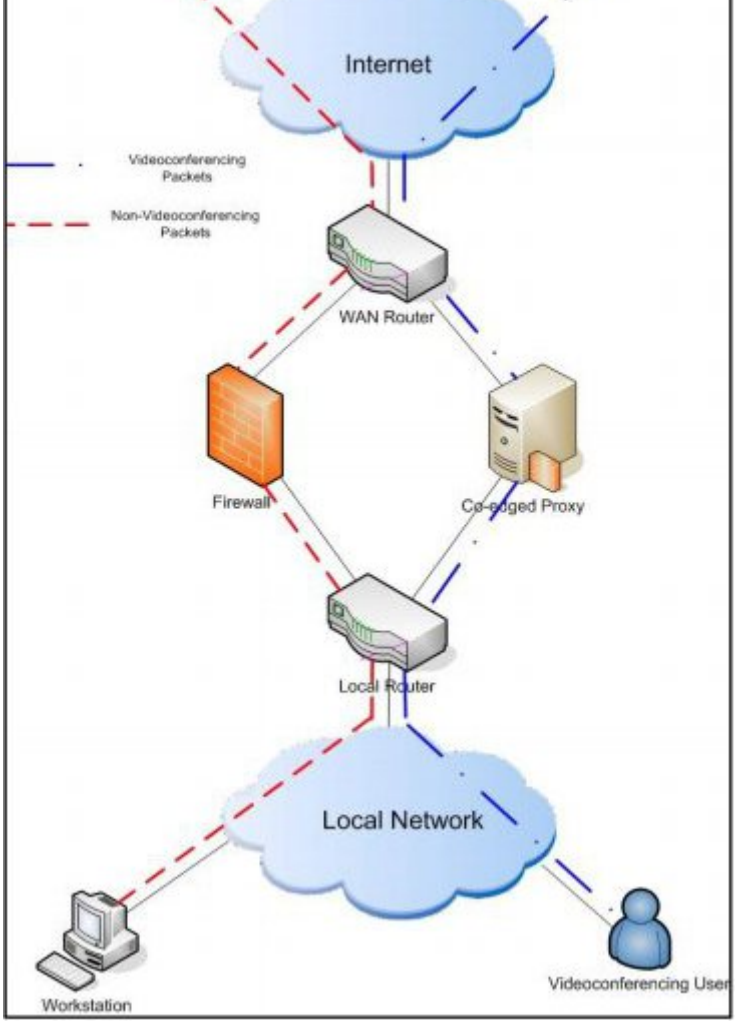
Solutions

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 [1] section.

Network solutions

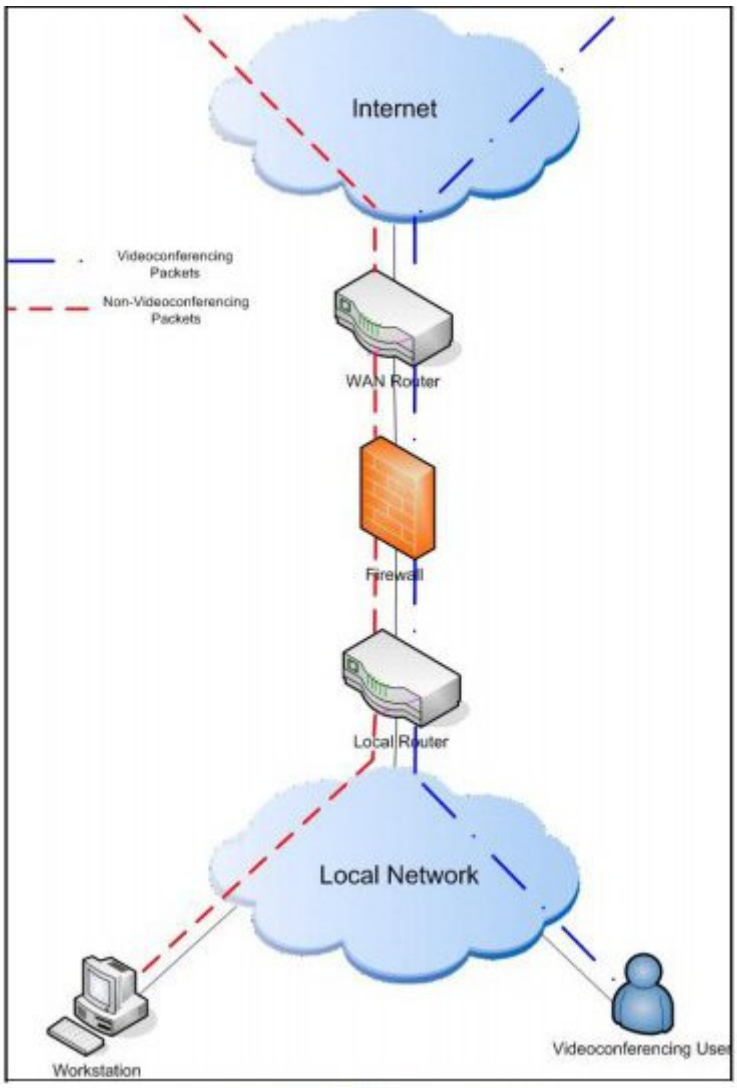
Co-edged proxy/router



[2]

Figure 1: 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.*



[3]

Figure 2: 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.

