Cheyenne Regional Medical Center

Telehealth Policy and Procedures

Table of Contents

Introduction

CRMC was the recipient of a $14.2 million, which $1.4 million was dedicated to telehealth. Telehealth has been tested and proven for clinical, educational and administrative applications across the state including: telpsychiartry, telecardiology, telewound, telestroke, bariatric surgery (pre and post op), diabetic education and follow-up, health care revenue cycle, neonatal and pediatric education. Physician desktop solutions support video-conferencing technology to provide telehealth/telemedicine at clinics and hospitals across Wyoming.

Room Considerations

Both the physician video conferencing room and the patient video conferencing room should adhere to normal exam room requirements based on HIPAA requirements and policies for your clinic or hospital. Treat patient privacy to the same level as if you were seeing the patient in person.

Recommended Room Color: Benjamin Moore paint numbers 1627 or 829 This light blue-grey contrasts well against skin tone.

Microphone placement should be close to the patient to receive appropriate patient intake in an Exam Room. Microphone placement should be central to all participants and the use of an omni-directional flat mic works well in small to medium groups. Permanent fixtures such as ceiling mount microphones should be considered for auditorium-like applications or for very large conference rooms. Ceiling mount microphones should not be mounted near in-ceiling speakers, PA announcement systems, HVAC vents, or ceiling mount fans; these items will create ambient noise which will be distracting for a video conference.

Lighting should be controlled room lighting and not natural lighting. Natural lighting from windows will cast heavy shadows and other uncontrollable effects. Windows should be covered or blinds closed during a video conference. Video conferencing equipment should not be facing windows as this will cause attendees to look like ‘silhouettes’. If overhead lighting is not adequate, provide ambient can-lighting fixtures near a wall. These fixtures sit on the floor and point upwards to provide additional ambient lighting and are very inexpensive.

Lighting considerations are especially true when working in an Exam Room environment as patient examination is critical.

Please refer to the Telehealth Provider document for more detailed information.

Video Conferencing Endpoints

System Requirements for H.323 Systems:

The ITU-T H.323 protocol standards should be adopted for Wyoming telehealth video conferencing as it is an industry standard. The following minimum requirements should be included for Room Based video conferencing units as well as H.323 based Desktop video conferencing implementations.

H.323 Stack Minimum Requirements

- IPv4/IPv6 Support
- H.460.17-19 Firewall/NAT Traversal
- UDP Signaling (Annex E)
- HTTP-Based Service Control for H.323 Devices (Annex K)
- Telephony Signaling Tunneling Through H.323 (Annex M)
- DNS support (Annex O)
- Remote Camera Control (Annex Q)
- H.341 MIB Support
- Q.931 Multiplexing
- High Capacity Registration (Additive Registration)
- H.245v13 Advanced Call Control
- H.235v3 Security
- Full H.450 Supplementary Services
- H.245 GEF API
- H.350 LDAP support

System Configurations for H.323 Room Based Systems:

In addition to room considerations and network considerations:

- All telehealth video units should be registered to a public gatekeeper. This gatekeeper will provide a registered alias for direct dialing.
- Video conferencing equipment must be kept up to date by using vendor supplied annual maintenance. Video conferencing equipment that is two (2) revisions of software older or no longer supported by the industry (end of life) should be replaced.
- Video conferencing equipment will be given a static IP address, DHCP is not an option.
- Duplex and Link set to 100 or 1000 Full
- SNMP community is set to: UMC
- Qos is set for Diffserv: Audio: 46, Video: 34, Data and Signaling: 26

- Each video conferencing endpoint will be set with an administrator password and provided only to pertinent video conferencing *IT administrators*.

System Configuration for H.323 Desktop Video Conferencing

Desktop video sessions use the Real Presence Desktop (RPD) application or Polycom PVX application. These applications allow for H.323 video conferences to occur using a web cam, instead of a room based application.

