Polycom VBP Architecture and Design Whitepaper

March 2010

POLYCOM®

Trademark Information

Polycom®, the Polycom "Triangles" logo, and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common-law marks 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.

3725-78300-003A

Polycom, Inc.

4750 Willow Road

Pleasanton, CA 94588-2708

USA

Contents

Introduction

Businesses today are facing both unique communication challenges and strong financial constraints. Globalization has resulted in more dispersed work teams. The business-to-business communication model has made communication with customers, partners, and vendors more important than ever. At the same time financial pressures are forcing businesses to reduce their travel budget.

IP video conferencing is one solution to these problems. It can provide businesses substantial communications efficiencies and cost savings. However, IP video conferencing is typically only possible between businesses that have similarly configured video conferencing equipment and firewall rules.

The biggest difficulty to IP video conferencing is Network Address Translation (NAT). NAT is a popular method for allowing a one-to-many relationship of IP addresses in a corporate network. NAT keeps track of requests from machines inside a network to machines outside the network. To the outside world, all requests appear to come from one IP address, the public address. As information comes back, NAT handles the translation from the one public facing address back into the internal addressing scheme.

NAT was originally designed to help reduce the size of the Internet address space corporations needed on their network. NAT was developed in a way that the NAT device was responsible for translating traffic from the internal, private address space to the external space. By performing the translation at the border to the public network, one address can be used for a multitude of machines.

NAT also hides the footprint of the network. Because all communication occurs through the NAT device, the network endpoints are obscured. This provides a level of security to the network as it is difficult for prying eyes to know how many hosts exist on a network, much less the types of devices located there. Another security consideration is that since the connection to the endpoint must be initiated from inside the network and cannot come from the outside, it is impossible to connect into the network uninvited. This security provided by NAT causes a headache for videoconferencing over IP.

Other challenges to video conferencing exist, including:

- Endpoint connectivity – A particular issue when using a standard firewall for a conference call. Many default configurations in standard firewalls cause an IP Videoconferencing call to terminate at given times, commonly 2 hours, due to a TCP Connection Timeout setting.Traffic management
- Differing security policies
- Differing vendor standards
- Encryption –Several firewalls do not allow an encrypted call to traverse, requiring an alternate method to ensure privacy is maintained. This is where a Polycom VBP appliance would be required.
- Generally, a 1-1 NAT for each endpoint on the Enterprise network is required, which means that a large public IP space must be maintained by the organization at substantial cost.

In addition to solving these problems, an IP video conferencing solution must provide:

- Quality of Service (QOS) for video traffic via packet queuing provisioning
- Support for video specific protocols
- Intrusion protection and secure inter-device communication
- Monitoring of the video infrastructure and calling instances

- Where possible, the management of internal and external video device operating system updates and problem resolution.
- Directory presence for ease-of-use execution of video calls

The Polycom Video Border Proxy™ (VBP™) Solution

The Polycom VBP series of NAT/firewall traversal appliances provide businesses with the means to overcome the barriers to IP video conferencing. They facilitate communication, speed decision-making, and accelerate execution by extending video conferencing to users beyond the enterprise network. With the Polycom VBP series of firewall appliances, customers, partners, vendors, and remote colleagues can be easily and securely incorporated into an extended video federation.

Polycom VBP appliances work in conjunction with, or in some cases can replace, your existing firewall, and provide a trusted route for IP video traffic.. Polycom VBP appliances are layer 7 H.323 video and voice-aware firewalls that perform network address translation (NAT) at the IP address boundary and forward video to the appropriate H.323 endpoint.. They also employ stateful packet inspection (SPI) in combination with an application layer gateway (ALG) to support standards-based H.323 video solutions.

It is also important to have an overall view of your network and how video will affect it. The Polycom website includes a good reference whitepaper entitled *Supporting Real-time Traffic - Preparing Your IP Network for Video Conferencing*. For this and other useful whitepapers, go to `http://www.polycom.com/products/resources/white_papers/index.html`.

Polycom VBP appliances fully protect H.323 gatekeepers, video endpoints, and multipoint conference platforms from external network-based attacks, while safeguarding video quality. They enhance network security with an H.323-aware packet inspection firewall that opens and closes TCP and UDP ports based on the session establishment. Their secure H.323 proxies allow one public IP to serve an enterprise's video communications needs. Available for throughput from 1 Mbps to 85 Mbps, the Polycom VBP series of appliances is also configurable for centralized or decentralized dial plans, depending on IT requirements.

With the following features, Polycom VBP appliances optimize video quality and video traffic management.

- Traffic shaping (QOS) for seamless prioritization of video packets over data across network
- Media routing via the shortest possible path
- Video and voice call control to prevent congestion of priority traffic
- Traffic management such as priority queuing, traffic shaping, and diffserv marking/policing
- Routing to H.323equipment
- H.323 bandwidth management of video, voice and data
- Video/data aware NAT server that allows for the dynamic mapping of ports for firewall traversal
- Demarcation point for troubleshooting
- Interoperability with legacy devices, H.239 and AES support
- Gain additional connectivity scenarios with H.460 and Polycom VBP NAT/firewall traversal appliances

Polycom VBP solutions support all standards-based video endpoints and multipoint conferencing units, such as the Polycom RMX 2000™ real-time media conferencing platform. Models with optional H.460 support for mobile users or remote locations without video-aware firewalls are also available.

The Polycom VBP series of appliances offer not only a secure network link but also have quality of service support for the protocols used in video communications. They can establish a solid connection between internet locations, which is required for a successful video conference call between multiple sites with several participants.

Polycom VBP Series

The Polycom VBP series includes models for all environments. Use the following table to determine the model best suited to the size of your enterprise.

Model	Purpose	Performance	Number of Registrations	Embedded Gatekeeper	Access Proxy
6400 ST	Large enterprise or service provider class. Configurations to support an endpoint edge or a server edge.	Up to 85 Mbps of traffic in any combination of voice, video or data	250	No	Yes
6400 E				Yes	No
5300 ST	Medium sized business models. Configurations to support an endpoint edge or a server edge.	Up to 25 Mbps of traffic in any combination of voice, video or data	5300 ST-10 = 50 5300 ST-25 = 100	No	Yes
5300 E			5300 E-10 = 50 5300 E-25 = 100	Yes	No
4350 E	Ideal for small, remote branch locations.	Up to 3 Mbps of traffic in any combination of voice, video or data	15	Yes	No
200 EW	Home office	Up to 1 Mbps of traffic in any combination of voice, video or data	3	Yes	No

Use the following table to choose between the four top Polycom VBP models.

The Polycom VBP-E appliance is a proxy for calls to and from unregistered external participants. The Polycom VBP-E appliance can also be used as a basic router and DHCP server for SOHO environments.

The Polycom VBP-ST appliance is a (VPN for video) way of allowing external parties to register to the internal call processing server (gatekeeper). The Polycom VBP-ST appliance also acts as a traversal server for remote clients who are behind a local firewall by using the H.460 tunneling protocol.

Function	VBP 5300-E	VBP 5300-S & 5300-ST	VBP 6400-E	VBP 6400-S & 6400-ST
Resolves NAT/firewall traversal problems by providing an application layer gateway (ALG) that supports voice and H.323 protocols. (The Polycom VBP provides NAT services for the protected softswitch, gatekeeper or other media devices. Application layer gateway dynamically provisions and closes UDP ports used for video and voice calls.)	X	X	X	X
Protects the enterprise LAN using a stateful packet inspection (SPI) firewall for both H.323 and data traffic. (A stateful firewall can track significant attributes of a video session from start to finish. This includes such details as the IP addresses and ports involved in the connection.)	X		X	
Protects the enterprise LAN using a stateful packet inspection (SPI) firewall for H.323 traffic		X		X
Application aware firewall dynamically opens and closes UDP ports used for H.323 (video and voice) calls.	X	X	X	X
Provides NAT and PAT for data that hides enterprise LAN topology	X		X	
Provides NAT and PAT for H323 that hides enterprise LAN topology	X	X	X	X
Provides integrated tools to facilitate problem isolation Logging and TCP Dump	X	X	X	X
Uses a simple web based GUI for configuration	X	X	X	X
Performs static IP routing	X	X	X	X
Supports logging to external syslog servers	X	X	X	X
Provides a DHCP server for enterprise PCs and video devices	X		X	
Supports access proxy – requires H.460 traversal “ST” - S systems will need to be upgraded.		X		X
Provides H.460-based traversal support (1)		X		X
Supports Ethernet WAN types	X	X	X	X
Supports WAN protocols, DHCP, ADSL-PPPoE, Static IP	X		X	
Supports WAN protocols, DHCP, Static IP	X	X	X	X
Supports up to 16 VLAN’s	X		X	

(1) ST models only

(2) ST models do not support data NAT related features placed parallel to the existing firewall installation.

Minimum Bandwidth Recommendations

Bandwidth is a major concern for video conferencing due to its high utilization of bandwidth. The bandwidth required for even a single conference using low quality audio and video adds up to a lot of bandwidth as the number of users increases. For this reason a careful evaluation of network capabilities must be made to ensure that conferences run smoothly at the desired quality and that they do not affect the normal traffic flowing on a network.

It is important for administrators to recognize the bandwidth demands video conferencing has on networks. Here is an introduction to this. A full discussion is available in the document referenced earlier - *Supporting Real-time Traffic - Preparing Your IP Network for Video Conferencing* located at `http://www.polycom.com/global/documents/whitepapers`.

The bandwidth component of the video conference is defined as client bandwidth and WAN Bandwidth. Client Bandwidth is the LAN network supporting the video endpoint and should be at 100mbps full-duplex. The WAN Bandwidth supports the external connections and is more variable and depends on the infrastructure supporting it.

The table below illustrates how leading Polycom endpoints and bridges consume bandwidth, per site.

Minimum bandwidth rates are listed per resolution. Both endpoints and bridges support a far wider range of resolutions than those shown at a wide variety of line rates, but the table illustrates the most frequently discussed call types with minimum bandwidths.

Resolution	**Audio**	**CIF 352x288**	**4CIF30 704x576**	**720p30 1280x720**	**720p60 1280x720**	**1080p30 1920x1080**
HDX endpoints	64k	128k	256k	832k	1.2Mb*	1.7M*
RMX 2000 Bridge	64k	128k	256k	1024k	1920k	4096k

*HDX 8000 series only

Deploying a Polycom VBP Appliance

The Polycom VBP series of firewall appliances are designed to support video conferencing while keeping certain types of traffic out of a network and are usually deployed in strategic points in the network infrastructure. The most common implementations include:

- Between the public Internet and the corporate network linking the internal locations but also have visibility to outside endpoints allowing calls in to the network.
- Between segments of the corporate network linking of internal locations of the business
- Between branch offices and the corporate network

For each of these designs to work well it is necessary to have or add sufficient bandwidth for video conferencing. Networks with point-to-point leased lines may want to leverage existing connections to the Internet for video conferencing and still have solid firewall security. This Internet solution helps to keep down congestion on their point-to-point leased lines.

Firewall rules are set based on the specific needs of the network it is protecting, so the first step in preparing your business for video conferencing across firewalls is a review of the current network infrastructure and an assessment of your company's video communication needs.

Regardless of where a Polycom VBP appliance is installed, the overall importance of using a Polycom VBP is to keep the network secure while offering solid performance of the video conferencing business tool.

