ICE, TURN and STUN for NAT Traversal

Stephen Strowes, stephen.strowes@nokia.com

Pizza Talk

15/Oct/2008

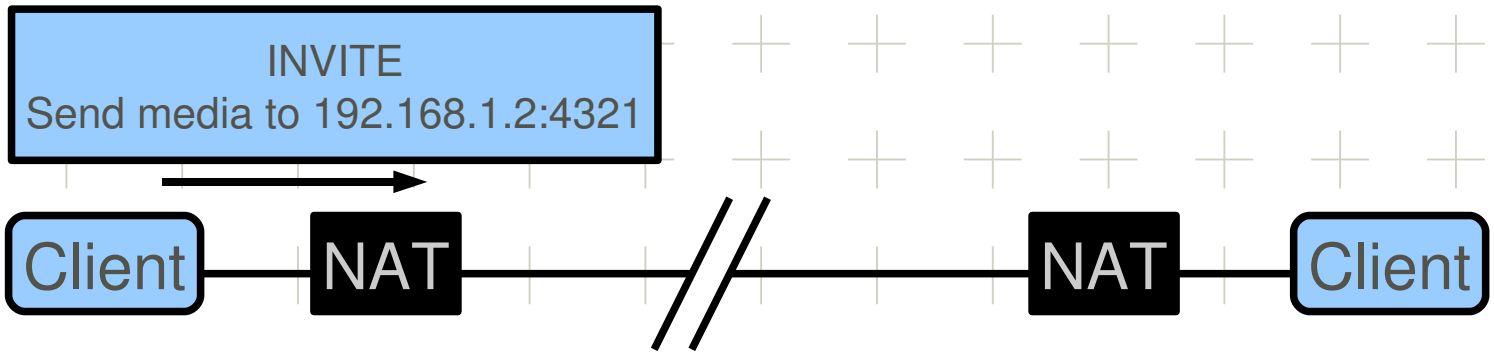
Nokia Research Center

NOKIA

Problem Space

NATs are commonplace, but they destroy the end-to-endianness of the Internet, making it difficult for two peers to talk to each other

Many protocols (e.g., SIP, SDP within SIP for media) contain IP addresses in the *body* of the message



Problem Space

NAT behaviour is vendor-specific (model-specific?), but in general:

NATs create transient mappings between private (ip:port) and public (ip:port) bindings.

NATs exhibit differing packet filtering rules when mapping from public to private address space.

Problem Space

Hosts have private transport addresses, associated public transport addresses, and possibly also restrictive NATs to traverse

ICE

Interactive Connectivity Establishment

- Intended to help two peers in difficult network conditions find the best transport to communicate
- Stand-alone, but designed with SIP/SDP in mind, allows endpoints to describe a set of candidate addresses to test for communication
- Uses STUN and TURN as tools to gather candidates...

STUN

Session Traversal Utilities for NAT

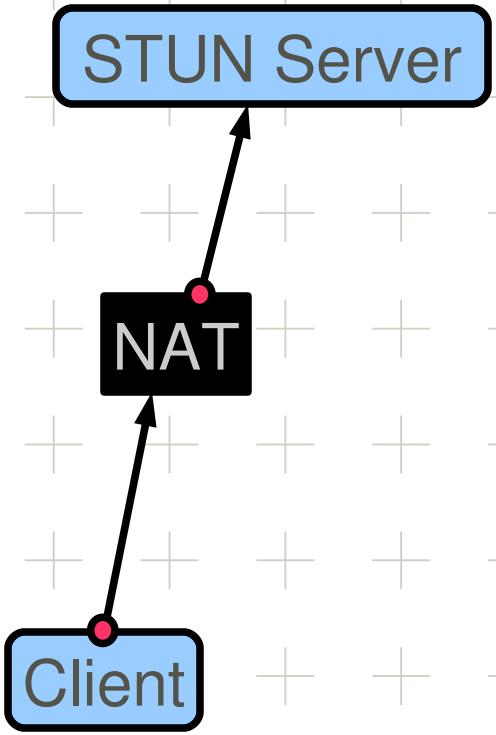
Dirt simple idea; defines one *method*

STUN

Session Traversal Utilities for NAT

Dirt simple idea:

- What's my public IP?

