

TFTP with MaxCS server behind NAT

AltiGen packages firmware and boot-code for its IP phones with a TFTP utility named TFTPNat. While this software is (as the name implies) designed to serve the firmware in a manner that is NAT friendly, there are a few items to be aware of when using TFTP through NAT:

IP Phone boot-code - IP phone boot-code versions 14 and earlier has a bug that prevents it from properly interacting with the TFTP proxy on some network firewalls. This is not a problem with the firewalls, and should not require any special firewall configuration. It is a bug in the IP phone boot code that is fixed in version 15 and above. This bug is known to impact IP705, IP710, and IP 20. It should not impact any versions of IP 805.

Updating IP phone boot code instructions are in this KB article. As a reminder, IP phone boot-code should be done over a highly stable link to prevent 'bricking' the IP phone. This means that boot code should be served from a TFTP server that is on the same LAN as the server over a physically wired (not WiFi) connection.

Speed As a protocol, TFTP is designed for absolute simplicity. In many ways this is done at the expense of performance. Unlike FTP, which utilizes TCP for flow control, TFTP requires that every block of data sent receive a TFTP ACK before the next block is sent. Because of this the round trip time of the connection will greatly impact the amount of time that it takes for a file to download over the Internet via TFTP. Additionally, TFTP's original RFC specification (RFC 1350) utilized a 512 byte block size. This was later increased via other RFCs. AltiGen's TFTPNat application was using the 512 byte block size up until the version that shipped with IP phone firmware version 2xA1. Using this newer version of TFTPNat will noticeably improve the speed over which IP Phone firmware is served over the Internet, although it will still be noticeably slower than serving the file from the LAN, despite the small overall file size.

Firewall - UDP port 69 must be open on the network firewall, but a Windows Firewall exception should also be created for the TFTPNat utility itself. This is easily done if Windows prompts to allow the traffic, but this does not seem to occur in all situations. If the firewall exceptions must be created manually, please refer to this KB article for instructions on how to do so.

<https://know.altigen.com/questions/1142/>