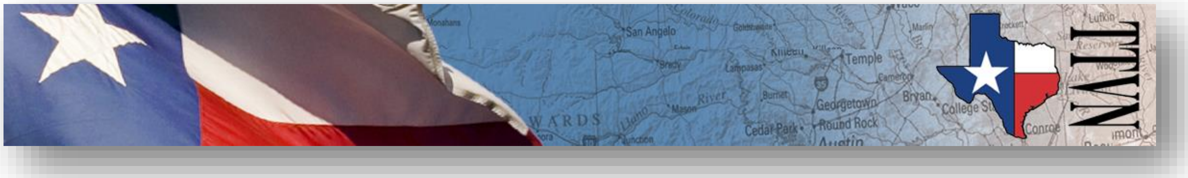

Texas A&M University System
Trans-Texas Videoconference Network (TTVN)
Resolving Firewall Timeout Issues

This information was compiled to address issues resulting in videoconference connection dropouts after approximately two hours of connection time. This issue has affected videoconference courses on several Texas A&M University System campuses off and on over the past two years. The TTVN staff has determined that these dropouts result from local network firewall settings.

Background

A firewall or network address translation (NAT) device, unlike a router or switch, has to maintain state information on the connections passing through it. In the normal case of TCP connections, there is a definite end to the connection, but there is also the possibility that one end or the other (half closed) or both (full timeout) could terminate the connection abnormally. If this occurs, the firewall won't receive the normal session disconnect messages and will hold the state indefinitely. Holding a "stale" session state would reduce the performance of the firewall.

Consequently, firewalls time-out idle connections. The timeout removes the connection if there is no traffic through the firewall over a set period of time.

Videoconference Application

There is no mandated standard “keep alive” signaling on the control channel of an H.323 IP videoconference connection to keep the firewall from detecting an idle connection. Only if the endpoints send frequent control messages, will the firewall detect traffic and keep the session running. Videoconference endpoint signaling varies according to the implementation of the signaling protocol by the vendor of the videoconference endpoint. In many videoconferences, no signaling occurs other than at the beginning and end of the videoconference call.

Essentially, if there is no recurring signaling during a videoconference, the firewall may detect the idle signal channel and shut down the call prematurely. The videoconference endpoints will eventually notice that the signaling channel connection is gone and disconnect the videoconference call.

Resolution

By setting the firewall or NAT timeout length for some period of time longer than your average session duration (3+ hours for the typical higher education class meeting), you avoid the problem of dropouts prior to the scheduled end of the videoconference.

Special note on Cisco PIX firewalls:

By default, Cisco PIX firewalls are set to disconnect all H.323 videoconference sessions after 2 hours. Please make sure you change this setting if you expect to have videoconferences longer than 2 hours.

There are two lines that should be changed:

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 0:00:00 *
```

```
timeout h323 16:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
```

Also note that we have found that upgrading to version Pix 6.3(4) or higher can
resolve issues within NATed environments.

ASA Firewall Configuration

The ASA requires the **H.323 Fixup** command to be configured. This instructs the ASA to keep the video connected and not time out.

This information was compiled by the TTVN Enterprise Network and Video Operations Groups
September, 2010

TTVN Enterprise Network Group
979-845-8437
wan@ttvn.tamus.edu

TTVN Video Operations Group
979-862-2241
ops@kamu.tamu.edu