BlueJeans

WITH

DOLBY VOICE®

FIREWALL SETUP AND NAT CONFIGURATION GUIDE FOR H.323 / SIP ROOM SYSTEMS – BLUEJEANS 2018

Table of Contents

How to setup Firewall and NAT to work with Blue Jeans Network

NAT (Network Address Translation) configuration has always been a challenge for video conferencing. H.323/SIP embeds the IP address in the data payload so that when the packet is de-encapsulated on the other end, the IP address that is presented is the endpoint's IP. If the endpoint's IP is an internal IP address (10.x, 172.x 192.x etc.) then the receiving system will try to send packets to this non-routable address and the audio or video will fail and call may drop. This is a common problem with H.323/SIP call signaling when the endpoint is on a private IP address.

Network Address Translation (NAT) primary job is to translate the private IP to a unique public IP. This way the receiving endpoint will be presented the unique public IP address that it can send back payload and reach the initiating endpoint. When NAT is not configured correctly problems with connecting calls or issues with content sharing can be the result.

This document was created to increase your understanding and show you how to overcome the related issues.

IP Range and Destination Ports Used by Blue Jeans for H.323 and SIP Connections:

1720 TCP Control Port (static) – for Q.931 call signaling (H.225 protocol) used in setting-up and terminating a call. Q.931 negotiates which dynamic port range to use between the endpoints for H.245 Call Parameters, data, audio and video.

5060 / 5061 TCP - SIP and TLS

These ports MUST be allowed for Blue Jeans Network entire IP ranges (see below):

5000-5999 TCP - Dynamic - H.245 (Call Parameters)

5000-5999 UDP - Dynamic - RTP (Video Stream Data)

5000-5999 UDP - Dynamic - RTP (Audio Stream Data)

5000-5999 UDP - Dynamic - RTCP (Control Information)

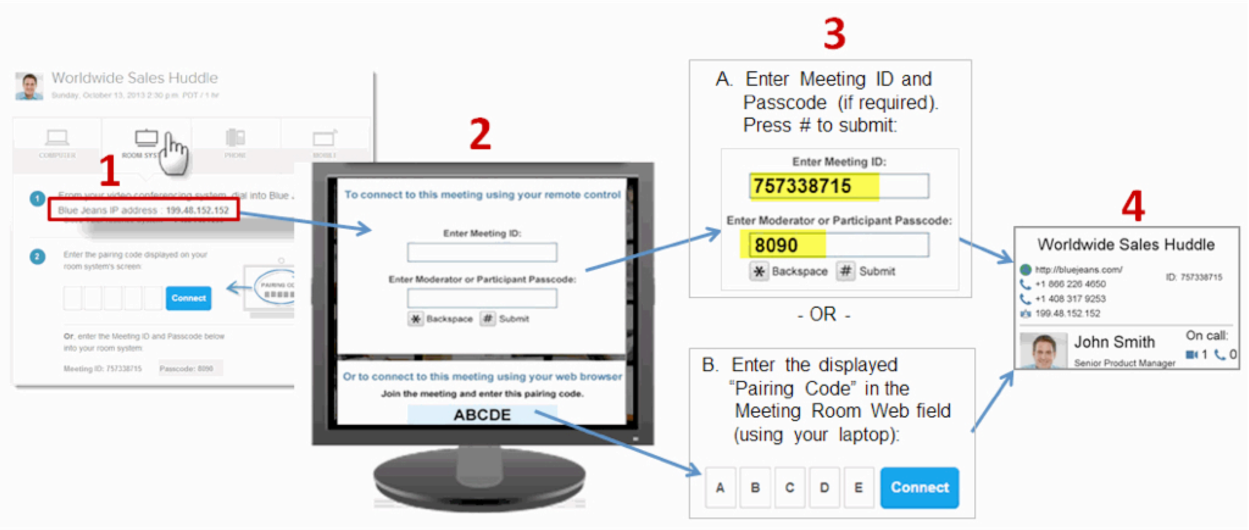
Blue Jeans Network IP ranges:

- **199.48.152.0/22**
- **31.171.208.0/21**
- **103.20.59.0/24**
- **103.255.54.0/24**
- **8.10.12.0/24**
- **165.254.117.0/24**
- **13.210.3.128/26**
- **34.245.240.192/26**
- **13.251.83.128/26**
- **104.238.240.0/21**
- **34.223.12.128/26**
- **35.175.114.0/26**
- **52.215.218.0/26**
- **13.233.177.128/26**

Note: Blue Jeans has several POPs distributed globally. The call will be automatically redirected by geo-location to the closest POP to the endpoint or media egress point. Audio/video traffic will be routed to any of above IP ranges based. Hence, it's important that firewall ports are opened against entire IP ranges. User end ports can be selected by Firewall or the endpoint.

Calling Blue Jeans from H.323 or SIP Room System

Entering a Blue Jeans Meeting


Worldwide Sales Huddle
Sunday, October 13, 2013 2:30 p.m. PDT / 1 hr
COMPUTER
ROOM SYSTEM
PHONE
MOBILE
1
From your video conferencing system, dial into Blue J
Blue Jeans IP address : 199.48.152.152
Enter the pairing code displayed on your room system's screen:
Connect
PAIRING CODE
Or, enter the Meeting ID and Passcode below into your room system:
Meeting ID: 757338715
Passcode: 8090
2
To connect to this meeting using your remote control
Enter Meeting ID:
Enter Moderator or Participant Passcode:
✱ Backspace
# Submit
Or to connect to this meeting using your web browser
Join the meeting and enter this pairing code.
ABCDE
3
A. Enter Meeting ID and Passcode (if required). Press # to submit:
Enter Meeting ID:
757338715
Enter Moderator or Participant Passcode:
8090
✱ Backspace
# Submit
- OR -
B. Enter the displayed "Pairing Code" in the Meeting Room Web field (using your laptop):
A
B
C
D
E
Connect
4
Worldwide Sales Huddle
http://bluejeans.com/
+1 866 226 4650
+1 408 317 9253
199.48.152.152
ID: 757338715
John Smith
Senior Product Manager
On call:
1
0

1) Click the "Room System" bar for instructions. Dial the IP address- **199.48.152.152 or the FQDN- bjn.vc** on your H.323 or SIP

2) After connection is made with Blue Jeans IVR, enter your 'meeting ID' or use "pairing" code panel.

3) You have two ways to enter the meeting from here:
- Enter the Meeting ID and Passcode (if applicable) in the boxes, using your Room System remote, and press # to submit, or,
- Enter the 5 letter pairing code in the BJN Meeting Room field on your browser, and press Connect

4) Blue Jeans then connects your room system to the meeting.

Figure 1

To call Blue Jeans from H.323 or SIP based Room System - Figure 1

1. Dial the Blue Jeans IP address 199.48.152.152 or bjn.vc or meet@bjn.vc (can also use *@bjn.vc) to reach the Blue Jeans IVR (Interactive Voice Response). The suggested dialing speed is 1 Mbps or higher for 720p resolution. For "speed dialing" instructions, see Dialing Direct with URI Dial String, below.

2. After connection is made with Blue Jeans IVR, enter your 'Meeting ID' or use 'pairing' code panel that will appear.

3. You have two ways to enter the meeting from here:

- Enter the Meeting ID and Passcode (if applicable) using your Room System remote, and press # to submit, or,
- Enter the 5-letter pairing code in the BJN Meeting Room field on your browser, and press Connect (this process must be used if you plan on changing your layouts from the web app).

4. Blue Jeans then connects your room system to the meeting.

URI Dialing for H.323 or SIP using domain: <Meeting ID>@bjn.vc

Note: When using Polycom RealPresence Mobile Version 3.1-44477, we suggest using the following URI methods:

* meetingID.passcode@bjn.vc (for h.323)

Dialing H.323 or SIP Direct with URI Dial String

You can also dial directly to meeting bypassing the Blue Jeans IVR by adding the meeting ID and passcode in URI string, letting you enter the meeting without having to complete steps 2 or 3 above:

From a Polycom, Cisco/Tandberg, Lifesize and Mirial/ClearSea endpoint you can dial H.323 directly into a Blue Jeans meeting using the following format: <Meeting ID>.<Passcode>@199.48.152.152 for example, if the meeting ID is 12345 and the passcode is 1111 the URI string will look like this 12345.1111@199.48.152.152

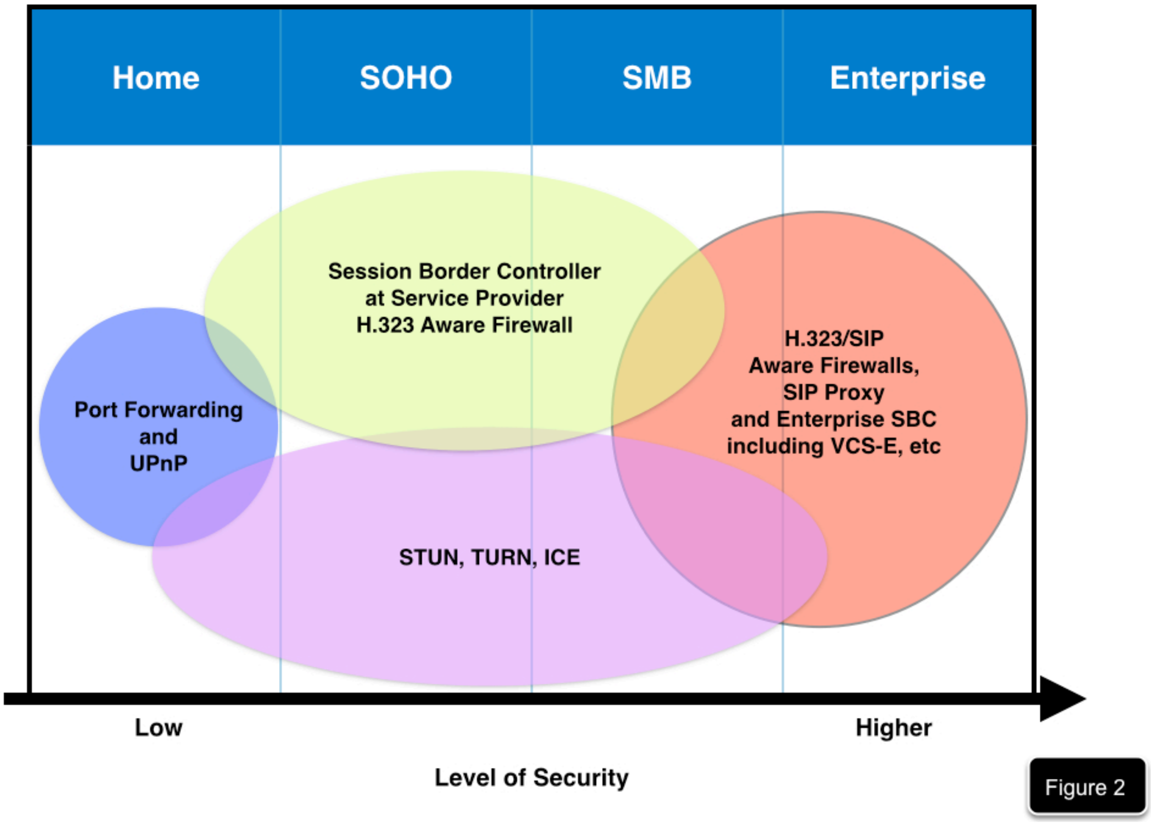
Should your meeting not contain a passcode then simply dial <Meeting ID>@199.48.152.152 e.g. 12345@199.48.152.152

Some older endpoints may not support the above dial string format. If you are experiencing issues connecting to Blue Jeans using the above format, please try one of the following:

- <IP>##<MeetingID>#<Passcode> (example:199.48.152.152##12345#1111)
- <IP>##<MeetingID>:<Passcode>
- <MeetingID>:<Passcode>@<IP>

NOTE: When using SIP protocol, the Room System should be configured for TLS or TCP.

Firewall/NAT Traversal Solutions



Firewall/NAT Traversal Solutions - Figure 2

Which solution is best for your organization or location can be dependent on many things. There is no "one" solution that fits all. Your IT department and required level of security needs will likely dictate what will be used. STUN, TURN, ICE solutions can be found used in many of these network topologies.

Home Networks

Small home networks will likely use 'port-forwarding' or UPnP. Most home networks do not have a dedicated firewall and use a NAT router running PPoE (Point-to-Point Protocol over Ethernet) to connect to their Internet Service Provider (ISP). Small home-based routers (like Linksys, D-Link, Actiontec, Apple, etc) can have public to private ports forwarded for internal private IP address. UPnP is protocol for allowing this automatically.