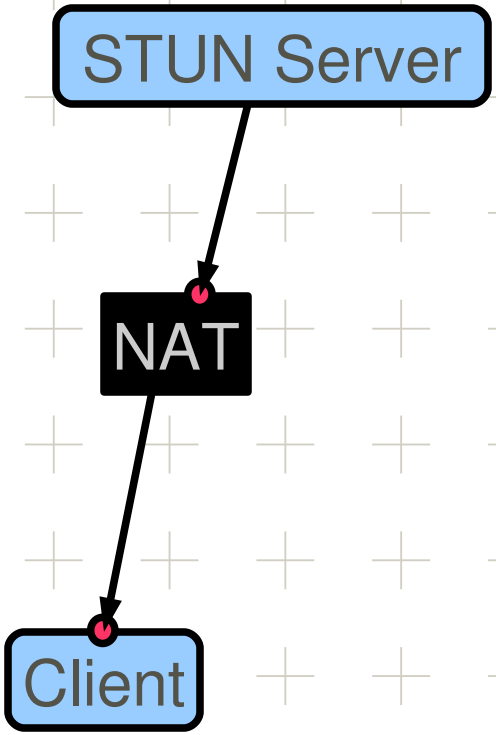


STUN

Session Traversal Utilities for NAT

Dirt simple idea:

- What's my public IP?
- THIS is your public IP!



TURN

Traversal Using Relays around NAT

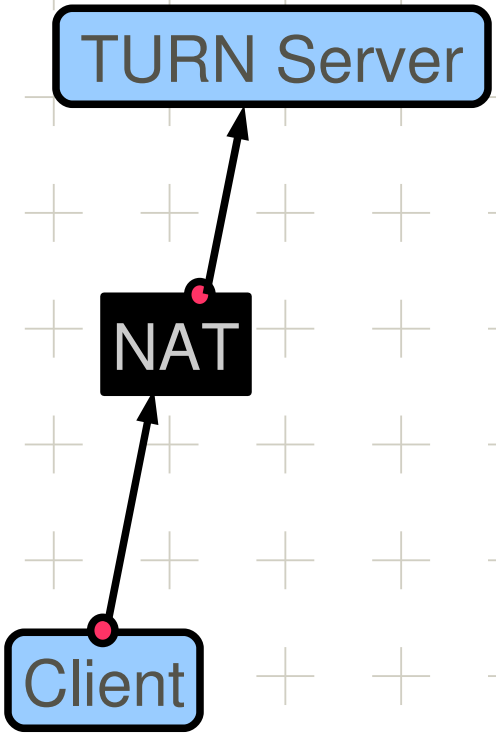
Allocate a relay on the public Internet

TURN

Traversal Using Relays around NAT

Allocate a relay on the public Internet

- Allocate an address?

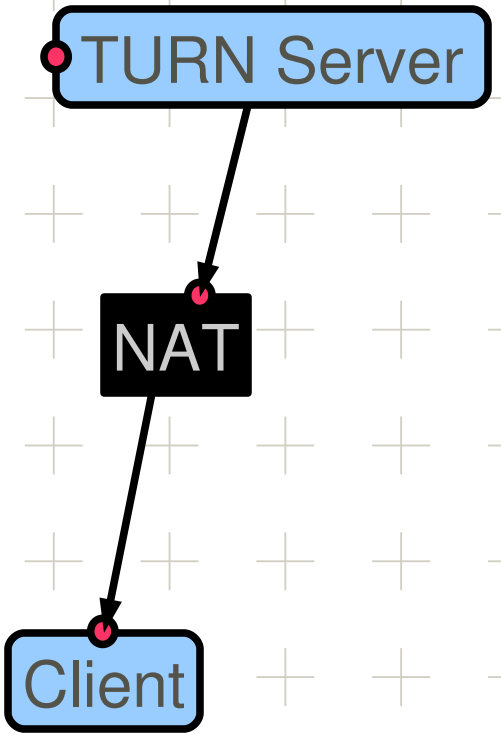


TURN

Traversal Using Relays around NAT

Allocate a relay on the public Internet

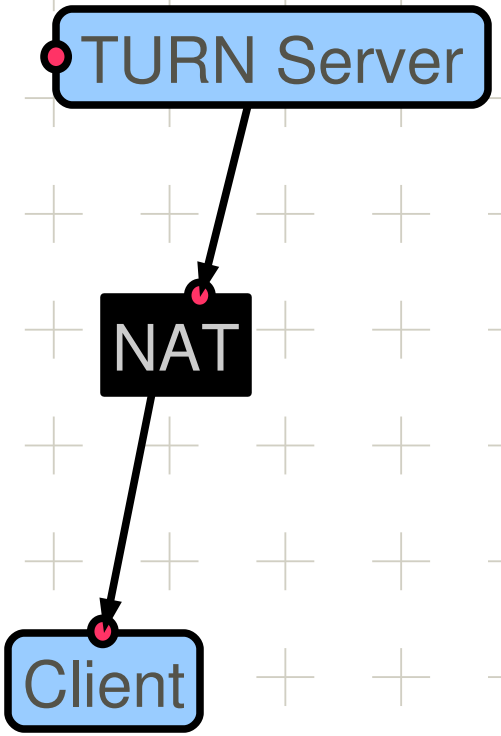
- Allocate an address?
- THIS is your allocation!