POLICY:

The CMA Desktop contains 300 licenses. In order for outside entities to use a CMA Desktop license, the CRMC video network administrator will need to know the name, address, phone, and email of the individual who would like to use it. The video network administrator will create a username and password for the individual. This will be documented.

PROCEDURE:

- The following is the configuration for a RPD Desktop installation:
    - Registration to: CRMC's external Video Border Proxy External Border Proxy: 65.121.101.125
    - The same firewall ports will be necessary for desktop video conferencing as room based video conferencing systems. Please refer to Appendix A for an overview of common video conferencing ports used.
    - Duplex and Link set to 100 or 1000 Full
    - Qos is set for Diffserv: Audio: 46, Video: 34, Data and Signaling: 26
    - Username and Password is created by the video conferencing administer on the RealPresence Resource Manager and will be provided to the end user.

- Alias Naming Scheme:

    - RPD Desktop Installation: the phone extension of the user
    - In the event of a duplication, add a 1 or successive number to the end of the extension
    - Those on the CRMCWY Network *and* that have an entry in the Outlook Directory will have an alias of their phone number in Outlook

Video Network

Video Network Consideration

The minimum network requirements for video conferencing at each hospital or clinic:

- Minimum bandwidth dedicated to basic video conferencing: 384k
- This number is the minimum, per video conferencing unit, that should be implemented for basic video conferencing which is defined as "people talking with possible H.239 graphics sharing".
- Minimum bandwidth dedicated to advanced video conferencing: at or above 2 Mbps

- This number is the minimum, per video conferencing unit, that should be implemented for advanced video conferencing which is defined as “high definition video of people talking with possible H.239 graphics sharing and advanced peripherals needed for specialty practice”.
- Managed Switch at the video conferencing segments – Layer 3 aware
- Duplex and Link set to 100 or 1000 Full
- Qos is set for Diffserv: Audio: 46, Video: 34, Data and Signaling: 26

Gatekeeper Functionality

For gatekeeper the ITU-T H.460.17, H.460.18, and H.460.19 protocol standards should be adopted for telehealth video conferencing in Wyoming.

- H.225 for RAS and Registration
- Q.931 for setup and connection
- H.245 for negotiated media channel
- H.323 Firewall / NAT Traversal
- H.323 / ALG aware Firewall

Video Conference Calling

POLICY:

- Point to point calls are accepted and encouraged. Point to point calls can be made within the network or with outside entities. Point to point calls within the network may be made by Alias dialing by using the alias, or may be made with the IP address. Video units which contain a Multi-Point feature may place point to point calls with up to 4 entities at one time (license permitting on that specific video unit). However, in most cases if more than 2 video units would like to be involved in a video call the bridge will need to be scheduled to launch the call to all participants.
- Bridging calls are accepted and encouraged. Bridging is ideal when more than 2 participants would like to be involved in a video call.

    - The bridge may also contact video units within the network or with outside entities. The bridge may dial video endpoints using Alias dialing or IP address. Bridge Cascading is not recommended, but may provide a connection method when direct contact with a video endpoint is not possible.

PROCEDURE:

- Scheduled Telehealth Bridged calls are scheduled with the following technology guidelines:
    - Bridge will dial outbound to all locations 15 minutes prior to event start time
    - Call speed: 384k – 1284K
    - Network Layout: Standard, Voice Switched (unless requested otherwise)
    - FECC (far-end camera control on)

- H.239 Graphics set to On
- AES Encryption set to when available
- Auto Video compression (to accommodate current and legacy video equipment)
- Auto Audio compression (to accommodate current and legacy video equipment)
- The organizer of the video event should also specify date, start and end times, lecture mode, continuous presence, or recurrence of event. Speak to the person in charge of scheduling to learn how.
- Meeting rooms are always available.