Port Forwarding can be configured on the router so the needed ports for video conferencing are passed from the home network's public IP to the private IP of the endpoint.

Universal Plug and Play (UPnP) permits networked devices to be able to automatically forward the needed ports. UPnP can provide support for NAT Traversal by learning the translated IP address and configure port mappings. Usually the initiation for this connection needs to begin from the inside of the home network. Not all home routers support UPnP or have it enabled by default.

Security for port forwarding and UPnP are on the low side, but for a home network are usually deemed adequate.

SOHO - Small Office

SOHO and small office environments commonly deploy Service Provider SBC (Session Border Controller) or make use of STUN, TURN, ICE. Some small offices may use a H.323 aware or SIP aware firewall that can be configured for static NAT to allow endpoint on private IP inside LAN to work with endpoints outside on the public Internet.

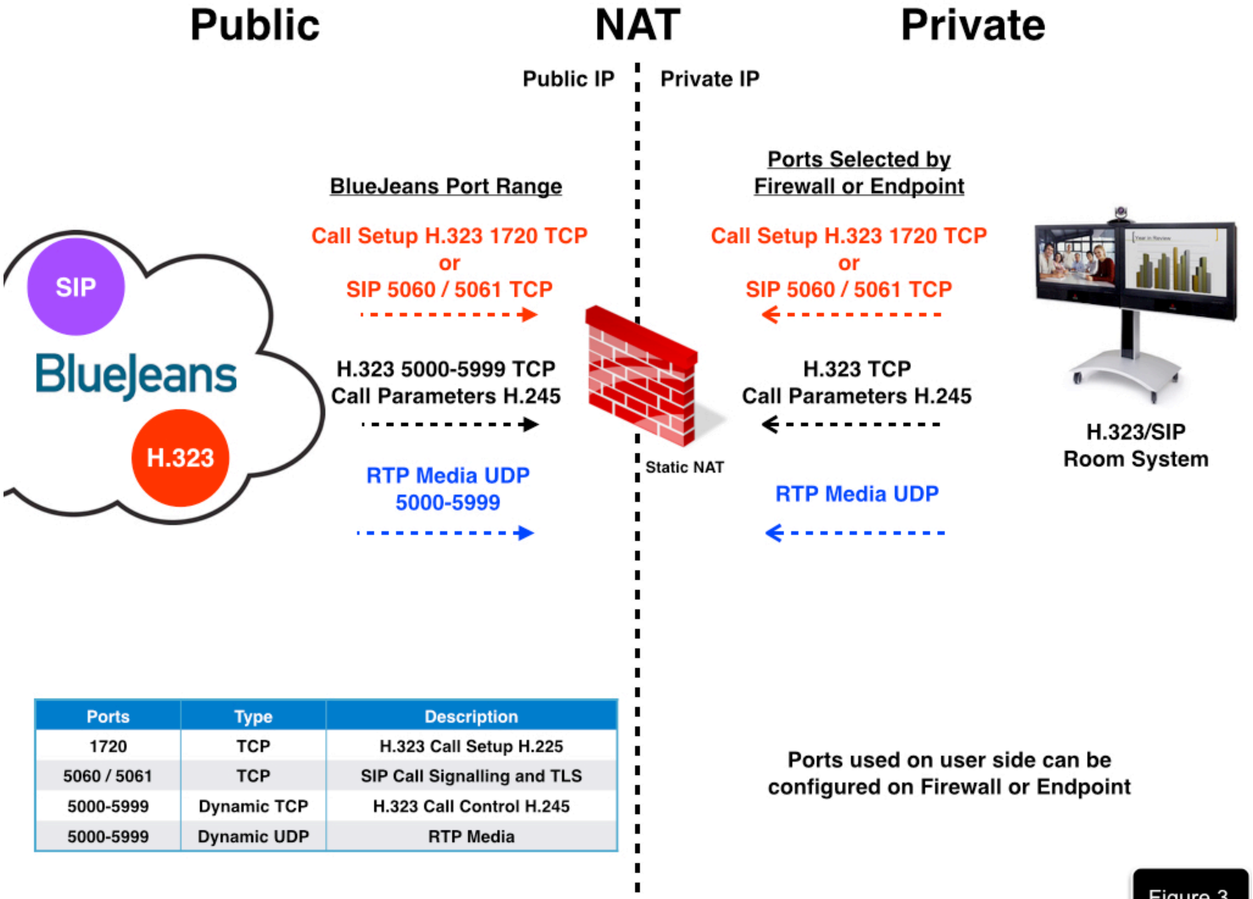
The security level is higher than what is commonly used on a residential home network.

SMB and Large Enterprises

Larger enterprises usually have higher security needs and budgets. They would usually deploy Enterprise SBCs, Firewall Transversal solutions or SIP Proxy solutions. Solutions like Cisco VCS, Polycom VBP, Lifesize Transit for firewall transversal is commonly used. Integrations with Microsoft Lync Server can be seen. SIP integrations with Cisco Unified Call Manager (CUCM) is common. Filtering solutions like Bluecoat and Websense may be running that can affect H.323 and SIP connections if exceptions have not been configured. Many enterprises use load balancers like Sonus, Radware, etc.

If is important to understand how the network and video environment is setup to fully understand the issues that can affect video conferencing.

Firewall and NAT Configuration



Ports	Type	Description
1720	TCP	H.323 Call Setup H.225
5060 / 5061	TCP	SIP Call Signalling and TLS
5000-5999	Dynamic TCP	H.323 Call Control H.245
5000-5999	Dynamic UDP	RTP Media

Figure 3

Recommendations

- Full-cone/ one-to-one/ Static NAT are recommended or have a suitable NAT traversal device (like VCS-E or VBP)
- If using Firewall recommended to open the ports manually with a separate policy/ accesslist instead of instead of relying on protocol inspection or transformation
- Firewall or NAT mechanism needs to allow for Blue Jeans IP/Port destination range
- Ports on the user side can be selected by Firewall or the Video Endpoint

IP Range and Destination Ports Used by BlueJeans for H.323 and SIP Connections:

1720 TCP Control Port (static) – for Q.931 call signaling (H.225 protocol) used in setting-up and terminating a call. Q.931 negotiates which dynamic port range to use between the endpoints for H.245 Call Parameters, data, audio and video.

5060 / 5061 TCP - SIP and TLS

These ports MUST be allowed for Blue Jeans Network entire IP ranges (see below):

5000-5999 TCP - Dynamic - H.245 (Call Parameters)

5000-5999 UDP - Dynamic - RTP (Video Stream Data)

5000-5999 UDP - Dynamic - RTP (Audio Stream Data)

5000-5999 UDP - Dynamic - RTCP (Control Information)

Blue Jeans Network IP ranges:

- **199.48.152.0/22**
- **31.171.208.0/21**
- **103.20.59.0/24**
- **103.255.54.0/24**
- **8.10.12.0/24**
- **165.254.117.0/24**
- **13.210.3.128/26**
- **34.245.240.192/26**
- **13.251.83.128/26**
- **104.238.240.0/21**
- **34.223.12.128/26**
- **35.175.114.0/26**
- **52.215.218.0/26**
- **13.233.177.128/26**

The Problems of NAT and Firewalls for video conferencing

- Many firewalls only allow connections to be initiated from the private network unless configured for video conferencing

- Firewalls commonly deny access to ports associated with video conferencing

- Some firewall even performs deep packet inspection to identify and reject VoIP traffic

- Unfortunately, no one traversal technique works with all existing NATs

Some NAT devices only allow packets from the remote endpoint to reach the NATed endpoint. This is often the case with “enterprise” NATs and this is called symmetric NATs (see STUN, TURN and ICE section).

The firewall can then open the ports accordingly; and/or it singles out H.323 exchanges and over-writes unrouteable IP addresses in outbound packets with a static NAT routable public IP address as the source and re- addresses inbound packets so they reach their destination.

NOTE: H.323 Inspection (some firewalls call this Transformations) is recommended to be enabled if not configured manually.

UDP Hole Punching

UDP hole punching is a common technique used to establish UDP connections with endpoints behind NAT. It is called UDP hole punching because it 'punches' a hole in the firewall which allows a packet from an outside system to successfully reach the desired client on a network using NAT. Contrary to what its name may suggest, hole punching does not compromise the security of a private network. This technique is incorporated into the ICE protocol (see STUN, TURN, ICE section).

NAT (Network Address Translation) - Figure 3

The Network Address Translation that is created on the firewall or by routers and is part of the security fabric for an Enterprise. NAT also became popular due to the shortage of Internet IPv4 unique IP addresses to allow all of the devices to be directly connected to the Internet. Migrating to IPv6 has the promise to resolve many of these issues, but likely will bring some new challenges. That is a discussion for another time however. With NAT only the firewall or router is given a publicly routable IP address. A NAT-mechanism works by associating a public address and port with a private (non-routable) destination address and port.

Example: Private 192.168.1.2:6102 &harr; Public 205.124.31.63:5199

This mapping is created when TCP SYN packet or first UDP packet is sent and is maintained as long as the TCP connection or UDP flow are “kept alive.”

If the H.323/SIP endpoint is behind firewall on a private IP address, the firewall and endpoint need to be properly configured. The private IP address that the endpoint is registered to will likely be a non-routable address. If the H.323/SIP endpoint advertises this address to the receiving endpoint you will likely end up with a dropped calls, "one-way" video or H.239 content sharing not working in Dual Stream mode. The reason is the receiving endpoint will try to contact the sending endpoint at this private IP address and will be unable to have proper communication.

In order to have successful calls when your H.323/SIP endpoint is on a private IP address is to configure a "one-to-one" static NAT that translate the private IP address to a unique public IP address. This is usually done at the firewall or using a transversal device like Cisco VCS-E (Video Communication Server - Expressway), Polycom VBP (Video Border Proxy), Edgewater SBC, Lifesize Transversal Server, etc.

There are two main reasons H.323 and firewalls sometimes don't get along:

1. The traffic requires a negotiated 'connection' on an unspecified higher UDP port. So, a firewall has to be configured to allow UDP traffic to these ports. BlueJeans uses TCP/UDP 5000 - 5999.

2. H.323 records the hosts' IP address in the payload of the packet. This causes problems if NAT is involved, since the H.323 packets will contain the private IP and not the translated public IP.

A properly configured H.323 aware firewall can handle both of these challenges. If you are using NAT, you must configure the H.323 aware firewall for static one-to-one NAT for H.323 traffic. Outbound ports to the Blue Jeans Network IP ranges need to be configured and then inbound traffic will be automatically allowed to go through once the pin hole is opened on stateful firewall.

Some issues seen also involve content sharing. Because H.239 (duo stream content sharing) is usually blocked unless there is a NAT traversal device or NAT-aware mechanism in place. What can happen is the H.239 content share can be transcoded replacing the main video and not present itself as "dual stream."

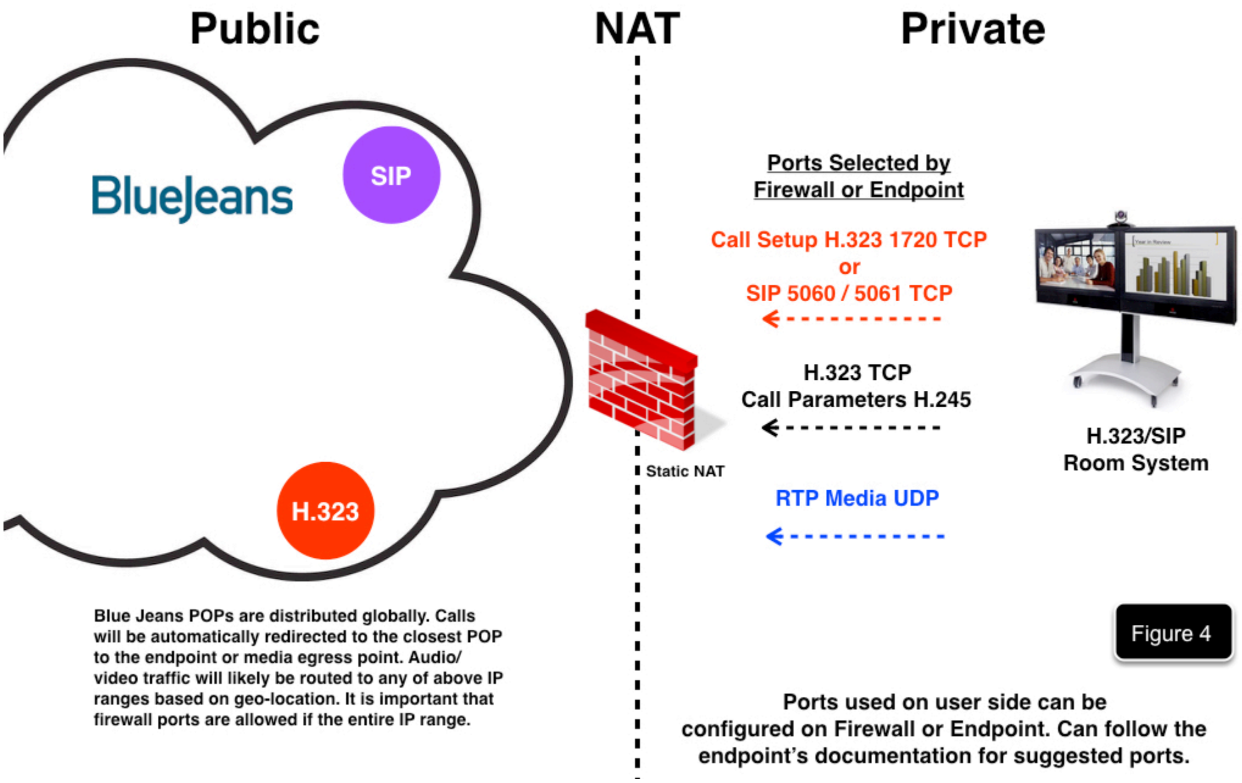
H.323 and Firewalls

By configuring a one-to-one static NAT and enabling H.323 inspection it is possible to give the firewall an awareness of the H.323 protocol. This will allow the firewall to manage the setup exchanges so that it 'learns' the ports to be negotiated. The firewall can then open the ports accordingly; and/or it singles out H.323 exchanges and over-writes unrouteable IP addresses in outbound packets with a static NAT routable public IP address as the source and re- addresses inbound packets so they reach their destination.

