** screen. 2. Select the desired call speeds.
Call streaming to the Web does not work.	You may be attempting to stream to a different subnet and the router is not set to allow multicasting.	Make sure the network is configured to allow multicast streaming. To send the stream across a subnet, enable multicasting on the network or unicast to a particular IP address, which will forward the stream to that IP address regardless of the location destination. You can also test this feature by directing the stream to a specific computer that uses Apple QuickTime as a streaming player.

Display

Symptom	Problem	Corrective action
Screen is blank; start music plays and Polycom logo appears briefly.	The system is starting. This is normal.	No action required.
Monitor goes blank after displaying the splash screen.	The system goes to “sleep” after a period of inactivity.	The system is sleeping. The system wakes up on any action from the remote control or on an incoming call.
Picture is blank on the main monitor.	The system is sleeping. This is normal.	Pick up the remote control to wake up the system.
The monitor screen remains blank when you pick up the remote control.	The monitor’s power cord is not plugged in.	Connect the monitor’s power cord and then power on the monitor.
	The monitor is powered off.	Power on the monitor.
	The monitor is not connected correctly to the system.	Verify that the monitor is connected correctly according to the manufacturer’s instructions and the setup sheet you received with the system.
The call connects but you cannot see or hear people at the far site although they can see and hear you.	The system is configured for use with a NAT but is not behind a NAT.	Go to **Admin Settings > Network > IP > Firewall** and ensure that **NAT Configuration** is **Off**.
The people at the far site cannot see you.	The privacy shutter is closed.	Open the privacy shutter.
Video is in black and white.	The monitor cable is not connected properly.	Verify that the monitor is connected correctly according to the manufacturer’s instructions and the setup sheet you received with the system.
	The monitor cable is bad.	Replace the cable.

Symptom	Problem	Corrective action
The people at your site show up in silhouette in the PIP.	The camera is pointing toward a source of bright light, such as a window.	If it is practical to do so, have the call participants sit in a location where there is no light source behind them. Otherwise, go to **Admin Settings > Camera** and select **Backlight Compensation**.
No content can be sent in an H.331 call.	The systems are configured with H.264 video and with People+Content turned off.	The site sending content should enable People+Content.
	The V.35 system has People+Content turned off and/or H.239 disabled.	Check that H.239 and People+Content are enabled.
People+Content IP will not run.	The Windows firewall is enabled and is preventing People+Content IP from running.	Disable the Microsoft firewall when using People+Content IP.
Video clips running in Windows Media Player cannot be sent over People+Content IP.	Windows Media Player is configured to use overlays.	Configure Windows Media Player so that it does not use overlays. In Windows Media Player, select **Tools > Options > Performance > Advanced**. Uncheck "Use overlays".
Picture freezes frequently or becomes blocky during an IP call.	There is too much traffic on the LAN. Check the error count on the Call Statistics screen.	Go to **Admin Settings > Network > IP > Quality of Service** and enable dynamic bandwidth.
	The network is experiencing packet loss.	Go to **Admin Settings > Network > IP > Quality of Service** and specify a smaller value for Maximum Transmission Unit Size.
Picture freezes frequently during an ISDN call.	Too many network line transmission errors. Check the error count on the **Diagnostics > Call Statistics** screen to verify this.	Try the call again.
	Network interface cable or cables may be bad.	Replace the cable or cables.

Symptom	Problem	Corrective action
Picture is slow or jerky.	The system is receiving video that includes a large amount of motion.	A background with less motion provides a better, smoother video picture.
	Too many network line transmission errors. Check the error count on the **Diagnostics > Call Statistics** screen to verify this.	Try the call again, possibly at a lower network speed.
	Only one 64 kbps channel is connecting in your call.	Check the ISDN number of the far site. Ask the far site to call your site.
No picture in the PIP window.	The privacy shutter is closed.	Open the privacy shutter.

Audio

Symptom	Problem	Corrective action
No audio at your site.	The far site is muted.	Look for the far site **Mute** icon. Ask the far site to unmute the microphone. **Note**: The far site's microphone may be muted even if you do not see a far site **Mute** icon.
	The volume may be turned all the way down.	Use the remote control to turn up the volume. Check the monitor's volume setting. Check the system's audio output using the **Speaker Test** under **Diagnostics > Audio**. You should hear a 473 Hz tone.
	The far site's microphones are not placed correctly.	Ensure that each person who speaks is facing a microphone and is close enough to it.
	The far site's microphone is not connected or does not have power.	Ask the far site to check the cable to the microphone.
	Too many line errors.	Try the call again later.
	ISDN voice algorithm is incorrect.	Go to **System > Admin Settings > Network > ISDN.** Change the **ISDN Voice Algorithm** selection (**aLaw** or **uLaw**).
	The monitor's audio inputs are not connected properly.	Check audio output using the **Speaker Test** screen under **Diagnostics > Audio**. You should hear a 473 Hz tone. Ask someone at the far site to speak into the microphone, and check the **Far Site Audio** meter on the **Audio Meter** screen under **Diagnostics > Audio** to determine whether your system is receiving audio.
	The system's audio outputs are not connected properly.	Check the system's audio connections to the monitor. Verify that the system is connected to the correct audio connectors on the monitor.
The people at the far site cannot hear you.	The people at your site are too far from the system.	Move closer to the system.
	Your system's microphone is muted.	Check your system for one or more of these mute indications: • Near site mute icon on the screen • System indicator is red To unmute the system, press the  **Mute** button on the remote control.
	Your system's microphone does not work.	Call Polycom Technical Support and arrange to return the system for service.

Symptom	Problem	Corrective action
Not enough volume during a call.	The people at the far site are too far from the microphone.	Ask the people at the far site to move closer to the microphone.
	The volume is set too low on the system.	Turn up the volume using the remote control.
	The volume is set too low on the monitor.	Turn up the volume on your monitor.
Sound effects such as the incoming call ring are too loud or too soft.	The sound effects volume is not set at desired level.	Adjust the sound effects volume on the **Audio Settings** screen. If you do not want to hear sound effects, set the volume to 0.
You hear the incoming call ring when you have set sound effects volume to 0.	The internal ringer is enabled.	On the **Audio Settings** screen, clear the **Enable Internal Ringer** option.
Audio sounds raspy in ISDN calls.	ISDN voice algorithm is incorrect.	Go to **System > Admin Settings > Network > ISDN.** Change the **ISDN Voice Algorithm** selection (**aLaw** or **uLaw**).
You can hear yourself on your system's monitor or external audio system.	The far site microphone is too close to the system's audio speaker. (Far-site systems with separate microphones only)	At the far site, make sure the microphone is placed away from the system's audio speaker.
	The far site audio volume may be too loud.	Turn down the audio volume at the far site.

Error Indications

Symptom	Problem	Corrective action
The **System Information** screen shows "waiting" in the IP Video Number field.	The LAN is not working.	Check the LAN connection. Contact your network service provider.
	The DHCP server is not available.	Contact your network service provider to correct the problem with the server or to assign a static IP address.

Symptom	Problem	Corrective action
The home screen shows "0.0.0.0" as the system's IP address.	The LAN cable is not connected.	Check the LAN cable connection to the LAN port on the system.
	The system was configured for a static IP address of 0.0.0.0.	Go to **System > Admin Settings > LAN Properties** and correct the IP address settings.
	The system is configured for DHCP, and no DHCP server is available or responding on the network.	Contact your network administrator to correct the problem with the server or to assign a static IP address.
	The system is partially or incorrectly configured for firewall/NAT operation.	Go to **System > Admin Settings > Network > IP > Firewall >** and verify the **NAT (WAN) Public Address** setting.
The system displays a message stating that there are too many global directory entries.	The system's global directory display is limited to 4000 entries.	1. Go to **System Information >** > > **System Status**, highlight Global Directories, and press the **Help** button. The system lists the Global Directory Servers to which it is registered, and the number of directory entries from each. 2. Unregister the system from one or more of the Global Directory Servers.
Low battery icon on the screen.	Low batteries in the remote control.	Replace the batteries in the remote control with 3 AAA batteries.

How to Contact Technical Support

If you are not able to make test calls successfully and you have verified that the equipment is installed and set up correctly, contact your Polycom distributor or Polycom Technical Support.

To contact Polycom Technical Support, go to www.polycom.com/support.

