Published on *Jisc community* (https://community-stg.jisc.ac.uk)

NAT, Firewalls and videoconferencing - H.323 Border Traversals

Please note that the diagrams couldn't be ported across from the .PDF document

NAT, Firewalls and Videoconferencing
H.323 Videoconferencing across Network Address Translation (NAT), Firewalls and Network Borders – A Description of the Problems and Solutions Author: Geoff Constable, Welsh Video Network Version 1.0 - Release Acknowledgement: With grateful thanks to Matthew Collins, Welsh Video Network, for the network diagrams in this report, and to Deirdre Magoris (Welsh Video Network) and Glen Sykes (Direct Visual) for their corrections and suggestions (grammatical and technical respectively).

Contents

1. Introduction
The deployment of H.323 (IP) videoconferencing has grown rapidly throughout the commercial, education and public sectors in the United Kingdom and around the world during the last five years. Decreases in bandwidth costs and more reliable and robust networks have contributed to this, as have the continuing improvements in the quality of the products available. This has been accompanied by a growth in demand, as cost and environmental considerations have combined with a growing appreciation of how videoconferencing can be used to enhance organisational partnerships and distance learning. However, this rapid growth in deployment has been made more difficult, and in some cases been held back, by difficulties inherent in the H.323 protocol itself, and this can cause problems for those concerned with organisational security and network administration. This report attempts to introduce the network difficulties that have been encountered in the deployment of H.323 videoconferencing. The issues are outlined here and references to more detailed technical explanations are supplied. Some of the methods used to overcome these difficulties are also

examined. Increasingly sophisticated methods have been developed to overcome the security issues encountered in deploying H.323, and those who have to plan, budget for and implement H.323 networks are faced with a bewildering array of jargon, firewalls, proxies, 'border devices' and security measures and appliances. This report aims to explain and clarify these concepts. A general appreciation of the purpose and location of a firewall is assumed. The JANET Video Technology Advisory Service (VTAS) intends to produce a series of guides which will examine different solutions that have been used in 'real-world' situations to overcome the security and network challenges inherent in making H.323 videoconferencing available across organisational borders. These will concentrate on organisations that are using the JANET Videoconferencing Service (JVCS) and will include deployment guides to major manufacturers' equipment. This document does not consider or evaluate the nature or scale of the security threat introduced by H.323 deployment. For a discussion of such issues please refer to the VTAS document “Security Guide for H.323 Videoconferencing”.

2. The H.323 Protocol

The H.323 protocol is the common name for the International Telecommunications Union (ITU) Recommendation that defines packet-based multimedia communications systems. The most commonly deployed packet-based networks are, of course, those based on the TCP/IP suite of communications, which inter-connect to form the Internet. The H.323 recommendation is a widely adopted umbrella protocol that defines standard behaviour for setting up and proceeding with audio and video calls. It is known as an umbrella protocol because it depends on, and references, other protocols for call signalling, media transport and media encoding. Full details of the protocol can be found in the Recommendation itself, which is available from the ITU, and in the VTAS document “An Introduction to H.323 Videoconferencing”.

The H.323 protocol works very well where it is used within the same organisational IP network. However, problems are likely to occur when an organisation wishes to make H.323 calls to other organisations. This will usually mean traversing firewalls and NAT boundaries. The issues that have to be solved in order for H.323 to work across NAT boundaries and/or firewalls can be summarised as „network border traversal problems?. Before considering these problems, and possible solutions, it is worth examining how the H.323 protocol works in more detail.