The latest releases of most vendors' endpoints including Polycom, Lifesize, Sony, Cisco/Tandberg all support NAT and allow you to specify the external IP address of the selected endpoint. Please investigate your User Guide for your H.323 endpoint for NAT settings.

Transversal Devices and Border Proxy Controllers like Cisco VCS -E, Polycom VBP or others can also provide a means for endpoints to transverse the firewall and/or NAT boundaries.

Blue Jeans POPs and Geo-location



Public
NAT
Private
BlueJeans
SIP
H.323
Ports Selected by Firewall or Endpoint
Call Setup H.323 1720 TCP or SIP 5060 / 5061 TCP
H.323 TCP Call Parameters H.245
RTP Media UDP
Static NAT
H.323/SIP Room System
Figure 4

Blue Jeans POPs are distributed globally. Calls will be automatically redirected to the closest POP to the endpoint or media egress point. Audio/ video traffic will likely be routed to any of above IP ranges based on geo-location. It is important that firewall ports are allowed if the entire IP range.

Ports used on user side can be configured on Firewall or Endpoint. Can follow the endpoint's documentation for suggested ports.

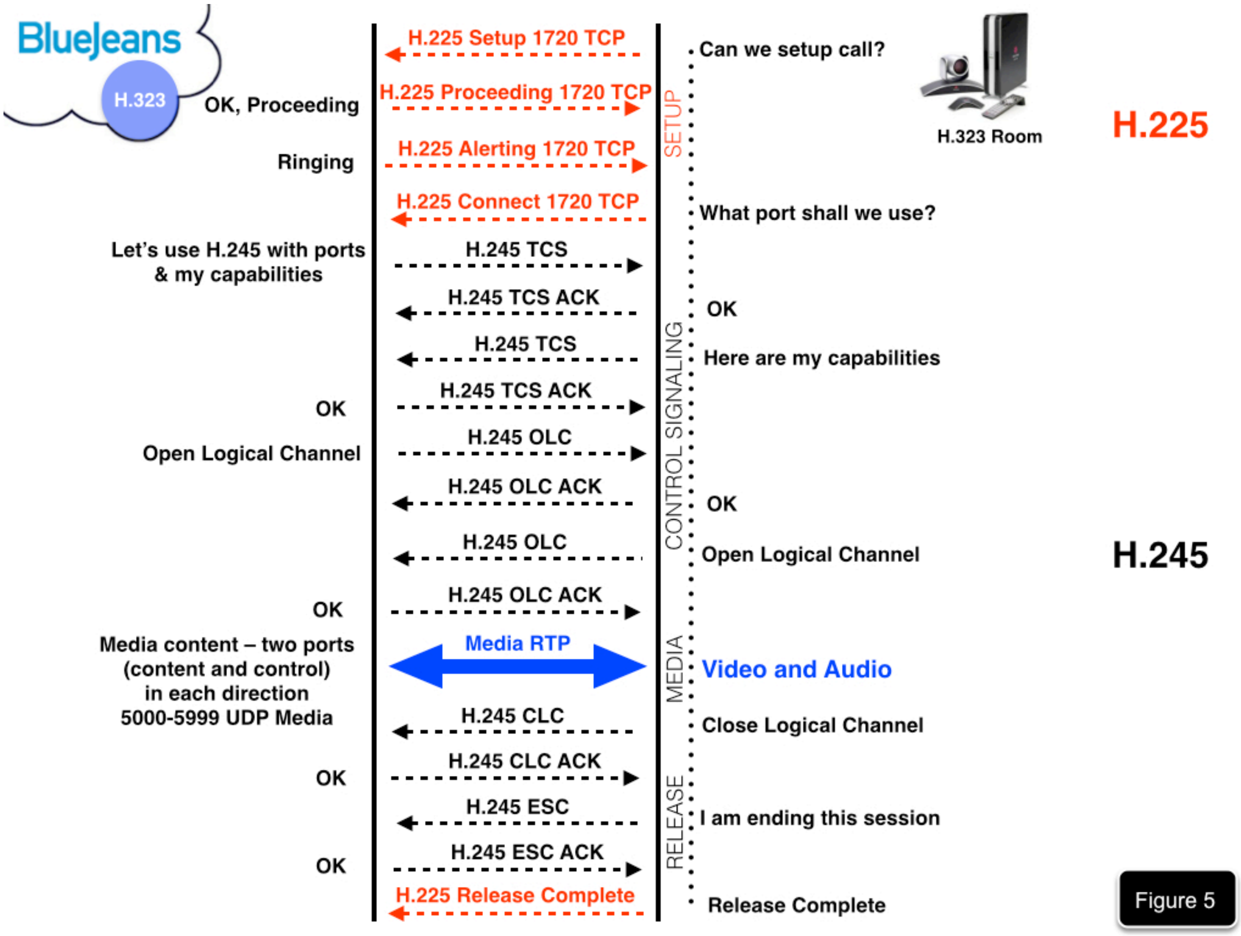
Geo-location with Blue Jeans

Blue Jeans has several POPs distributed globally. The call will be automatically redirected by geo-location to the closest POP to the endpoint or media egress point. Audio/video traffic will be routed to any of above IP ranges based. Hence, it's important that firewall ports are opened against entire IP ranges. User end ports can be selected by Firewall or the endpoint.

Blue Jeans Network IP ranges:

- **199.48.152.0/22**
- **31.171.208.0/21**
- **103.20.59.0/24**
- **103.255.54.0/24**
- **8.10.12.0/24**
- **165.254.117.0/24**
- **13.210.3.128/26**
- **34.245.240.192/26**
- **13.251.83.128/26**
- **104.238.240.0/21**
- **34.223.12.128/26**
- **35.175.114.0/26**
- **52.215.218.0/26**
- **13.233.177.128/26**

H.323 Call Signaling Explained



H.323 Call Flow Explained

Call Signaling is used to establish, control and end an H.323 call. The call signaling of H.225 (based on the call setup procedures for ISDN H.320) uses Q.931 communication.

Call Flow - H.323 Room System making outbound call to Blue Jeans - Figure 5

Call Setup H.225

1) H.323 endpoint initiating the call via port 1720 TCP - "Can we setup call?"

- After receiving the SETUP message, Remote endpoint stores IP addresses, port numbers, etc.

2) Blue Jeans accepts the incoming call - "OK, Proceeding"

3) Blue Jeans sends Alert Message - "Ringing"

4) H.323 endpoint sends Connect message - "What port shall we use?"

- The most important information in the CONNECT message is about the setup of an H.245 control channel, which is used for capability exchange (TCS), master-slave determination (MS), and opening logical channels (OLC), that is, creating media streams for audio, video, and content.

Control Signaling H.245

Systems discover highest common capabilities. Once both endpoints exchange capabilities they send (ACK) acknowledge message

1) Blue Jeans sends ports to use and Terminal Capabilities Set (TCS) telling remote endpoint what it can do - " Let's use H.245 and here is my capabilities"

- TCS advertises what capabilities the device can use like video and audio codecs, content sharing (H.239), security (H.235), far-end camera control FECC (H.224), etc.

2) H.323 endpoint sends Acknowledgement (ACK) - "OK"

3) H.323 endpoint sends Terminal Capabilities Set (TCS) telling BlueJeans what it can do - " Here are my capabilities"

- TCS is a procedure for exchanging preferred audio and video codecs and settings between the two H.323 endpoints. Once both sides agree parameters they go the next phase which is the H.245 Master Slave Determination

4) Blue Jeans sends Acknowledgement (ACK) - "OK"

This completes a required four-way H.245 protocol handshake before opening up the logical channels for the session. After sending TCS message a Master/Slave Determination (MSD), is completed. The master in a call controls actions between the two H.323 devices. Example, if both endpoints attempt to open incompatible media flows, the master takes action to reject the incompatible flow. Once the TCS is complete between endpoints Logical Channels are Opened and the session can proceed.

5) Blue Jeans sends message Open Logical Channel (OLC)

- Logical Channel Request procedure creates media channels between the endpoints. These channels are always created in pairs with the video channel from Initiating Endpoint to Remote Endpoint different and separate from the video channel from Remote Endpoint to Initiating Endpoint. Communication can be asymmetric: Initiating Endpoint can send high quality video to Remote Endpoint, and receive lower quality video from Remote Endpoint, and vice versa.

6) H.323 endpoint sends Acknowledgement (ACK) - "OK"

7) H.323 Endpoint sends message Open Logical Channel (OLC)

8) Blue Jeans sends Acknowledgement (ACK) - "OK"

H.245 control channel is also used to transmit the Flow Control command, which is used by the receiver to set an upper limit for the transmitter bit rate on any logical channel, and the Fast Video Update (FVU) command, which is used by the receiver to request resending video frames that were lost in the transmission. The FVU can be used to modify the bit rate when the receiver detects high packet loss. Seeing lots of FVU messages in the H.323 call flow can be a good indication of high packet loss.

Media RTP H.245 - RTP/RTCP

When TCS and MSD are complete Logical Channels or Media flows are opened (OLC) and ACKs are sent between endpoints. Logical Channels are basically multiplexed paths between the endpoints used for data transfer. RTP/RTCP video and audio are sent over media port range 5000 - 5999 UDP negotiated by H.323 endpoints

RTP - Real-time Transport Protocol defines standardized packet format for delivering audio and video over IP networks.

RTCP - Real Time Control Protocol is used to monitor transmission statistics and quality of service (QoS) of multiple media streams. The primary function of RTCP is to provide feedback on the quality of service being provided by RTP.

Release H.245 - Closing Logical Channels and End Session Command

1) H.323 endpoint sends Close Logical Channel (CLC) request

2) BlueJeans sends Acknowledgement (ACK) - "OK"

3) H.323 endpoint sends End Session Command - "I am ending this session"

4) BlueJeans sends Acknowledgement (ACK) - "OK"

5) H.323 endpoint sends H.225 Release Complete Message

Important Things to Understand

Dual Video Streams (H.239) allows content shared to be created in parallel to the primary "live" audio- video stream. Common issue is when improperly configured NAT will cause the "share" to be transcoded replacing the main video stream.

H.323 implements H.235 for secure connections which uses Advanced Encryption Standard (AES). Endpoints can be set to None, Optional or Strict.

DTMF tones (Dual-tone multi-frequency signaling) are used to enter Meeting ID (and Passcode if there is one) or activate other functions during the conference.

