NAT Traversal for VoIP

ITS 441
Bibliography

- RFC 5389 Session Traversal Utilities for NAT (STUN)
- I.D.: draft-ietf-behave-turn Traversal Using Relays around NAT (TURN)
- RFC 5626 Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)
- I.D. draft-ietf-mmusic-ice Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
NAPT

192.168.1.2:1234 -> 192.0.2.1:80
192.0.2.1:80 -> 192.168.1.2

132.235.3.5:4567 -> 192.0.2.1:80
192.0.2.1:80 -> 132.235.3.5:4567
Some Notes on NAT

• The most common NAPT today has a single external IP address
  – NAPT insures that every connection has a unique port number
  – The port number determines where the packet is forwarded to, and how it is translated
  – The NAPT may attempt to preserve the internal port number if it is not already in use
  – NAPT “bindings” are created, or renewed, by an out-bound packet.
  – NAPT bindings can be static, or set up with a signaling protocol such as UPnP
NAT Behavior

• Outbound packet creates a binding
  – TCP bindings usually persist until the TCP connection is closed
  – UDP bindings are deleted after some time

• Scope of bindings
  – Most liberal: packets from anywhere to the external IP address and mapped port number go to the internal host that created the binding
  – Address specific: only the recipient IP of the outbound packet can send a packet back
  – Address/Port specific: only the recipient IP of the outbound packet can send a packet back, and only from the port used in that outbound packet.
Why is NAT “Bad”

• Invisible to some protocols (e.g. Web)
  – (That is why we put up with it)
• Bad for “Signaling” and “Offer/Answer” Protocols
• Think SIP
  – UA includes its address in the INVITE
  – SDP sends address/port to send RTP to
Proxy tells other UA to connect to 192.168.1.2
FAILS

SIP header contains 192.168.1.2 as the connection address
What if NAT translates the INVITE (ALG)

INVITE

192.168.1.2:1234->192.0.2.1:5060
132.235.3.5:4567->192.0.2.1:5060

SIP header contains 192.168.1.2 as the connection address

Proxy tells other UA to connect to 132.235.3.5:5060
Might Work;
What about RTP?

Wednesday, November 11, 2009
NAT-based solutions

- Remember: end-to-end security (encryption or integrity checks) breaks all this
- There may be more than one NAT in the sequence
- If the second UA is behind a NAT, this cannot work
- UAs have no way to tell if a connection (call) will work
Host based solutions

• **STUN**
  – Uses a server in the Internet to allow a client to discover the external NAT IP address
  – May be enough for some NAT versions
  – Won’t work in general

• **Meant to be used as a tool in a larger solution**
“sip-outbound” (RFC 5626)

• Incoming calls
  – require an inbound SIP INVITE
  – NAT won’t forward it

• RFC 5626
  – Updates SIP
  – UA sends REGISTER and keeps that connection open
  – Proxy sends SIP INVITES over this existing connection
TURN

- Defines a relay server
- Client creates a connection to a TURN server
- All packets are encapsulated in TURN messages and sent via the relay
ICE

- Extends SDP
  - Can also be used for non-sip-based protocols
- UA collects all possible addresses
  - Local NICs (could be more than one)
  - Outside NAT address discovered via STUN
  - Address of a TURN relay
- UAs rank-order the addresses and try every pair until a connection succeeds