Enter the following information, then ask a question or describe the problem. This information helps us to respond faster to your issue:

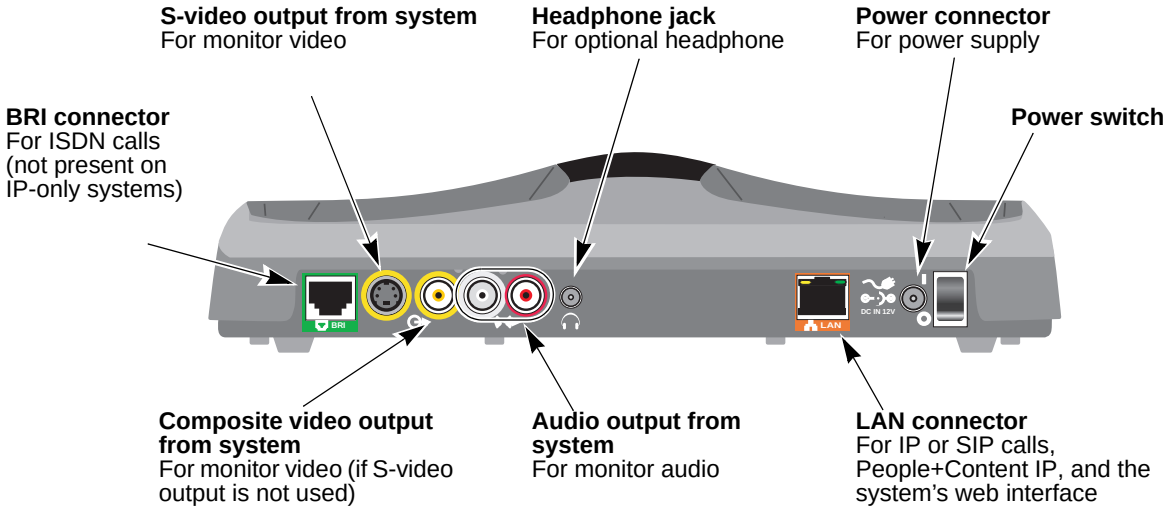
- The 14-digit serial number from the System Information screen, the bottom of the system, or the back of the system
- The software version (from the home screen, select **System > System Information**)
- Information about your network
- Troubleshooting steps you have already tried

A

System Back Panel Views

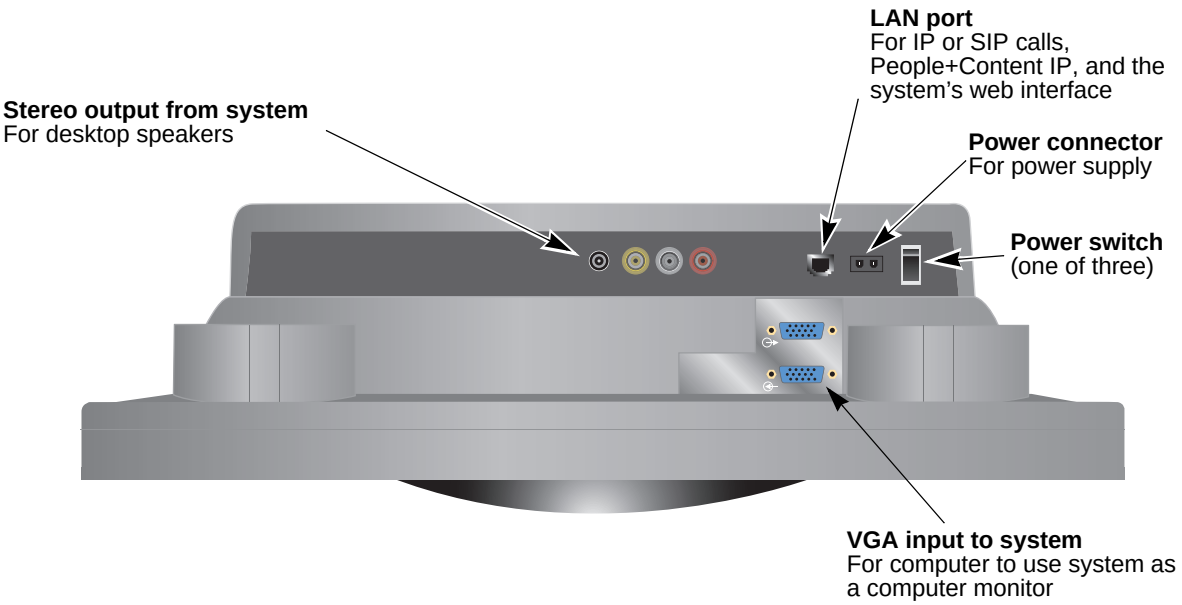
V500 System Back Panel

This illustration identifies the system's back panel connectors.



V700 System Connector Panel

The connectors face downward on the V700 system. This is a view from underneath the system.



B

Port Usage

You may need this information when you configure your network equipment for video conferencing.

The following table shows IP port usage.

Port	Function
80-Static	TCP HTTP interface (optional)
389-Static	TCP ILS registration (LDAP)
1503-Static	TCP T.120
1718-Static	TCP Gatekeeper discovery (must be bidirectional)
1719-Static	TCP Gatekeeper RAS (must be bidirectional)
1720-Static	TCP H.323 call setup (must be bidirectional)
1731-Static	TCP Audio call control (must be bidirectional)
5001-Static	UDP/TCP People+Content IP communication
8080-Static	TCP HTTP server push (optional)
1024-65535	Dynamic TCP H245. Can be set to “Fixed Ports” on Polycom systems.
1024-65535	Dynamic UDP - RTP (video data). Can be set to “Fixed Ports” on Polycom systems.
1024-65535	Dynamic UDP - RTP (audio data). Can be set to “Fixed Ports” on Polycom systems.
1024-65535	Dynamic UDP - RTCP (control information). Can be set to “Fixed Ports” on Polycom systems.

The following table shows Global Management System port usage.

Port	Function
21	(FTP) Software upgrades and provisioning for V Series systems and ViewStation systems
24	Polycom API
80	(HTTP) Pulling V Series system, ViewStation, and VS4000 information
80	(HTTP) Software upgrades and provisioning for iPower™
123	UPD Network time protocol (NTP)
161-162	TCP/UDP SNMP
3601	(Proprietary - data traffic) - Global directory data
3603	TCP - Pulling ViaVideo® information (since might be non-web server computer)
389	LDAP and ILS Static - TCP/UDP ILS registration (LDAP)
443	TCP HTTPS
514	UDP syslog
636	Secure LDAP communication (LDAPS)
1002	ILS

The following table shows other V Series system port usage.

Port	Function
21	(FTP) Software upgrades and Global Management System provisioning
23	(Telnet) For diagnostics
24	(Telnet) API control

C

Cables

The following table gives information about the cables shipped with the V500 system.

For information about the cables that ship with the V700 system, refer to the *Setting up the V700 System* document.

Cable	Part number and length
LAN cable Orange RJ-45	2457-08343-001 12 ft (3.6 m) [Maximum approved length: 100 ft (30 m)]
Composite video cable Triple RCA with S-video	2457-08674-001 6 ft (1.8m)

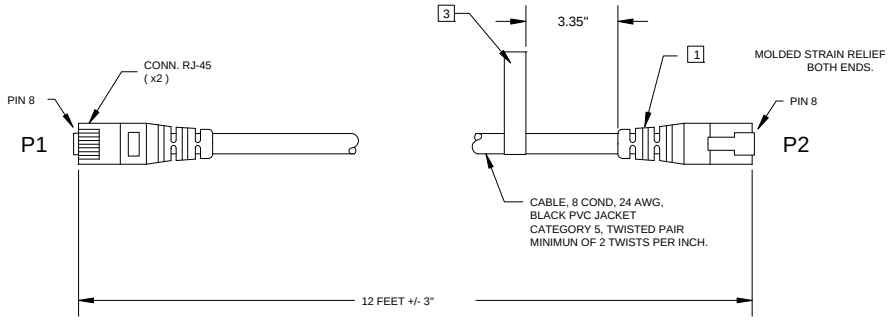
If you have the ISDN option on the V500 system, you can also attach a BRI cable. The part number for this cable is 2457-08717-001 and the length is 20 ft.

The pin-outs for the standard cables are shown in the following drawings.