H.323 Gatekeepers

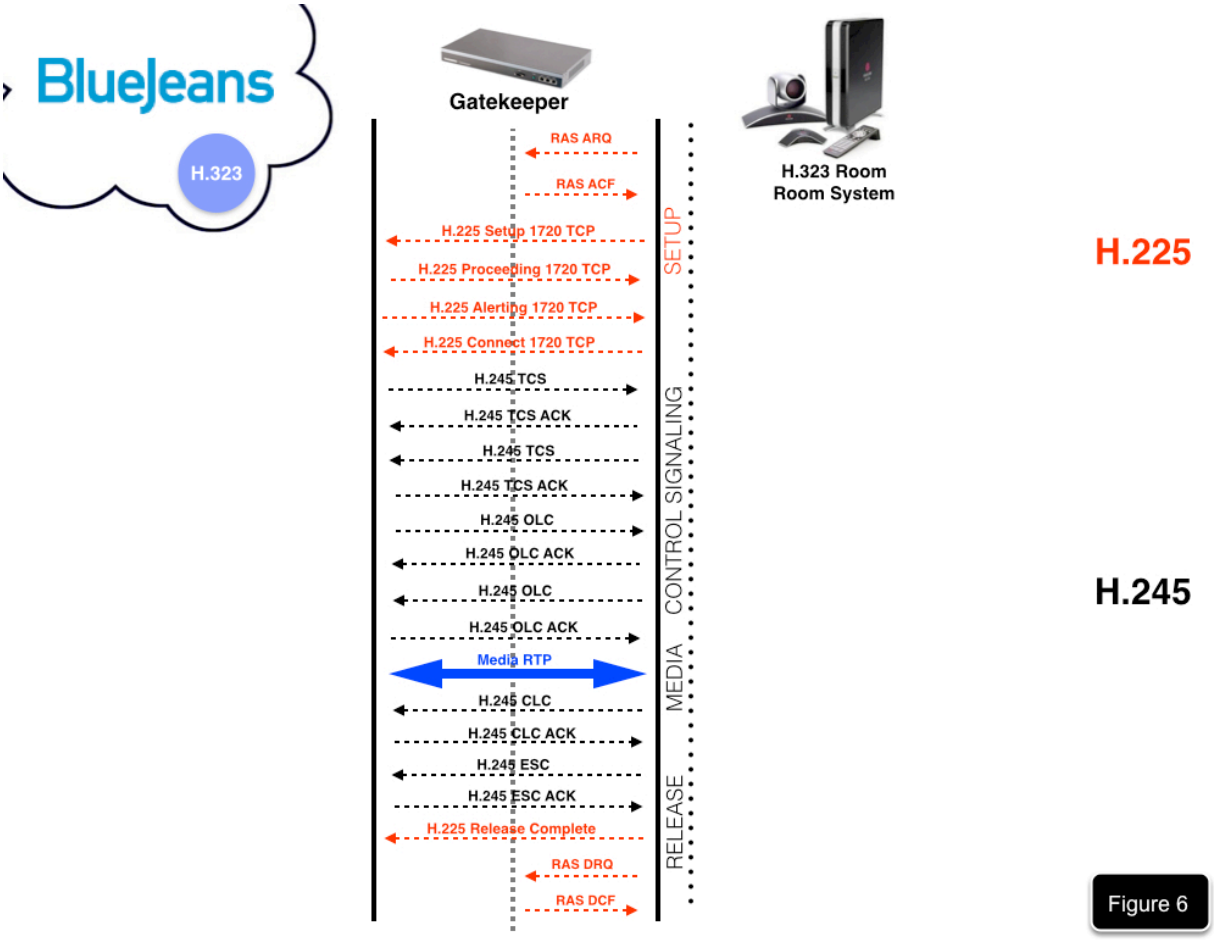


Figure 6

What is a H323 Gatekeeper for?

Think of the Gatekeeper as the traffic cop on the video network. - Figure 6

H.323 Gatekeeper functions:

- Call Admission Control
- Address Translation - E.164 dialing
- Bandwidth Control and Zone Management - Deny or Limit Calls and Limit Bandwidth to prevent network congestion

- Accounting and Dial Plan Implementation
- Call Management and Authorization - redirect calls and time of day policies
- Call Signaling Control - direct or routed mode - can allow for direct connection between H.323 endpoints (direct mode) or route call-signaling between H.323 endpoints
- Monitoring which systems are on-line and are in a conference
- Proxy / NAT Traversal (tunnel H.323 calls through a firewall or NATed network using H.460)
- Session Border Controller - work with additional gateway device
- Gatekeepers are optional in an H.323 network, but if a gatekeeper is present, endpoints must use the services provided and follow the rules applied

If H.323 endpoint is registered to a Gatekeeper, it must ask the Gatekeeper permission to initiate call using RAS (Registration, Admission and Status) messaging. RAS is usually located on port 1719 as part of the H.323 Protocol Suite. The H.323 endpoint initiating the call will send an admission request ARQ to the gatekeeper. Gatekeeper will resolve the address of the remote endpoint and give admission confirm message ACF. The initiating H.323 endpoint can then place the call.

Gatekeepers can work in Direct or Routed Mode:

- Direct Mode the endpoints utilize the RAS protocol in order to learn the IP address of the remote endpoint and a call is established directly with the remote device. Media and signaling runs directly between the endpoints.
- Routed Mode the call signaling always passes through the gatekeeper which requires the gatekeeper to have more processing power, it also gives the gatekeeper complete control over the call. Routed Mode allows for Call Forwarding, Alternate Routing and Least Cost Routing (choosing desired network).

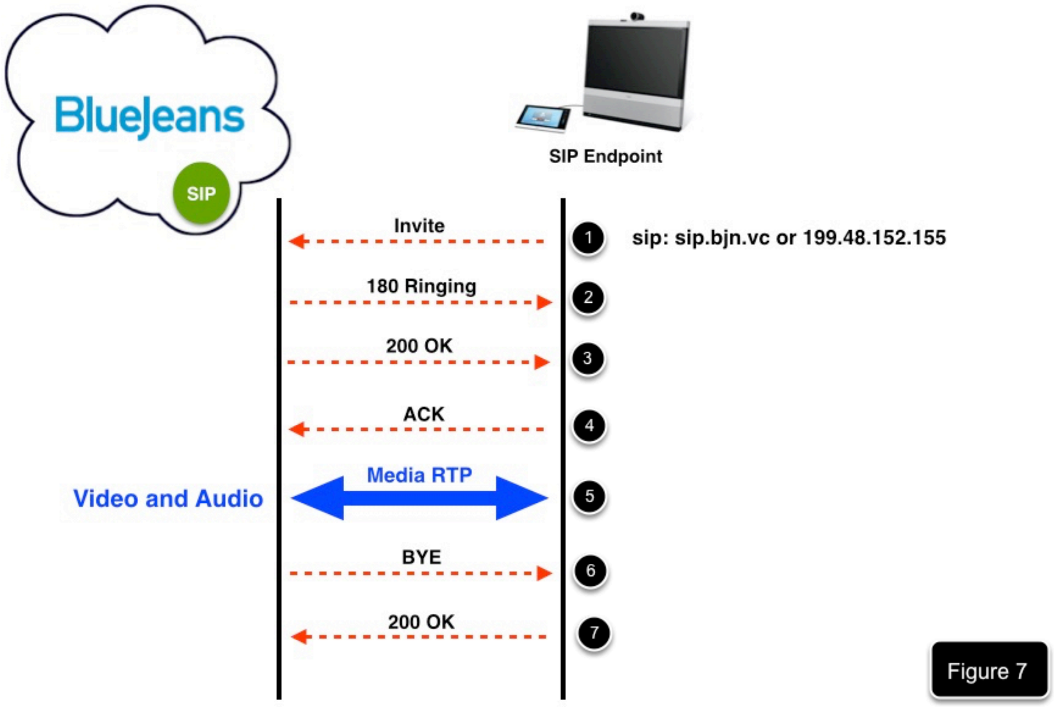
Gatekeepers can manage or limit bandwidth and enforce calling policies. When H.323 endpoints register with a single Gatekeeper this is called a zone. Gatekeepers can also "neighbor" with other Gatekeepers or zones. This can use a Dialing Plan that allow “inter-zone” dialing so that two endpoints in separate zones can still communicate with each other. This is the main way Legacy video conferencing networks are managed.

Address Resolution enables two endpoints to contact each other without either endpoint having to know the IP address of the other endpoint. In order for this to work all the endpoints involved would need to be registered to Gatekeeper.

Gatekeepers resolve the addresses of the various H.323 endpoints registered to it and allows for the facilitation of the Administrator's Dialing Plan. Since the Gatekeeper keeps track of all the H.323 endpoints, users can dial endpoints using just an E.164 alias.

If placing a call to an endpoint on the outside of the network (Internet) it is important to understand that the Gatekeeper must allow this call to proceed.

SIP Call Flow Explained



SIP Signaling Explained - Figure 7

Basic SIP Call Flow:

1) Invite sent to Blue Jeans using bjn.vc or meet@bjn.vc (or 199.48.152.152) to port 5060 or 5061 (TLS) - Used to establish a media session between user agents. Included in the invitation are the parameters for the audio or video that will be used. These parameters are included in

the SDP (Session Description Protocol). When both endpoints agree and are ready to start exchanging media or data.

2) 180 Ringing - received INVITE, and is alerting user of call.

3) 200 OK - indicates the request was successful

4) ACK - confirms reliable message exchange.

5) RTP (Realtime Transport Protocol) Media - contains the audio and video packets in both directions.

6) BYE - terminates a session between two users in a conference.

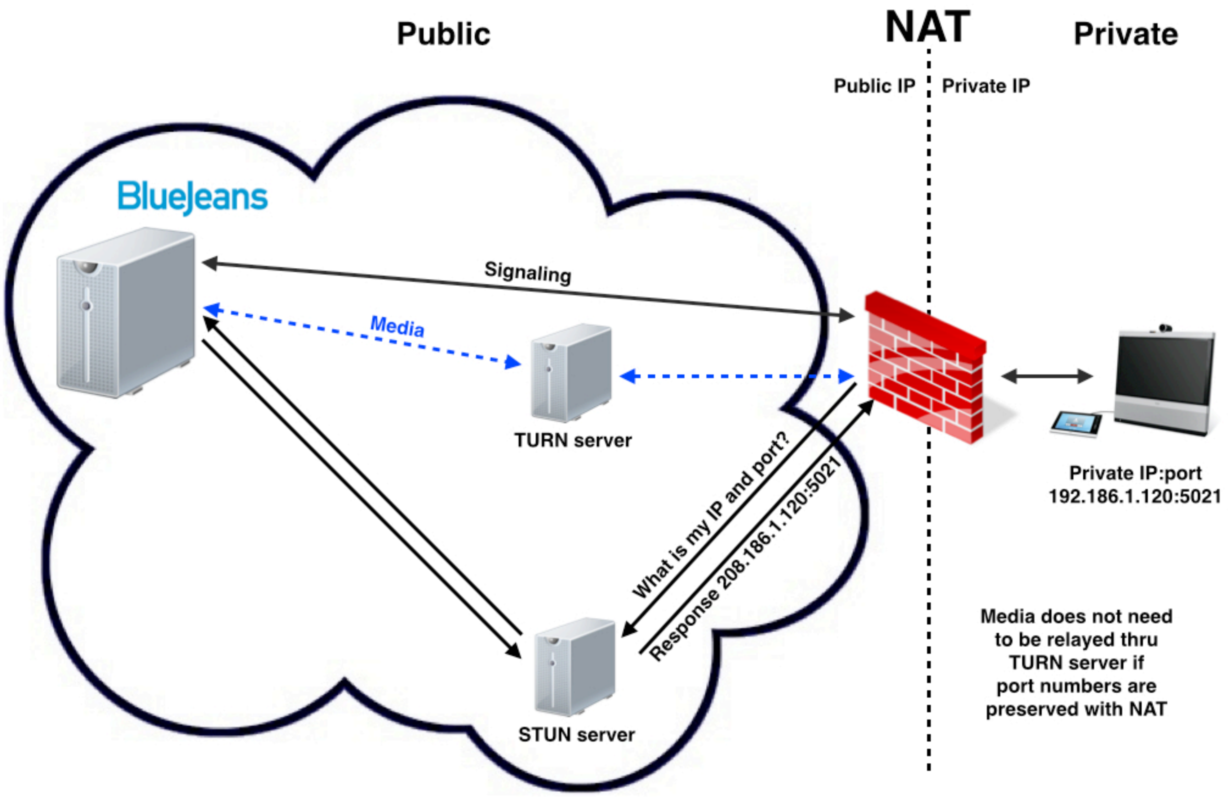
7) 200 OK - indicates the request was successful

When analyzing SIP Call Flow you may see other Response codes that may or not indicate a problem. You can look these up on the Internet.

