



go green with

21st Century Video

...become environmentally friendly
use green solutions

IP Ports and Protocols used by H.323 Devices

Overview:

The purpose of this paper is to explain in greater detail the IP Ports and Protocols used by H.323 devices during Video Conferences. This is essential information if there are endpoints that are protected by a Firewall. It lists the Port and the Protocol used for various H.323 functions along with the H.323 devices that may use this Port. This paper also mentions using Virtual Private Networks (VPN) and Encryption as well as Firewall/NAT Traversal.

It is assumed that the reader has a general knowledge of Video Conferencing systems and the standards involved. However, the following technical papers are available to provide more information on these topics:

- ***How do I choose a Video Conferencing system?***
- ***Video Conferencing Standards and Terminology.***
- ***H.323 Terminals, Gatekeepers, Gateways & MCUs.***
- ***Global Dialling Scheme (GDS) for Schools Video Conferencing.***
- ***H.323 Dial Plan and Service Codes used by Gatekeepers etc.***
- ***Cost Efficient ISDN Conferencing, including Multipoint Access.***
- ***H.221 Framing used in ISDN Conferences.***

Firewall and Proxy Server:

A firewall is a set of security mechanisms that an organisation implements to prevent unsecured access from the outside world to its internal network. An organisation with its own internal network (intranet) whose users also requires access to the Internet, usually installs a firewall to prevent unauthorised Internet users from accessing its internal network. Firewalls usually work by blocking access of certain network protocols to specific ports. The firewall can also control what Internet resources the organisations users may access. The firewall is generally installed at a specific location in much a manner that no incoming requests can by-pass it and gain access to the internal network.

A Proxy Server acts as an intermediary server that makes network requests on behalf of internal users, so that organisations can ensure security, control and caching services. Proxy Servers are now equipping themselves with security features such as Network Address Translation (NAT). The NAT or Proxy Server works on the concept that there is an outside world (Internet) and an inside world (intranet) and it separates and protects the intranet from the Internet.

Firewalls now usually include a NAT capability. Certainly, most ADSL Routers have a built-in Firewall and NAT functionality that can be setup to work with H.323 videoconferencing systems.

Network Address Translation (NAT):

NAT helps protect the intranet from exposure to unwanted traffic by providing one single external address to remote users. NAT uses a system of local and external addresses to hide an intranet user from other networks. NAT translates the local intranet users address to an external address, which is then used to identify the local user to remote users. Therefore, remote users use this external address to call the local user, without knowing its actual local address. The latest releases of most vendors software including **Sony, Polycom** and **Emblaze-VCON** all support NAT and allow you to specify the external IP address of the selected endpoint.

IP Ports and Protocols used by H.323 Devices						
Port	Type	Description	H.323 Client	Microsoft ILS	H.323 MCU	H.323 Gatekeeper
80	Static TCP	HTTP Interface (optional)			x	
389	Static TCP	ILS v2.0 Registration (LDAP)	x	x		
1002	Static TCP	Win 2000 ILS Registration	x	x		
1503	Static TCP	T.120	x	x		
1718	Static TCP	Gatekeeper Discovery	x		x	x
1719	Static TCP	Gatekeeper RAS	x		x	x
1720	Static TCP	H.323 Call Setup	x		x	
1731	Static TCP	Audio Call Control	x		x	
2253 - 2263	TCP	Sony endpoints	x			
3230 - 3253	TCP & UDP	Polycom endpoints	x			
5001	TCP & UDP	Polycom PPCIP client	x			
5004 - 6004	TCP & UDP	Emblaze-VCON endpoints	x			
8080	Static TCP	HTTP Server Push (optional)			x	
22136	Static TCP	MXM endpoint administration	x			x (MXM)
26505	Static TCP	MXM remote admin login				x (MXM)
49152-49239	UDP	Sony endpoints	x			
1024 - 65535	Dynamic TCP	H.245 (Call Parameters)	x		x	
1024 - 65535	Dynamic UDP	RTP (Video Stream Data)	x		x	
1024 - 65535	Dynamic UDP	RTP (Audio Stream Data)	x		x	
1024 - 65535	Dynamic UDP	RTCP (Control Information)	x		x	

General H.323 issues and Protocols:

The table above shows that the H.323 protocol requires the use of specific static ports as well as a number of dynamic ports within the range 1024-65535. For the H.323 protocol to cross a firewall, the specific static ports and all ports within the dynamic range must be opened for all traffic. This clearly causes a security issue that could render a firewall ineffective.

There are several standards based transport protocols used within H.323 Conferencing. Generally, each configures the data into packets, with each packet having a 'header' that identifies its contents. The protocol used is usually determined by the need to have reliable or unreliable communications. Transmission Control Protocol (TCP) is a reliable protocol designed for transmitting alphanumeric data; it can stop and correct itself when data is lost. This protocol is used to guarantee sequenced, error-free transmission, but its very nature can cause delays and reduced throughput. This can be annoying, especially with audio. User Datagram Protocol (UDP) within the IP stack, is by contrast, an unreliable protocol in which data is lost in preference to maintaining the flow. Real-Time Protocol (RTP) was developed to handle streaming audio and video and uses IP Multicast. RTP is a derivative of UDP in which a time-stamp and sequence number is added to the packet header. This extra information allows the receiving client to re-order out of sequence packets, discard duplicates and synchronise audio and video after an initial buffering period. Real-Time Control Protocol (RTCP) is used to control RTP.