Whether the call is mediated by a gatekeeper or not, the communication between the endpoints uses ITU Recommendation H.225.0 for call signalling. The call setup procedure can be paraphrased as shown in Table 1:

Endpoint	Protocol	Message	Port
A	H.225.0	Can we set up a call?	1720
B	H.225.0	OK, call proceeding	1720
B	H.225.0	Alerting user (ringing)	

1720
A
H.225.0
What port shall we use for the next bit?
1720
B
H.225.0
Let's do H.245 on these ports
1720
A
H.245
I can do this and that (these are the speeds/encodings/decodings/etc I am capable of)...
Ports as defined in last step: between 1024 - 65535
B
H.245
I can do this, and that...
As above
A
H.245
Shall we use this encoding, that speed etc? On these ports?
As above
B
H.245
Yes, OK
As above
A
H.245
Right, let's go...
As above
A + B
RTP
Media content – two ports (content and control) in each direction, per media
A group of up to six contiguous ports, defined in the last step: between 1024 - 65535

Table 1: Paraphrase of an H.323 call setup conversation

The acceptable play-out of real-time media is dependent on the media data being delivered in a timely manner. There is no point in resending media packets as they are continuously being decoded and passed to the application for display at the other end. By the time the re-sent snippet arrived it would be too late for inclusion in this rolling process. TCP/IP has built-in checks to ensure that data packets are delivered. In the face of a congested network, TCP will control the transmission of packets by 'backing-off' and actually slowing transmission rates. TCP will also check on packet delivery and ask for the re-transmission of any packets that have not arrived at their destination. This is obviously unsuitable for videoconferencing and telephony applications, and for this reason (amongst others) TCP and IP datagrams are not used for media transmission; instead they use the User Datagram Protocol (UDP), which does not have the control element of TCP. This means that media does not get delayed but is churned out by the transmitter regardless of what is happening on the network from moment to moment. UDP does lack some of the functionality required for a real-time exchange, and so there is another protocol layer between the UDP packet and the actual data payload of encoded media. This layer is provided by the Real Time Protocol (RTP) which provides features like time stamping. The Real Time Control Protocol (RTCP) allows participating endpoints in a call to report back on QoS (Quality of Service) parameters. This creates the potential for the endpoint to make adjustments to the encoding and transmission during the call in order to improve QoS.

3. Firewalls and ports

A simple firewall uses rules based on virtual 'ports' and IP addresses to filter traffic. Most Internet applications and services have well known ports on which machines 'listen' for communications (as standardised by the Internet Assigned Numbers Authority (IANA)). Firewalls will generally be configured to block anything by default but then allow traffic to flow through certain ports, either to and from any IP address or to a subset of IP addresses. Most communication through a firewall is initiated from within the network (a browser contacts a web site for example), and so a firewall can leave well-known ports open outbound, and learn from outgoing messages what to expect back from where. Very often all ports inbound will be closed by default but be left open for the duration of an exchange between machines that has been initiated from within the network. Once the exchange has finished, the firewall will close the port inbound again. The firewall can thus maintain a table of the traffic flow and the 'conversations' that are passing through it at any time. The H.323 protocol uses well known ports to set up videoconference calls but, as illustrated in the previous section, H.323 dynamically (i.e. on a per call basis) selects ports from a large number of possible port numbers. Whereas initial communication may take place on a well known port, much of the conversation that ensues takes place on dynamically selected ports chosen by the endpoints involved as they complete their call setup dialogue and media exchange. Calls may also be started from within or from outside the network, and so a typical firewall is going to block any attempts by anyone on a remote network to call inbound.

The ports used by H.323 protocols are listed in Table 2. Dynamic ports are those that are assigned in an ad hoc and temporary way; static ports are those which are pre-determined, standardised and permanent.

Early applications of H.323, such as Microsoft® NetMeeting® (Version 3.xx), gave advice on firewall configuration. This advice was to leave all the ports specified in Table 1 open at all times in both directions.

Port No.	Protocol Type	Purpose
1503	Static TCP	T.120 (Data)
1718	Static TCP	Gatekeeper discovery
1719	Static TCP	Gatekeeper RAS
1720	Static TCP	H.323 call setup
1731	Static TCP	