Try http://en.wikipedia.org/wiki/List_of_SIP_response_codes

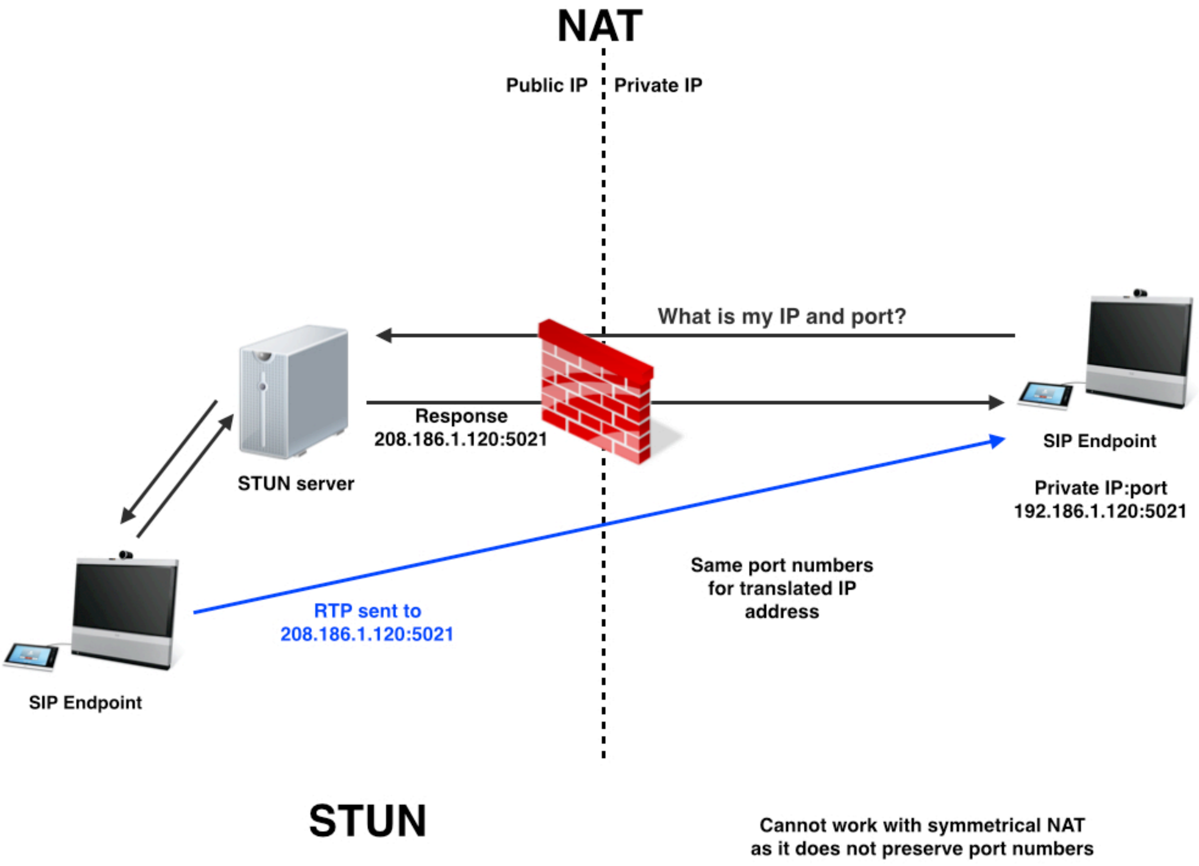
NOTE: BlueJeans supports SIP over TLS and TCP

STUN, TURN and ICE



STUN, TURN and ICE Deployed

Figure 8



Cannot work with symmetrical NAT
as it does not preserve port numbers

Figure 9

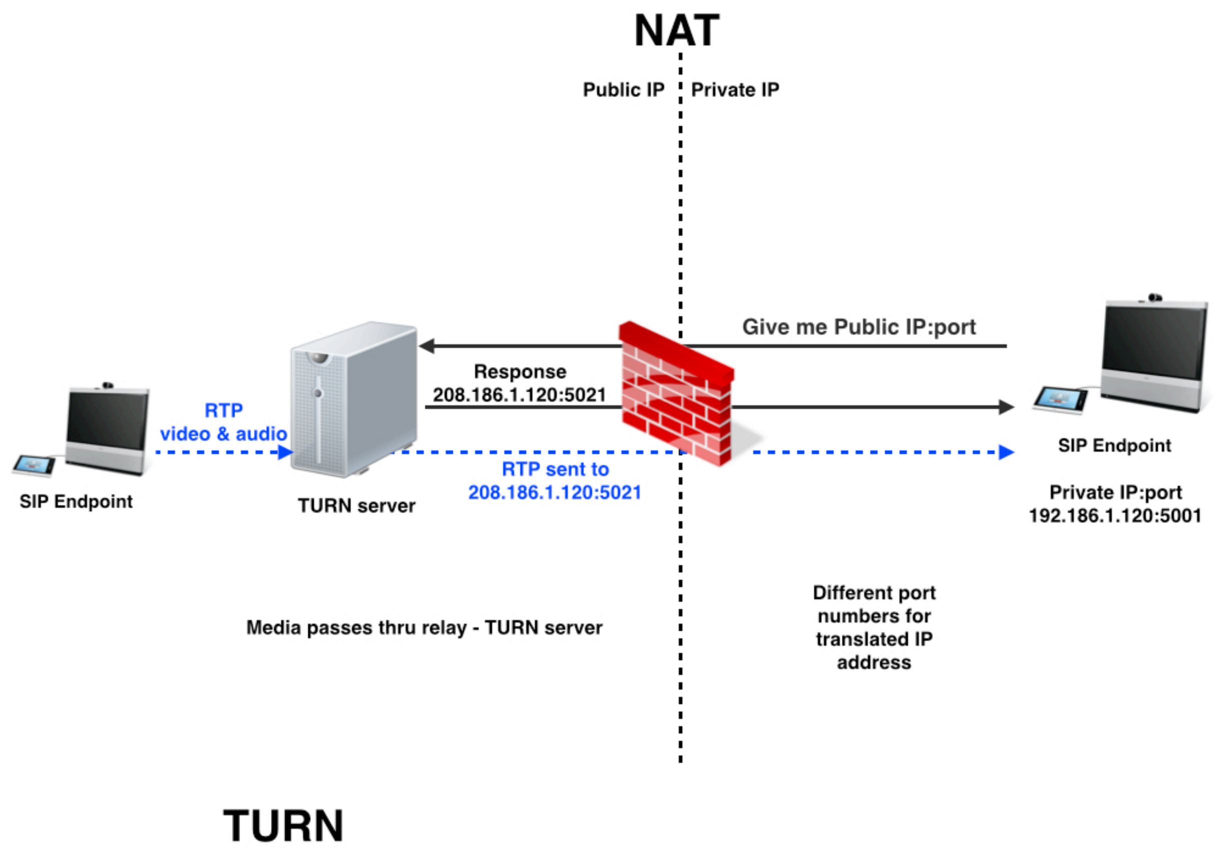


Figure 10

STUN, TURN, ICE Explained - Figure 7

Basically, if your endpoint is behind a NAT it may need some external help to connect. That external help is the STUN server. A STUN server's job is to provide NAT traversal (UDP hole punching) by making your endpoint aware of its public IP address.

STUN, TURN, ICE are all protocols for solving the firewall/NAT traversal issue using intelligence in the endpoint together with external servers (STUN and TURN servers). This is accomplished by a pinhole (hole punching as it is known) being created in the NAT/firewall for SIP signaling and media to pass through. The firewall must be configured to allow the endpoint to create the necessary pinhole.

STUN (Session Traversal Utilities for NAT) - Figure 9

STUN is a protocol for discovering the public IP address and port that the NAT has allocated for UDP connections to remote endpoints. A STUN server is located on the public Internet (or ISP's network offered as a service). STUN is a tool to that is used ICE (Interactive Connectivity Establishment) protocol.

A STUN server does one task. It checks the IP address and port of an incoming request and sends it back to see it gets a response.

The NAT endpoint (running STUN protocol) initiates a connection to the STUN server and creates binding. The STUN server inspects the IP address sends back a message containing the IP address and port in its payload allowing the endpoint to client learn its public IP address and port. The NAT endpoint that learns its public IP address and port can use this instead of its private address in the SIP headers and RTP ports in the SDP.

Firewall/NAT MUST allow for this to work. Therefore, STUN cannot be used with 'symmetric' NATs. Here is where relays using TURN comes into play.

STUN is not a fix-all. If the endpoint is behind a 'symmetric' NAT even though the public IP address can be found by utilizing the STUN server, it likely cannot create a connection.

Symmetric NAT is Different

In the case of a symmetric NAT every single connection has a different mapping with a different randomly generated port and this creates a unique challenge for video conferencing.

NAT (full cone NAT, restricted cone NAT, and port restricted cone NAT) do not change the source port when making NAT connections. When a client accesses the Internet using 192.168.0.1:5672 (IP:source port) NAT changes the source IP to say 56.34.66.12 but keeps the port number the same. For example, 192.168.0.1:5672 to 56.34.66.12:5672. This is known as port preservation.

UDP hole punching will not work with symmetric NAT devices (also known as bi-directional NAT) which tend to be found in most large corporate networks.

A symmetric NAT differs from other types of NAT as it does not keep the same port number, it randomly generated new ones. This is known as ephemeral port that is a short-lived transport protocol port. With a symmetric NAT the example would be 192.168.0.1:5672 to 56.34.66.12:5001. Since symmetric NAT maps new ports to the found source IP, utilizing STUN server alone cannot create the connection needed. The use of ephemeral ports for each communication renders NAT port prediction impossible. This is where TURN servers come into play.

TURN (Traversal Using Relays around NAT) - Figure 10

In the case of symmetric NATs (commonly found), STUN alone cannot be used as the NAT devices only allow packets from the remote endpoint to reach the NATed endpoint. Endpoint that is behind a symmetric NAT needs to initiate and maintain a connection to a relay in order to be successful. TURN is a protocol for communicating with the relay that was built on top of STUN.

TURN is used to relay media between peers, not signaling.

TURN servers have public addresses and can be contacted by peers (even when behind firewalls or proxies). TURN servers only relay media stream.

The TURN server is located on the public Internet (or ISP's network offered as a service). A NATed TURN client asks this server to allocate a public address and port and "relay" packets to and from that relayed address. The endpoint can use this instead of its private address in the SIP headers and RTP ports in the SDP. TURN usually guarantees communication in most all NAT configurations unless there is a firewall policy to prohibit using it. The connection does require a bit more overhead and the media quality can be a bit lower.

ICE (Interactive Connectivity Establishment)

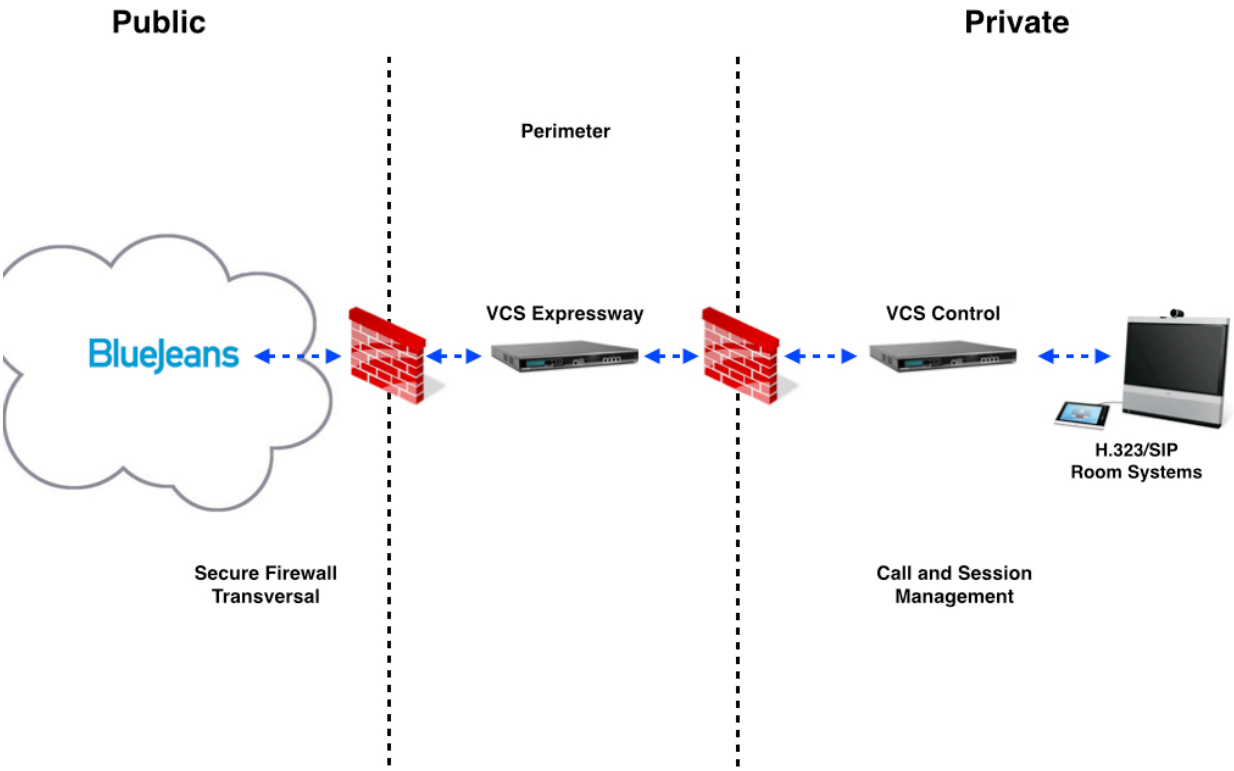
ICE is a protocol that performs connectivity checks and tries to find the best path to connect endpoints. ICE first tries to make a direct connection. If endpoint is behind NAT, then ICE tries to obtain the public address using a STUN server. If this fails, the traffic is relayed via a TURN server. ICE only uses relay in the worst case when there is no other way to connect.