Video Conference Call Methods

Have Someone Call You

Other video networks may call you directly, via video. In order to do this the following must occur:
- You must provide the far-site your video number IP address
- The video unit must be plugged in; with power and internet access

How to Call Others

You may call other video sites, there are several different ways to do this.
- You will need to know which method to use to call the far-site (please see examples below).
- The far-site must provide you a good, public, IP address for their video conferencing unit.

Method 1: Direct IP Address

Video conferencing networks use a Public IP address. Each address is unique. You will need the specific number from the person you want to call. You may need to ask their IT person for this information. An IP address is a sequence of numbers separated by four periods, such as: 64.238.3.15

Non-Routable IP Address: If you are given the following IP addresses the call will fail as these IP addresses are not public: 10.x.x.x, 192.168.x.x, 172.x.x.x (x can be any number)

Method 2: Alias Dialing

While all video networks are set up differently, some may choose to use an Alias for dialing. Each address is unique. You will need the specific number from the person you want to call. You may need to ask their IT person for this information. An alias will look like a string of numbers, then an '@' symbol, then a public IP address. This routes the call to the proper endpoint on another network. An alias address will look like: 242020@65.121.101.125 or 65.121.101.125##242020.

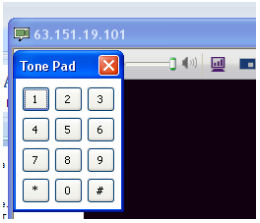
Method 3: Dialing in to a Bridge

In some cases you may be part of a larger conference which uses a bridge. In this case, if you are asked to dial in to their bridge ask which method they would like you to use. Each address is unique. You may need to ask their IT person for this information. They may want you to dial in to their bridge using:

- Direct IP address which looks like 159.238.3.15
- Alias Dialing which looks like 1004@65.121.59.12
- Direct IP address with Room Entry Code which looks like 159.238.3.15##40

If you need to use a Room Entry Code (sometimes referred to as DTMF code) do the following:
Enter the IP address you have been instructed to call (which looks like 159.238.3.15) and choose Call.

Once in the call, choose the Tone Pad from the main menu.
Enter the conference number or entry code you have been given.
Once in the conference close the Tone Pad window.



Real Presence Desktop (RPD) Clinical selection considerations

Cost:

For clinical applications, there are several needs that need to be met in order to bring video conferencing successfully into a clinic environment. Among the most important is that the endpoint costs need to be low, as every provider has several exam rooms and his own desktop. CMA/RPD Desktop is not a computer resource hog. Almost any computer that is from 2-3 years old to any new computer today will have the capacity to facilitate video conferencing. That being the case, it should be almost no cost to find a computer to load the application onto. The software application is free and a high definition web camera is less than $100. This is a very compelling cost proposal to health care providers at this cost of entry level.

Physical space:

With EMR being mandated across the country, either every provider will have a computer or every exam room will have a desktop to facilitate EMR. These very same computers can have the zero cost RPD Desktop application installed. This effectively places video conferencing in every Dr's office and clinic room for zero cost and for not any additional desk space or room required in the exam room.

Availability:

In the recent past it was thought necessary to have equipment for telehealth video conferencing mounted to a cart that was stored somewhere and wheeled in when needed. The size of the cart, relative to a small exam room and the disruption in clinic flow, were large barriers to use. The $20,000 per video codec cost was a barrier

to having them available at all. Today, to be available for a video conference in any exam room in a clinic, the only additional item needed would be to plug in a web cam.

Image:

With technology advances, today's high definition web cam offers superior images to expensive codecs that are just a few years old. For many years other telehealth networks have been using standard definition cameras to deliver telehealth. Today's availability of low cost, high quality images should help diminish any providers concern over visually missing some important aspect of the exam.

Collateral equipment:

There continues to be additional clinical exam support equipment for telehealth. The great news is that with the PC being centric to the exam, the computing power enables many functions that, in the past with dumb video codec's, required separate boxes. Today we have wireless stethoscopes, USB enabled ECG's, and exam cameras. There have been a few pc based ultrasound devices. This availability of PC centric devices should continue to expand.