Audio Call Control
1024 - 65535
Dynamic TCP
H245
1024 - 65535
Dynamic UDP
RTP (Video Data)
1024 - 65535
Dynamic UDP
RTP (Audio Data)
1024 - 65535
Dynamic UDP
RTCP (Control Information)
Table 2: H.323 protocols port usage As described above, firewalls can be set up to leave certain well known ports open, but in order to cater for every eventuality in an H.323 call it would be necessary to leave 64,000 ports open (1024 - 65,535) – an unacceptably high number for most firewall administrators and one that virtually negates the point of having a firewall in the first place. So, H.323 calls are set up in a way that makes life difficult for firewalls – the call setup starts on well-known ports, but as the call setup is in progress, the two endpoints agree on a subset of the 64,000 ports available in order to exchange further setup information and/or for the transmission of media and media control messages. The precise subset of ports selected is random and unpredictable. Also, media is exchanged inbound on different ports to those used outbound and it is not possible to say from which end the first media packet will arrive. The prospect of opening 64,000 inbound ports provisionally, in case they are selected during an H.323 call setup, will almost certainly transgress an organisation?s firewall policy, so this is not a realistic solution. The problem is exacerbated by the fact that H.323 uses UDP (as explained above). This is a 'connectionless' protocol, which does not have the TCP control messages used in the more common IP: this makes it harder for the firewall to track 'conversations' between machines.

4. Network Address Translation (NAT)

NAT should be familiar to network managers – it is widely deployed in large private networks. NAT is described fully in RFC1918 “Address Allocation for Private Internets”. NAT was introduced partly as a means of conserving real or public (also sometimes called 'routable') IP addresses. The deployment of NAT allows large organisations to give every computer a unique Internet address without diminishing the available pool of public IP addresses. It does this by defining a set of addresses that should not be used on the public Internet and should only be used within the private network. Thus these addresses are 'unroutable'. Using NAT in a network also has the potential to add a layer of security – if the addresses within an organisation are not routable from the Internet it may be harder to 'attack' them. By definition, there must be some kind of translation machine between the inner and outer network. Whether this actually helps security is open to debate, but the practice of deploying NAT'd private networks has certainly helped conserve Internet addresses.

NAT is usually overcome by deploying a NAT server at the network boundary, which maintains mappings between private (NAT) addresses and public IP addresses. These mappings may be static (i.e. permanent) or dynamic (i.e. ad hoc and temporary). The problem that NAT presents to a deployment of H.323 is due to the fact that both H.225 messages and H.245 call setup messages bury their network (IP) address deep in the data payload of the IP packet. This payload is examined by the equipment at the other end and the source address within is used as the return address. If the return address is one that is behind a NAT boundary then the packet will never reach its destination, as NAT addresses are unroutable in the public Internet and the call will eventually time-out and fail. A 'naïve' NAT server will only change the addresses in the UDP or IP datagram header and footer, and not alter anything deeper in the protocol stack or in the data payload itself. This explains why H.323 works perfectly well when the two endpoints are within the same network, even when that network is using private (NAT) addresses. As long as the two endpoints have a route to each other then the call will succeed, as the packets exchanged never go beyond their particular NAT domain and so no translation is effected on the IP addresses used.

5. Solutions

The firewall and NAT problems described above have inhibited the uptake of H.323 videoconferencing and this has hampered the market growth of the associated industry. It is not surprising, then, to find that the industry has addressed the problems posed by NAT boundary traversal and firewall traversal (hereafter referred to jointly as 'border traversal') in a number of ways and there are now a number of proprietary and standards-based solutions to these problems available. These are described below, and have been loosely grouped as 'network solutions' (those involving a centralised approach with some kind of intervention at the network border) and 'endpoint solutions' (those that involve intervention from the endpoint itself). Some solutions involve interaction between these two elements and may be called hybrid solutions. Many of the solutions described below have not yet been fully tested by VTAS and so some of what follows is based on limited experience. Where a product has been tested by VTAS, or has featured in a Case Study, the item is in italics below and appropriate references appear in the References section.