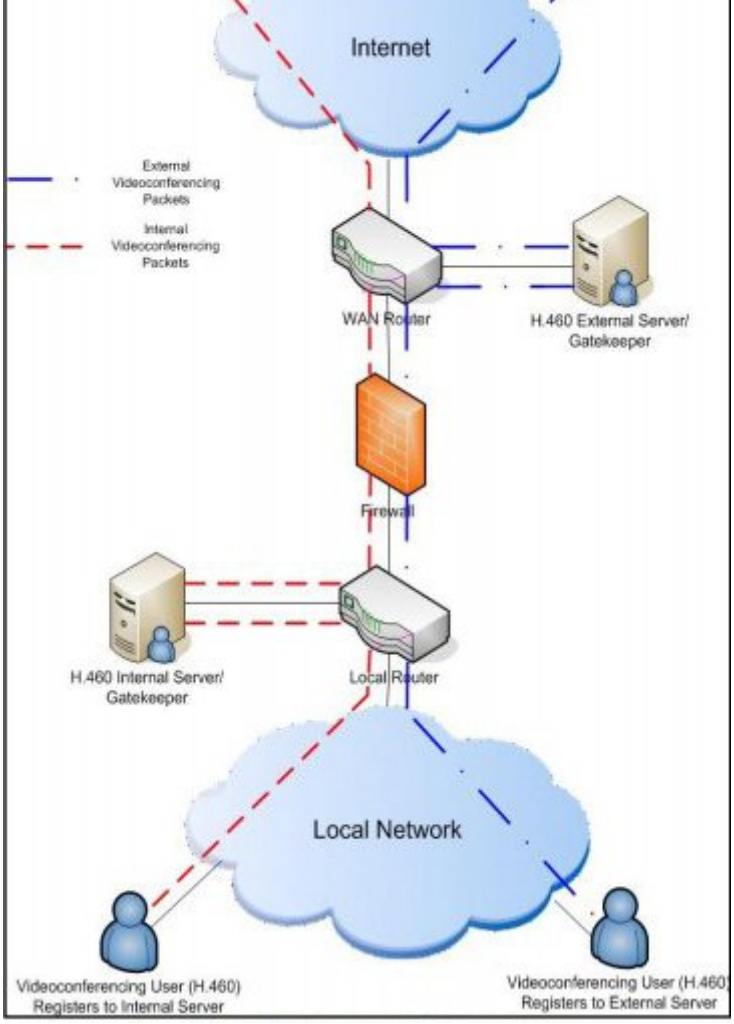
Firewalls that perform these kind of functions are said to be 'H.323 aware' – in short, they have some extra functionality that makes them able to allow H.323 calls to be set up and completed without adding any undue latency to the call. These are often referred to as 'H.323 fix-ups 'or 'VoIP fix-ups'. 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®.

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.



[4]