Infrastructure:

What enables the endpoint cost to be so low is the infrastructure already in place for classic video conferencing along with the free Polycom CMA/RPD desktop application. With Polycom, a DMA 7000 is necessary to manage video bridge conferencing. By adding equipment to enable external access via the DMA 7000 we are able to acquire and then offer low cost per user licenses.

Real Presence download and Configuration

Download the latest version of Real Presence desktop and install it.

Goto:
http://support.polycom.com/PolycomService/support/us/support/video/realpresence_desktop/realpresence_desktop.html

Scroll down to Windows Software Downloads
Select the latest version for Windows (Individual installation) or MAC OS.
Select "I have read the RPD EULA and accept the terms and conditions of updated RPD EULA"
And hit the Submit button. Then select that you agree to the license agreement.
Select Language and hit ok.

Select Enterprise
Leave email blank
Next Screen you will enter 65.121.101.125 for external, 10.252.30.80 for internal.

Accept anything the installer wants to do. Once everything is installed launch the Real Presence desktop. Your user name will start with "Local\" without the quotes. Your logon id should look like:

Local\xxxxxx Capital letters are recognized there is a space between first and last name.

For internal network users check the box that states “use local credentialing”.

TeleHealth/TeleConference Standards

The use of the term “standards-based” and “consumer-grade” to define the different videoconferencing markets may result in some concerns or confusion. After all, some consumer-grade products use standards for video encoding, while other standards-based systems may not implement all of the possible videoconferencing standards.

Below is a collection of many of the standards that are pertinent to videoconferencing, with the caveat that they focus on IP-based, packet-switched networks and products as opposed to ISDN-based or telephony-based systems. You will find a description of the standards below.

Multimedia Call Control Standards – SIP and H.323

These two standards help initiate, manage, and terminate audio-video communications on networks. SIP and H.323 do not communicate between one another, although interoperability can be established with a gateway device, which helps translate between the two protocols. A standard included within the H.323 standard is H.245, which serves as the primary call control “handshake” that occurs between devices at the start of a videoconferencing session. The H.245 standard has been updated to include a faster call control protocol based on the H.255 standard, supporting something called the “Fast Connect” procedure.

Video Standards – H.263 and H.264

These two standards are used to compress video, specifically in this context to reduce bandwidth when sending video data over a network between two video systems. H.264 provides significant improvements in compression over H.263 and older H.26X standards. H.264 is also referred to as H.264/AVC for “Advanced Video Coding,” or Single-Layer H.264.

Audio Standards – G.711, G.722, G.729

These standards are used for commanding audio in video conferencing. G.711 is the standard required by H.323, whereas G.722 and G.729 are optional. The primary difference between these standards is the sampling frequency and compression of the audio. G.722 provides improvements by doubling the sampling frequency of the audio when compared to G.711, which results in a potential improvement in the quality and clarity of the received audio, but an increase in the required bandwidth. G.729 requires less bandwidth by providing a less literally accurate transmission of sound that has been optimized for speech. This may make speech sound clearer, but less true to the actual voice data (and likely to be non-ideal for medical diagnosis, such as electronic stethoscopy).

Testing to confirm teleconferencing capability interoperability

There are two types of dialing supported by video conferencing bridges. End point to end point dialing and meeting room dialing. These tests, to be considered valid for interpretational reasons, need to be performed between two or more differing manufactures equipment. Today the major manufactures are Polycom, Cisco, Radvision, and Logitech.

Open end point to endpoint dialing. Both audio and video connections need to be present and stable.

1. Direct IP dialing. This test should be performed bi-directionally. That is defined for these purposes that one video codec is first an endpoint originator of the call and then for the second part of the test it is the receiving endpoint of the call. This test is for video codecs that typical have static IP address either in the open or behind a firewall. Obviously firewall traversal and NAT may play a pivotal role in this test. The test will consist of entering a ip address and successfully connecting with endpoint.