LAN Cable

WIRING COLOR CODE STANDARDS: (WIRE/STRIPE)

P1 PIN #	P2 PIN #	AT&T 258A/268B
1	1	WHITE/ORANGE
2	2	ORANGE/WHITE
3	3	WHITE/GREEN
4	4	BLUE/WHITE
5	5	WHITE/BLUE
6	6	GREEN/WHITE
7	7	WHITE/BROWN
8	8	BROWN/WHITE

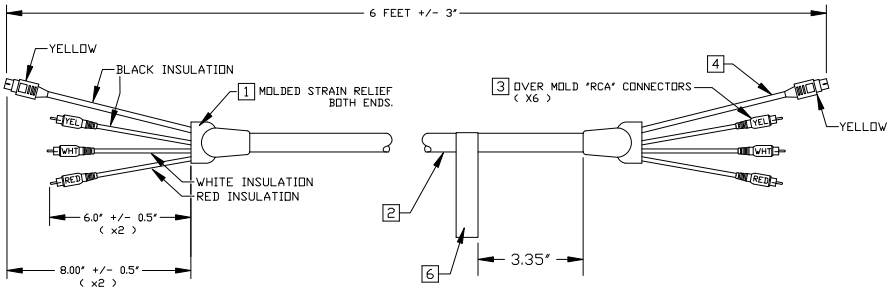


NOTES: (UNLESS OTHERWISE SPECIFIED).

1 MOLDING MATERIAL: PVC UL94 V-0
COLOR: ORANGE, APPROXIMATE MATCH TO PANTONE #1665 U.

LAN Cable 2457-08343-001

Composite Video Cable



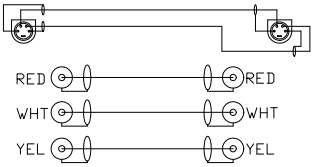
NOTES: (UNLESS OTHERWISE SPECIFIED).

1 MOLDING MATERIAL: PVC UL94 V-0
COLOR: BLACK

2 CABLE: COMPOSITE, ROUND MADE UP OF 3 COAXIAL-MINIATURE 75 ohm., 30 AWG, CELLULAR POLYOLEFIN, 90% TINNED COPPER SHIELD, CABLES WITH FILLER FOR ROUNDNESS, JACKET COLOR BLACK, MATTE FINISH.

3 OVER MOLDED CABLE END COLORS:
RED = APPROXIMATE MATCH TO PANTONE #199C.
WHT = WHITE (PANTONE DOES NOT HAVE SAMPLE).
YEL= APPROXIMATE MATCH TO PANTONE #109C.

4 ALTERNATE CABLE CONSTRUCTION FOR S-VIDEO LEAD IS NON-JACKETED CABLE WITH 2 INDIVIDUAL COAX CABLES.



WIRING DIAGRAM

Composite Video Cable 2457-08674-001

D

PathNavigator Error Codes and Q.850 Cause Codes

PathNavigator Error Codes

The following table lists PathNavigator error codes.

Code	Cause	Description
150	No Network Resources	The network does not have enough resources to complete your call. Try calling at a lower rate, or try the call again later.
151	No Network Resources	The network does not have enough resources to complete your call. Try calling at a lower rate, or try the call again later.
152	Gatekeeper Problems	Your call could not be completed because of an internal error in the gatekeeper or system. Contact the gatekeeper or system vendor for assistance.
153	Incorrect Address	Your call could not be completed because of an internal error in the gatekeeper or system. Contact the gatekeeper or system vendor for assistance.
154	Gatekeeper Problems	Your call could not be completed because of an internal error in the gatekeeper or system. Contact the gatekeeper or system vendor for assistance.
155	Gatekeeper Problems	Your call could not be completed because of an internal error in the gatekeeper or system. Contact the gatekeeper or system vendor for assistance.
156	Gatekeeper Problems	Your call was rejected by the gatekeeper. Contact your Network Administrator for assistance.

Code	Cause	Description
157	Gatekeeper Problems	Your call could not be completed because of an internal error in the gatekeeper or system. Contact the gatekeeper or system vendor for assistance.
158	Gatekeeper Problems	Your call could not be completed due to gatekeeper problems. Try the call again later.
159	System Not Registered with Gatekeeper	Your system must be registered with the gatekeeper before you can place a call. Contact your Network Administrator for assistance.
160	Far Site Not Registered with Gatekeeper	The system you are trying to call is not registered with the gatekeeper.
164	Far Site Busy	The system you called is busy. Try the call again later.
167	System Not Registered with Gatekeeper	Your system must be registered with the gatekeeper before you can place a call. Contact your Network Administrator for assistance.
168	Unknown Issues	Your call could not be completed due to an unknown problem. Try the call again later.
169	Call Rejected by Gatekeeper.	Your call was rejected by the gatekeeper. Contact your Network Administrator for assistance.
172	No Network Resources	The network does not have the necessary resources to complete your call. Try the call again later.
173	Site Not Found	The site you called could not be located. Check the calling information and try again.
174	Security/Permission Denial	Your call could not be completed because of security or permission issues. Contact your Network Administrator for assistance.
175	QoS Not Supported	The network cannot provide sufficient Quality of Service for your call. Contact your Network Administrator for assistance.
176	No Network Resources	The network does not have the necessary resources to complete your call. Try the call again later.
179	QoS Not Supported	The network cannot provide sufficient Quality of Service for your call. Contact your Network Administrator for assistance.
180	Invalid Address	The address you entered is not valid. Check the calling information and try again.

Code	Cause	Description
203	Call Rejected	The far site system did not accept the call. Check the calling information and try again.
204	Connection Problem	Your call cannot be completed because the far-end system is not compatible with the H.323 communication standards used by this system.
208	Invalid Address	The address you entered is not valid. Check the calling information and try again.
221	Far Site Busy	The system you called is busy. Try the call again later.
222	Site Not Responding	The site you called did not answer. Try the call again later.
255	ISDN command processing error	The ISDN signaling code has encountered an error processing an ISDN action. ISDN adapter busy-wait and retry.
516	Invalid Address	The address you entered is not valid. Check the calling information and try again.
518	Invalid Address	The address you entered is not valid. Check the calling information and try again.
521	Gatekeeper Problems	Your call could not be completed due to gatekeeper problems. Try the call again later.
531	Invalid Address	The address you entered is not valid. Check the calling information and try again.
534	Gatekeeper Problems	Your call could not be completed due to gatekeeper problems. Try the call again later.
551	Invalid Address	The address you entered is not valid. Check the calling information and try again.
552	Invalid Address	The address you entered is not valid. Check the calling information and try again.
553	Invalid Address	The address you entered is not valid. Check the calling information and try again.
554	Invalid Address	The address you entered is not valid. Check the calling information and try again.
576	Invalid Address	The address you entered is not valid. Check the calling information and try again.
595	Invalid Address	The address you entered is not valid. Check the calling information and try again.
596	Invalid Address	The address you entered is not valid. Check the calling information and try again.

Code	Cause	Description
621	Invalid Address	The address you entered is not valid. Check the calling information and try again.
626	Invalid Address	The address you entered is not valid. Check the calling information and try again.
627	Invalid Address	The address you entered is not valid. Check the calling information and try again.
648	No Network Resources	The network does not have the necessary resources to complete your call. Try the call again later.
681	No Network Resources	The network does not have the necessary resources to complete your call. Try the call again later.

Q.850 Cause Codes

The following table describes codes that the ISDN switch sends to the V Series system to indicate call status. Although the codes are standardized, each ISDN service provider defines them differently. Because of this, the definitions in the table may not exactly match the messages that you see.

You must have the V500 system with the ISDN option in order to place an ISDN call.

Code	Cause	Definition
1	Unassigned number	The switch received the sent ISDN number in the correct format, but no destination equipment uses the number.
2	No route to specified transit network	The ISDN exchange does not recognize the intermediate network through which to route the call.
3	No route to destination	The intermediate network through which the call is routed does not serve the destination address.
6	Channel unacceptable	The specified channel does not provide adequate service quality to accept the requested connection.
7	Call awarded and delivered	The user is assigned an incoming call that is being connected to a call channel that has already been established for this user and this type of call.