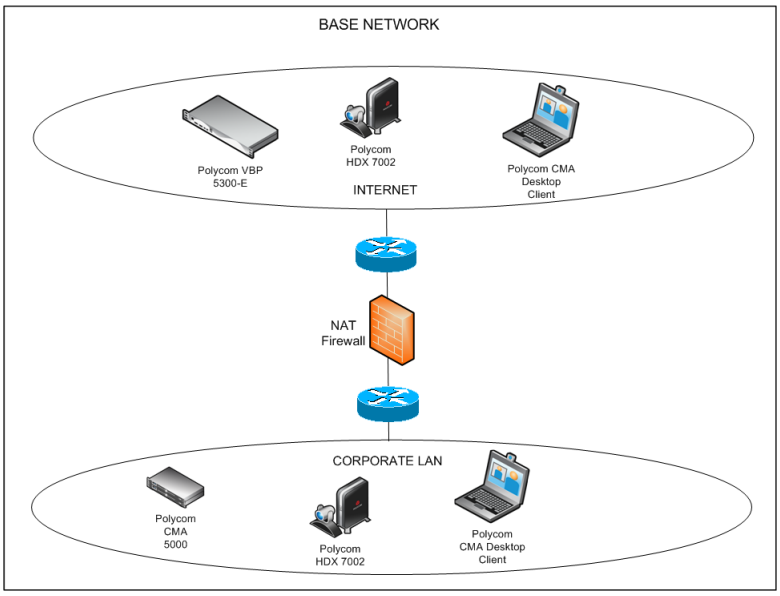
General Network Firewall Considerations

Polycom VBP Appliance Placement

A Polycom VBP appliance can be placed in the corporate network with or without consideration of the existing corporate firewall. As discussed earlier, the Polycom VBP is a very secure appliance designed for securing video conferencing. The nine network designs that follow show the possible placement of Polycom VBP appliances. A discussion of these installation scenarios is important for a clear understanding of how the Polycom VBP enhances the security of your network..

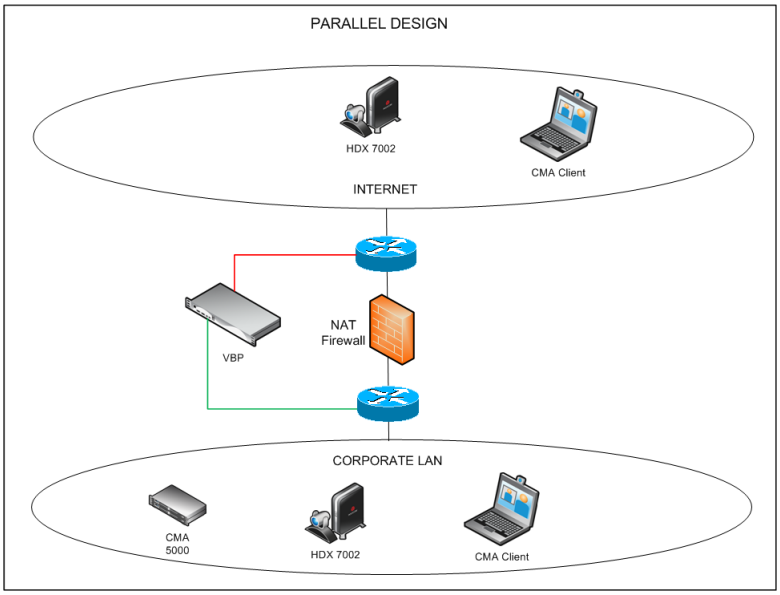
The primary configuration decision is the location of the H.323 gatekeeper. For the Polycom VBP E-Series to perform its mapping of many private-IP endpoints to a single public IP address, and allowing both inbound and outbound calls, there must be an H.323 gatekeeper in use; the gatekeeper can be the Polycom VBP E-Series itself. The Polycom VBP E-Series works in conjunction with a gatekeeper to map endpoints names (alias string or E.164 number) to IP addresses, and to map public IP addresses to/from private ones.

Polycom VBP Operating Outside NAT Firewall



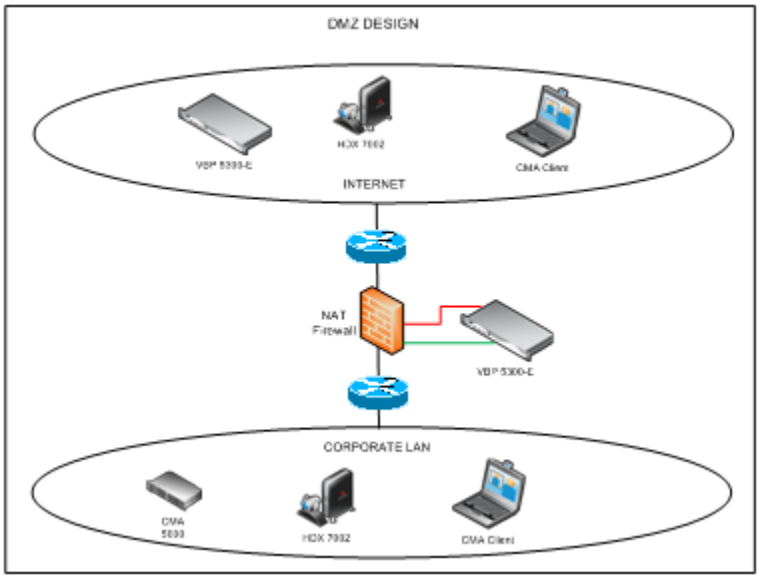
This Polycom VBP installed outside the firewall will pass all of the video traffic through the firewall. Traditional firewall/NAT solutions are not H.323 aware and will block H.323 video conferencing traffic. The firewall will need to be configured for passing the video traffic both ways for all of the ports listed in the Network Security section below. This is possible and can be considered a viable solution with careful configuration of the firewall so as to keep the troubleshooting capabilites of video calls placed via the Internet.

Polycom VBP Operating in Parallel with NAT Firewall – Recommended Solution



This Polycom VBP video firewall appliance is best installed to work parallel to the corporate firewall. The configuration and management of ports necessary for a video call, done via the Internet, is integrated in the Polycom VBP appliance. The Polycom VBP is specifically designed to support the secure and controlled flow of real-time audio and video traffic. One of the main advantages of the Polycom VBP appliance is the way it successfully passes the H.323 signals through the firewall. Bandwidth management and quality of service for the call are other advantages of having the Polycom VBP placed parallel to the firewall.

Polycom VBP Operating in Parallel with NAT Firewall and Polycom VBP Operating Outside NAT Firewall



This Polycom VBP installed in a DMZ configuration will also need to pass all of the video traffic through the firewall. The same concerns apply to this design as described earlier in *Polycom VBP Operating Outside NAT Firewall* on page 9 design. The implementation is can be done with the WAN port of the VBP in a

publicly-addressed DMZ space. Additionally the traffic shaping (QOS) and bandwidth management are restrained.

Network Security

The application layer gateway dynamically provisions and closes UDP ports used for video and voice calls. The NAT/PAT server hides enterprise LAN topology. Applying the use of the H.323 protocol and the H.460 protocol along with stateful packet inspection of the traffic crossing the firewall protects the network against outside vulnerabilities. The use of H.460.18 is critical to the video call connection process. The adoption and use of these protocols in inter-business, business-to-business communications positions the Polycom VBP as a system designed as the perfect complement to the corporate data firewall.

- Polycom VBP-E Series—Enables LAN- or WAN-side gatekeeper functionality, prefix dialing, neighboring of other Polycom VBP appliances, and federation of system sites. This series is designed for enabling video conferencing with video endpoints outside the network that are not registered with a gatekeeper, as may be the case with a distributed dial plan.
- Polycom VBP-ST Series—Optimized for networks in which all endpoints are registered to a central gatekeeper. It also enables external endpoint management, LAN-side gatekeeper functionality, and allows for external endpoints to register to the internal gatekeeper. It also supports LDAP directory, XMPP and provisioning for unified communications devices. This series is the best choice when H.460-based traversal services are needed in conjunction with a centralized gatekeeper

Polycom VBP Access Proxy – What is it and How is it Secure?

Users can use video regardless of being on the network or on the Internet.

Users are not required to use VPN for video. Most VPNs are not set up for real-time traffic, so customers should expect a better experience with access proxy than through the VPN

The experience for the users to use video is the same inside the network or outside. Access proxy helps make video VERY easy to use.

- Access proxy helps users that are behind firewalls without having to reconfigure NAT or open up ports.
- Access proxy allows partners/customers to use Polycom CMA Desktop client even though they are not part of their corporation.
- Access proxy allows IT to manage devices that are on or off the network the same way.

Simply defined, access proxy is a feature added to the Polycom VBP-ST that will allow authorized outside endpoints access to the Polycom CMA system for unified communications services, which includes the Polycom CMA system managing the endpoints.

What are those services?

- HTTPS – Port 443 – Used for initial connection creation and user authentication
- XMPP – Port 5222 – Jabber or presence information to/from the remote clients
- LDAP – Port 389 – Directory searching for users that you want to add as buddies

The Polycom VBP-ST is a secure reverse proxy – reverse because proxies usually go out instead of in. The access proxy accepts Internet/Subscriber side requests for unified communications services and proxies them to Polycom CMA system as the Provider IP address

Proxy clarification – A proxy will re-source the layer 3 IP of the request going in or out

NAT clarification – NAT will re-source the layer 3 IP on outbound to the source IP address and for inbound it will resource to the destination IP address.

Access proxy re-sources the Layer 3 IP going both ways, so the packets will always look like they're coming from the Subscriber or Provider interface IPs.

The E-Series is designed to be the gateway from your enterprise network to the Internet. Calls to/from internet-based H.323 devices securely traverse the E-Series to your video network. The E-Series is analogous to a POTS Gateway in a VoIP/PBX system.

Certificates and SSL

The Polycom VBP comes with default self signed certificates to configure the access proxy. These certificates can be changed by the customer to use their own signed certificates. The access proxy can have different certificates for each protocol making the SSL encryption different for each service

All unified communications protocol's are wrapped in SSL headers, so nothing is sent in the clear.

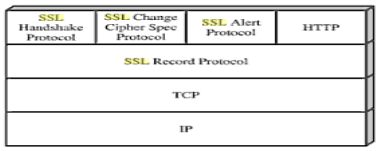
H.323 functionality is completely standards-based, utilizing AES for payload encryption to enable media security. .

Polycom VBP Access Proxy – What is SSL?

TLS/SSL (Transport Layer Security/Secured Sockets Layer) is a method to encapsulate data by using a public/private key exchange.

Imagine sending mail through the postal system in a clear envelope. Anyone with access to it can see the data. If it looks valuable, they might take it or change it. An SSL certificate establishes a private communication channel enabling encryption of the data during transmission. Encryption scrambles the data, essentially creating an envelope for message privacy.

Each SSL certificate consists of a public key and a private key. The public key is used to encrypt information and the private key is used to decipher it. When a web browser points to a secured domain, a SSL handshake authenticates the server (web site) and the client (web browser). An encryption method is established with a unique session key and secure transmission can begin.



Polycom VBP Access Proxy – What SoHo routers work?

Below is a list of what routers were tested during the initial development efforts, this is not a complete list, and will be updated as more routers and software version are tested. If you have a router that is not on this list and you know it works, and/or, have made a router work, please send that information to your Polycom

representative along with any work-arounds that you have made to that device. The unified communications related services should work with no issues. The most important issue is how the routers react to the H.460 protocol and having multiple H.460 devices behind them.

Manufacture	Model –HW version	SW version	Multiple H.460 endpoints	Issues noticed
Netgear	WGR614-v9	1.2.2NA	Yes	none
Linksys	WRT54GL-v1.1	4.30.11	Yes	none
Dlink	WBR-1310-B1	2.00	No *	Router tends to reboot occasionally
Linksys	WRT54G2-v1	1.0.01	Yes	none
Belkin	F5D9231-4-v1	1.00.01	Yes	none

Port & Protocol List for Deploying a VBP Access proxy in the DMZ

The VBP line can be installed with the WAN interface directly Internet-connected, as well as with either interface in a DMZ, or both interfaces in a DMZ. The ports and protocols required for proper VBP operation are similar for the E and ST Series units, while the ST utilizing the Access proxy feature has additional requirements. When creating the ruleset for the firewall interface(s), remember that the VBP is a Proxy for H.323 (and Access proxy functions if in use), which means that packets seen on the LAN side will be sourced from the VBP's LAN IP and destined to the VBP's LAN IP, while packets on the WAN side will be sourced from the WAN IP and destined to the WAN IP.