2. Direct IP dialing with the addition of an alias. This is the same test as above with the added requirement that the aliased endpoint can be reached. The ideal situation would be a single string of numbers and characters that would result in and endpoint being connected. The reason for this is to be able to build global address books that span differing systems but require easy use by a user with no knowledge of which system they are dialing into. With a single click the user would connect two endpoints. The test would consist of entering a single string of characters that includes an IP address and successful connecting with another endpoint. with additional characters or numbers

3. It needs to be determined by the user community that if first connecting to and entry cue and then dialing an alias is acceptable. It is not known if this can be a part of a address book entry.

Virtual Meeting Rooms (VMR) dialing.

VMR's are used sometimes because an unknown number of people attending a conference or the people joining may not be known in advance. Other reasons are to give a persistent electronic place to conduct business or deliver care. There are no tests that need to be applied for meeting rooms that are on the same network. For connecting with a meeting room externally the connection scheme should be the same as above. Either direct IP dial or dial with an alias.

Encryption.

Video conferencing equipment is expected to be able to negotiate an encrypted connection using AES 256 bit encryption algorithm between two different systems

Appendix A

Which H.323 TCP_UDP ports are needed or used by Polycom Video and Network Products?

Following is a summary of TCP/IP ports needed.

• **SIP Related Port Usage**

• 5060 – UDP or TCP depending on the SIP server – Signalling

LCS & Alcatel OXE use TCP

• RTP data is the same as for H.323 so same media ports apply

• **H.323 Related Port Usage**

H.323 Ports:

• 80 - Static TCP - HTTP Interface (optional) Address Book Utility

• 389 - Static TCP - ILS Registration (LDAP)

• 1503 - Static TCP - T.120

• 1718 - Static UDP - Gatekeeper discovery (Must be bidirectional)

• 1719 - Static UDP - Gatekeeper RAS (Must be bidirectional)

• 1720 - Static TCP - H.323 call setup (Must be bidirectional)

• 1731 - Static TCP - Audio Call Control (Must be bidirectional)

• 1024-65535 Dynamic TCP H245

• 1024-65535 Dynamic UDP - RTP (Video data)

• 1024-65535 Dynamic UDP - RTP (Audio data)

• 1024-65535 Dynamic UDP RTCP (Control Information)

These ports above, can be set to "Fixed Ports" on Polycom systems, as opposed to dynamic.

Other ViewStations/VSX/HDX/Group Series Ports:

• 21 (FTP) - Software Updates, GMS Provisioning, & Address Book Utility

• 23 (Telnet) - For Diagnostics & API Control (used by PCS) by MP/512/ect.

• 24 (Telnet) – For Diagnostics & API Control (used by PCS) by FX/EX/4000, VSX, and HDX

• 123 – UDP – Used for NTP (time server) on the VSX

• 3231 to 3236 - TCP Ports (default fixed ports VSX version 8.5)

• 3231 to 3254 - UDP Ports (default fixed ports VSX version 8.5)

• 16384 & 16386 – Multicast Streaming ports for audio & video

VSX/HDX Security Mode additional/alternate ports:

• 443 (TCP) – secure HTTP; HTTPS

• 992 or 993 (TLS) – secure Telnet

• 990 (FTPS-TLS) – secure FTP

People+Content IP Ports:

• 5001 - Static TCP

GMS Ports:

• 21 (FTP/TCP) - Software Updates & Provisioning

• 23 (Telnet/TCP) – Diagnostic Logging

• 25 (SMTP:TCP) – Remote e-mail alerts

• 80 (HTTP) - Pulling ViewStation/VS4000/VSX/HDX info

• 162 (SMTP:UDP) – Remote Alerts to an SNMP server

• 389 (LDAP:TCP) - LDAP and ILS

• 1002 (LDAP:ILS) - ILS

• 3601 (Proprietary/TCP) (Data Traffic) - GAB data

• 3603 (TCP)- Pulling ViaVideo / PVX info (since might be non-web server PC)