Code	Cause	Definition
16	Normal call clearing	The originator or receiver of the call has requested that it be cleared.
17	User busy	All B channels are in use; the called system acknowledges the connection request, but is unable to accept the call.
18	No user responding	The destination equipment does not respond to the call, so the connection cannot be completed.
19	No answer from user (user alerted)	The destination equipment did not complete the connection within the prescribed time after responding to the connection request. The problem is at the remote end of the connection.
21	Call rejected	The destination equipment is capable of accepting the call, but has rejected it for an unknown reason.
22	Number changed	The ISDN number used to set up the call is no longer valid. (The diagnostic field of the message may return an alternate address assigned to the called equipment.)
26	Non-selected user clearing	The destination is capable of accepting the call, but did not assign it to the user.
27	Destination out of order	A signaling message cannot be delivered because the interface is not functioning correctly, and the destination cannot be reached. This condition might be temporary; for example, remote equipment might be turned off.
28	Invalid number format	Destination address was incomplete or presented in an unrecognizable format, which prevented the connection from being established.
29	Facility rejected	The network cannot provide the facility requested by the user.
30	Response to STATUS INQUIRY	The equipment returns this message when it receives a STATUS INQUIRY message.
31	Normal, unspecified	A normal event has occurred with no standard cause applying. No resulting action is required.
34	No circuit/channel available	The call cannot be taken because no appropriate channel is available to establish the connection.
38	Network out of order	A network problem prevented the call from reaching its destination. Attempts to reconnect will probably fail until the network problem is corrected.
41	Temporary failure	A network error occurred. The problem will be resolved shortly. Attempts to reconnect may succeed.

Code	Cause	Definition
42	Switching equipment congestion	The destination cannot be reached because the network switching equipment is temporarily overloaded.
43	Access information discarded	The requested access information cannot be provided by the network. The diagnostic message may explain the problem.
44	Requested circuit/channel not available	The remote equipment cannot provide the requested channel. This may be temporary.
47	Resource unavailable, unspecified	An unknown problem prevents the remote equipment from providing the requested resource.
49	Quality of service unavailable	The network cannot provide the requested quality of service (as defined by CCITT recommendation X.213). This may be a subscription problem.
50	Requested facility not subscribed	The remote equipment is capable of providing the requested supplementary service, but is not subscribed to it.
57	Bearer capability not authorized	The caller has requested a bearer capability that the network can provide, but the user is not authorized to use. This may be a subscription problem.
58	Bearer capability not presently available	The network normally provides the requested bearer capability, but cannot provide it now. This may be a temporary network problem or a subscription problem.
63	Service or option not available, unspecified	An unspecified problem prevents the network or remote equipment from providing the requested service or option. This might be a subscription problem.
65	Bearer capability not implemented	The network is not capable of providing the bearer capability requested by the user.
66	Channel type not implemented	The requested channel type is not supported by the equipment sending this code.
69	Requested facility not implemented	The remote equipment is not capable of providing the requested supplementary service.
70	Only restricted digital information bearer is available	The network is unable to provide unrestricted digital information over bearer capability.

Code	Cause	Definition
79	Service or option not available, unspecified	The network or remote equipment is unable to provide the requested service option for an unspecified reason. This might be a subscription problem.
81	Invalid call reference value	The remote equipment received a call with a call reference that is not currently in use on the user-network interface.
82	Identified channel does not exist	The receiving equipment is requested to use a channel that is not activated on the interface for calls.
83	A suspended call exists but this call identity does not	The network received a call resume request that contained a call identity information element that does not match any suspended call.
84	Call identity in use	The network received a call suspend request that contained a call identity information element for a call that is already suspended.
85	No call suspended	The network received a call resume request when there was not a suspended call pending. This might be a transient error that will be resolved by successive call retries.
86	Call having requested call identity has been cleared	The network received a call resume request containing a call identity information element for a call that was cleared while suspended, either by timeout or by the remote user.
88	Incompatible destination	Indicates that an attempt was made to connect to non-ISDN equipment, such as an analog line.
91	Invalid transit network specified	The ISDN exchange was asked to route the call through an unrecognized intermediate network.
95	Invalid message, unspecified	An invalid message was received, for an unknown reason. This is usually due to a D-channel error. If this error occurs systematically, report it to your ISDN service provider.
96	Mandatory information element is missing	The equipment received a message that did not include one of the mandatory information elements. This is usually due to a D-channel error. If this error occurs systematically, report it to your ISDN service provider.
97	Message type nonexistent or not implemented	The equipment received a message of a type that is invalid or not supported. This code indicates either a problem with the remote configuration or a problem with the local D channel.

Code	Cause	Definition
98	Message incompatible with call state or message type nonexistent	The equipment received a message that is not valid in the current call state. Cause 98 is usually due to a D-channel error. If this error occurs systematically, report it to your ISDN service provider.
99	Information element nonexistent or not implemented	The equipment received a message that includes information elements which were not recognized. This is usually due to a D-channel error. If this error occurs systematically, report it to your ISDN service provider.
100	Invalid information element contents	The equipment received a message that includes invalid information in the information element. This is usually due to a D-channel error.
101	Message not compatible with call state	The remote equipment received a message that does not correspond to the current state of the connection. This is usually due to a D-channel error.
102	Recovery on timer expiry	A time-out has triggered an error-handling (recovery) procedure. This problem is typically temporary.
111	Protocol error, unspecified	An unspecified D-channel error when no other standard cause applies.
127	Interworking, unspecified	An event occurred within a network that does not provide causes for the action that it takes. The precise problem is unknown.
145	ISDN layer 1 and/or 2 link not established	User needs to check cabling, ISDN adapter status, and network connections.
146	ISDN layer 3 connection to the ISDN switch/network inactive	There is either a switch protocol error, or (in the United States or Canada) a SPID assignment problem.
255	ISDN command processing error	The ISDN signaling code has encountered an error processing an ISDN action. ISDN adapter busy-wait and retry.

Regulatory Notices

Important Safeguards
Read and understand the following instructions before using the system: • Close supervision is necessary when the system is used by or near children. Do not leave unattended while in use. • Only use electrical extension cords with a current rating at least equal to that of the system. • Always disconnect the system from power before cleaning and servicing and when not in use. • Do not spray liquids directly onto the system when cleaning. Always apply the liquid first to a static free cloth. • Do not immerse the system in any liquid or place any liquids on it. • Do not disassemble this system. To reduce the risk of shock and to maintain the warranty on the system, a qualified technician must perform service or repair work. • Connect this appliance to a grounded outlet. • Only connect the system to surge protected power outlets. • Keep ventilation openings free of any obstructions. • If the system or any accessories are installed in an enclosed space such as a cabinet, ensure that the air temperature in the enclosure does not exceed 40°C (104° F). You may need to provide forced cooling to keep the equipment within its operating temperature range. SAVE THESE INSTRUCTIONS.

Electrical Specifications
V700 System: 100-240VAC, 47-63Hz, 1.9A, 80W max

License Restrictions

THE SOFTWARE PROGRAMS CONTAINED OR DESCRIBED HEREIN ARE CONFIDENTIAL INFORMATION AND PROPRIETARY PRODUCTS OF POLYCOM, INC. OR ITS LICENSORS.

Buyer shall not sublicense or otherwise distribute any of the Subject Programs except to End Users and/or resellers who have entered into a Sublicense Agreement. For purposes of this Agreement a "Sublicense Agreement" shall mean a written license agreement between the Buyer and its purchaser, or, in the case of any sale by Buyer to a reseller, between such reseller and the End User, that is either 1) signed by the End User or 2) included with the Documentation, in such a manner that the End User reasonably indicates its acceptance of the Sublicense Agreement by turning on and using the Computer Equipment. Polycom, Inc. shall include so-called "break the seal software licenses" with the Documentation, and Buyer shall not remove or alter any such Sublicense Agreements or any notifications or warning stickers relating thereto. Buyer shall not waive, amend, or otherwise modify any Sublicense Agreement without Polycom's prior consent.

Title to all Subject Programs shall at all times remain and vest solely with Polycom, Inc. and its licensors. Buyer acknowledges Polycom's claim that the Subject Programs are its trade secret and confidential property, and shall treat them as such. Buyer will not attempt to disassemble, decompile, reverse-engineer or otherwise endeavor to discover or disclose the methods and concepts embodied in the Subject Programs. Except as expressly allowed under this Agreement, the Buyer shall not copy, modify, transcribe, store, translate, sell, lease, or otherwise transfer or distribute any of the Subject Programs in whole or in part, without prior authorization, in writing, from Polycom, Inc. Buyer shall not remove or destroy any copyright, patent, trademark or other proprietary mark or notice on Computer Equipment, and shall reproduce any such marks on any copies of Subject Programs that it makes hereunder.

You shall not, and shall not allow, any third party to 1) decompile, disassemble, or otherwise reverse-engineer or attempt to reconstruct or discover any source code or underlying ideas or algorithms of the software by any means whatsoever or 2) remove any product.