Note that for public-Internet connectivity, the VBP requires a publicly-routable, non-NAT'ed IP address to be assigned to the WAN interface.

The following tables enumerate the ports and protocols for the VBP line.

Using the Polycom VBP in a firewall DMZ configuration, the following protocols are required, RAS, Q.931 (H.225), H.245, RTP as specified per platform.

For H.323 specific ports, see Table 2, Table 3, and Table 4.

- Table 2 explains the H.323 ports inbound and outbound from the WAN interface.
- Table 3 explains the H.323 and access proxy ports inbound and outbound from the WAN interface.
- Table 4 explains the H.323 ports inbound and outbound from the LAN interface.

The firewall in front of the Polycom VBP must allow the following ports inbound to the Polycom VBP:

Table 1

This table lists all ports and all protocols for all models that may be required.

FTP	TCP	21 (optional)
HTTP	TCP	80 (optional for management)
HTTPS	TCP	445 (optional for management, this port is adjustable in the **HTTPS Certificate** page)
HTTPS	TCP	443 (access proxy)
XMPP	TCP	5222 (access proxy)
LDAP	TCP	389 (access proxy)
RTP	UDP	16386 - 17286 (4300T-E3) 16386 - 25386 (5300-E10 and E25) 16386 - 34386 6400-E and S85)
SNMP	UDP	161 (optional for management)
SSH	TCP	22 (optional for management)
Telnet	TCP	23 (optional for management)
TFTP	UDP	69 (optional)
SNTP	TCP	123 (optional)
H.323 Endpoints		
Q.931 (H.225)	TCP	1720
RAS	UDP	1719
H.245	TCP	14085 -15084

Table 2

Table 2 lists the ports and protocols required for standard H.323 operation on the WAN interface of the VBP. The top section lists the requirements for packets from Internet to VBP WAN interface, and the bottom section lists from VBP WAN to Internet.

H.323 Endpoints Specific				
Inbound from the Internet to Polycom VBP WAN/Subscriber Interface IP				
SRC IP	SRC Port	DST IP	Proto	DST port
Any	1024 - 65535	VBP WAN IP	UDP	1719
Any	1024 - 65535	VBP WAN IP	TCP	1720
Any	1024 – 65535	VBP WAN IP	TCP	14085 - 15084 (contiguous range)
Any	1024 – 65535	VBP WAN IP	UDP	16386 - 17286 (200EW,4300,4350,4350EW) (contiguous range)
				16386 - 25386 (5300-E/S10 and E/S25) (contiguous range)
				16386 - 34386 (6400-E and S85) (contiguous range)
Outbound to the Internet from Polycom VBP WAN/Subscriber Interface IP				
SRC IP	SRC Port	DST IP	Proto	DST port
VBP WAN IP	1024 – 65535	Any	TCP	1024 – 65535
VBP WAN IP	1024 – 65535	Any	UDP	1024 – 65535

Table 3

Table 3 lists the ports and protocols required for the VBP-ST Series when utilizing the Access Proxy feature. Again, these are listed with the top section having the requirements for packets from Internet to VBP-ST/AP WAN interface, and the bottom section lists from VBP-ST/AP WAN to Internet.

Inbound from the Internet to Polycom VBP WAN/Subscriber Interface IP				
SRC IP	SRC Port	DST IP	Proto	DST port
Any	1024 – 65535	VBP WAN IP	UDP	1719
Any	1024 – 65535	VBP WAN IP	TCP	1720
Any	1024 – 65535	VBP WAN IP	TCP	443
Any	1024 – 65535	VBP WAN IP	TCP	5222
Any	1024 – 65535	VBP WAN IP	TCP	389
Any	1024 – 65535	VBP WAN IP	TCP	14085 - 15084 (contiguous range)
Any	1024 – 65535	VBP WAN IP	UDP	Access proxy in version 9.1.5.1 is only supported on the ST related platforms
				16386 - 25386 (5300-E/S10 and E/S25) (contiguous range)
				16386 - 34386 (6400-E and S85) (contiguous range)
Outbound to the Internet from Polycom VBP WAN/Subscriber Interface IP				
SRC IP	SRC Port	DST IP	Proto	DST port
VBP WAN IP	1024 – 65535	Any	TCP	1024 - 65535
VBP WAN IP	1024 – 65535	Any	UDP	1024 - 65535

Use the below chart to configure the Polycom VBP in a DMZ/port filtering on the LAN side, this is sometimes required for IT departments that want to monitor traffic going to/from the LAN interface of the Polycom VBP.

The Layer 3 traffic to and from the LAN interface of the Polycom VBP cannot be NATed by the firewall, the Polycom VBP must see the real LAN IP of the H.323 endpoint.

Table 4

Table 4 lists the ports and protocols required for proper operation on the LAN interface of the VBP. Note that there can not be any NAT taking place between the endpoints and the LAN IP of VBP. The table lists the requirements with the top section being for packets from the LAN H.323 device to the VBP LAN interface, and the bottom section being from the VBP LAN interface to the H.323 device.

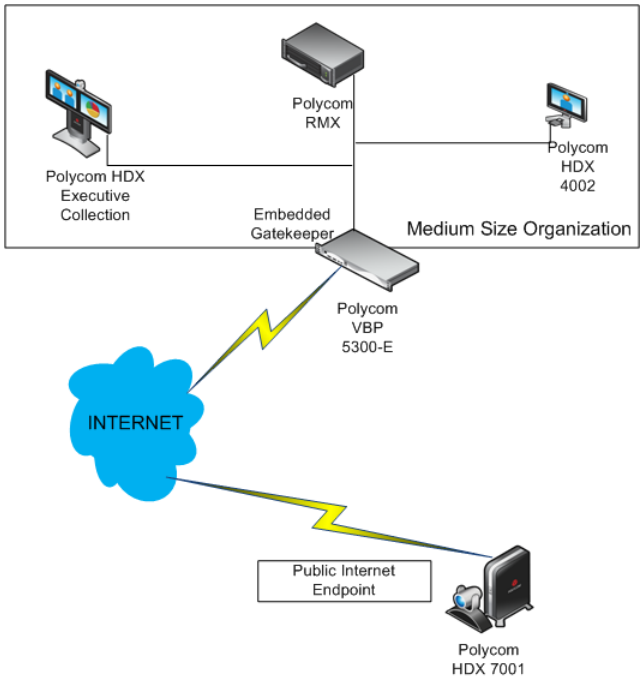
Inbound from the H.323 endpoint to Polycom VBP LAN/Provider Interface IP				
SRC IP	SRC Port	DST IP	Proto	DST port
Any	1024 – 65535	VBP LAN IP	UDP	1719
Any	1024 – 65535	VBP LAN IP	TCP	1720
Any	1024 – 65535	VBP LAN IP	TCP	14085 - 15084 (contiguous range)
Any	1024 – 65535	VBP LAN IP	UDP	16386 - 34386 (6400-E and S85) (contiguous range)
				16386 - 17286 (200EW,4300,4350,4350EW) (contiguous range)
				16386 - 25386 (5300-E/S10 and E/S25) (contiguous range)
Outbound from the LAN/Provider interface IP to H.323 endpoint				
SRC IP	SRC Port	DST IP	Proto	DST port
VBP LAN IP	1024 – 65535	Any	TCP	1024 - 65535
VBP LAN IP	1024 – 65535	Any	UDP	1024 - 65535

Example Polycom VBP-E Solution Architectures

The following five examples describe the implementation of Polycom VBP-E appliances in a business, education, or government environment.

Scenario One: Communication Between a Company and an Internet Endpoint

This scenario shows a public endpoint being called from inside the corporation via a Polycom VBP-E using the Embedded Gatekeeper mode. The Embedded Gatekeeper mode allows the calls to be routed to outbound public IP endpoints. This scenario is for a calling solution where the public endpoint is directly accessible from the Polycom VBP-E.



How it Works

In this scenario, a call is placed from inside the corporation to a public endpoint. The corporation endpoint uses E.164 alias (user@ip_address) dialing to make the video call. The call is routed to the Polycom VPB-E internal interface where the embedded gatekeeper looks at the call address.

The IP address of the call indicates it is to be placed via the Internet. The Polycom VBP routes the call out its external interface directly to the public Polycom HDX endpoint.

The public Polycom HDX endpoint can also call the corporations endpoints as long as the corporation's video endpoint calling numbers are known. The public endpoint would call using the Polycom VBP external IP address along with the endpoint calling number. A Polycom example of this would be 150.202.19.22##12345 or 12345@150.202.19.22. The format will vary based on the conditions at the remote endpoint.

The internal sites could call each other using the alias or endpoint extension or to other Annex-O capable locations using ann@company3.com for example.

The benefit here is a pretty straight forward solution for Internet video dialing.

Capabilities

In this scenario, the remote endpoint can call into the corporation as long as the extension of the video endpoint is known to the caller

The LAN-side endpoints are registered to the Polycom VPB-E and can call other LAN-side endpoints using a dialing plan. They also can dial out to the Internet video endpoint depicted here using this dialing plan.

The WAN-side endpoint cannot register with the Polycom VPB-E embedded gatekeeper and must dial an IP and extension. A Polycom example would be 50.202.19.22##12345" where 150.202.19.22 is the WAN IP address of the Polycom VBP and 12345 is the alias of the endpoint.

For Public Endpoint	WHAT WORKS	WHAT DOESN'T WORK
Polycom HDX systems	Endpoint can call into the corporation Endpoint can receive calls from the corporation	None of the Polycom system administrative capabilities work in this scenario.
Third Party endpoints		

For Corporate Endpoints	WHAT WORKS	WHAT DOESN'T WORK
Polycom HDX systems	Endpoint can call and receive calls from any other LAN-side endpoint using a dialing plan. Endpoint can call and receive calls to the public endpoint. Directory services Content Presence Scheduled software updates Commands to LAN-side endpoints. The systems on the LAN-side will be able to use the advanced Polycom RMX video conferencing functions.	If a public endpoint is on the inside of a firewall then it will not be able to communicate with the LAN-side endpoints.
Polycom CMA Desktop clients Polycom VVX 1500		

System Requirements

The minimum Polycom systems required for this scenario include:

- Polycom VBP-E with an external Internet connection directly or behind a firewall correctly configured.
- Polycom RMX system for a conferencing platform for multipoint conferencing.
- One or more Polycom endpoints or approved video endpoints directly connected to the Internet. This could also be a Polycom CMA Desktop client.
- One or more video Polycom or third party endpoints inside the corporate network communicating in H.323

Optional Polycom systems that interoperate in this scenario include:

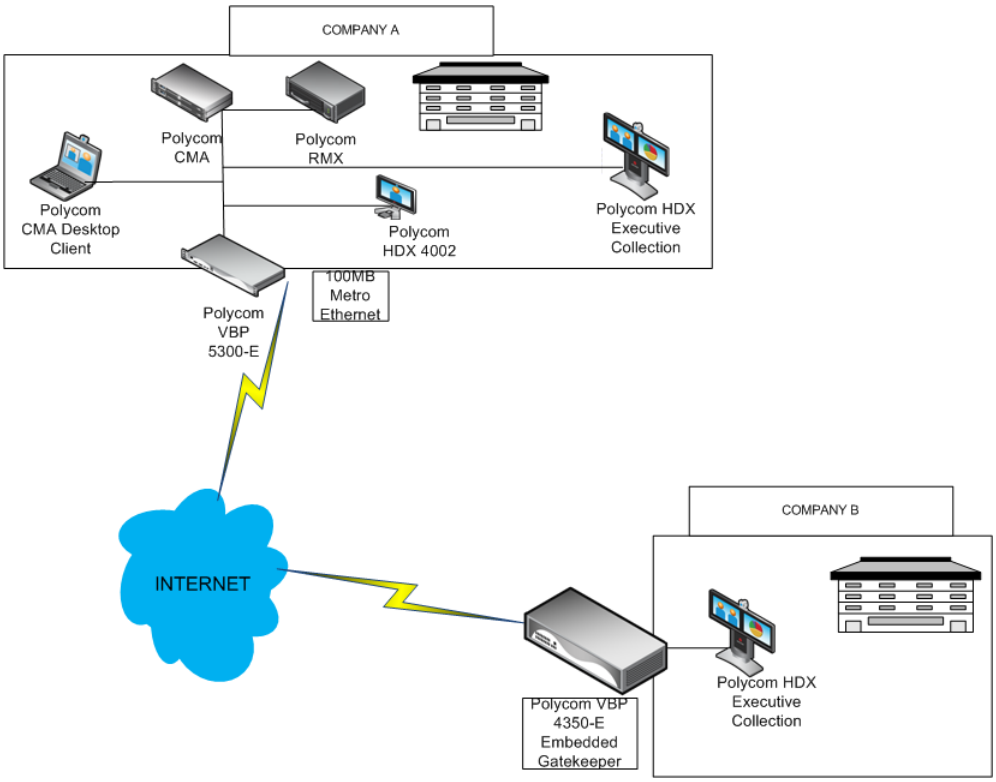
- Polycom CMA system for management and gatekeeper
- Polycom RSS – The Recording and Streaming Server for sharing knowledge and also communicate more effectively by recording and streaming video communications
- Polycom VMC – The Video Media Center for connecting dispersed workforces and improving collaboration by seamlessly integrating video content with enterprise communications
- Polycom VSX – State-of-the-art video conferencing collaboration tool with crisp, clean video and crystal-clear sound.
- Third-party firewall/routers (see listing of these earlier in this document) other devices
- Many industry standard endpoints work with the Polycom equipment. It most cases there should be a good video connection. Discuss with your Polycom representative what your requirements are for video endpoints on the network**.**

Network and Configuration Requirements

- Network design = Embedded gatekeeper design. This is a simpler design and will accommodate a medium size installation of LAN-side endpoints depending on the size of the Polycom VPB-E that is placed here. Typically a Polycom VBP 5300-E would be placed here.
- Polycom VBP configuration settings = Embedded gatekeeper configuration
- The Internet connections for these locations should be a business class Internet connection. This is necessary for good quality of service for video conferencing.

Scenario Two:
Communication Between Two Companies

This scenario shows the Polycom VPB-E communicating to another Polycom VPB-E showing the added functionality of having the E model. Company B's Polycom VPB-E uses Embedded Gatekeeper mode, which allows it to address endpoints not on company A's network. This also allows the endpoints at both locations to use a dial plan to make the video call internal and external.



How it Works

In this scenario, Company B's Polycom HDX makes a call to Company A using a prefix of 04 with the destination HDX's extension number. That would be 0412345. This would equate to entering 12345@150.202.19.22 to reach Company A's HDX.

When the call setup is received by Company A's Polycom VBP-E, it is sent to the Polycom CMA system, which then directs the call to the correct HDX endpoint.

This dialing plan will work for other locations managed endpoints using a Polycom VPB-E appliance. Company B also has the capability to schedule calls to dial into Company A.

The connection between two Polycom VBP-E video firewall appliances simplifies the process of communicating between two separate entities. This is done by configuring prefixes in the routing table of the VBP-E.

The Polycom VBP 4350-E also can prioritize video traffic by using quality of service(QOS) for Traffic Shaping.

Capabilities

In this scenario, the two Polycom VPB-Es offer a good deal of flexibility to the video conferencing capabilities. The first advantage is the capability of the separate companies to use a dialing plan to call each other. Also both companies can participate in multi-point conference calls or ad-hoc call point-to-point.

Company A	WHAT WORKS	WHAT DOESN'T WORK
Polycom Video endpoint systems **Third Party endpoints**	LAN-side endpoints can call each other with a dialing plan WAN-side endpoints can call each other using a dialing plan QOS Scheduling dial-in Presence for LAN-side if a Polycom CMA Desktop client is used. Directory Services	Scheduling dial-out Presence is not available for Company B Directory services for Company B

Company B	WHAT WORKS	WHAT DOESN'T WORK
Polycom Video endpoint systems **Third Party endpoints**	LAN-side endpoints can call each other with a dialing plan WAN-side endpoints can call each other using a dialing plan Scheduling dial-in Presence for LAN-side if a Polycom CMA Desktop client is used. Directory services	Scheduling dial-out Presence is not available for Company A Directory services for Company A

System Requirements

The minimum Polycom systems required for this scenario include:

- Polycom VBP-E in both locations with an external Internet connection directly or behind a firewall correctly configured.
- Polycom RMX system for a conferencing platform for multipoint conferencing.
- One or more Polycom HDX (version 2.5.0.4 or greater) or approved video endpoints directly connected to the Internet.
- Polycom CMA Desktop client

Optional Polycom systems that interoperate in this scenario include:

- Polycom RSS – The Recording and Streaming Server for sharing knowledge and also communicate more effectively by recording and streaming video communications

- Polycom VMC– The Video Media Center for connecting dispersed workforces and improving collaboration by seamlessly integrating video content with enterprise communications
- Polycom VSX–Video conferencing collaboration tool with crisp, clean video and crystal-clear sound.

Optional third-party systems that interoperate in this scenario include:

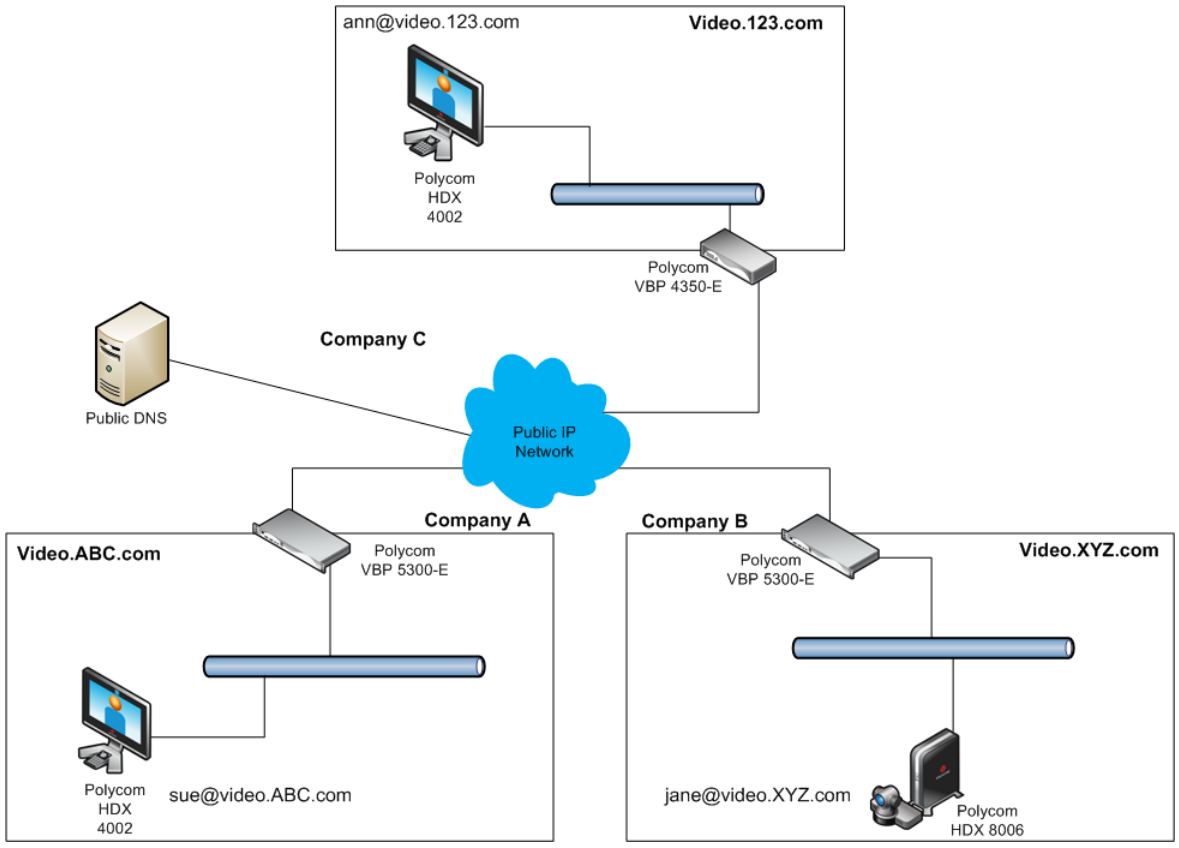
- Many industry standard endpoints work with the Polycom equipment. It most cases there should be a good video connection. Discuss with your Polycom representative what your requirements are for video endpoints on the network

Network and Configuration Requirements

- Network design = Distributed gatekeeper design – one for each location. Since these are two separate entities it would be possible for there to be a gatekeeper at each end with the video endpoints.
- Polycom VBP configuration settings = LAN-side gatekeeper configuration for both companies.
- The Internet connections for these locations should be a business class Internet connection. This is necessary for good quality of service for video conferencing.

Scenario Three: Communication Between Three Companies

In this example, Company A, B, and C want to communicate via H.323 video conferencing. All three companies are using Embedded Gatekeeper mode on their Polycom VBP-E appliances.



This example could also represent a single company that only had a single endpoint requirement and had no existing H.323 infrastructure. This diagram also shows the use of DNS-based ANNEX O (E.164@VBP-WAN-IP) dialing, and again direct gatekeeper neighboring is also possible by configuring prefix based gatekeeper neighboring.

How it Works

This scenario is similar to Scenario Two. A call placed by one company to another is accomplished with a dialing prefix and the extension number or by using a full E.164 address. When an external DNS is defined the DNS name can also be used (sue@video.ABC.com).

Capabilities

In this scenario, the three VPB-Es offer useful flexibility to the video conferencing capabilities. The first advantage is the capability of the separate companies to use a dialing plan to call each other. Also the companies can participate in multi-point conference calls or ad-hoc call point-to-point.

Company A	WHAT WORKS	WHAT DOESN'T WORK
Polycom Video endpoint systems **Third Party endpoints**	LAN-side endpoints can call each other with a dialing plan WAN-side endpoints can call each other using a dialing plan QOS Scheduling dial-in Presence for LAN-side if a Polycom CMA Desktop client is used. Directory services	Scheduling dial-out Presence is not available for Company B or C Directory services for Company B or C

Company B	WHAT WORKS	WHAT DOESN'T WORK
Polycom Video endpoint systems **Third Party endpoints**	LAN-side endpoints can call each other with a dialing plan WAN-side endpoints can call each other using a dialing plan Scheduling dial-in QOS Presence for LAN-side if a Polycom CMA Desktop client is used. Directory services	Scheduling dial-out Presence is not available for Company A or C Directory services for Company A or C

Company C	WHAT WORKS	WHAT DOESN'T WORK
Polycom Video endpoint systems **Third Party endpoints**	LAN-side endpoints can call each other with a dialing plan WAN-side endpoints can call each other using a dialing plan Scheduling dial-in QOS Directory services	Scheduling dial-out Presence is not available for Company A or B Directory services for Company A or B

System Requirements

The minimum Polycom systems required for this scenario include:

- Polycom VBP-E in all locations with a direct external Internet connection.
- Polycom RMX system for a conferencing platform for multipoint conferencing.
- One or more Polycom HDX (version 2.5.0.4 or greater) or approved video endpoints directly connected to the Internet.