• 9090 (formally 8080) (HTTP:TCP) – Proprietary database communications, port is user-configurable

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

PCS Ports:

Communication between PCS and Devices:

• 23 (Telnet) – Management & Control – Tandberg Codecs

• 24 (Telnet) – Management & Control – Polycom ViewStations, VSX, and HDX

• 161(SNMP) – Managed device

• 2000 (TCP/IP) – Gatekeeper call authorization for outbound communications – Cisco MCM

• 2773 (TCP/IP) – Management & Control – Polycom iPower, VCON codecs

• 3603 (HTTP) – Management & Control – Polycom ViaVideo and PVX

• 4000-4004 (TCP/IP) – Management & Control – Lantronix

• 5001 (API via TCP/IP) – Management & Control – Polycom MGC

• 8000 (TCP/IP) – Gatekeeper call authorization for outbound communications – Cisco MCM, RADVision ECS

Communication between PCS and Client:

• 80 (HTTP) – General Communication – Web browser

• 2771 (TCP/IP) – Data communication – Remote SQL server, Outlook / Notes Mail server

• 2773 (TCP/IP) – remote – Polycom Conferencing Suite Server

• 2777 (TCP/IP) – Mail & Calendar communication – Outlook / Notes mail server

Communication between PCS Servers:

• 700 (TCP/IP) – Redundant server communication - PCS

• 2771 (TCP/IP) – Distributed Server communication - PCS

Other ViaVideo / PVX Ports:

• 3230-3235 (TCP / UDP) Signaling and control for audio, call, video and data/FECC

• 3230-3237 (TCP / UDP) Signaling and control for audio, call, video and data/FECC, version 8.0 and beyond

• 3604 (GMS Server Discovery)(Used by ViaVideo & PVX)(Broadcast) used by PCS

RMX 2000 (Polycom Network Systems) Additional Ports:

• 5001/1025 Static TCP for RMX Manager.

• RMX Manager can also use TCP 443 for secure connections or TCP 80 unsecured access.

• 21 - Static TCP - FTP (retrieve RMX config. Files etc.)

• 5003 TCP for diagnostics access.

• TCP 17 For Diagnostic Remote Desktop access to RMX's running XPEK OS.

PathNavigator Ports:

From PathNavigator to Endpoint

• Varies by endpoint - UDP – RAS (Registration, Admission and Status)

• 1720 – TCP (Q.931) – Setting up calls when PathNavigator is in routed mode

From Endpoint to PathNavigator

• 1719 – UDP – RAS

• 1720 – TCP (Q.931) - Setting up calls when PathNavigator is in routed mode

From Monitoring Workstation

• 80 – TCP – for HTTP communication with PathNavigator UI

SE200 Ports:

Open ports on the SE200

• 80 / 85 (HTTP / TCP) – The Apache Web server through which the web application displays and where the Polycom endpoints post status messages

• 123 – An NTP listener

• 135 – The Microsoft RPC port

• 137 – The NetBIOS name service listener

• 139 – The NetBIOS SMB listener

• 161 – The SNMP listener

• 781, 782, 783, 784, 785 – Used by the Administrative Diagnostic Tool

• 1042 – A .NET listener used for the SQL server

• 1063 – A .NET listener

• 1167 – A .NET listener

• 1433 The internal NSDE server listens on this port which enables views into the database from outside the SE200

• 1720 The gatekeeper listener for RAS messages

• 2771, 2773 – Used by the scheduling plug-ins

• 3601 The Global Management System listener that endpoints register with

• 5005 – The .NET listener for the MGC Authentication Service and API adapter

• 8009 – the .NET listener for Tomcat-related services

• 8080 – The Apache Tomcat Java server which displays the Java Sever Pages for the user interface. It is proxied through the Apache server running on port 80