TURN

Traversal Using Relays around NAT

Client can then create *permissions* to dictate who can send data to the allocated relay address for forwarding to the client...



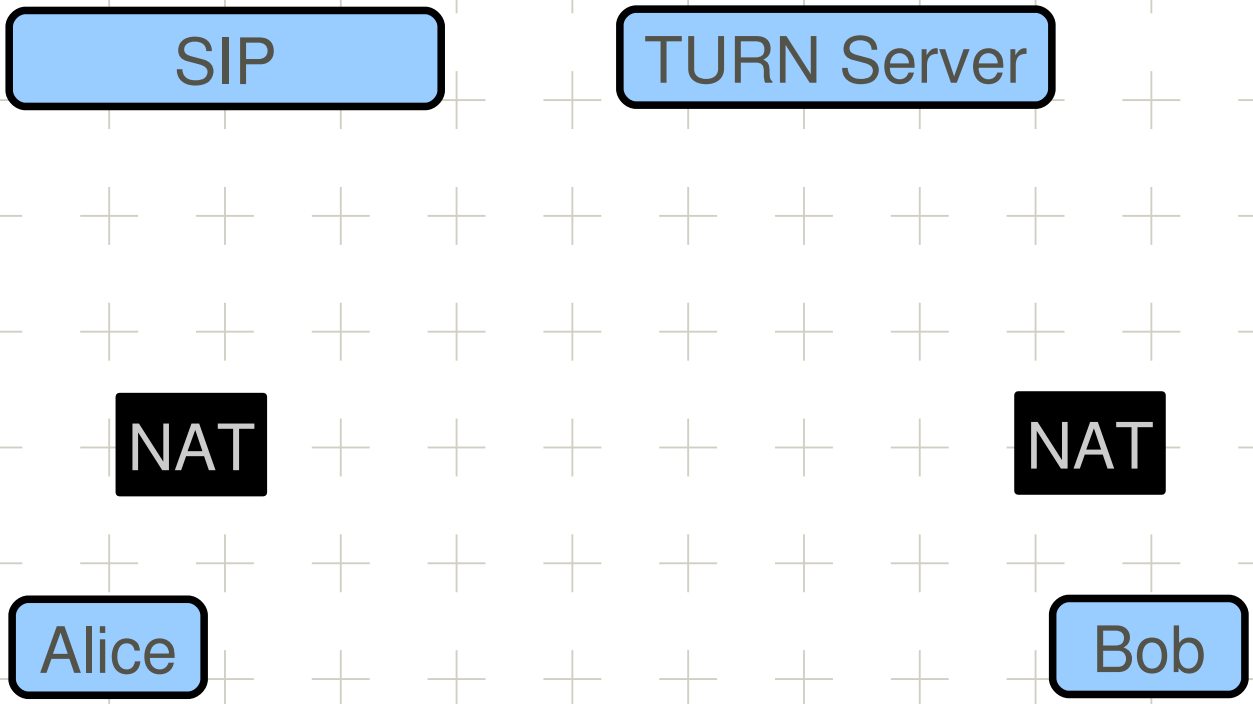
ICE

Interactive Connectivity Establishment

- Intended to help two peers in difficult network conditions find the best transport to communicate
- Extension to the offer/answer model, allows endpoints to describe a set of candidate addresses for communication
- Uses STUN and TURN to gather candidates
- Defines a process for pairing and checking these candidates