Optional Polycom systems that interoperate in this scenario include:

- Polycom RSS – The Recording and Streaming Server for sharing knowledge and also communicate more effectively by recording and streaming video communications
- Polycom CMA Desktop client
- Polycom VMC– The Video Media Center for connecting dispersed workforces and improving collaboration by seamlessly integrating video content with enterprise communications
- Polycom VSX–Video conferencing collaboration tool with crisp, clean video and crystal-clear sound.

Optional third-party systems that interoperate in this scenario include:

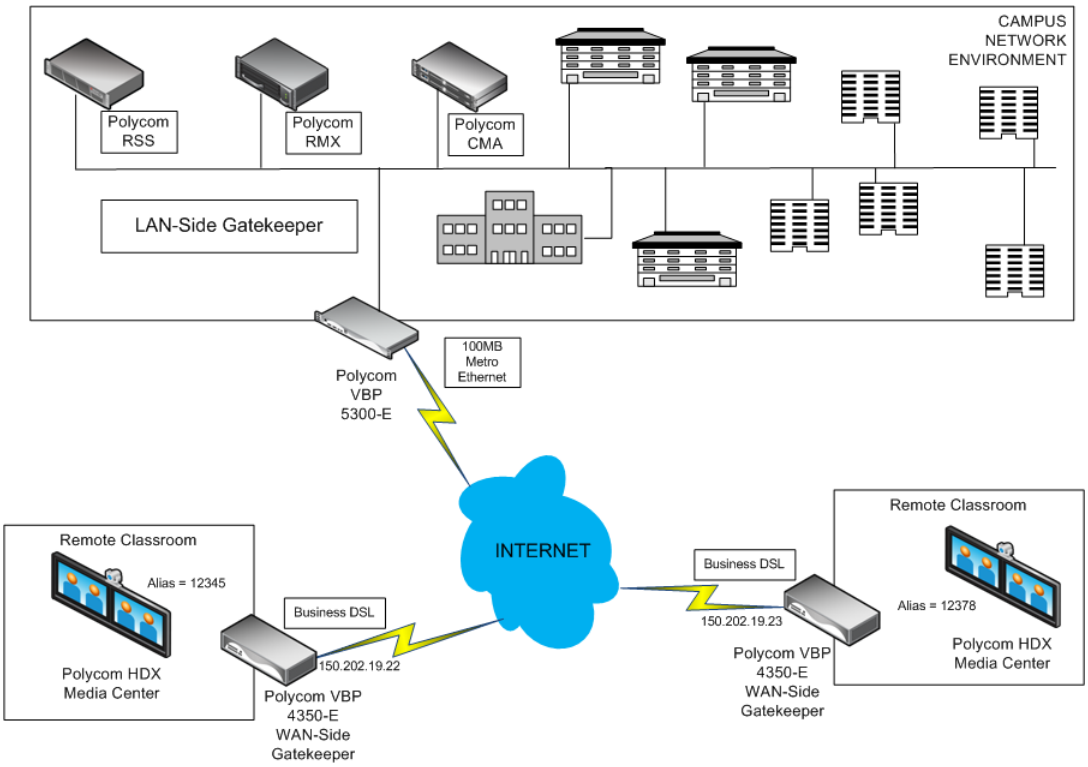
- Many industry standard endpoints work with the Polycom equipment. It most cases there should be a good video connection. Discuss with your Polycom representative what your requirements are for video endpoints on the network

Network and Configuration Requirements

- Network design = Distributed gatekeeper design – one for each location. Since these are separate entities it would be possible for there to be a gatekeeper at each end with the video endpoints.
- Polycom VBP configuration settings = LAN-side gatekeeper configuration for the Polycom VBP-5300 systems and embedded gatekeeper for the Polycom VBP-4350 systems.
- The Internet connections for these locations should be a business class Internet connection. This is necessary for good quality of service for video conferencing.

Scenario Four:
Communications on a Campus Learning Network System

This design is taking the setup of Scenario Four and adding on to it for a Campus Learning Network System. The remote classrooms are not on the campus network but are easily reachable since they are included in the campus network dialing plan. Calls will use dialing plans that would relate to the classrooms where systems are installed.



How it Works

The main advantage here is the capability to expand the learning experience to remote classrooms where they would be geographically diverse. It would be possible also for a remote classroom to also broadcast its class presentation to the campus network. Both scenarios are valid for expansion of this type of network.

A presentation lecture in a Campus classroom makes a call to a Remote classroom using a prefix of 04 with the HDX Media Center alias. That would be 0412345. This would equate to entering 12345@150.202.19.22to reach the Remote classrooms HDX Media Center. Assuming the Polycom VBP external interface IP address is 150.202.19.22 and the HDX Media Center calling number is 12345.

When the call setup is received by the Campus Polycom VBP-E it is sent to the Polycom CMA system which then directs the call out the Polycom VBP-E external interface to the Remote classroom Polycom VPB-E. From here it is sent to the correct HDX Media Center endpoint.

This dialing plan will work for other locations managed endpoints using a Polycom VPB-E appliance. Remote classrooms can call other Remote classrooms

The Polycom VBP 4350-E also can prioritize video traffic for quality of service.

NOTE: This Scenario Four is also applicable to the Government sector since they share similar network configurations. Video calls between diverse government entities could be placed on a scheduled or ad hoc basis.

Capabilities

This scenario shows multiple Polycom VPB-E communicating in a networked setting, so video sessions can be established for sharing classroom content. The network is essentially distributed to trusted endpoints so a snap shot of how one installation can be used at another with minor modifications. The administrative overhead of the video network is reduced due to the similar design used at each location.

The Polycom RMX can share one presentation to multiple classrooms thereby allowing a lesson to be shared out to other locations and also have possible interactive communication.

The Polycom RSS will record classroom sessions for later viewing when necessary.

Campus Network	WHAT WORKS	WHAT DOESN'T WORK
Polycom Video endpoint systems **Third Party endpoints**	LAN-side endpoints can call the WAN-side endpoints with a dialing plan LAN-side endpoints can call each other using a dialing plan QOS Scheduling dial-in Presence for LAN-side Directory services Content – People and Pictures Management of home office endpoint.	Scheduling dial-out Presence of the Remote Classrooms Directory services

Remote Classrooms	WHAT WORKS	WHAT DOESN'T WORK
Polycom HDX Media Center **Third Party endpoints**	LAN-side endpoints can call each other with a dialing plan LAN-side endpoints can call the WAN-side endpoints with a dialing plan QOS Directory services	Scheduling dial-out Presence is not available Directory services

System Requirements

The minimum Polycom systems required for this scenario include:

- Polycom VBP-E in all locations with an external Internet connection or behind a firewall correctly configured.
- Polycom RMX system for a conferencing platform for multipoint conferencing.

- One or more Polycom HDX Media Center
- Polycom RSS for recording, streaming, and archiving multimedia conferences

Optional Polycom systems that interoperate in this scenario include:

- Polycom VMC – The Video Media Center for connecting dispersed workforces and improving collaboration by seamlessly integrating video content with enterprise communications
- Polycom HDX 4000

Optional third-party systems that interoperate in this scenario include:

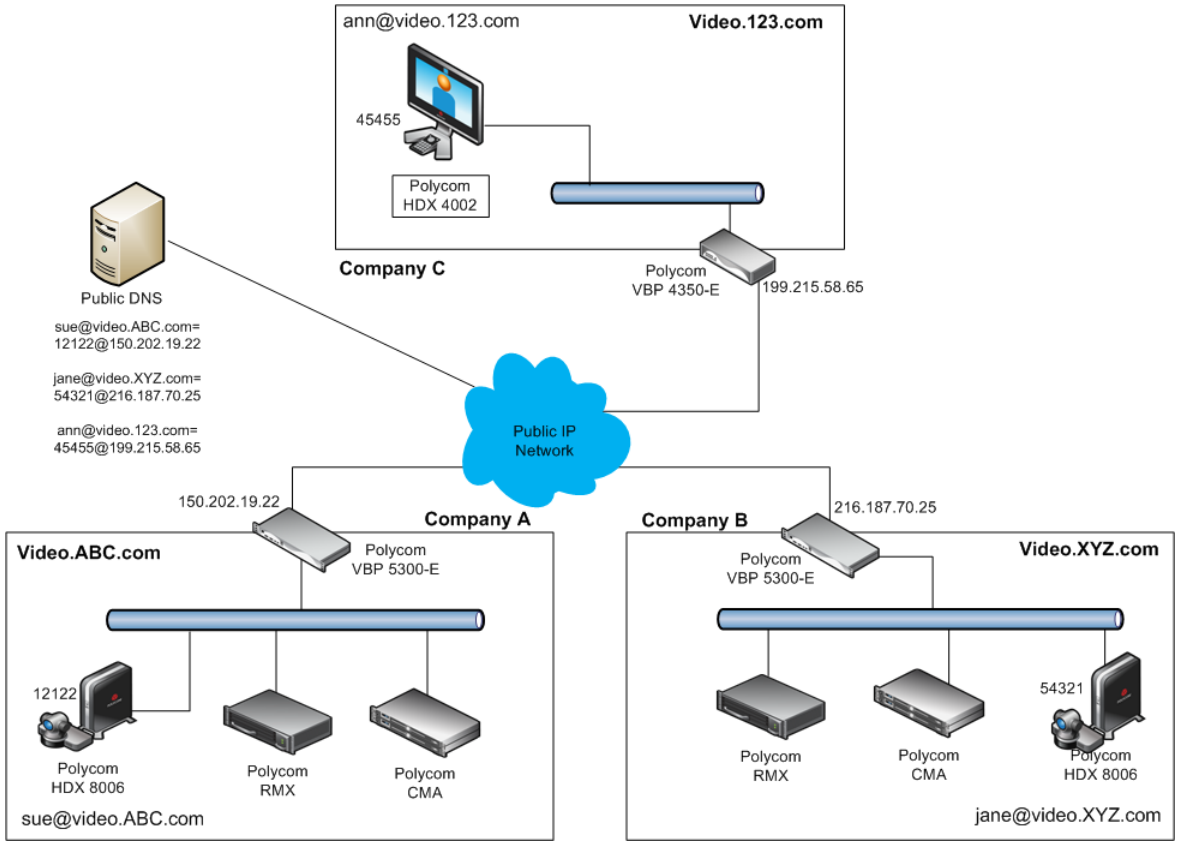
- Many industry standard endpoints work with the Polycom equipment. It most cases there should be a good video connection. Discuss with your Polycom representative what your requirements are for video endpoints on the network

Network and Configuration Requirements

- Network design = Centralized gatekeeper design for ease of use and centralized administration of all the endpoints. A dial plan can be used for calling to the main campus or to the other Remote Classrooms.
- Polycom VBP configuration settings = LAN-side gatekeeper configuration for the Campus Polycom VPB-E. The Remote Classrooms would be WAN-side gatekeeper configuration. All of the Polycom VBP-Es would be neighbored for to allow calls from any location to any for efficient routing of video traffic.
- The Campus Network would use a Polycom VBP-E 5300 or 6400 series Polycom VBP depending on the throughput requirements of the location.
- Depending on the number of video endpoints at the Remote classroom(s) you could use Polycom VBP 4350-E for a one video endpoint Remote classroom location. For multiple and video endpoint Remote classroom locations you would use a Polycom VBP 5300-E.

Scenario Five:
Communications in an Enterprise Distributed Gatekeeper Network

In a distributed gatekeeper model, H.323 calls are forwarded to two or more gatekeepers on the enterprise network. This can be a mix of Polycom VBP appliances configured in Embedded Gatekeeper mode and LAN/Subscriber-side mode.