Warranty Information

LIMITED WARRANTY. Polycom warrants to the end user ("Customer") that the product will be free from defects in workmanship and materials, under normal use and service, for one year, or such longer period as Polycom may announce publicly from time to time for particular products, from the date of purchase from Polycom or its authorized reseller.

Polycom's sole obligation under this express warranty shall be, at Polycom's option and expense, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or if neither of the two foregoing options is reasonably available, Polycom may, in its sole discretion, refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of Polycom. Replacement products or parts may be new or reconditioned. Polycom warrants any replaced or repaired product or part for ninety (90) days from shipment, or the remainder of the initial warranty period, whichever is longer.

Products returned to Polycom must be sent prepaid and packaged appropriately for safe shipment, and it is recommended that they be insured or sent by a method that provides for tracking of the package. Responsibility for loss or damage does not transfer to Polycom until the returned item is received by Polycom. The repaired or replaced item will be shipped to Customer, at Polycom's expense, not later than thirty (30) days after Polycom receives the defective product, and Polycom will retain risk of loss or damage until the item is delivered to Customer.

Warranty Information

EXCLUSIONS. Polycom will not be liable under this limited warranty if its testing and examination disclose that the alleged defect or malfunction in the product does not exist or results from:

- Failure to follow Polycom's installation, operation, or maintenance instructions.
- Unauthorized product modification or alteration.
- Unauthorized use of common carrier communication services accessed through the product.
- Abuse, misuse, negligent acts or omissions of Customer and persons under Customer's control; or
- Acts of third parties, acts of God, accident, fire, lighting, power surges or outages, or other hazards.

WARRANTY EXCLUSIVE. IF A POLYCOM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT POLYCOM'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. POLYCOM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

SUPPORT & SERVICE AGREEMENTS. If you purchased your product from a Polycom Authorized Reseller, contact the Authorized Reseller for information about support and service agreements applicable to your product. For information on Polycom service, go to the Polycom web site www.polycom.com, products and services menu, or call 1-800-765-9266, outside the US call 1-408-526-9000, or your local Polycom Office, as listed on the Polycom Web site.

LIMITATION OF LIABILITY. TO THE FULL EXTENT ALLOWED BY LAW, POLYCOM EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF POLYCOM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT POLYCOM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

DISCLAIMER. Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

GOVERNING LAW. This Limited Warranty and Limitation of Liability shall be governed by the laws of the State of California, U.S.A., and by the laws of the United States, excluding their conflicts of laws principles. The United Nations Convention on Contracts for the International Sale of Goods is hereby excluded in its entirety from application to this Limited Warranty and Limitation of Liability.

Regulatory Notices

Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

USA and Canadian Regulatory Notices

FCC Notice

Class A Digital Device or Peripheral

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

In accordance with Part 15 of the FCC rules, the user is cautioned that any changes or modifications not expressly approved by Polycom Inc. could void the user's authority to operate this equipment.

The socket outlet to which this apparatus is connected must be installed near the equipment and must always be readily accessible.

Part 15 FCC Rules

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference, and

2) this device must accept any interference received, including interference that may cause undesired operation.

Part 68 FCC Rules

This equipment complies with part 68 of the FCC rules and the rules adopted by the ACTA. On the Network Interface Module of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ#TXXX. If requested, this number must be provided to the telephone company.

This equipment may not be used on a coin service or party line.

If you experience trouble with your Polycom system, disconnect it from the telephone line to determine if the registered equipment is malfunctioning. For repair or warranty information, please contact Polycom Inc. at 1-888-248-4143 or 4750 Willow Road, Pleasanton, CA 94588-2708, USA. Contact information may also be found at http://www.polycom.com. If the system is causing harm to the network, the telephone company may request that you disconnect it until the problem is corrected.

If your Polycom system causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. However, if advance notice is not practical, you will be notified as soon as possible. You will be advised of your right to file a complaint with the FCC if you believe it is necessary.

Your telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of your equipment. If they do, you will be given advance notice so that you may make any changes necessary to maintain uninterrupted service.

The REN is useful to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs of all devices that may be connected to a line, is determined by the total RENs, contact the local telephone company.

Regulatory Notices

FCC compliant telephone cords and modular plugs are provided with this equipment. This equipment is designed to be connected to the telephone network or premises' wiring using a compatible modular jack, which is Part 68 compliant. See installation instructions for details.

WHEN PROGRAMMING EMERGENCY NUMBERS AND/OR MAKING TEST CALLS TO EMERGENCY NUMBERS:

1) Remain on the line and briefly explain to the dispatcher the reason for the call.

2) Perform such activities in the off-peak hours, such as early morning or late evening.

Industry Canada (IC)

This Class [A] digital apparatus complies with Canadian ICES-003.

Cet appareil numerique de la Classe [A] est conforme à la norme NMB-003 du Canada.

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

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations. Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

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

The REN of this equipment is either marked on the unit or included in the new style USA FCC registration number. In the case that the REN is included in the FCC number, the user should use the following key to determine the value:

The FCC number is formatted as US:AAAEQ#TXXX.

is the Ringer Equivalence Number without a decimal point (e.g. REN of 1.0 will be shown as 10, REN of 0.3 will be shown as 03). In the case of a Z ringer, ZZ shall appear. In the case of approved equipment without a network interface or equipment not to be connected to circuits with analog ringing supplied, NA shall appear.

Regulatory Notices

Mexico Regulatory Notices

Información del contacto para el importador de México
Polycom MÉXICO
Paseo de los Tamarindos
400-A 5to piso Suite: 21
Bosques de las Lomas
Cuajimalpa 05120 México, D.F.
Teléfono: +52-55-5091-4341
Fax: +52-55-5091-4472

EEA Regulatory Notices

CE Mark R & TTE Directive

This Polycom system has been marked with the CE mark. This mark indicates compliance with EEC Directives 89/336/EEC, 73/23/EEC 1999/5/EC. A full copy of the Declaration of Conformity can be obtained from Polycom Ltd., 270 Bath Road, Slough UK SL1 4DX.

Declaration of Conformity:

Hereby, Polycom Ltd. declares that this Polycom system is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Konformitetserklæring:

Hermed erklærer Polycom Ltd., at indestående Polycom system er i overensstemmelse med de grundlæggende krav og de relevante punkter i direktiv 1999/5/EF.

Konformitätserklärung:

Hiermit erklärt Polycom Ltd., dass der Polycom system die grundlegenden Anforderungen und sonstige maßgebliche Bestimmungen der Richtlinie 1999/5/EG erfüllt.

Δήλωση Συμμόρφωσης:
Δια του παρόντος, η εταιρεία Polycom Ltd. δηλώνει ότι η παρούσα συσκευή (δρομολογητής) V500; πληροί τις βασικές απαιτήσεις και άλλες βασικές προϋποθέσεις της Οδηγίας 1999/5/ΕΚ.

Vaatimustenmukaisuusvakuutus:

Polycom Ltd. vakuuttaa täten, että Polycom system on direktiivin 1999/5/EC keskeisten vaatimusten ja sen muiden tätä koskevien säännösten mukainen.

Déclaration de conformité:

Par la présente, Polycom Ltd. déclare que ce Polycom system est conforme aux conditions essentielles et à toute autre modalité pertinente de la Directive 1999/5/CE.

Dichiarazione di conformità:

Con la presente Polycom Ltd. dichiara che il Polycom system soddisfa i requisiti essenziali e le altre disposizioni pertinenti della direttiva 1999/5/CE.

Verklaring van overeenstemming:

Hierbij verklaart Polycom Ltd. dat diens Polycom system voldoet aan de basisvereisten en andere relevante voorwaarden van EG-richtlijn 1999/5/EG.

Regulatory Notices

Declaração de Conformidade:

Através da presente, a Polycom Ltd. declara que este Polycom system se encontra em conformidade com os requisitos essenciais e outras disposições relevantes da Directiva 1999/5/CE.

Declaración de conformidad:

Por la presente declaración, Polycom Ltd. declara que este Polycom system cumple los requisitos esenciales y otras cláusulas importantes de la directiva 1999/5/CE.

Överensstämmelseförklaring:

Polycom Ltd. förklarar härmed att denna Polycom system överensstämmer med de väsentliga kraven och övriga relevanta stadganden i direktiv 1999/5/EG.

CE Mark LVD and EMC Directive

This Polycom system has been marked with the CE mark. This mark indicates compliance with EEC Directives 89/336/EEC and 73/23/EEC. A full copy of the Declaration of Conformity can be obtained from Polycom Ltd., 270 Bath Road, Slough UK SL1 4DX, UK.