Summary:

- STUN server is used to get an external network address for NAT endpoint
- TURN server is used to relay media traffic if direct (peer to peer) connection fails
- ICE is the protocol that is used to facilitate the communication between endpoints and does the connectivity checks

NOTE: The endpoint must support ICE/STUN/TURN

Border Controllers and Proxies



Cisco VCS-E Deployed

Figure 11

Cisco Video Communication Server (VCS) - Figure 11

Transversal solutions like Cisco Video Communication Server (VCS) provides session control and firewall traversal. Cisco VCS transversal solution is comprised of Cisco Video Communication Server Control (VCS-C) installed typically "inside" the private network and the Cisco Video Communication Server Expressway (VCS-E) that uses public network domain name is installed outside on the Internet or in DMZ.

Cisco VCS-C provides video call and session control, registrations, and enhanced security for video conferences. It also enables definitions such as routing, dial plans, and bandwidth usage, while allowing organizations to define video call-management. To accomplish firewall transversal to connect with endpoints outside the private network the Cisco VCS-E is required alongside Cisco VCS Control. The Cisco VCS-E allows video traffic to traverse the firewall and requires "transversal licenses" to allow for connections to endpoints on the Internet. Proper configuration is required for the "inside" endpoints to communicate with "outside" connections as well as a properly configured firewall.

The Cisco VCS Expressway uses SIP or H.460.18/19 for firewall traversal of signaling and media across a range of ports. The Cisco VCS Expressway provides TURN relay services to Interactive Connectivity Establishment (ICE)-enabled endpoints to allocate relays for the media components of the call. The endpoints perform connectivity checks through ICE to determine how they will communicate.

Cisco VCS can replace standalone H.323 gatekeeper or SIP proxy. Cisco VCS solution can allow for SIP and H.323 interworking. Natively, H.323 and SIP endpoints cannot directly communicate. With Cisco VCS deployed, video calls can be made between H.323 and SIP endpoints. This can be done by creating a "transform" for call routing on the Cisco VCS Control.

There are three basic ways to bridge SIP and H.323 using multi-protocol conference server (like Blue Jeans) or MCU, dual-stack endpoints (endpoint with ability to run both SIP and H.323 protocols) and signaling video conference gateways (like Cisco VCS).

Interworking

When using Cisco VCS for call control, the VCS provides a gateway functionality that allows interoperability between endpoints using different protocols (interworking) like SIP/H323. In general, this gateway feature of Cisco VCS works very well in most cases, but there are some cases where interworking SIP/H323 may cause issues and strange behaviors, depending upon which endpoints are involved on the call and the features negotiated.

Issues involving encryption negotiation, DTMF interoperability and content sharing can sometimes be seen. This kind of problem is common when using VCS Expressway to internet integration, where the endpoints have conferences with different companies and with so many different type of video systems.

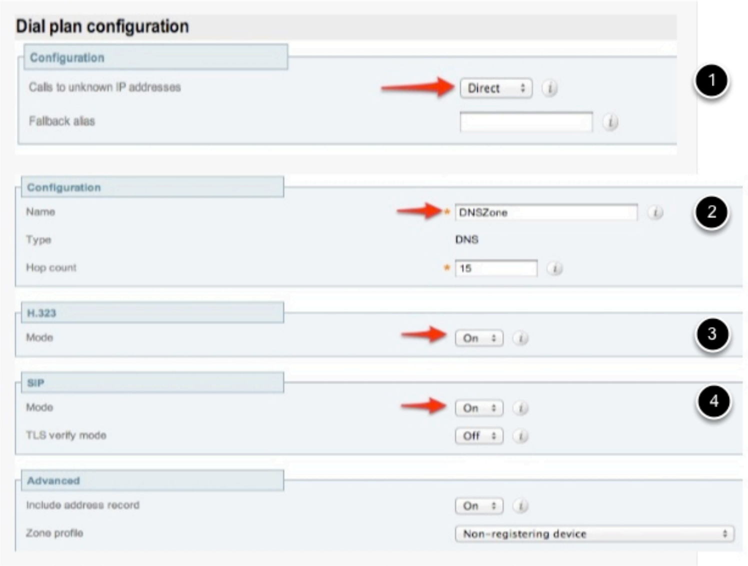
Considering the possibility of having these problems related to SIP/H323 interworking. Try to test with interworking disabled using the native H.323/SIP protocol is issues arise.

Polycom Video Border Proxy (VBP) and Lifesize UVC Transit

Polycom VBP and Lifesize UVC Transit (and other similar solutions) work in a very similar fashion as the Cisco VSC solution securely connecting video participants "inside" and "outside" the corporate firewall. These solutions work along with Gatekeeper functionality to hide the corporate LAN topology and integrate with firewalls. Most use H.460 which is an extension of H.323 protocol suite that deals with firewall and NAT traversal.

Cisco VCS Configuration to Connect to Blue Jeans

Cisco VCS Expressway



Dial plan configuration

Configuration

Calls to unknown IP addresses: Direct (1)

Fallback alias:

Configuration

Name: DNSZone (2)

Type: DNS

Hop count: 15

H.323

Mode: On (3)

SIP

Mode: On (4)

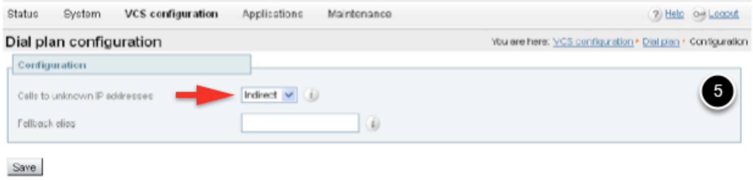
TLS verify mode: Off

Advanced

Include address record: On

Zone profile: Non-registering device

Cisco VCS Control



Dial plan configuration

You are here: VCS configuration • Dial plan • Configuration

Configuration

Calls to unknown IP addresses: Indirect (5)

Fallback alias:

Figure 12

The following steps is a required one-time setup for endpoint that registers to Cisco Video Communication Server (VCS) to connect to Blue Jeans - Figure 12

Configure the Cisco VCS-Expressway to route calls to Blue Jeans. Make sure VCS has the appropriate DNS server configured System -> DNS.

Make sure VCS is setup for dual network interfaces and the firewall rules are setup correctly, refer to firewall requirement.

1. **On VCS-Expressway** -> VCS configuration -> Dial plan -> Configuration, set "Calls to unknown IP addresses" to direct

2. Create a DNS zone to route outbound calls by going to VCS Configuration > Zones > New DNS Zone and adding a zone

3. H.323 Mode set to On
4. SIP Mode set to On
5. **On VCS-Control** -> Dial plan -> Configuration, set "Calls to unknown IP addresses" and configure Cisco VCS-Control to Indirect

Note: Cisco recommends that any SIP or H.323 'fixup' ALG (application-level gateway) or awareness functionality be disabled on the NAT firewall. If enabled this could adversely interfere with the VCS functionality. Full setup and configuration for Cisco VCS is beyond the scope of this document. For more information please investigate the Cisco VCS Deployment Guide.

Room Systems behind Firewalls configured with ALG can sometimes expereince random audio issues as well!

SIP Proxy

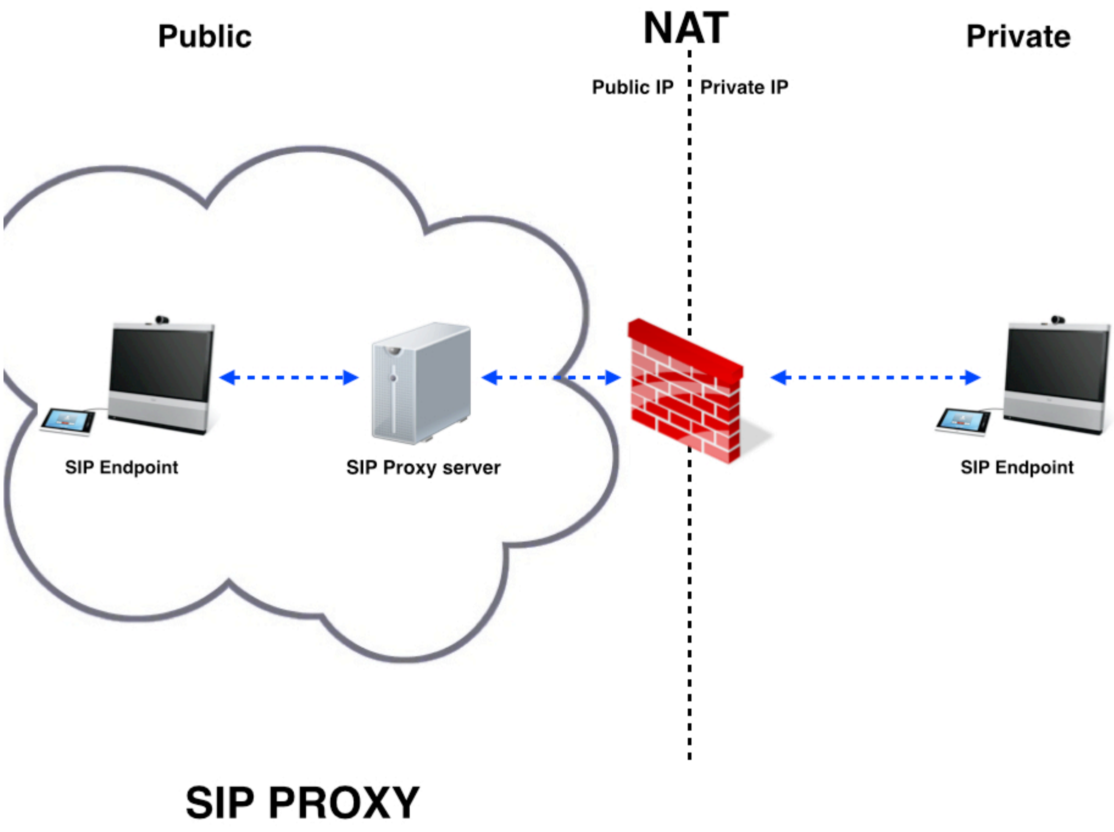


Figure 13

SIP Proxy - Figure 13

SIP proxy manages the setup of calls between SIP devices including the controlling of call routing and it also performs necessary functions such as registration, authorization, network access control and network security. The SIP "Proxy" basically acts as the intermediate or "go-between" and this is how it protects the SIP network and provides for a higher level of security.

The proxy server is the intermediate entity that acts as both a server and a client for the purpose of making requests from other clients primarily doing the routing. Proxies are also used for enforcing policy (example: is user allowed to make this call). A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it.

The registrar is a server that accepts REGISTER requests and places the information it receives for the domain it handles.

The redirect server is a user agent server that generates 3xx responses to requests it receives, directing the client to contact an alternate set of URIs.The redirect server allows SIP Proxy Servers to direct SIP session invitations to external domains.