How it Works

In this example, Company A, B, and C want to connect via H.323 video conferencing. Company A and B have Polycom VBP-E appliances configured in the LAN/Subscriber-side gatekeeper mode. Because Company C did not have an established H.323 infrastructure, they chose to use the Embedded Gatekeeper mode on their Polycom VBP-E appliances.

These three companies deployed the Polycom VBP appliance as a security border device to allow secure traversal from their internal network to the external un-trusted network. In this case the Internet was the transport of choice. This diagram also shows the use of DNS-based ANNEX O (E.164@VBP-WAN-IP) dialing. Direct gatekeeper neighboring is also possible by configuring prefix based gatekeeper neighboring. Calls are also allowed with full numeric dialing of endpoints.

Capabilities

The video calling to the different sites can be point to point or multipoint with the help of the RMX 2000. The RMX2000 also supports on demand conferencing with virtual meeting rooms. The Polycom CMA

system at two of the locations enables endpoint management at those locations and collaboration and efficient sharing of content with users.

Company A	WHAT WORKS	WHAT DOESN'T WORK
Polycom Video endpoint systems **Third Party endpoints**	WAN-side endpoints can call the LAN-side endpoints using a dialing plan WAN-side endpoints can call each other using a dialing plan All normal calling scenarios found while on the LAN Scheduling dial-in Commands – reboot, change cameras Directory Services for systems that support access proxy. An example would be Polycom CMA Desktop client. Monitoring Content – People and Pictures Automatic software update	Commands – reboot, change cameras of remote systems Schedule calls for dial out

Company B	WHAT WORKS	WHAT DOESN'T WORK
Polycom Video endpoint systems **Third Party endpoints**	WAN-side endpoints can call the LAN-side endpoints using a dialing plan WAN-side endpoints can call each other using a dialing plan All normal calling scenarios found while on the LAN Scheduling dial-in Directory Services for systems that support Access proxy. An example would be Polycom CMA Desktop client. Monitoring Content – People and Pictures Automatic soft update	Commands – reboot, change cameras of remote systems Schedule calls for dial out

Company C	WHAT WORKS	WHAT DOESN'T WORK
Polycom Video endpoint systems **Third Party endpoints**	WAN-side endpoints can call the LAN-side endpoints using a dialing plan WAN-side endpoints can call each other using a dialing plan Scheduling dial-in Directory Services for systems that support Access proxy. An example would be Polycom CMA Desktop client. Content – People and Pictures All normal calling scenarios found while on the LAN Automatic soft update	Scheduled soft update Commands – reboot, change cameras Schedule calls for dial out Monitoring

System Requirements

The minimum Polycom systems required for this scenario include:

- Polycom VBP-E in all locations with an external Internet connection or behind a firewall correctly configured.
- A Polycom CMA system (version 4.1 or greater) acting as the corporate LAN-side gatekeeper OR any other video/voice gatekeeper product of comparable capacity for managing video calls.
- Polycom RMX system for a conferencing platform for multipoint conferencing.
- One or more Polycom HDX 8006 and 4002.

Optional Polycom systems that interoperate in this scenario include:

- Polycom VMC – The Video Media Center for connecting dispersed workforces and improving collaboration by seamlessly integrating video content with enterprise communications
- Polycom RSS for recording, streaming, and archiving multimedia conferences
- Polycom HDX 4000

Optional third-party systems that interoperate in this scenario include:

- Many industry standard endpoints work with the Polycom equipment. It most cases there should be a good video connection. Discuss with your Polycom representative what your requirements are for video endpoints on the network

Network and Configuration Requirements

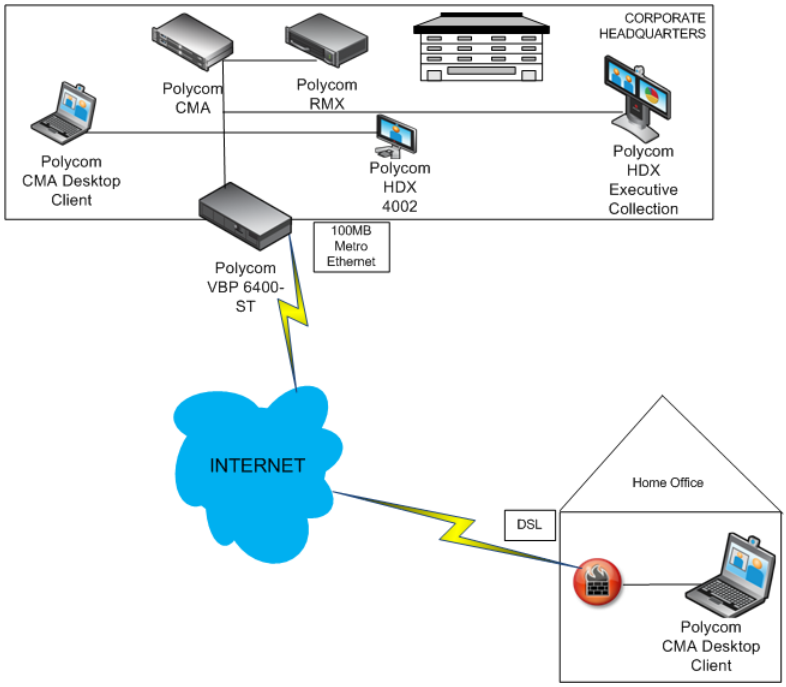
- Network design = Distributed gatekeeper design – one for each location. Since these are two separate entities it would be possible for there to be a gatekeeper at each end with the video endpoints.
- Polycom VBP configuration settings = LAN-side gatekeeper configuration for both companies.
- The Internet connections for these locations should be a business class Internet connection. This is necessary for good quality of service for video conferencing.
- The Network would use a Polycom VBP-E 5300 or 6400 for the Enterprise locations and a 4350 series Polycom VBP depending on the throughput requirements of the location.

The Polycom VBP-ST Video Firewall

The next two Polycom VBP scenarios focus on the ST series. The Polycom VBP-ST is designed to offer video conferencing to the small office/home office (SOHO) and business vendors for business-to-business communication.

Scenario Six:
Small Office/Home Office Communication through the Internet

In this scenario, remote employees outside the corporate firewall with personal Polycom HDX systems or Polycom CMA Desktop clients can securely access the corporate network from their home offices through a personal third-party firewall to the public Internet. The video call experience is the same as if the SOHO caller was in the corporate headquarters making the call.



How it Works

In this scenario, remote employees provision their video endpoint with the WAN-Side IP address of the Polycom VBP-ST. When a remote employee initiates a call into the corporate network, the endpoint sends standard H.323 signaling using H.460 through the SoHo FW to the VBP-ST.

The VBP-ST receives the request and forwards it to the Polycom CMA system (Provider-side Gatekeeper), which then performs a lookup of the dialed digits and routes the call accordingly.

In this scenario, the remote employee's endpoint is seen as being on the corporate LAN by the rest of the H.323 devices, making it very easy to communicate. The remote endpoint dials and receives calls using the same work-flow as a device on the LAN, and is a part of the corporate dial-plan.Unregistered Subscriber-side (Internet) endpoints cannot call Provider-side endpoints.

Capabilities

In this scenario, the remote endpoint has the same calling capabilities available to employees on the local network and access to the management features of automatic provisioning, automatic soft update, directory services, contact list, content, presence and scheduling support as endpoints on the local network. Note that some management features such as monitoring are not yet available for remote video endpoints.

For SOHO…	WHAT WORKS	WHAT DOESN'T WORK
Polycom HDX systems **Polycom CMA Desktop clients**	All normal calling scenarios found while on the LAN (Because of access proxy) Automatic Provisioning Directory Services Presence Contact lists Content Schedule calls for dial in Automatic soft update	Scheduled soft update Commands – reboot, change cameras Schedule calls for dial out Monitoring
Polycom VSX systems	(Does not use the access proxy) Call in to managed endpoints	Automatic Provisioning Directory Services Presence Contact lists Content Schedule calls for dial in Automatic soft update All normal calling scenarios found while on the LAN

An additional benefit the video network administrator will be able to manage this endpoint and the SOHO user will be able to set it up quickly.

System Requirements

The minimum Polycom systems required for this scenario include:

- A Polycom VBP 5300 or 6400 ST (version 9.1.5 or greater) appliance protecting the corporate network working in parallel with a corporate firewall or in a DMZ
- A Polycom CMA system (version 4.1 or greater) acting as the corporate LAN-side gatekeeper OR any other video/voice gatekeeper product of comparable capacity for managing video calls.
- One or more Polycom HDX (version 2.5.0.4 or greater) or Polycom CMA Desktop (version 4.1 or greater) video endpoints outside the corporate network
- One or more video Polycom or third party endpoints inside the corporate network communicating in H.323.
- Optional Polycom systems that interoperate in this scenario include: One or more Polycom RMX systems that supports multiple network types to extend the power of unified collaboration within—and beyond—the enterprise. This systems a platform for multipoint conferencing

- Polycom DMA – The centralized application appliance for efficiently managing and distributing multipoint conferences throughout the network.
- Polycom RSS – The Recording and Streaming Server for sharing knowledge and also communicate more effectively by recording and streaming video communications
- Polycom VMC – The Video Media Center for connecting dispersed workforces and improving collaboration by seamlessly integrating video content with enterprise communications

Optional third-party systems that interoperate in this scenario include:

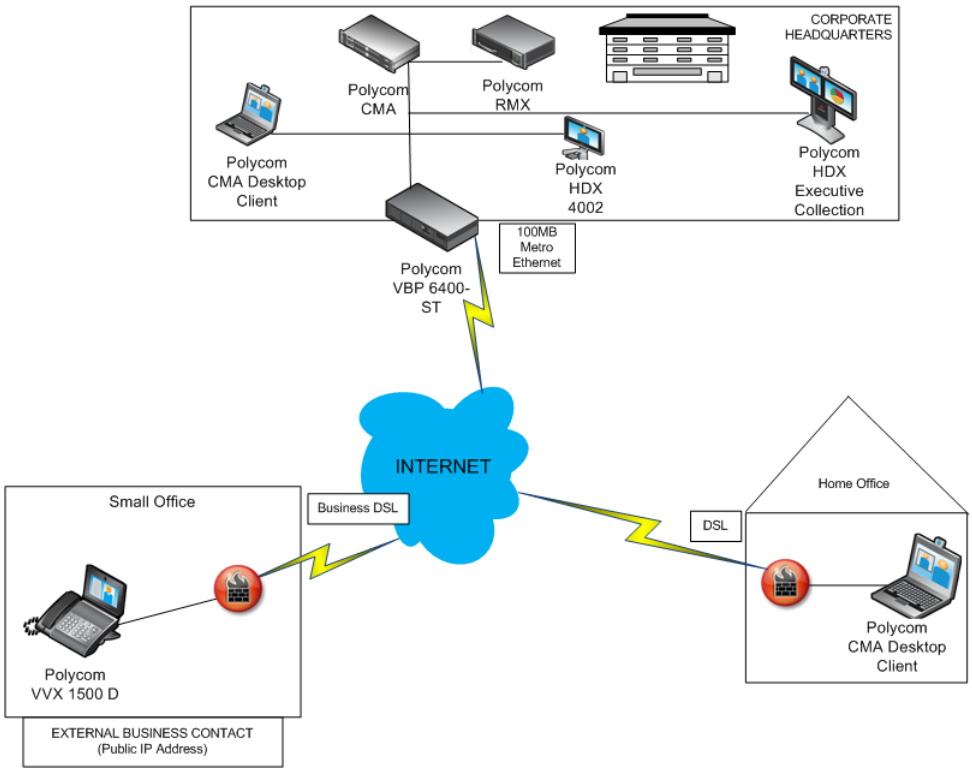
- Third-party firewall/routers (see listing of these earlier in this document).
- Many industry standard endpoints work with the Polycom equipment. It most cases there should be a good video connection. Discuss with your Polycom representative what your requirements are for video endpoints on the network

Network and Configuration Requirements

- Network design = Centralized gatekeeper design. This is a design for expansion that will accommodate a medium size installation of LAN-side endpoints depending on the size of the VPB-ST that is placed here. A Polycom VBP 5300ST would work in this scenario if the number of connections to the corporate headquarters doesn't exceed its operational limit.
- Polycom VBP configuration settings = LAN-side gatekeeper configuration
- Polycom recommends an Internet connection bandwidth of moderate speed. Normal business class bandwidth will deliver an even better video call experience
- LAN (Subscriber-Internet) and WAN (Provider(private)) endpoints MUST be registered to the LAN-side gatekeeper
- Third-party firewall/routers (see listing of these earlier in this document).