Mains Powered POTS Voice Telephony Without Emergency 000 Dialing

Warning: This equipment will be inoperable when mains power fails.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

声　明

此为 A 级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

A급 기기 (업무용 정보통신기기)

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Underwriters Laboratories Statement

The system is intended to be powered only by the supplied power supply unit.

Special Safety Instructions

Follow existing safety instructions and observe all safeguards as directed.

Installation Instructions

Installation must be performed in accordance with all relevant national wiring rules.

故障の原因となりますので、システムの電源がオンになっているときは、マイク入力への機器の接続や取り外しをしないでください。

Regulatory Notices

Plug Acts as Disconnect Device

The socket outlet to which this apparatus is connected must be installed near the equipment and must always be readily accessible.

Restriction of Hazardous Substances Directive (RoHS)

Polycom products are RoHS compliant, which means we have eliminated or brought to within acceptable limits: Lead, Mercury, Cadmium, Hexavalent Chromium, Polybrominated Biphenyls, and Polybrominated Diphenylethers.

End of Life Products

Polycom encourages you to recycle your end-of-life Polycom products in an environmentally considerate way.

In accordance with the requirements of the European Waste Electronic and Electrical Equipment (WEEE) Directive, all Polycom products are marked with the crossed wheelie bin symbol shown below. Products that carry this symbol should be not be disposed of in the household or general waste stream.

Battery Guidelines

Battery Usage

Observe battery polarity when you install or replace batteries in the remote control.

Replace batteries as a complete set, using new, quality batteries of the correct size and rating.

Do not short circuit batteries.

Batteries should be treated and used in accordance with the battery manufacturers guidance.

Battery Disposal

When the remote control batteries have reached the end of their working life, remove them and take them to a collection point where they can be recycled or disposed of in an environmentally friendly manner. Do not dispose of batteries in unsorted municipal waste.

Do not dispose of batteries in the fire.

Index

A

access
  allowing 7-4, 8-3
  levels 7-3, 8-5
  limiting 8-2, 8-3, 8-4
  remote 8-3
access code, ISDN, for international calls 7-1
account number 9-5, 11-7
address
  default gateway 2-3
  IP 2-2
  WINS server 2-3
Address Displayed in Global Directory (setting) 2-13
addresses
  console IP 9-8
  directory, displaying 2-13
  DNS server 2-3
  Global Directory Server 6-5
  IP multicast 6-7
  IP, displaying 7-4
  ISDN, displaying 7-4
  NAT public (WAN) 2-12
  primary gatekeeper 2-5
  SIP proxy server 2-9
  SIP registrar server 2-9
AES Encryption (setting) 8-3
AES encryption, *See* encryption
aLaw 2-15
alert tones 4-1, 4-2, 7-8
Allow Access to User Settings (setting) 8-3
Allow Directory Changes (setting) 6-3
Allow Streaming (setting) 6-7
Allow Video Display on Web (setting) 8-3
Always Dial Area Code (setting) 7-2
answering calls automatically 6-1
answering mode 6-2
Appearance (screen) 7-10
Area Code (setting) 2-7, 2-16
Area Code Required (setting) 7-1
aspect ratio 3-2
audio
  configuring 4-1, 4-2
  port, web streaming 6-7
  settings on V500 4-1
  settings on V700 4-2
  testing 11-5
  troubleshooting 12-12
  volume 4-1, 4-2, 4-3
Audio Meter screen 11-5, 12-12
Audio Port (setting) 6-7
authentication name
  SIP 2-8
Authentication Name, SIP 2-8
Authentication PIN (setting) 2-5
Auto Adjust for Daylight Saving Time (setting) 7-2
Auto Answer Point-to-Point (setting) 6-1
Auto BRI Configuration (setting) 2-15
auto-answer, muting 4-2
auto-detecting SPIDs 2-16
automatic restart, actions that cause 8-3
Avaya network integration 2-6

B

back panel view
  V500 A-1
  V700 A-2
Backlight Compensation (setting) 3-6
bandwidth
  allowing users to specify 7-4
  dynamic 2-11
  managing 2-18
  specifying 2-11
Bandwidth (screen) 2-11
basic mode 2-16, 12-2
bass adjustment 4-1, 4-3
battery icon 12-14
blank screen, troubleshooting 12-9

BRI network interface
  configuring 2-15
  connecting 2-14
  lights 2-14
brightness, camera 3-6
burn-in prevention for monitors 3-4

C

cable
  connections A-1, A-2
  descriptions C-1
  drawings C-1
  monitor (drawing) C-2
calendar, accessing with the remote control 10-1
call
  answering mode 6-2
  auto-answer 6-1
  bonding 12-8
  dialing display 7-4
  do not disturb 7-5
  elapsed time, displaying 7-2
  list of recent calls 7-5
  progress indicators 12-7, 12-8
  quality, troubleshooting 12-10, 12-11
  settings, configuring 6-1
  statistics 11-3
  status 11-3
  status tools 11-2
  test 12-1
  time, maximum 6-1
  tracking 9-5
  troubleshooting 12-6
  type, allowing users to specify 7-4
  type, statistics 11-3
Call Detail Report (CDR)
  account numbers 9-5
  archives 11-10
  configuring 7-5
  generating 6-2
  information in 11-7
  viewing and downloading 11-6
Call Detail Report (setting) 6-2, 7-5
Call Preference (screen) 2-16
call preferences 2-16
call progress indicators 11-3
Call Quality (setting) 2-18, 7-4
call speed
  allowing users to specify 7-4
  for streaming calls 6-7
  preferred 2-18
call statistics
  accessing with the remote control 10-1
Call Status screen 11-3
Call Summary (screen) 11-3
calls
  recent 11-6
  streaming 6-7, 6-8
Camera Brightness (setting) 3-6
Chinese Virtual Keyboard (setting) 10-1
Click2Call
  Lotus Sametime or Lotus Notes 2-9
closed captions
  displaying 5-2
  Telnet session connection 5-3
  web interface connection 5-3
color balance adjustment 3-4
color bar test 3-4, 11-4
Color Scheme (setting) 7-7
color schemes 7-6
computers
  V700 as computer monitor 3-1
Conference On Demand
  multipoint calls 2-5
configuring
  audio 4-1, 4-2
  BRI 2-15
  Dual Monitor Emulation 3-2
  for VPN 2-12
  ISDN dialing rules 7-2
  microphones
    Polycom 4-2
  monitor 3-2
  monitors
    color, sharpness, brightness 3-5
  NAT 2-12
  PIP 3-2
  remote control 10-1
  SNMP 9-7
  to use a gatekeeper 2-5
  web streaming 6-7
Confirm Directory Additions (setting) 6-3
Confirm Directory Deletions (setting) 6-3
Connect to my LAN (setting) 2-2
connecting
  ISDN 2-14, 12-7
  LAN 2-1
  monitor 3-1
connectivity tests 11-4
connectors
  V500 A-1
  V700 A-2
Console IP Address (setting) 9-8

contact list
  home screen display 7-5
Contact List (setting) 7-4
content
  displaying 5-1
Country (setting) 7-1
Country Code (setting) 2-7, 7-1
customizing
  home screen 7-3
  workspace 7-3

D

data collaboration 2-17, 5-1
date and time, displaying 7-4
Date Format (setting) 7-2
daylight saving time adjustment 7-2
Default Gateway (setting) 2-3
DHCP 2-2
diagnostics 11-5
  audio meter 11-5
  color bar test 3-4, 11-4
  IP connectivity tests 11-4
  near end loop 11-4
  network and call status tools 11-2
  reset and restart 11-5
Dial 1+ for all USA Calls (setting) 7-2
dialing
  last number dialed 7-5
  options display 7-4
  order 2-17
  preferred method 2-17
  prefix for ISDN 2-15
  rules 7-2
  speed dialing 7-5
  troubleshooting 12-8
Dialing Display (setting) 7-4
Dialing Order (setting) 2-17, 2-18
DiffServ 2-10
Direct Inward Dial (setting) 2-7
directory
  allowing access 7-4
  allowing changes 6-3
  configuring settings 6-3
  confirming changes 6-3
  managing with web interface 6-4
  server 6-5
Directory (setting) 7-4
Directory Numbers (setting) 2-16
Display Global Addresses (setting) 6-5
Display H.323 Extension (setting) 2-4
Display Icons in a Call (setting) 3-2
Display Name in Global Directory (setting) 6-5
Display Time in Call (setting) 6-1, 7-2
display, troubleshooting 12-9
displaying
  content 3-2
  date and time 7-4
  files from a computer 5-1
  PIP 3-2
  system name 7-4
  time in call 6-1
displays
  V700 as computer monitor 3-1
DNS name 2-2
DNS Servers (setting) 2-3
Do Not Disturb 6-2
Do Not Disturb (setting) 7-5
Domain Name (setting) 2-2
DTMF tones 10-1
Dual Monitor Emulation 3-3
Dual Monitor Emulation (setting) 3-2
Duplex Mode (setting) 2-3
Dynamic Bandwidth (setting) 2-11