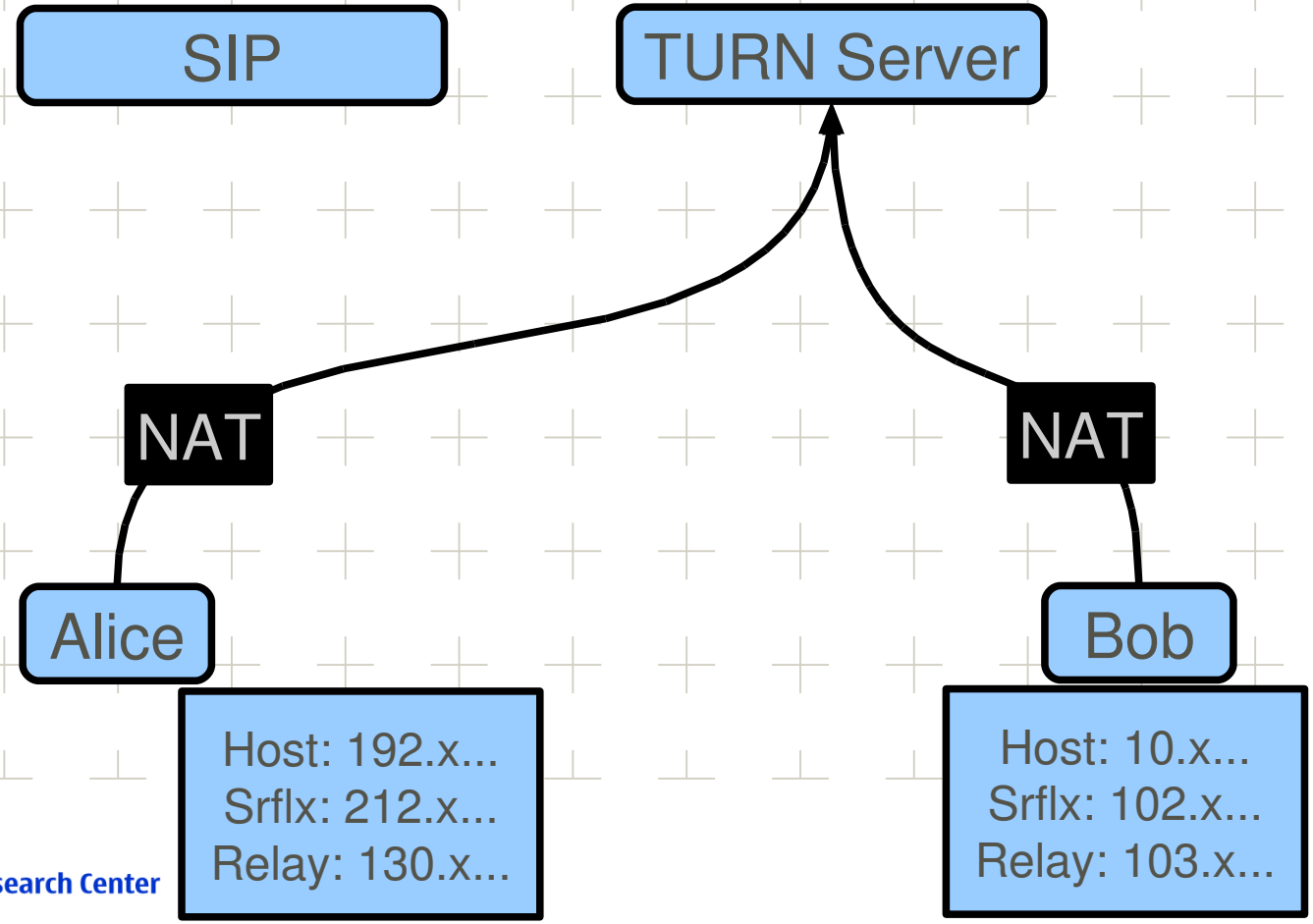
ICE

- Consider...