Scenario Seven:
Communication Between a Vendor, a Corporation, and a SOHO

In this scenario, the corporate IT department opens communications to remote customers or vendors endpoints for business-to-business video communications. Remote customers or vendors outside the corporate firewall with personal Polycom legacy endpoint systems such as Polycom VSX systems can securely access the corporate network through the public Internet. This design is flexible enough for use of other video endpoints using standard H.323 protocols for communication.



How it Works

In this scenario, when a customer or vendor outside the corporate network initiates a call from his or her video endpoint, the endpoint sends the H.323 alias (the video endpoint's extension) since they are registered to the internal CMA server. The call goes through the remote business firewall and the public Internet to the corporate Polycom VBP-ST appliance via H.460 protocol.

The dialing is via the H.460 protocol. The outside interface IP address of the Polycom VBP-ST is called using H.323 alias thru a SOHO firewall to the Internet and through to the corporate headquarters. The RAS request is received by the Polycom VBP-ST. It sends it to the Polycom CMA system (LAN-side gatekeeper), which then routes the request to an endpoint on the corporate LAN.

The Polycom VBP-ST uses the Application Layer Gateway working in conjunction with the firewall service and gatekeeper to let the authorized outside endpoint to call in to the corporate headquarters.

Benefits for this business-to-business communications - the calls can be scheduled calls, for dial in.

The remote endpoint initiates a call from his or her video endpoint into the corporate network. The endpoint sends the H.323 alias through the SOHO firewall and the public Internet to the corporate Polycom VBP-ST

appliance via H.460 protocol. The NAT between the Internet and the Corporate Network is one of the fundamental capabilities of the Polycom VBP-ST.

In this scenario, the remote employee's video endpoint appears as if it is located on the corporate headquarters LAN thereby making it easy to open communications to LAN-side endpoints and vice-versa. The external business contact can be permitted to register with the LAN-side gatekeeper of the corporate headquarters. This affords the external business contact the capability to place and receive calls to the corporate headquarters the same as the remote employee's endpoint.

Capabilities

In this scenario, the system is designed to allow SOHO video conferencing with trusted and untrusted sources. There are limitations on what this configuration affords but the advantage of being able to have directory services, content and schedule calls for dial-in gives value to this installation. Note that some management features such as monitoring are not yet available for remote video endpoints.

For Corporate Headquarters	WHAT WORKS	WHAT DOESN'T WORK
Polycom video endpoint systems **Third Party endpoints**	Endpoint can call within the corporate headquarters Remote endpoint can receive calls from the corporate headquarters Directory Services Content Presence Scheduled software updates Commands to LAN-side endpoints.	Traffic Shaping for Internet calls Quality of Service for Internet calls (The Polycom VBP can remark traffic with QOS on its wan port. If the ISP supports QOS, it will be applied.) DHCP server or relay for Internet calls

Remote SOHO endpoints	WHAT WORKS	WHAT DOESN'T WORK
Polycom video endpoint systems **Third Party endpoints**	Endpoint can call within the corporate headquarters Remote endpoint can receive calls from the corporate headquarters Directory Services Content	Presence Scheduled software updates Commands to LAN-side endpoints Calls from unregistered endpoints Data NAT Embedded Gatekeeper mode Traffic Shaping QoS DHCP Server or relay

System Requirements

The minimum Polycom systems required for this scenario include:

- A Polycom VBP 5300 or 6400 ST (version 9.1.5 or greater) appliance protecting the corporate network working in parallel with the corporate firewall.
- A Polycom CMA system (version 4.1 or greater) acting as the corporate LAN-side gatekeeper OR any other video/voice gatekeeper product.
- One or more video endpoints capable of H.460 communications—There are many other Polycom and other video industry endpoints that use H.460 communication protocol.
- One or more video endpoints inside the corporate network managed by the Polycom CMA system.

Optional Polycom systems that interoperate in this scenario include:

- One or more Polycom RMX systems that support multiple network types to extend the power of unified collaboration within—and beyond—the enterprise. This systems a platform for multipoint conferencing

  Polycom DMA – The centralized application appliance for efficiently managing and distributing
- Multipoint conferences throughout the network.
- Polycom RSS – The Recording and Streaming Server for sharing knowledge and also communicate more effectively by recording and streaming video communications
- Polycom VMC – The Video Media Center for connecting dispersed workforces and improving collaboration by seamlessly integrating video content with enterprise communications

Optional third-party systems that interoperate in this scenario include:

- Third-party firewall/routers (see listing of these in this document).
- Many industry standard endpoints work with the Polycom equipment. It most cases there should be a good video connection. Discuss with your Polycom representative what your requirements are for video endpoints on the network.

Network and Configuration Requirements

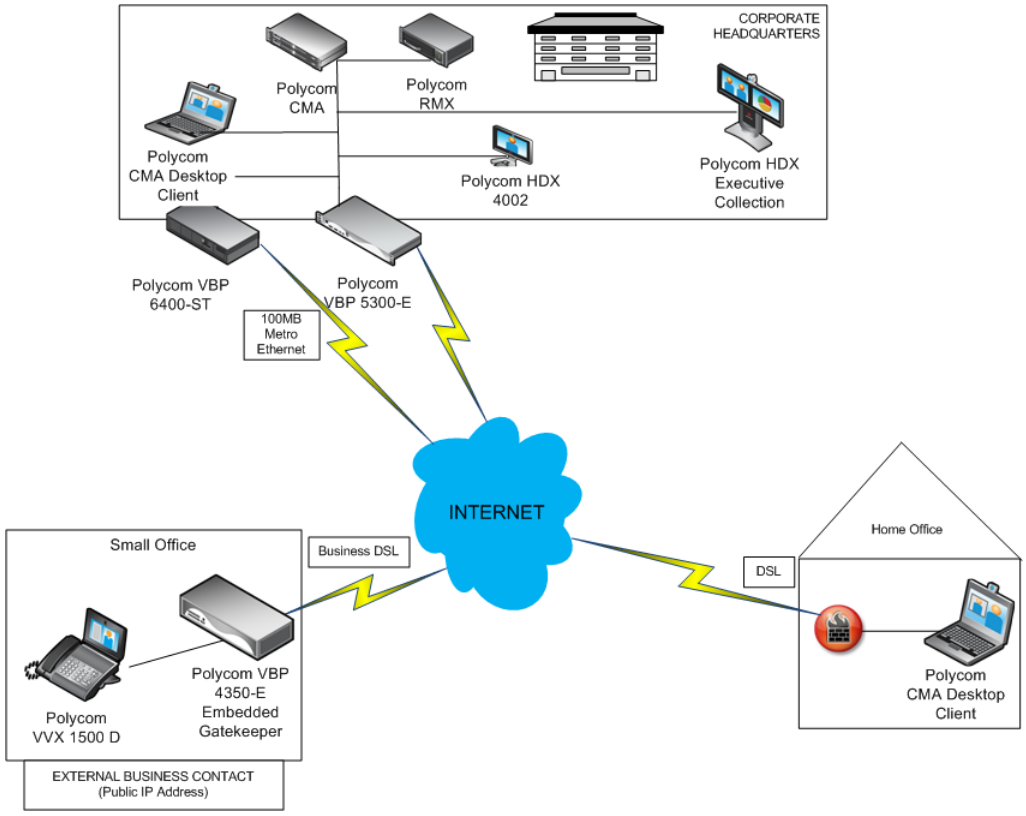
- Network design = Centralized gatekeeper design. This is a design that will accommodate a medium size installation of LAN-side endpoints depending on the size of the VPB-ST that is placed here. A Polycom VBP 5300ST would work in this scenario if the number of connections to the corporate headquarters doesn't exceed its operational limit.
- Polycom VBP configuration settings = LAN-side gatekeeper configuration
- The SOHO setup requires an Internet connection of moderate speed. Normal business class bandwidth will deliver an even better video call experience LAN (Subscriber-Internet) and WAN (Provider(private)) endpoints MUST be registered to the LAN-side gatekeeper
- Third-party firewall/routers (see listing of these earlier in this document).

Combining the Polycom VBP-E and the Polycom VBP-ST video firewalls

The last two scenarios demonstrates where installing both of the Polycom VBP firewalls on the corporate network enables a flexible video conference call platform.

Scenario Eight: Full Internet Call Flexibility with Polycom VBP-E and Polycom VBP-ST

In this scenario the VSX, located in the SOHO with a Private IP address, wants to place a call to the Polycom CMA Desktop client located in the SOHO that is considered part of the corporate headquarters LAN. This is a full design using the both Polycom VBP-E and Polycom VBP-ST systems for managing video calls. This installation is flexible so video communications to and from the corporate headquarters is accommodating to company and non-company contacts.



How it Works

By using both a Polycom VBP-ST and Polycom VBP-E, any video call out to the Internet or in from the Internet is possible. In this scenario the VSX located in the SOHO calls the Polycom CMA Desktop client in the SOHO using a dialing plan. The Polycom VPB-E in the SOHO has the Embedded Gatekeeper mode enabled. The call is placed using 0498765. This is in place of 98765@150.202.19.22 to reach the SOHO Polycom CMA Desktop client.

The Polycom VBP-E at the SOHO knows this should be directed to the corporate headquarters Polycom VPB-E external interface. The corporate headquarters Polycom VPB-E receives the call request and sends it

to the Polycom CMA system (LAN-side gatekeeper) for call signal routing. The Polycom CMA system then routes the call to the Polycom VBP-ST which sends it to the home office Polycom CMA Desktop client.

The real benefit now is that the call media is hair pinned at the Polycom VBP-ST thereby releasing other network resources and making the call quality better by lowering latency.

This setup is designed for maximum flexibility in placing and accepting video conference calls.

Capabilities

In this scenario, the corporate headquarters network has positioned its Polycom VBP video firewall appliances to allow the maximum flexibility for calling into and out of the corporate headquarters. The Polycom VBP-E will communicate with devices directly connected to the Internet while the Polycom VBP-ST allows video devices behind remote firewalls to communicate to the LAN-side endpoints. The Polycom VBP-ST gives the remote home office endpoint many of the capabilities as if it were on the corporate network.