E

E.164 2-4, 2-5
E.164 extension 2-7
Enable Basic Mode (setting) 2-16
Enable H.239 (setting) 2-17
Enable H.460 Firewall Traversal setting 2-12
Enable Internal Ringer (setting) 4-2
Enable IP H.323 (setting) 2-17
Enable ISDN Gateway setting 2-17
Enable ISDN H.320 (setting) 2-17
Enable Live Music Mode (setting) 4-2
Enable Polycom Microphones (setting) 4-2
Enable Polycom StereoSurround (setting) 4-2
Enable PVEC (setting) 2-11
Enable Remote Access (setting) 8-3
Enable RSVP (setting) 2-11
Enable SIP (setting) 2-17
Enable SNMP (setting) 9-8
Enable Streaming Announcement (setting) 6-7
Enable Voice Over ISDN (setting) 2-17
encryption
  enabling 8-3, 8-6
  information in Call Statistics 11-3
Enter IP Address Manually (setting) 2-2

error concealment, PVEC 2-11
error indications, troubleshooting 12-13
error messages 12-6, 12-8
extensions
  E.164 2-4, 2-5, 2-7
  entering on home screen 7-4
  H.323 2-4, 2-5, 2-7, 7-4

F

far site
  system information 11-3
  system name 6-2
Far Site Name Display Time (setting) 6-2
firewall
  configuring properties 2-11
Firewall (screen) 2-11
firewalls
  traversal feature 2-13
Fixed Ports (setting) 2-12
flicker, eliminating 3-6
FTP access, controlling 8-3

G

gatekeeper
  name 2-4
  specifying 2-5
Gatekeeper (screen) 2-5
gateway
  default 2-3
  placing call 2-4
  specifying 2-7
Gateway Number Type (setting) 2-7
generating DTMF tones 10-1
Global Address Book, *see* Global Directory
Global Directory
  configuring 6-5
  copying to local system 6-6
  displaying addresses 2-13
  displaying names 6-5
  password 6-5
Global Directory (GDS) (setting) 6-5
Global Directory Server addresses 6-5
Global Management System
  description 9-4
  management servers list 9-5
  requesting support from administrator 9-6
  See also remote management
global services, configuring 9-4

H

H.320, *See* ISDN
H.323
  configuring 2-4
  enabling 2-17
  extension 2-4, 2-5
  specifying for home screen 7-4
  See also IP
H.323 extension 2-7
H.323 Extension (E.164) (setting) 2-4, 2-5, 2-7, 7-4
H.323 Name (setting) 2-4, 2-5
H.323 Settings (screen) 2-4, 2-7
H.460 NAT Firewall Traversal 2-13
help
  from Global Management System administrator 9-6
  on-screen 7-6, 7-8
home screen
  adding sites 7-5
  customizing 7-3
  settings 7-4
Home Screen Settings (screen) 7-5
Host Name (setting) 2-2

I

icons
  displaying 3-2
  line status 12-7
  low battery 12-14
indicators
  call progress 11-3, 12-7
  low battery icon 12-14
  progress 12-8
  status 1-4
initial system configuration 1-5
instructions, on-screen 7-6, 7-8, 9-4
internal ringer 4-2
international access code, ISDN 7-1

IP
  address
    displaying 7-4
    obtaining automatically 2-2
    SIP proxy server 2-9
    SIP registrar server 2-9
  allowing IP calls 2-17
  configuring Quality of Service settings 2-10
  configuring SIP settings 2-8
  connectivity tests 11-4
  error message 12-6
  network
    configuring H.323 settings 2-4
  video number field 12-13
IP address
  multicast 6-7
  primary gatekeeper 2-5
  unicast, of streaming server 6-7
IP Address (setting) 2-2
IP Multicast Address (setting) 6-7
IP or ISDN Information (setting) 7-4
IP precedence 2-10
ISDN
  allowing ISDN calls 2-17
  configuring network connection 2-15
  configuring network interface 2-15
  connecting 2-14
  enabling ISDN line 2-16
  numbers, displaying 7-4
  preparing network 2-1
  SPIDs 2-16
  switch protocol 2-16
  troubleshooting 12-7, 12-8
  voice over 2-17
ISDN International Access Code (setting) 7-1
ISDN Switch Protocol (setting) 2-15
ISDN Voice Algorithm (setting) 2-15

K

Keypad Audio Confirmation (setting) 10-1
kiosk mode
  home screen example 7-3
  managing user access 8-5

L

LAN
  cable, drawing C-2
  connecting 2-1
LAN Speed (setting) 2-3
Language (setting) 7-1
Last Number Dialed (setting) 7-5
lighting
  backlight compensation 3-6
  brightness 3-6
lights
  BRI network interface 2-14
  status 1-4
line status icons 12-7
Local Date and Time (setting) 7-4
localized system name
  creating with web interface 6-4
  setting 6-3
Localized System Name (setting) 6-3
Location (screen) 7-1
location settings 7-1, 7-2
Lotus Notes 2-9
Lotus Sametime 2-9
low battery icon 12-14

M

management servers list 9-5
marquee text 7-6
master audio volume 4-1, 4-3
Master Audio Volume (setting) 4-1, 4-3
Maximum Receive Bandwidth (setting) 2-11
Maximum Speed for Receiving Calls (setting) 2-18
Maximum Time in Call (setting) 6-1
Maximum Transmission Unit Size (setting) 2-10
Maximum Transmit Bandwidth (setting) 2-11
meeting password 8-2
menu map 8-1
messages
  sending to call participants 9-4
MIBs, downloading 9-7
microphones
  configuring 4-2
Microsoft LCS
  displaying contacts on home screen 7-4
  displaying contacts on the home screen 7-5
monitor
  aspect ratio, specifying 3-2
  brightness adjustment 3-4
  burn-in prevention 3-4
  color balance adjustment 3-4
  configuring 3-2, 3-5
  connecting 3-1
  sharpness setting 3-4
  troubleshooting 12-4, 12-9
  video format, specifying 3-2

Monitor (setting) 3-2
monitor cable (drawing) C-2
monitors
  configuring 3-2
  V700 as computer monitor 3-1
multicast IP address 6-7
multicasting, *See* web streaming
multipoint calls
  using PathNavigator 2-5
Mute Auto-Answer Calls (setting) 4-2
muting, auto-answer calls 4-2
My Contacts list 7-5
My Information (screen) 9-6

N

name
  displaying in directory 6-5
  far-site system 6-2
  H.323 2-4**,** 2-5
  host (DNS) 2-2
  SIP 2-8
  system 2-5**,** 6-3**,** 7-4
NAT
  configuring 2-12
  configuring properties 2-11
NAT Configuration (setting) 2-12
NAT is H.323 Compatible (setting) 2-13
NAT Public (WAN) Address (setting) 2-12
near end loop test 11-4
network
  configuring ISDN connection 2-15
  diagnostic tools 11-2
  IP, connecting 2-1
  ISDN, connecting 2-14
  requirements, ISDN 2-14
network interface
  BRI 2-14
  lights 2-14
newsfeed, screen saver 7-9
NT-1 device 2-14
Number (setting, for gateway), gateway 2-7
Number + Extension (setting) 2-7
Number of Digits in DID Number (setting) 2-8
Number of Digits in Extension (setting) 2-8
Number of Router Hops (setting) 6-7

O

Obtain IP Address Automatically (setting) 2-2
on-screen instructions 7-6**,** 7-8
on-screen instructions, providing 9-4
out-of-box setup 1-5
Outside Line Dialing Prefix (setting) 2-15
overlay
  video 7-7