Network solutions

Co-edged proxy/router

This method is also referred to as an IP/IP gateway as it provides an alternate gateway between the Local Area Network (LAN) and the adjacent network Point of Presence (PoP). This solution involves locating a gateway device at the edge of the network. In fact this device will straddle the two networks in the same way as the firewall. Using routing rules within the network, H.323 packets are routed to a device that is located alongside, but independent of, the firewall (see Figure 1, above). The device has two or more network addresses, and routes to both the outer and the inner network. It monitors H.323 setup conversations between endpoints and replaces all internal network addresses with its own address. It then maintains a table of current calls and routes incoming packets accordingly. By deploying such a device, the firewall is circumvented completely and there is no need to make any changes to firewall configuration. The H.323 proxy also handles the problem of NAT as the concept works in exactly the same way, whether the internal network uses public or private addresses – either way, they are hidden from the external network, as only the proxy's external address is ever forwarded. Examples of products of this kind include the now discontinued Cisco® Multimedia Communications Manager, the Cisco® Unified Border Element, the Codian® IP Gateway, the Polycom® Video Border Proxy and the gnu-gk gatekeeper/proxy.

Figure 1: Co-edged proxy/router

H.323-aware firewall

It is possible to give a firewall (that is often also performing NAT) an awareness of the H.323 protocol, so that it can manage a table of calls and either track the setup exchanges so that it 'learns' the ports to be used by the endpoints concerned. Then it can open them accordingly; and/or it singles out H.323 exchanges and over-writes unroutable IP addresses in outbound packets with a static NAT routable address as the source and re-addresses inbound packets so they reach their destination.

Firewalls that perform these kind of functions are said to be 'H.323 aware' – in short, they have some extra functionality that makes them able to allow H.323 calls to be set up and completed without adding any undue latency to the call. These are often referred to as 'H.323 fix-ups 'or 'VoIP fix-ups'. For H.323, network latency is a crucial element of the overall QoS, and is an issue here because the protocol inspection required by H.323 aware firewalls can be computing intensive and thus has the potential to add to the round-trip time for the media being exchanged between the two endpoints. Firewall manufacturers have had varying degrees of success with producing H.323 aware firewalls, and the H.323 elements are sometimes sold as an additional add-on to the basic product, so this approach has failed to solve the problem to the satisfaction of many network managers. During its development – H.323 has been through six versions since 1996 – each new version of the protocol may mean that the H.323 firewall module needs updating, so it can be difficult to match the correct module to the current H.323 version: as a result, firewall manufacturers have had to play catch-up to a certain extent. Examples of firewalls whose documentation states that they have some H.323-awareness include the Firewall Checkpoint NGX®, Cisco® PIX®, Fortinet® Fortigate® and Borderware®.

Figure 2: H.323-aware firewall

Border Negotiation Devices

Also known as traversal servers, these devices are situated in the external network and provide a means for endpoints to traverse the firewall and/or NAT boundary without the need for unacceptable alterations to the firewall. Where the endpoint also supports H.460.18, there is no need for a server element within the network, but, as the recommendations were not published until September 2005, many endpoints do not support these recommendations. Where it is necessary to support such legacy endpoints, the external border device works with an internal proxy-server device, which can incorporate an H.323 gatekeeper in the same physical unit.

While the traversal server is placed outside the protected network, the proxy-server/gatekeeper is placed within the network and a tunnel through the firewall is built between the two elements. The internal devices are placed in serial with the firewall so that all packets that are passed through them also pass through the firewall, thence to the traversal server and then on into the external network. A typical topology is illustrated in Figure 3, below.

Figure 3: Border negotiation devices

Figure 3 includes H.460 endpoints and non-H.460 endpoints. All may connect directly to the gatekeeper on the internal network, or those that support the recommendation can register directly with a traversal device (which may also include a gatekeeper). The firewall manager only has to open four well known ports and, crucially, these are outbound only, but this still allows the endpoint to be called from an external endpoint. Examples of Border Traversal Devices of this kind include the Tandberg Border Controller, Aethra PF, Visual-Nexus Secure Transport server and the Emblaze-VCON Firewall Traversal Advances Encryption Server. It should be noted that some implementations support only a proprietary mechanism to traverse the network boundary, whilst others offer both a proprietary and a standards-based option for border traversal.