Corporate Headquarters	WHAT WORKS	WHAT DOESN'T WORK
Polycom Video endpoint systems **Third Party endpoints**	LAN-side endpoints can call the WAN-side endpoints with a dialing plan WAN-side endpoints can call the LAN-side endpoints using a dialing plan QOS and Provisioning Scheduling dial-in Presence for LAN-side Directory Services Content – People + Content Management of home office endpoint. Routing flexibility – Hair pin from outside endpoint to outside endpoint.	Directory services of SOHO

Home office	WHAT WORKS	WHAT DOESN'T WORK
Polycom Video endpoint systems **Third Party endpoints**	WAN-side endpoints can call the LAN-side endpoints using a dialing plan WAN-side endpoints can call each other using a dialing plan Scheduling dial-in Directory Services for systems that support Access proxy. An example would be Polycom CMA Desktop client. Content – People and Pictures All normal calling scenarios found while on the LAN Automatic soft update	Scheduled soft update Commands – reboot, change cameras Schedule calls for dial out Monitoring

SOHO	WHAT WORKS	WHAT DOESN'T WORK
Polycom Video endpoint systems **Third Party endpoints**	LAN-side endpoints can call the WAN-side endpoints with a dialing plan WAN-side endpoints can call the LAN-side endpoints using a dialing plan Scheduling dial-in	Presence Directory Services Scheduling dial-out

System Requirements

The minimum Polycom systems required for this scenario include:

- A Polycom VBP 5300E and VBP 6400ST (version 9.1.5 or greater) video firewall appliance protecting the corporate network working in parallel with the corporate firewall. The VBP can be located behind the corporate firewall configured correctly.
- A Polycom CMA system (version 4.1 or greater) acting as the corporate LAN-side gatekeeper OR any other video/voice gatekeeper product of comparable capacity for managing video calls.
- Two or more video endpoints capable of H.460 communications—(There are many other Polycom and other video industry endpoints that use H.460 communication protocol. Many industry standard endpoints work with the Polycom equipment. It most cases there should be a good video connection. Discuss with your Polycom representative what your requirements are for video endpoints on the network
- One or more video endpoints inside the corporate network managed by the Polycom CMA system.

Optional Polycom systems that interoperate in this scenario include:

- One or more Polycom RMX systems as the conferencing platform for multipoint conferencing
- A Polycom DMA system for balancing
- Polycom RSS– The Recording and Streaming Server for sharing knowledge and also communicate more effectively by recording and streaming video communications
- Polycom VMC– The Video Media Center for connecting dispersed workforces and improving collaboration by seamlessly integrating video content with enterprise communications

Optional third-party systems that interoperate in this scenario include:

- Third-party firewall/routers (see listing of these earlier in this document).
- Many industry standard endpoints work with the Polycom equipment. It most cases there should be a good video connection. Discuss with your Polycom representative what your requirements are for video endpoints on the network

Network and Configuration Requirements

- Network design = Centralized gatekeeper design (what are its limitations)
- Polycom VBP's configuration settings = LAN-side gatekeeper configuration for both of these

The Corporate network needs two links to the Internet for the two separate Polycom VBPs used here. The SOHO setup requires an Internet connection of moderate speed. Normal business class bandwidth will deliver an even better video call experience Third-party firewall/routers (see listing of these in this document)

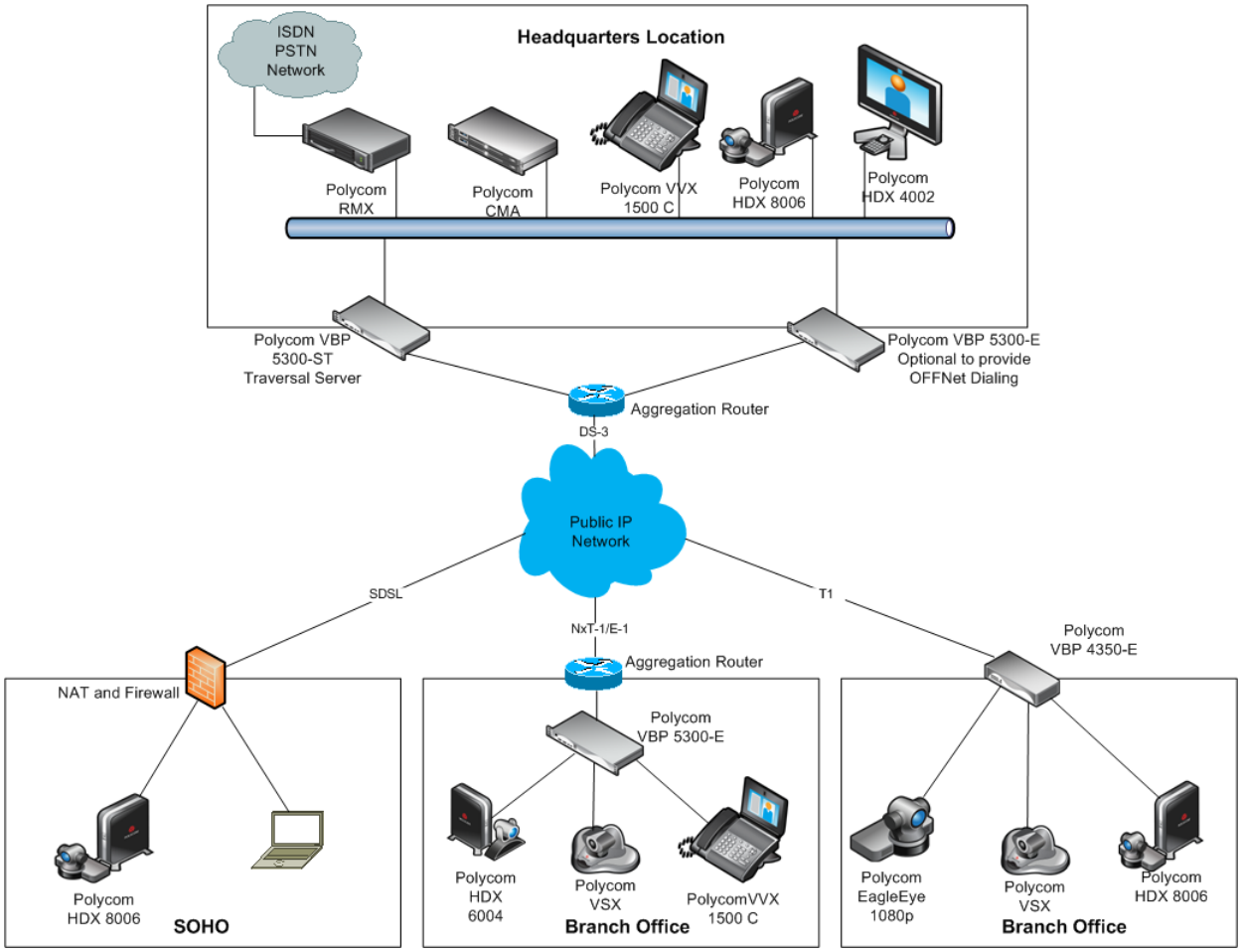
Scenario Nine:
Additional Example of Call Flexibility with Polycom VBP-E and Polycom VBP-ST

Gatekeeper Design—Polycom VBP Series Supported Topologies

Polycom VBP appliances can communicate with remote sites that have differing topologies and administrative policies. They can also work with a centralized gatekeeper or one or more distributed gatekeepers, or act as an embedded gatekeeper in a distributed model.

Centralized Gatekeeper Model

In a centralized gatekeeper model as illustrated in the following diagram, there is a single corporate gatekeeper on the enterprise network to which all H.323 calls are forwarded.



How it Works

In this diagram, the Polycom CMA system is the centralized gatekeeper. (Most industry standard H.323 gatekeepers that support routed mode work in this configuration.) The Polycom VBP 5300-ST appliance is configured in LAN/Subscriber-side gatekeeper mode and directs traffic to the Polycom CMA system. The Polycom VBP-E appliances in the branch offices are configured in WAN/Provider-side gatekeeper mode and direct traffic to the subscriber/public IP address of the Polycom VBP 5300-ST appliance.

This configuration allows authorized H.323 endpoints on the Internet/subscriber side of the Polycom VBP-ST using H.460 traversal methods to centrally register to the Polycom CMA system for call control. These remote endpoints may be located in branch offices behind another Polycom VBP appliance or on the Internet. By default, a Polycom VBP-ST appliance will allow any device to send a registration request (RAS) to the gatekeeper. The gatekeeper controls which aliases are allowed to register. The Polycom VBP-ST can provide additional security when it is configured to allow only defined endpoints to create connections to the system.

This configuration also allows the Polycom CMA system's services to extend beyond the enterprise network.

Capabilities

In this scenario, the corporate headquarters network has positioned its Polycom VBP video firewall appliances to allow the maximum flexibility for calling into and out of the corporate headquarters. The Polycom VBP-E will communicate with devices directly connected to the Internet while the Polycom VBP-ST allows video devices behind remote firewalls to communicate to the LAN-side endpoints. The Polycom VBP-ST gives the remote home office endpoint many of the capabilities as if it were on the Corporate Network.

The What Works and What Doesn't Work comparison chart for Scenario Eight is applicable here.

System Requirements

The minimum Polycom systems required for this scenario include:

- A Polycom VBP 5300E and Polycom VBP 6400ST (version 9.1.5 or greater) video firewall appliance protecting the corporate network working in parallel with the corporate firewall. The Polycom VBP can be located behind the corporate firewall if configured correctly. In this scenario the Polycom VBP is linked to the Internet via a communication router.
- A Polycom VBP 4350E for connection to the Branch Office as both Data and Video firewall. The 4350 also has the interface for connection to the T1 communications link.
- A Polycom CMA system (version 4.1 or greater) acting as the corporate LAN-side gatekeeper OR any other video/voice gatekeeper product of comparable capacity for managing video calls.
- Two or more video endpoints capable of H.460 communications—(There are many other Polycom and other video industry endpoints that use H.460 communication protocol. Many industry standard endpoints work with the Polycom equipment. It most cases there should be a good video connection. Discuss with your Polycom representative what your requirements are for video endpoints on the network
- One or more Polycom RMX systems that support multiple network types to extend the power of unified collaboration within—and beyond—the enterprise. This system is a platform for multipoint conferencing.
- One or more video endpoints inside the corporate network managed by the Polycom CMA system.

Optional Polycom systems that interoperate in this scenario include:

- One or more Polycom RMX systems as the conferencing platform for multipoint conferencing
- A Polycom DMA system for balancing

- Polycom RSS– The Recording and Streaming Server for sharing knowledge and also communicate more effectively by recording and streaming video communications
- Polycom VMC– The Video Media Center for connecting dispersed workforces and improving collaboration by seamlessly integrating video content with enterprise communications

Optional third-party systems that interoperate in this scenario include:

- Third-party firewall/routers (see listing of these earlier in this document).
- Many industry standard endpoints work with the Polycom equipment. It most cases there should be a good video connection. Discuss with your Polycom representative what your requirements are for video endpoints on the network

Network and Configuration Requirements

- Network design = Centralized gatekeeper design at the corporate headquarters. This allows for prefix dialing and Annex O dialing.
- Polycom VBP's configuration settings = LAN-side gatekeeper configuration for both of these

The corporate network needs two links to the Internet for the two separate Polycom VBP's used here. The SOHO setup requires an Internet connection of moderate speed. Normal business class bandwidth will deliver an even better video call experience Third-party firewall/routers (see listing of these in this document)

Summary

Polycom VBP firewall appliances are designed to be part of a cohesive video platform. The design is flexible enough to be integrated into the business network alongside existing data security systems. The VBP solves many of the issues presented when using the Internet for video communications making it a viable solution for secure Business to Business collaboration.

Many of the video systems today operate over private networks communicating on DS3, T1, and PSTN, to name a few. This communication model now includes the Internet. This makes it possible to have a video call between corporate offices and the Branch Office, the Regional Office, the home office and the International Office without dedicated point-to-point leased lines. The VBP allows this to happen, while using secure encryption of the call, over the public network. Those companies that already have the leased line model installed can leverage much of their existing network equipment for Internet video conferencing.

The difficulty of managing the video network is resolved since the VBP offers:

- Firewall security comparable to standard data firewall systems.
- Network Address Translation (NAT) of video endpoint communication through the network access point
- Traffic management with Quality of Service provisioning for solid video calls
- Encryption of the video calls
- Support for standard video conference protocols
- Monitoring system designed specifically for video conference troubleshooting