

## **Interacting with Firewalls using Fixed ports and Polycom H.323 products**

H.323 uses a single fixed TCP port (1720) to start a call using the H.225 protocol (defined by H.323 spec) for call control. Once that protocol is complete, it then uses a dynamic TCP port for the H.245 protocol (also defined by the H.323 spec) for caps and channel control. Finally, it opens up 2 dynamic UDP ports for each type of media that was negotiated for the call (audio, video, far-end camera control). This first port carries the RTP protocol data (defined by the H.225 spec) and the second one carries the RTCP data (defined by the H.225 spec).

Any site that UTN connects to for videoconferencing must allow bi-directional IP H.323 calling. The site's network administrators must "punch holes" in the firewall using the exact port numbers and exact protocol types for outgoing calls. UTN recommends they use the following fixed ports:

### **H.323 Ports (IP based video conferencing):**

- 80 - Static TCP - HTTP Interface (optional)
- 389 - Static TCP - ILS Registration (LDAP)
- 1503 - Static TCP - T.120
- 1718 - Static UDP - Gatekeeper discovery (Must be bidirectional)
- 1719 - Static UDP - Gatekeeper RAS (Must be bidirectional)
- 1720 - Static TCP - H.323 call setup (Must be bidirectional)
- 1731 - Static TCP - Audio Call Control (Must be bidirectional)
- 5060 TCP and UDP for Gatekeeper registration

### **Other HDX, VSX, PVX, & ViewStations Ports:**

- 21 (FTP) - Software Updates & GMS Provisioning
- 23 (Telnet) - For Diagnostics & API Control (used by PCS) by MP/512/etc.
- 24 (Telnet) - For Diagnostics & API Control (used by PCS) by FX/EX/4000 and VSX
- 3230 to 3288 - TCP Ports
- 3230 to 3288 - UDP Ports

### **People+Content IP Ports:**

- 5001 - Static TCP

Sites that have a Cisco PIX or ASA firewalls must either allow the H.323 Fixup without enabling the listed ports or else must enable the ports but not the fixup. If both are enabled, the call might establish but not pass two-way audio or video.