NOTE: In some cases the proxy server and registrar will run on the same server

Common Issues and How to Overcome Them

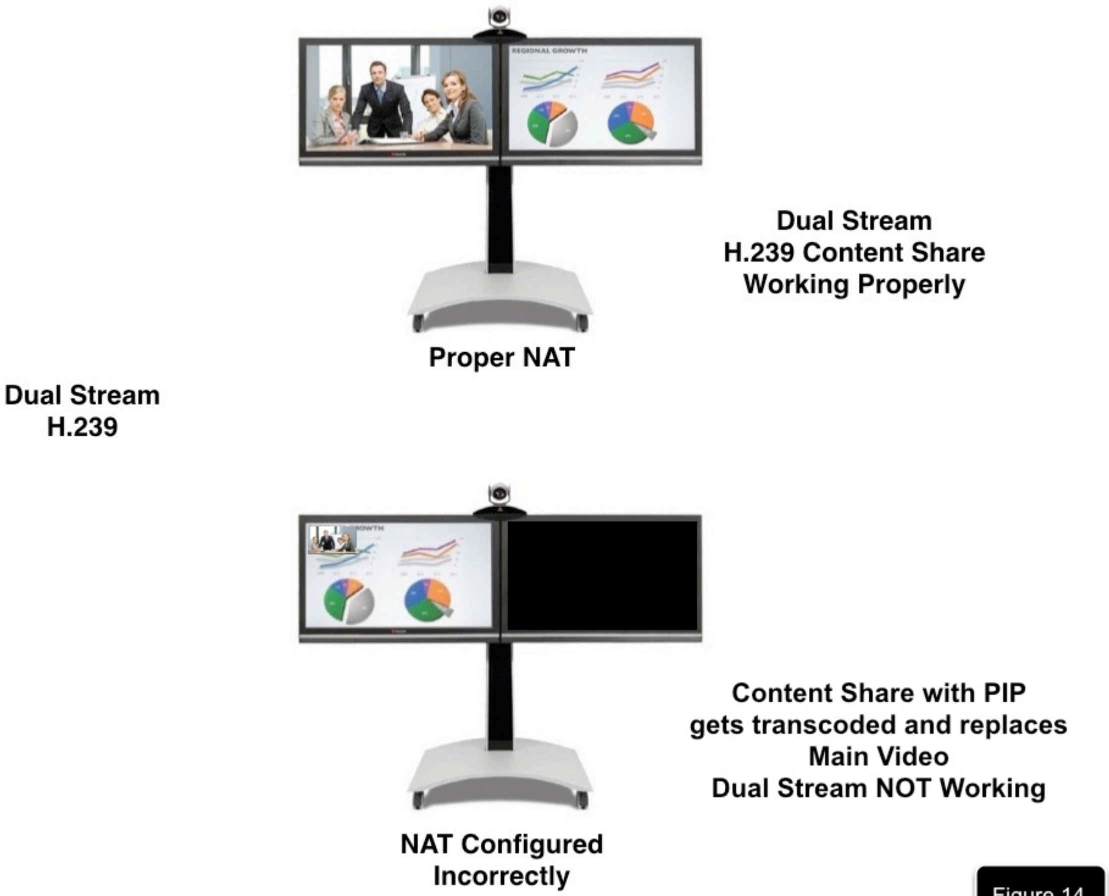


Figure 14

Content Sharing Replaces Main Video Stream - Figure 14

Symptom:

User tries to share content (H.239) from H.323 endpoint and the content is transcoded and replaces the main video camera feed instead of opening up a second window.

Likely Cause:

Because H.239 (duo stream content sharing) is usually blocked unless there is a NAT traversal device or properly configured NAT-aware mechanism in place. If the H.323 endpoint advertises its Private IP address to BlueJeans the H.239 content sharing will not be working in Dual Stream mode. The reason is the receiving endpoint will try to contact the sending endpoint at this private IP address and will be unable to communicate properly.

Dual stream video (H.239) can only operate correctly when the video conferencing endpoint is either NOT behind a NAT, NAT mechanism is properly configured or there is a NAT/FW traversal device in place to proxy both signal and media, such as VCS, VBP or other Session Border Controller.

Fix:

Always make sure H.239 content sharing is enabled on H.323 endpoint to establish dual stream/ separate Presentation channel. Please check the Admin guide of that specific model for the endpoint for this setting.

1. Implement NAT/FW traversal solution so that H.239 channel can be opened cross NAT/FW.

2. Put end point temporarily in DMZ with public ip without going through NAT/FW.

Check Firewall and NAT-aware mechanism. A one-to-one static NAT is required. You may try turning on H.323 inspection on H.323 aware firewall if no transversal device is being used.

Polycom Endpoints

When you dial into a BlueJeans meeting from a Polycom endpoint you may experience one of the following:

- No video received from BlueJeans
- Green artifacts across the screen
- Issues sending/receiving content via H.239
- This typically occurs when your Polycom endpoint has the option "Basic Mode" enabled, which uses the legacy codecs G.711 (audio) and H.261 (video).

To turn off this configuration, log into your Polycom web admin interface, and go to:

1. Admin Settings
2. Network
3. Call Settings, and
4. Uncheck "enable Basic Mode"

On HDX systems running firmware version 3.0.3 or higher this option is now called "Diagnostic Mode" and can be found in the following menu:

1. Admin Settings
2. Network
3. Call Preference, and
4. Uncheck "Diagnostic Mode"

NOTE: Some models like Polycom HDX and Group Series have a setting called "SIP keep alive messages, which can help to create pinhole on some Firewalls in order to allow separate content channel for media coming from BlueJeans .

- Check: Admin Settings > Network > IP Network > Firewall

You may need to reboot the endpoint for the new settings to take effect. Once you reconnect to the meeting your endpoint should begin using the G.722 (audio) and H.264 (video) codecs.

When placing a call/re-dialing, ensure that the Call Quality is set to 1024 or higher.

Endpoint Settings

In case of dual monitors, please check if in the Admin settings that the endpoint is correctly configured to show the Content and Main Video on separate monitors.

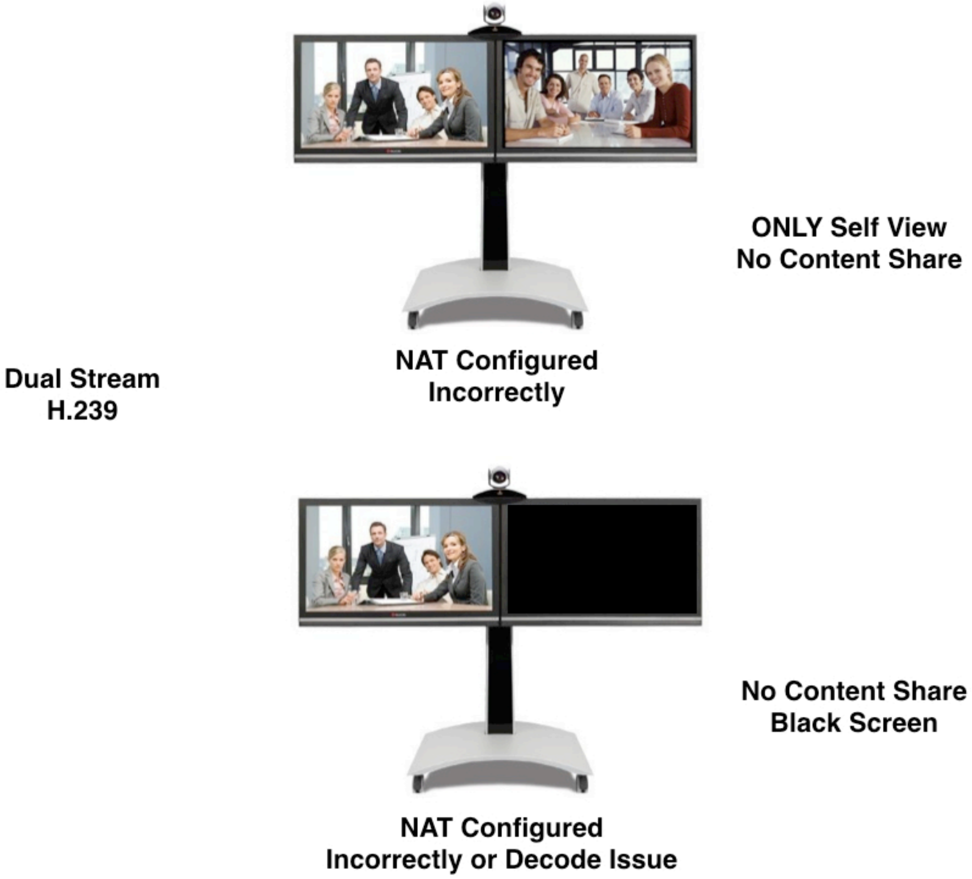


Figure 15

No Content Sharing - Figure 15

Symptom:

User tries to share content (H.239) and either nothing happens, you only see self-view or a black screen appears on receiving endpoint where the content should be displayed.

Likely Cause:

Receiving endpoint may be improperly configured for NAT or firewall is blocking content share. What may be happening is the receiving endpoint is advertising a private address and sending endpoint is sending shared content to this private address that cannot be reached. Possible decode issue if you see black screen where content should display.

Fix:

Always make sure H.239 content sharing is enabled on H.323 endpoint.

Check Firewall and NAT-aware mechanism. Turn on H.323 inspection on H.323 aware firewall if no transversal device is being used.

Some Firewalls H323 ALG setting limit the session to 2 (audio/video) which could prevent content from working properly. Check to re-configure Firewall.

NOTE: In some rare scenarios the firewall pinhole mechanism may block the content media. When a video call is initiated from the endpoint, the audio and video channels are established from internal private network to external public network (Internet) and so the return traffic from public to private network is trusted and pinholes are created to traverse it. However, the content is entirely new media traffic coming from Blue Jeans (public network) to the endpoint on private network, which may get blocked by firewall.

To verify this and use this workaround:

The content needs to be firstly initiated from the endpoint so that the firewall learns about this H.323 content traffic and then it allows the content coming from public in that same session.

- Check for any software updates for the firewall to fix this behavior
- Manually open the Transport TCP/ UDP ports on the firewall, instead of having the H.323 inspect or SIP ALG (Application Layer Gateway) controlling the port opening

Call Drops at the Same Interval or Time Frame on Each Call Attempt

Symptom:

Call connects but drops in the exact same amount of time. If all endpoints are dropping calls at exactly the same interval, please check firewall UDP time-out.

Likely Cause:

UDP Timeout setting on firewall is set too short. What may be happening is that the firewall is stopping the UDP Media traffic and causing the call to drop. Calls that drop at exactly 2 hours are a common issue with some Cisco Firewalls where the UDP Timeout is not configured properly for video conferencing.

There is also a 'keep-alive' sent by H.323 endpoint that can be discarded by firewalls. Keep-Alive settings can have a similar result in dropping calls. Some firewalls will close port 1720 if it does not see any traffic after an H.323 call has been established. This action generally will drop the call.

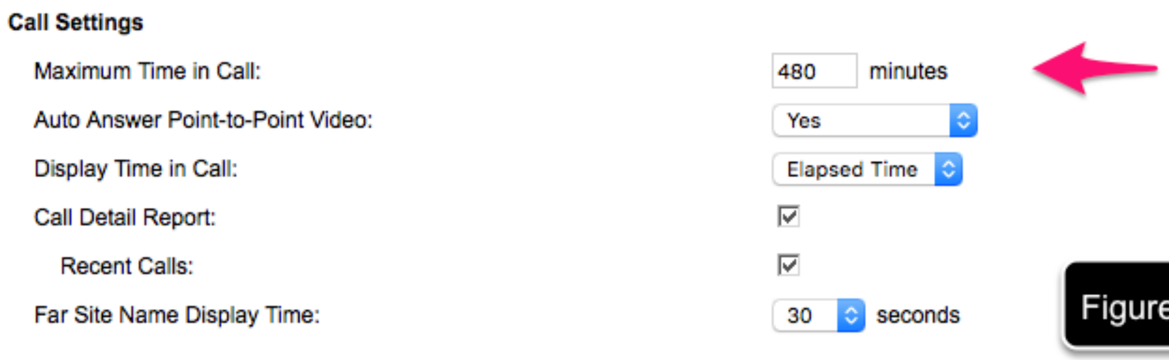
Check to see if the room system has "Maximum Time in Call"

Fix:

Adjust UDP Timeout on firewall to longer time. It is recommended to set the UDP time out to the maximum allowed time (3 or 4 hours on some firewalls). It is important to be aware of any UDP Timeout setting that may exist on firewall. This setting can end calls pre-maturely.

Adjust the 'keep-alive' interval on the H.323 endpoint. Investigate that the firewall is allowing the 'keep-alive' message to get thru.

Check the room system "Maximum Time in Call" time is configured.



Call Settings

Maximum Time in Call:	480 minutes
Auto Answer Point-to-Point Video:	Yes
Display Time in Call:	Elapsed Time
Call Detail Report:	☑
Recent Calls:	☑
Far Site Name Display Time:	30 seconds

Figure 16

Call Drops Quickly or Call Never Establishes

Symptom:

Call to Blue Jeans drops almost instantly or never connects at all.

Likely Cause:

Firewall is blocking outgoing call or H.323 endpoint is not connected to network. Typically occurs when TCP port 1720 for call setup is open, but the TCP and UDP port range 5000-5999 for flow control and media are being blocked by a firewall.