• 8085 – The .NET listener for remote access

Ports used by the SE200

• 20,21 – Used to FTP data to endpoints

• 23 - Used to access the Telnet interfaces on endpoints
• 24 – Used to access a secondary Telnet interface on endpoints
• 25 – Used to send e-mail messages to SMTP servers
• 53 – Used to access domain name servers (DNS)
• 80 – Used to access the web application on endpoints and MGCs (version 7.x and higher)
• 389 – Access by the SE200 when contacting Active Directory
• 1205 – Used to access MGCs for management and monitoring
• 1719 – Used by the gatekeeper for H.323 datagrams
• 1720 – Used by the gatekeeper for H.323 RAS messages
• 3268 – Used to access the Active Directory Global catalog
• 5001 – Used to access MGCs for management and monitoring

WebOffice Ports:

• 80 / 85 (HTTP / TCP) – WO client communications with WO sever
• 443 / 85 (HTTP / TCP) – WO client communications with WO sever
• 5005 (proprietary) – WO Server uses this service to translate commands to MGC (usually internal port)
• 5001 / 1205 (proprietary) – WO server and MGC communication

V 2 IU (firewall must allow these ports to and from the V 2 IU):

In all cases

• 21 (FTP / TCP) - optional
• 80 (HTTP / TCP) - optional for management
• 443 (HTTPS / TCP) - optional for management
• 16386:17286 (RTP / UDP) - 4300T-E3
• 16386:25386 (RTP / UDP) - 5300-E10 and E25
• 16386:34386 (RTP / UDP) - 6400-E and S85
• 161 (SNMP / UDP) - optional for management
• 22 (SSH / TCP) - optional for management
• 23 (Telnet / TCP) - optional for management
• 69 (TFTP / UDP) – optional
• 123 (SNTP / TCP) – 123 optional

MGCP phones

• 2427, 2429, 2432, 272 (MGCP / UDP) – optional

SIP Phones

• 5060 (SIP / UDP) - plus and additional ports specified on the VoIP ALG page – optional

• 5050 (SIP / UDP) – when survivability enabled optional

H.323 Endpoints

• 1720 (Q.931 (H.225) / TCP)

• 1719 (RAS / UDP)

• 14085:15084 (H.245 / TCP)

Please see the Polycom knowledge base for the White Paper defining this information for the V 2 IU ports.

RSS 2000 and 4000 Recording and Streaming Device:

In all cases

• 81 (TCP) - Manger

• 80 (HTTP / TCP) - Web

• 30011 (UDP) – Trace

• Endpoint H.323

• 1719 - Static UDP - Gatekeeper RAS (Must be bidirectional)

• 1720 - Static UDP - RAS (Must be bidirectional)

• 1720 - Static TCP – Q931 socket

• 1730 -1739 - Static TCP – H.245 Socket

• 2000 – 2099 – UDP - Audio/Video/Data

• Media

• 1800 -1801 - Static TCP – Live Broadcast

• 2800 – 2859 – Static TCP – On Demand Archive

RTP Type (VSX, HDX and Group Series applicable):

See 6/RFC3551. RFC3551 it defines static payload type values for some RTP data (such as G.722, G.711, H.261, H.263, etc), but not for the newer codecs such as G.722.1, H.263 +, H.263 ++ and H.264. For the newer codecs, dynamic payload type values in the range 96 - 127 are used.

Appendix B

Polycom RPD and Polycom RMX System Requirements and Documentation

Please refer to the Polycom website for the most current documentation:

http://support.polycom.com/PolycomService/support/us/support/video/index.html
or
http://support.polycom.com/PolycomService/knowledgebase/search.htm

Web cam recommendations may become outdated. Therefore a make and model will not be specified in this document. Today's technology allows for better web conferencing with advances in web cam manufacturing. To obtain the best experience it is recommended to avoid using a web cam older than 5 years old.