De-Militarised Zone (DMZ) deployment

The DMZ is a concept well-known to the network administrator. It is a subnet between the internal and external networks, usually with public addresses, where hosts on the internal network can initiate contact with servers or other machines within the DMZ but not vice-versa. Machines on the Internet or external network can contact those in an organisation's DMZ but, from there, can find no route to the internal, protected network. This is often the location of (outwardly accessible) web or e-mail servers, for example. Placing H.323

equipment within the DMZ will not protect the H.323 endpoints themselves but will protect the rest of the local network from the security issues raised by H.323 deployment. In practice this is not always a practical option, as it may involve dedicated cabling etc. to the location of the H.323 equipment. This arrangement may be attractive to smaller, outreach locations. See Figure 4, below, for an example DMZ deployment.
Figure 4: DMZ deployment
It is also possible to deploy a variation of this topology where H.323 devices and endpoints are located physically together in the communications or server room, and audio-visual cables are used to carry sound and video to studios and back. One Canadian university, for example, has put all its H.323 terminals in a central rack, whose network is in a DMZ directly connected to the firewall. From the central rack, audio and video are transported over cabling to the locations of the cameras and microphones etc., as illustrated in Figure 5, below.

Figure 5: DMZ central deployment with audio-visual cables to studios
Endpoint Solutions
Because NAT and firewall traversal have proven such a headache in the past for H.323 deployment, manufacturers have also tried to make life easier by adding some border awareness to the endpoint itself. If static NAT is implemented, and therefore there is a reserved public IP address that is always mapped to a particular internal private address, then it is possible to add the external, public address as a configuration parameter to the endpoint. The endpoint then uses the external address within its data payload, and the return packets from the remote end are addressed correctly and find their way back to the local endpoint. This feature has had limited testing within VTAS as yet. As described above, it is usual during H.323 call setup for the two endpoints involved in the call to allocate ports for further dialogue and media transport dynamically from a potential pool of thousands. This behaviour will usually be blocked by a secure firewall and the call will fail. Some endpoints offer a configuration parameter whereby it is possible to pre-determine the ports that will be used for media transport for every call made from that endpoint. If the same port range is used by all endpoints in a particular local network then the firewall manager only needs to open these ports. In a sense this forces the endpoints to use 'well known ports'.

Theoretically, by using both these elements it is possible to use endpoint management to reduce the security risks normally associated with H.323 deployment to an acceptable level, depending on an organisation?s security policy. However, this method does not allow for legacy equipment that does not offer this functionality.

6. Conclusion

The H.323 protocol was designed as a flexible and accessible standard. It has been very successful in the videoconferencing arena and is easily the most widely deployed standards-based videoconferencing protocol. However, dynamically negotiated transport details, and the burying of transport addresses lower in the protocol stack, have led to difficulties in passing securely from one network to another, particularly where there is NAT at the network boundary. The industry has addressed these problems and there is a now a range of methods and products available that allow traversal of NAT and firewall boundaries in a secure and timely manner. Some of these solutions will be tested in further VTAS documents.

7. References

An Introduction to H.323 Videoconferencing, June 2002, D. E. Price and A.J. Spence, http://www.video.ja.net/documents/services/video/vtas/323intro.pdf [1]

Security Guide for H.323 Videoconferencing, Jan 2004, Tim Chown and Ben Juby, http://www.ja.net/documents/services/video/vtas/323security.pdf [2]

Request For Comments: 1918 “Address Allocation For Private Internets” Feb 1996, Y. Rekhter, B. Moskowitz, D. Karrenberg, G.J. de Groot, and E. Lear http://www.rfc-archive.org/getrfc.php?rfc=1918 [3]

H.323 and Firewalls: Problem Statement and Solution Framework, Feb 2000, Melinda Shore (Expired Internet Draft) http://old.iptel.org/info/players/ietf/firewall/draft-shore-h323-firewal... [4]

Packet-based Multimedia Communications Systems Telecommunication Standardization Sector of the International Telecommunications Union, Recommendation H.323, June 2006. http://www.itu.int/rec/T-REC-H.323/e [5]