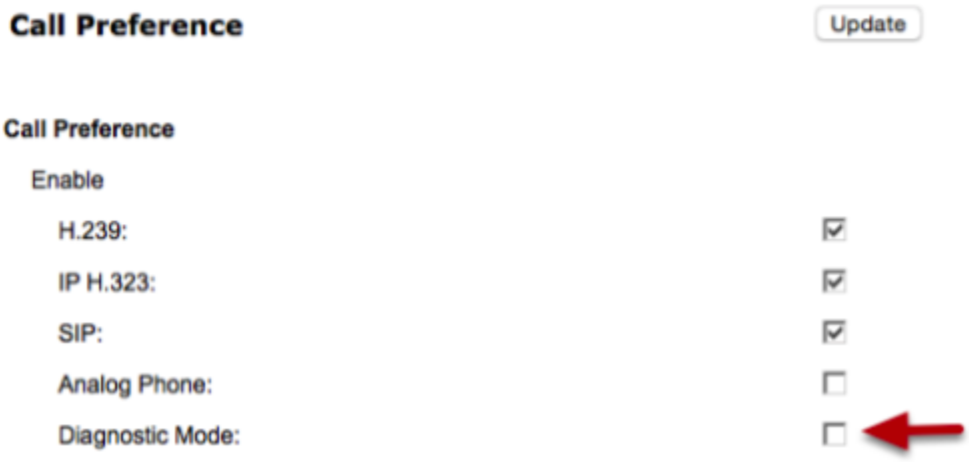
Possible NAT issue if call connects and drops within 30 seconds. Usually this is where the H.323 endpoint is advertising only its private IP address to Blue Jeans. The return media cannot reach the H.323 endpoint and after less than 30 seconds or so the call will be dropped as the endpoint does not receive any media. This is almost always due to NAT being improperly setup.

Fix:

Make sure H.323 endpoint is properly connected to network. Can you call any other endpoint?

Check firewall and NAT-aware mechanism. A one-to-one static NAT is required. Turn on H.323 inspection on H.323 aware firewall if no Transversal Device is not being used.

May need to monitor Firewall or perform a packet capture to see if the call dialed is leaving your network.



Call Preference

Call Preference

Enable

H.239: ☑

IP H.323: ☑

SIP: ☑

Analog Phone: □

Diagnostic Mode: □

Video or Audio is Poor Quality

Symptom:

Poor video or audio quality seen or heard on H.323 or SIP room system.

Video is flickering or pulsating.

Likely Causes:

This can be due to high packet loss. There could be a mismatch on the switch ports or bandwidth restriction that is causing the high packet loss. Firewall can be doing a deep packet inspection, or a filtering is occurring on local network (Websense, BlueCoat, etc.). Low bitrates can also cause lower quality video.

If your endpoint is behind a restrictive firewall, your connection to Blue Jeans service is likely over TCP relay. This restricts video bandwidth and tends to produce a lower quality call than one without relay. Allowing UDP packets through directly to Blue Jeans Network can improve the quality.

If video quality seems to be the issue make sure that the endpoint is using H.264 video codec (if it has this capability). Video endpoint using H.261 can suffer from a poorer quality.

If the video is flickering or pulsating this can be due to many FVU (Fast Video Updates) where the endpoint receives corrupted video packets it cannot properly decode so it requests a new Intra Frame (complete image) from Blue Jeans. This is usually caused by packet loss. Every time a new Intra Frame is received it generates this flickering or pulsating effect can be very distracting.

Fix:

1. Make sure the following network firewall configurations are in place to allow:

- Allow TCP 5000 - 5999
- Allow UDP 5000 – 5999

Ports should be open to the FULL Blue Jeans IP Ranges (see above).

NOTE: Some firewalls, such as Palo Alto Networks, prefer to filter network traffic based on the Fully Qualified Domain Name (FQDN). If this applies to your firewall configuration please use the following FQDN in order to connect to Blue Jeans: bjn.vc

2. Set speed/duplex settings to 100/full for the endpoint LAN (via the web interface) and the network switch port LAN. ("Auto negotiation" unfortunately does not often work as you would expect with video units. With the deployment of 1000/full switches being more common, many video units only do 100/full and leaving them to AUTO/AUTO results many times in speed/duplex mismatches)

3. If your local network bandwidth is capping at 1Mb, adjust the room system's call rate/speed to 768Kbps, or even 512Kbps. For HD resolution the user should be using a call speed at least 786 to about 1152kbps or more.

4. To see if the packet loss is happening on all video calls (not just with Blue Jeans), please make calls to test calls to another public endpoint such as Polycom's video test number page (IP address 140.242.250.205). If you see similar issues with packet loss ask your IT team to investigate possible packet loss causes within your local network. They might try running an MTR or Trace Route to see where the packet loss is occurring. If the packet loss is shown to be

out on Internet, you may have to open a support ticket with your Internet Service Provider (ISP). An excess of too many hops can also be a factor and should be discussed with your ISP.

5. If a filtering issue is suspected, check to make sure that an exception has been added to the "filtering" solution. Check to make sure that no deep packet inspection is enabled for video conferencing packets.

6. If low bitrate is suspected to be can causing a lower quality video we suggest you disable the Dynamic Bandwidth setting (Polycom) on the endpoint. Make sure if using a Polycom room system that Basic or Dynamic Mode is NOT enabled as this will cause your room system to use H.261 video codec and G.711 audio codec that may yield poorer quality than what is preferred.

7. Check to make sure that the video endpoint is using H.264 video codec. Polycom endpoints can be set to Basic or Diagnostic Mode (depending on software version) where it forces the use of H.261 video codec. Disabling this Basic or Diagnostic Mode will allow endpoint to use higher quality video codec like H.264.

Additional Information

Methods of Port Translation in NAT

There are four main ways that are commonly used for implementing network address and port translation.

1. Full-cone NAT (one-to-one NAT) is the only type of NAT where the port is permanently open and allows inbound connections from any external host. This type of NAT is also known as port forwarding and is the least restrictive type of NAT. The only requirement is that the connection comes in on a specific port (the one you opened). The port numbers do not have to be the same.

The internal private address and port is mapped to an external public address and port. Packets from internal IP address: port are sent through to external IP address: port.

Any external host can send packets to the external IP address: port and reach the endpoint on the internal IP address: port. The IP address is translated, but the port number is preserved.

2. Address-restricted-cone NAT works in the same way as a full-cone NAT but applies additional restrictions based on IP address. The internal client must first have sent packets to external IP address before it can receive packets from external endpoint. The only requirement is that packets come in on the mapped port and from an IP address that the internal client has sent packets to.

Once an internal address: port is mapped to an external address: port packets from internal address: port are sent through external address: port.

An external host can send packets to internal address: port by sending packets to external address: port ONLY if internal address: port has previously sent a packet to host at address: any-port. "Any" means the port number doesn't matter.

3. Port-restricted cone NAT

Similar to address-restricted-cone NAT, but the restriction also includes port numbers by only accepting connections from the IP address and port it sent the outbound request to.

Once an internal address: port is mapped to an external address: port packets from internal address: port are sent through external address: port.

An external host can send packets to internal address: port by sending packets to external address: port ONLY if internal address: port has previously sent a packet to host.

4. Symmetric NAT applies restrictions exactly the same way as a port-restricted cone NAT but handles the NAT translation quite differently. Other types of NAT do not change the source port when making connections. This is called port preservation. Symmetric NAT will randomly change the port numbers and this creates some unique challenges for video conferencing.

Each request from the same internal IP address and port to a specific destination IP address and port is mapped to a unique external source IP address and port; if the same internal host sends a packet even with the same source address and port but to a different destination, a different mapping is used. Only an external host that receives a packet from an internal host can send a packet back.

Full-cone NAT is the most permissive and Symmetric NAT is the most restrictive.

More on Configuring Firewalls

Configuring Firewalls

This is for example only. Depending on your firewall and network this may be different and should be used to help basic understanding only. Please contact your firewall vendor for the proper configuration needed for your specific firewall.

Sample Cisco ASA firewall for H323 conferencing (Depending on software version this may vary).

1. Create an IP Service Group - You can use any naming convention. Example: BlueJeans

- From the ASDM configuration tool, click on Configuration, Firewall, and then Access Rules
- Click on the Services tab from the menu which appears on the right, and then click Add and select Service Group
- Enter a Group Name, such as H323-Group. A description can be entered if desired, but not necessary
- Click the radial button Create new member. Create three new services, configure these services with the following parameters (making sure to click Add after creating service):

Service Type: TCP

Destination Port/Range: 1720 Source Port/Range: default

Service Type: TCP

Destination Port/Range: 5000-5999 Source Port/Range: default

Service Type: UDP

Destination Port/Range: 5000-5999 Source Port/Range: default

- Now click OK and the IP Service Group is created.

NOTE: Typically, ASA’s have a predefined service for TCP 1720, so you may see TCP h323 listed.

2. Create Network Objects - defining a host for both the internal private IP address as well as the external public IP address.

- From the ASDM configuration tool, click on Configuration, Firewall, and then Access Rules
- Click on the Addresses tab from the menu, then click Add and select Network Object

- Enter a name and description for your object (if no name is entered then the IP address will display). Two objects must be created for each system to allow endpoint to make and receive calls through the ASA, one reflecting the internal IP configuration, and one reflecting the external IP the system will be translated to. After entering this information, you should have completed Network Objects. Now move on to NAT Rules.

3. Define NAT Rules - Static NAT (need to create a one-to-one static NAT)

- From the ASDM configuration tool, click on Configuration, Firewall, and then Access Rules

- Add Static NAT Rule for the inside interface translated to the outside interface and click OK

4. Define Access Rules - theses rules are to allow inbound traffic thru the outside interface where Source: = any Destination: <BlueJeans Object>

- From the ASDM configuration tool, click on Configuration, Firewall, and then Access Rules

- Click Add, and then Add Access Rule

- Configure the Access Rule:

Example ONLY:

Interface: Inside

Action: Permit

Source: Any

Destination: Any

- Configure the Service and select the H323-Group configured and click OK. In order to create the Access Rule which will allow traffic to traverse the firewall from External to Internal, repeat the steps above, but ensure the Interface is set to Outside.

5. Confirm the ACL Manger

- From the ASDM configuration tool, click on Configuration, Firewall. Expand Advanced menu and then click ACL Manager. In most cases the ASA will automatically create the appropriate ACL entries. If your ACL Manager does not show the access rules for the H323-Group, right click the Inside Access.

- In ACL, Add ACE and ensure the following parameters are configured:

Example ONLY:

Action: Permit

Source: Any

Destination: Any

Service: H323-Group

- Once the ACE is configured click OK.
- Right click the Outside Access In ACL, and then Add ACE
- Configure the ACE

NOTE: With the later versions of Cisco ASA firewalls there are no fixup protocols to configure; however, common issues noted with many Cisco ASA models relate to their use of fixup protocols. It is important to ensure that you disable the following if they are enabled on your ASA. Fixup Protocol H323, Fixup Protocol H323, RAS Fixup Protocol H323 H225

NAT support for SIP may be enabled by default on port 5060. If this feature has been disabled, perform this task to re-enable NAT support for SIP. To disable the NAT support for SIP, use the no ip nat service sip command. Please investigate your firewall admin guide for more information.

Access List for Example ONLY:

```
access-list outside_access_in line 1 extended permit ip any any

access-list outside_access_in line 2 extended permit tcp any any eq www

access-list outside_access_in line 3 extended permit tcp any any eq https

access-list outside_access_in line 4 extended permit tcp any host 199.xx.xx.xx range 5000 5999

access-list outside_access_in line 4 extended permit udp any host 199.xx.xx.xx range 5000 5999

access-list outside_access_in line 4 extended permit tcp any host 199.xx.xx.xx eq 1720

access-list outside_access_in line 4 extended permit tcp any host 199.xx.xx.xx eq h323
```

You need to create an access list for all of the Blue Jeans IP ranges.

Note: When a Cisco VCS Expressway is deployed, Cisco recommends that any SIP or H.323 ‘fixup’ ALG (application-level gateway) or awareness functionality be disabled on the NAT firewall. If enabled this could adversely interfere with the VCS functionality. Several room system vendors also recommend to not use ALG as it can potentially cause intermittent issues with audio. It is not recommended to use ALG for video conferencing.

Application Firewalls

An application level firewall can control access to and from a specific application or service. It is built to control all network traffic on any OSI layer up to the application layer. These application firewalls monitor all input/output and service calls for a particular application. They are configured by choosing the application and setting what that application is allowed to do in simple terms.