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.

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/firewalls-and-ports