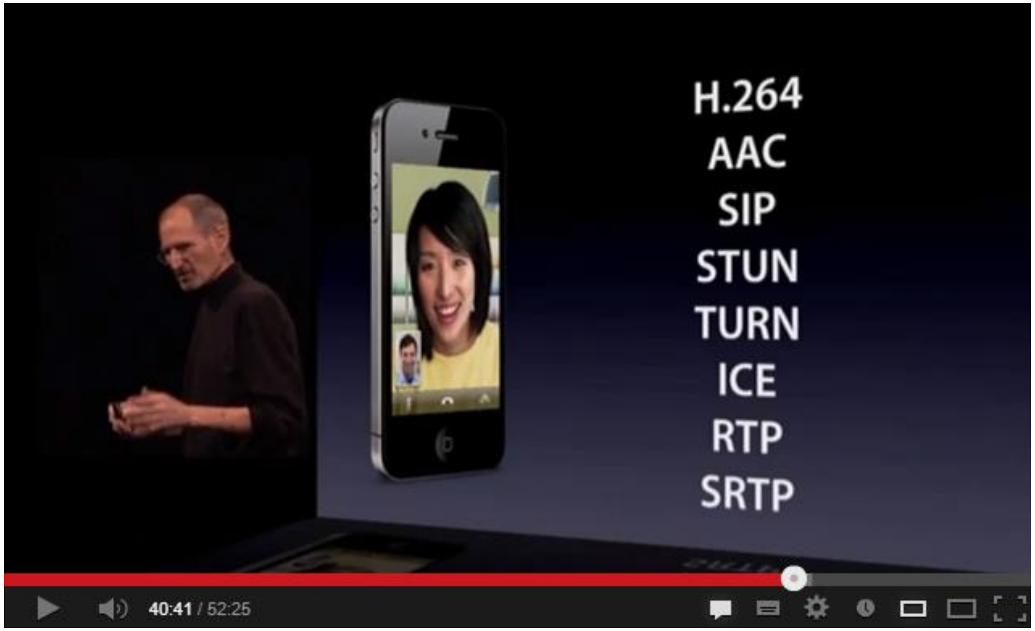
Network Address Translation (NAT)

7강

Why should we know this?

- Because you are using it
  - http://www.youtube.com/watch?v=z__jxoczNWc (40:00 →)



It all started with IPv4 address depletion fears

- Two-pronged attack
  - IPv6 (long-term solution)
  - NAT (short-term solution)
    - But became permanent
    - “NAT is IPv4ever”

NAT

- What’s good about it
  - Obviates the need for long-term solution
    - If address shortage is the issue

- What’s bad about it
  - Can’t translate IP addresses and port numbers in the payload of application protocols unless taught so
    - Internet telophony, FTP, ICMP (error), etc.
  - Breaks the end-to-end principle: “middlebox” problem

Traditional NAT

- Basic NAT
  - m:n address mapping (m>>n)
- NAPT
  - Can share the same global address
  - Distinction is made by port numbers

Servers behind NAT

- Clients are okay behind NAT
- Servers need globally known address
  - NAT address can be used
  - Port mapping/forwarding
    - Based on the destination port number, NAT forwards the requests from global Internet to an internal server
    - E.g. TCP port 80 → Web server behind NAT

NAT traversal

- Pinholes
  - Mapping made at NAT is called “pinhole”
    - Lives during application execution, which created the pinhole
- Hole punching
  - Method that allows two or more systems behind NAT to communicate directly using pinholes
    - E.g. Skype peer-to-peer app

STUN

- Session Traversal Utilities for NAT

- Two objectives
  - Ascertain the “external” IP and port used on a NAT for an application behind it
  - Keep the NAT binding alive

- STUN servers on the global Internet are necessary

STUN

- STUN server echoes back STUN requests

- Uses port 3478 with TCP/UDP

- STUN message format: Fig. 7-8

STUN

- Mapped address is the external address being used
  - “reflexive transport address”

- XOR-MAPPED-ADDRESS exclusive-OR’s the mapped address w/ magic cookie
  - To avoid ALG’s unwanted intervention

TURN

- STUN is asking, and getting an answer from, the STUN server
  - STUN server does not do anything more than that
- Traversal Using Relays around NAT extends STUN
- TURN provides a way for two systems behind uncooperative NATs to communicate

TURN

- TURN client uses the “relayed transport address” at the TURN server
    - The client uses the address to communicate with its peer
- Fig. 7-11
- Allocation is made at the TURN server
    - Requires authentication, as TURN service involves costly traffic relaying operation

ICE

- Interactive Connectivity Establishment
  - A generic facility
- Developed to help UDP-based applications behind a NAT establish connectivity

- Uses STUN and TURN

ICE

- Prefers more direction communication
- Priority
  - Host transport > server-reflexive > relayed