A Case Study of Changes Made to a Nokia/Checkpoint Firewall-protected H.323 Gatekeeper/Proxy Topology, March 2007, G. Constable and T. Fullard http://www.ja.net/documents/services/video/vtas/wrexham.pdf [6]

Configuring an H.323 gatekeeper for use with the JANET Videoconferencing Service, Dec 2004, G. Constable http://www.ja.net/documents/services/video/vtas/gkconfig.pdf [7]

Glossary of Terms

CODEC
COder DECoder
DMZ
De-Militarised Zone
IANA
Internet Assigned Numbers Authority
IP
Internet Protocol
ITU
International Telecommunications Union
JVCS
JANET Videoconferencing Service
LAN
Local Area Network
NAT
Network Address Translation
PoP
Point of Presence
QoS
Quality of Service
RFC
Request For Comments
RTCP
Real Time Control Protocol
RTP
Real Time Protocol

TCP
Transport Control Protocol
UDP
User Datagram Protocol
UK
United Kingdom
VTAS
Video Technology Advisory Service

JANET(UK) manages the operation and development of JANET, the United Kingdom?s education and research network, on behalf of the combined UK Higher and Further Education Funding Councils represented by JISC (Joint Information Systems Committee). For further information please contact:
JANET Service Desk JANET(UK) Tel: 0300 300 2212 Lumen House, Fax: 0300 300 2213 Harwell Science and Innovation Campus E-mail: service@ja.net [8] Didcot, Oxfordshire, OX11 0QS Copyright: This document is copyright The JNT Association trading as JANET(UK). Parts of it, as appropriate, may be freely copied and incorporated unaltered into another document unless produced for commercial gain, subject to the source being appropriately acknowledged and the copyright preserved. The reproduction of logos without permission is expressly forbidden. Permission should be sought from the JANET Service Desk. Trademarks: JANET® is a registered trademark of the Higher Education Funding Councils for England, Scotland and Wales. The JNT Association is the registered user of this trademark. JANET(UK)® is a trademark of The JNT Association. AethraTM is a trademark of Aethra, SpA and Aethra, Inc. in the United States and other countries. Borderware® is a registered trademark of BorderWare Technologies Inc. in the U.S. and other countries. Check Point® is a registered trademark of Check Point Software Technologies Ltd. in the U.S. and other countries. Cisco® and PIX® are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Emblaze-VCON® is a registered trademark of Emblaze-VCON Ltd. in the U.S. and certain other countries. Fortinet® is a registered trademark of Fortinet, Inc. in the U.S. and other countries. Microsoft® and NetMeeting® are registered trademarks of Microsoft Corporation in the United States and/or other countries. Polycom® is a registered trademark of Polycom, Inc. in the United States and/or other countries. TANDBERG® and Codian® are registered trademarks or trademarks of TANDBERG in the U.S. and other countries. Visual NexusTM is a trademark of Tomen Cyber-Business Solutions, Inc. All (other) company or brand names may be trademarks of the respective companies with which they are associated. Disclaimer: The information contained herein is believed to be correct at the time of issue, but no liability can be accepted for any inaccuracies. The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas such as internet addressing, and consequently URLs and e-mail addresses should be used with caution. The JNT Association cannot accept any responsibility for any loss or damage resulting from the use of the material contained herein. Availability: Further copies of this document may be obtained from the JANET Service Desk at the above address.

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/nat-firewalls-and-videoconferencing-h323-border-traversals

Links
[1] http://www.video.ja.net/documents/services/video/vtas/323intro.pdf
[2] http://www.ja.net/documents/services/video/vtas/323security.pdf
[3] http://www.rfc-archive.org/getrfc.php?rfc=1918
[4] http://old.iptel.org/info/players/ietf/firewall/draft-shore-h323-firewalls-00.txt

[5] http://www.itu.int/rec/T-REC-H.323/e
[6] http://www.ja.net/documents/services/video/vtas/wrexham.pdf
[7] http://www.ja.net/documents/services/video/vtas/gkconfig.pdf
[8] mailto:service@ja.net