P

packet loss, in Call Statistics 11-3
passwords
  administrator 8-2
  Global Directory 6-5
  meeting 8-2
  meeting, setting 8-2
  remote access 8-2**,** 8-4
  room, default 1-5**,** 8-4
  room, setting and deleting 1-5**,** 8-2**,** 8-4
  SIP authentication 2-9
PathNavigator, using for multipoint calls 2-5
PCAS
  Lotus Sametime or Lotus Notes 2-9
PCAS (setting) 2-9
PCAS Server Address (setting) 2-9
People+Content IP
  displaying content 5-1
  enabling 2-17
  installing 5-2
  requirements 5-1
  supported resolutions 5-1
picture-in-picture, *See* PIP
PIP
  configuring 3-2
  troubleshooting 12-11
PIP (setting) 3-2
Place a Call screen
  See home screen
plasma monitors and burn-in prevention 3-4
point to point, call answer mode 6-2
ports
  fixed 2-12
  SIP proxy server 2-9
  SIP registrar server 2-9
  TCP 2-12
  UDP 2-12
power
  resetting system 11-5
  switch 1-5
  troubleshooting 12-3
Power Frequency (setting) 3-6
preferences, call 2-16
Preferred Dialing Method (setting) 2-17

Preferred Speed for Placing Calls (setting) 2-18
Primary Gatekeeper IP Address (setting) 2-5
profile
  managing 9-3
  storing 9-3
  uploading 9-3
protocol
  ISDN switch 2-15, 2-16
Proxy Server (setting) 2-9

Q

quality
  call 12-10, 12-11
Quality of Service (screen) 2-10

R

RAS200I
  Lotus Sametime or Lotus Notes 2-9
rear panel view
  V500 A-1
  V700 A-2
Recent Calls
  accessing with the remote control 10-1
recent calls
  button 6-2
  button on home screen 7-5
  calls not listed 11-6
  list 11-6
  See also Call Detail Report (CDR)
  viewing 11-6
Recent Calls (setting) 6-2, 7-5
registering with Global Directory Server 6-5
Registrar Server (setting) 2-9
remote access
  enabling 8-3
  password 8-4
Remote Access Password (setting) 8-2
remote control
  configuring 10-1
  keypad audio confirmation 10-1
Remote Control Keypad (setting) 10-1
remote management
  enabling 8-3
  using web browser 9-1
requirements
  software, for viewing web streams 6-8
reset system 11-5
Reset System (screen) 8-4
resolution, VGA, for People+Content IP 5-1
restart system
  actions that cause 8-3
  diagnostic tool 11-5
ring tones 4-1, 4-2, 7-8
ringer, internal 4-2
room monitoring 8-3, 9-2
room password
  default 1-5, 8-4
  screens that require 8-1
  setting and deleting 1-5, 8-2, 8-4
Room Telephone Number (setting) 7-2
router
  selecting UPnP 2-12

S

Save Global Directory to System (setting) 6-6
screen saver 7-8, 7-9, 7-10
Screen Saver (screen) 7-9
Screen Saver Wait Time (setting) 7-10
Screen Saver web interface 7-10
screens
  blank, troubleshooting 12-9
  diagram of system 8-1
security
  controlling remote access 8-3, 9-2
  home screen settings 7-4
  setting options 8-2
  System screen access 7-4
  systems outside firewalls 2-13
Security (screen) 8-2, 8-4
servers
  directory 6-5
  DNS 2-3
  streaming 6-7
  WINS 2-3
setup wizard 1-5
sharing files 5-1
SIP
  authentication name 2-8
  configuring settings 2-8
  enabling 2-17
  Lotus Sametime or Lotus Notes 2-9
  password 2-9
  proxy server 2-9
  registrar server 2-9
  transport protocol 2-8
  user name 2-8
SIP Settings (screen) 2-8
site buttons, adding 7-5
site considerations 1-3

Sites (screen) 7-5
Sites (setting) 7-5
Snap Button Option (setting) 10-1
Snapshot Timeout (setting) 3-2
SNMP
  access, controlling 8-3
  configuring for SNMP management 9-7
  setting up 9-7
Softupdate 9-8
software version 12-14
software, upgrading 9-8
sound effects volume 4-1, 4-2
Sound Effects Volume (setting) 4-1, 4-2
speakers
  desktop, for V700 4-1
Speed (setting) 6-7
speed dial 7-5
speed, call 2-18
speed, call statistics 11-3
SPIDs 2-15, 2-16
start-up, troubleshooting 12-3
status
  call 11-3
  network and call diagnostic tools 11-2
  system 11-2
Streaming (screen) 6-7
streaming calls 6-6
streaming web 6-6
Subnet Mask (setting) 2-3
switch protocol, ISDN 2-15, 2-16
switch, power 1-5
system
  lights 1-4
  name 2-5, 6-4, 7-4
  placement 1-3
  profiles 9-3
System (setting) 7-4
System button 12-5
System Info, accessing with the remote control 10-1
System Information screen 12-13
System Name (setting) 6-3, 7-4
System screen
  allowing access 7-4
  unable to access 12-5

T

TCP
  specifying fixed ports 2-12
TCP Ports (setting) 2-12
technical support
  contacting 12-14
  from Global Management System administrator 9-6
Telnet
  access, controlling 8-3
  using for closed captions 5-3
test calls 12-1
tests
  audio meter 11-5
  color bar 3-4, 11-4
  near end loop 11-4
  speaker test 11-5
time
  daylight saving 7-2
  displaying 7-4
  displaying call length 6-1
  elapsed, displaying 7-2
  maximum call duration 6-1
  setting 7-1
  zone 7-2
Time Difference from GMT (setting) 7-2
Time Format (setting) 7-2
Time Server (setting) 7-2
timeout
  content display 3-2
  screen saver 7-10
tones
  alert 4-1, 4-2, 7-8
  DTMF, generating 10-1
  internal ringer 4-2
  ring 4-1, 4-2, 7-8
tracking calls 9-5
Transport Protocol (setting) 2-8
treble adjustment 4-2, 4-3
troubleshooting
  access to screens and systems 12-5
  audio 12-12
  calling 12-6
  display 12-9
  error indications 12-13
  general 12-2
  power and start-up 12-3
  video 12-9
TV, *See* monitor
Type of Service (setting) 2-10
Type of Service Value (setting) 2-10

U
UDP
  specifying fixed ports 2-12
UDP Ports (setting) 2-12
uLaw 2-15
upgrading software 9-8
UPnP 2-12
Use Gatekeeper (setting) 2-5
Use PathNavigator for Multipoint Calls (setting) 2-5
Use Room Password for Remote Access (setting) 8-2
Use the Following IP Address (setting) 2-2
User Alert Tones (setting) 4-1, 4-2
User Name, SIP 2-8
user settings
  allowing access 8-3
  backlight compensation 3-6
  color schemes 7-6
  list of 8-5
  managing access 8-5
  PIP 3-2
User Settings (screen), allowing access 8-3
utilities
  web streaming 6-7

V
V500
  audio settings 4-1
  positioning 1-3
  powering on 1-5
  system 1-1
V700
  audio settings 4-2
  positioning 1-3
  powering on 1-5
  streaming calls 6-6
  system 1-2
VGA resolution, for People+Content IP 5-1
video
  brightness adjustment 3-4
  color balance adjustment 3-4
  eliminating flicker 3-6
  monitor format 3-2
  port, web streaming 6-7
  sharpness adjustment 3-4
  troubleshooting 12-9, 12-10, 12-11
video cable (drawing) C-2
video error concealment 2-11
video overlay
  applying 7-7
Video Port (setting) 6-7
voice over ISDN, enabling 2-17
voice-mail menu navigation, *See* Remote Control Keypad (setting)
volume
  adjusting 12-13
  alert tones 12-13
  bass 4-1, 4-3
  master control 4-1, 4-3
  setting 4-1, 4-3, 12-13
  sound effects 4-1, 4-2, 12-13
  treble 4-2, 4-3
  troubleshooting 12-13
VPN, configuring 2-12

W
Web Access Port (setting) 8-3
web access, controlling 8-3
Web Director 8-3
web interface
  accessing diagnostic screens 11-2
  managing directories 6-4
  managing system profiles 9-3
  room monitoring 9-2
  sending message 9-4
  sending messages to call participants 9-4
  viewing Call Detail Report 11-2, 11-7
web streaming
  configuring 6-7
  restrictions 6-6
  starting and stopping 6-7
  viewing 6-8
wide-screen monitor, configuring 3-2
WINS Resolution (setting) 2-3
WINS Server (setting) 2-3

Y
Your IP Address is (setting) 2-2