Reliable transport is required for control signals and data because they must be received in the proper order and cannot be lost. Consequently, TCP is used with the H.245 control channel and Call control. Unreliable UDP is used for audio and video streams where time sensitive issues become a priority.

H.323 and Intelligent Firewalls:

Q.931 is the Call Signalling protocol used in setting-up and terminating a call. H.323 uses TCP on port 1720 for Q.931 and negotiates which

dynamic port range to use between the endpoints for H.245 Call Parameters, data, audio and video. Clearly, to open all ports within the dynamic range would cause security issues, so the firewall must be able to allow H.323 related traffic through on an intelligent basis. Some special H.323 intelligent firewall can do this by *snooping* on the control channel to determine which dynamic ports are being used and then only allowing these ports to pass traffic when the control channel is busy. However, most firewalls that state they support H.323 just open port 1720 and you have to make additional rules to open the endpoints specific TCP and UDP port ranges.

The latest releases of **Sony**, **Polycom** and **Emblaze-VCON** endpoint software all allow you to specify the dynamic port ranges to be used by TCP and UDP. This allows you to reduce the number of ports that need to be open, and hence the security risk. Furthermore, these latest versions support 'Port Pinholing', so that inbound data can be returned using the same port as the initiating outbound call.

Using NAT to Enhance Security:

When H.323 terminals communicate directly with each other, they must have direct access to each others IP address. This exposes key network information to a potential attacker. By using NAT, only limited number of addresses are exposed, keeping the majority of address information hidden.

Conferencing successfully through a firewall depends upon how well the firewall is capable of dealing with the complexities of the H.323 protocol. If the firewall cannot provide dynamic access control based on looking at the control channel status, then NAT inside the firewall can be used to provide access control. Since only the Gatekeeper, via RAS on port 1719 and NAT via Call Setup on port 1720 are the only systems that interact with H.323 device outside the firewall, access rules in the firewall can be set to pass traffic destined for the Gatekeeper or NAT'ed endpoint.

When you specify that an endpoint should use NAT, it embeds the outside world IP address of the firewall into it's IP header. This is how the far end system knows the outside world IP address to return the call. The endpoint cannot use it's internal IP address as this is non-routable and you want it hidden. On receiving inbound traffic, the firewall uses NAT to forward to the traffic to the endpoint.

Using VPN or Encryption:

Creating a Virtual Private Network (VPN) by definition provides you with your own private network, so as long as you stay within this network, you do not need any firewalls. However, this is not always possible and you may have a necessity to conference with others outside your own VPN. This can cause a problem as using NAT is typically incompatible with routers setup for a VPN. The solution is to use a Firewall/NAT Traversal device.

When configuring the VPN, be wary of using a long key and hence applying too much encryption as this can cause an unacceptable delay in the transmission between sites and impact the overall efficiency of the video conference. Similarly, enabling H.235 compliant AES Encryption that is supported by most endpoints can have an impact on the overall efficiency of the conference, especially if low bandwidths are used.

H.460 Firewall/NAT Traversal:

As mentioned above, when H.323 endpoints are set to use NAT, the outside world IP address of the firewall is embedded in their IP header. This is done so that the far end system know where to return the call. This is part of complying to the H.323 protocol. However, this typically causes a problem when you then want to call an H.323 endpoint over a VPN.

To call an H.323 endpoint over a VPN, you call it's IP address, which is usually on a different internal network segment. With NAT enabled, the H.323 endpoint has the external IP address of the firewall in it's IP header. When you make a call over the VPN, this external address is still in the IP header, so the far end system on the VPN will try to return the call to the external address via the outside world and not over the VPN. The call will fail, typically with no audio and video. It will work to endpoints on the same internal network segment, but not to endpoints on different segments. Disabling NAT on the endpoint will allow calls over the VPN, but then you cannot call outside world endpoints!

The solution is provided by implementing H.460 Firewall/NAT Traversal. **Emblaze-VCON's NetPoint** or **Radvision's PathFinder** are H.460 devices that work in-conjunction with H.460 enabled endpoints. Most vendors have implemented H.460 support into their latest software revisions. Alternatively, the Sony **PCS-XG80** has two network interfaces, one that supports NAT for connecting to the outside world and the other that doesn't for connecting internally.

Subject to change without notice; no liability accepted for use. Company or product names mentioned are trademarks of their respective owners.
©2006-2010 21st Century Video Ltd. Registered in England No. 4121866. UK VAT Registration No. GB 890 1684 06. Updated: 18 December 2009.