H323 Border Traversal

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.

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 document Security Guide for H.323 Videoconferencing [1].

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.

Links
[1] https://community.ja.net/library/videoconferencing-booking-service/security-guide-h323