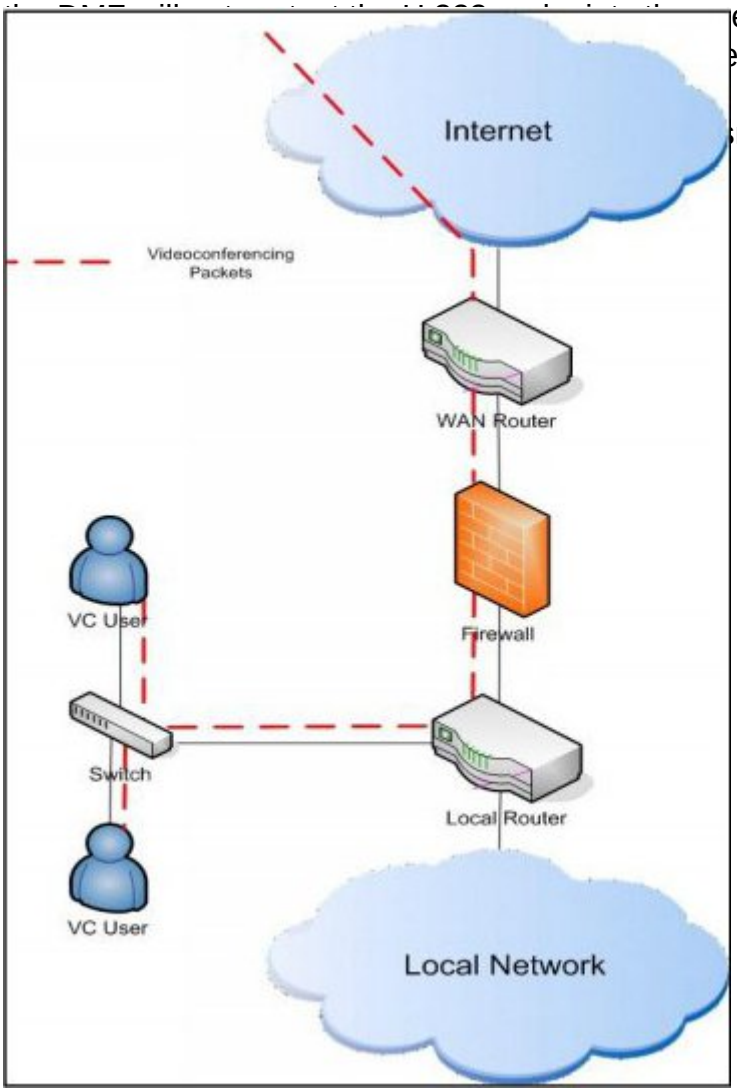
Figure 3: Border negotiation devices

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

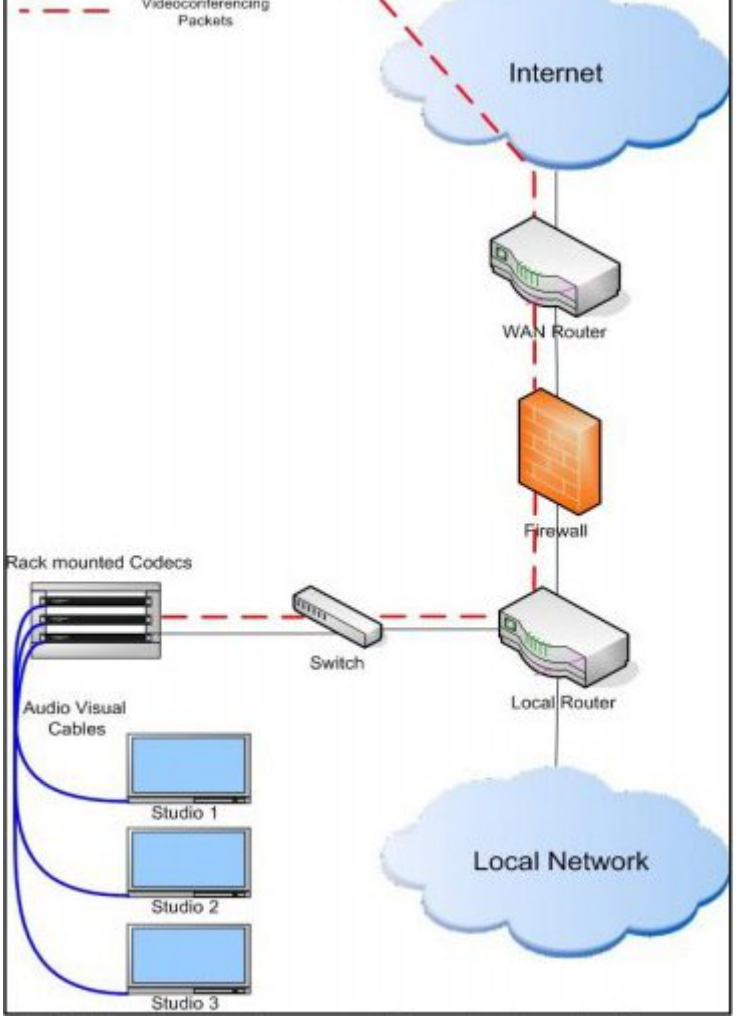
(outwardly accessible) web or e-mail servers, for example. Placing H.323 equipment within
elves but will protect the rest of the local
eployment. In practice this is not always a
etc. to the location of the H.323
maller, outreach locations. See Figure 4,



[5]

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.



[6]

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.

Links
[1] https://community.ja.net/library/janet-services-documentation/references-5
[2] https://community-stg.jisc.ac.uk/system/files/images/vc-h323-border-traversal-01.jpg
[3] http://community.ja.net/system/files/images/vc-h323-border-traversal-02.jpg
[4] http://community.ja.net/system/files/images/vc-h323-border-traversal-03.jpg
[5] http://community.ja.net/system/files/images/vc-h323-border-traversal-04.jpg
[6] http://community.ja.net/system/files/images/vc-h323-border-traversal-05.jpg