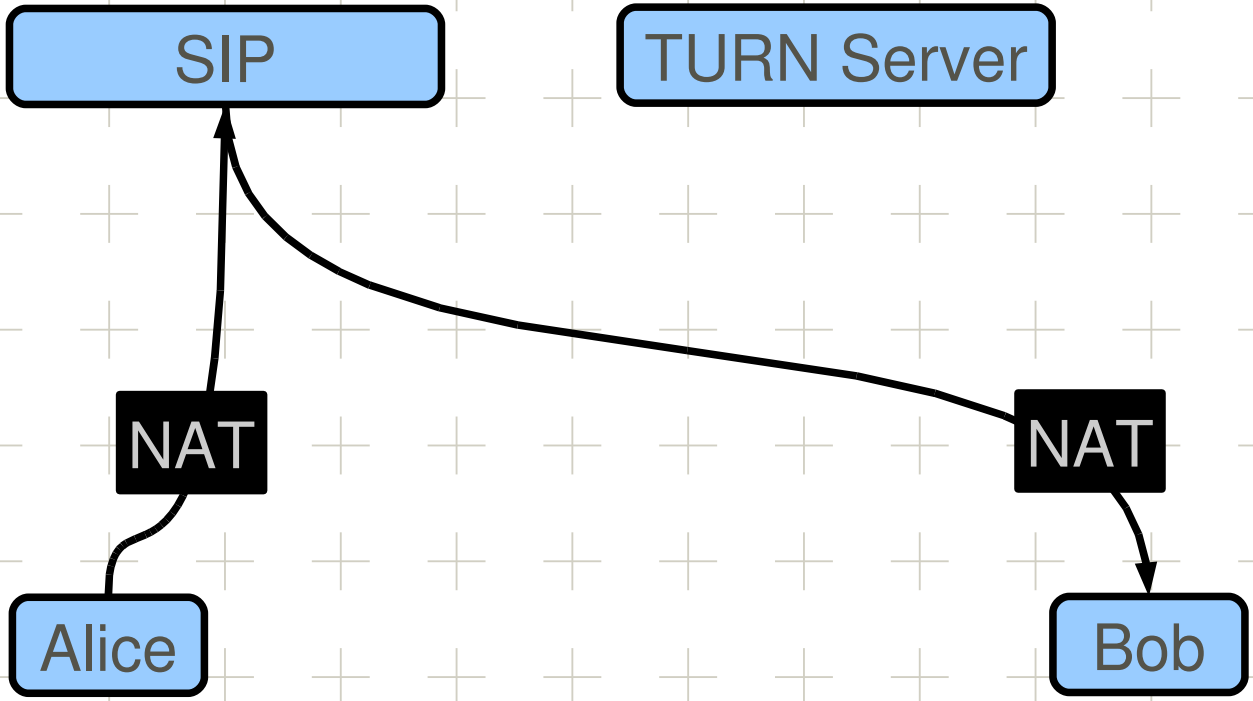
ICE

- Candidate gathering...



ICE

- Exchange candidate sets...

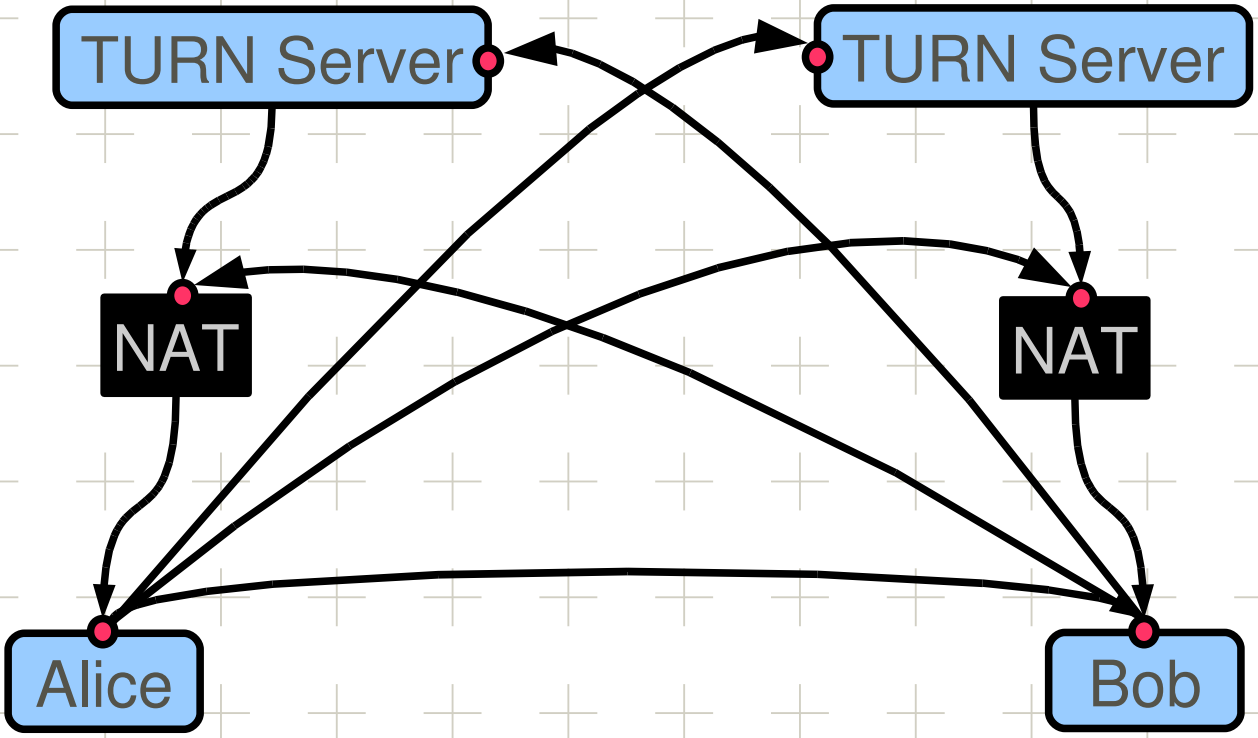


ICE

- Candidates are paired in order of decreasing priority and tested
  - Host candidates are good!
  - Relay candidates are bad!

ICE

- Connectivity checks...

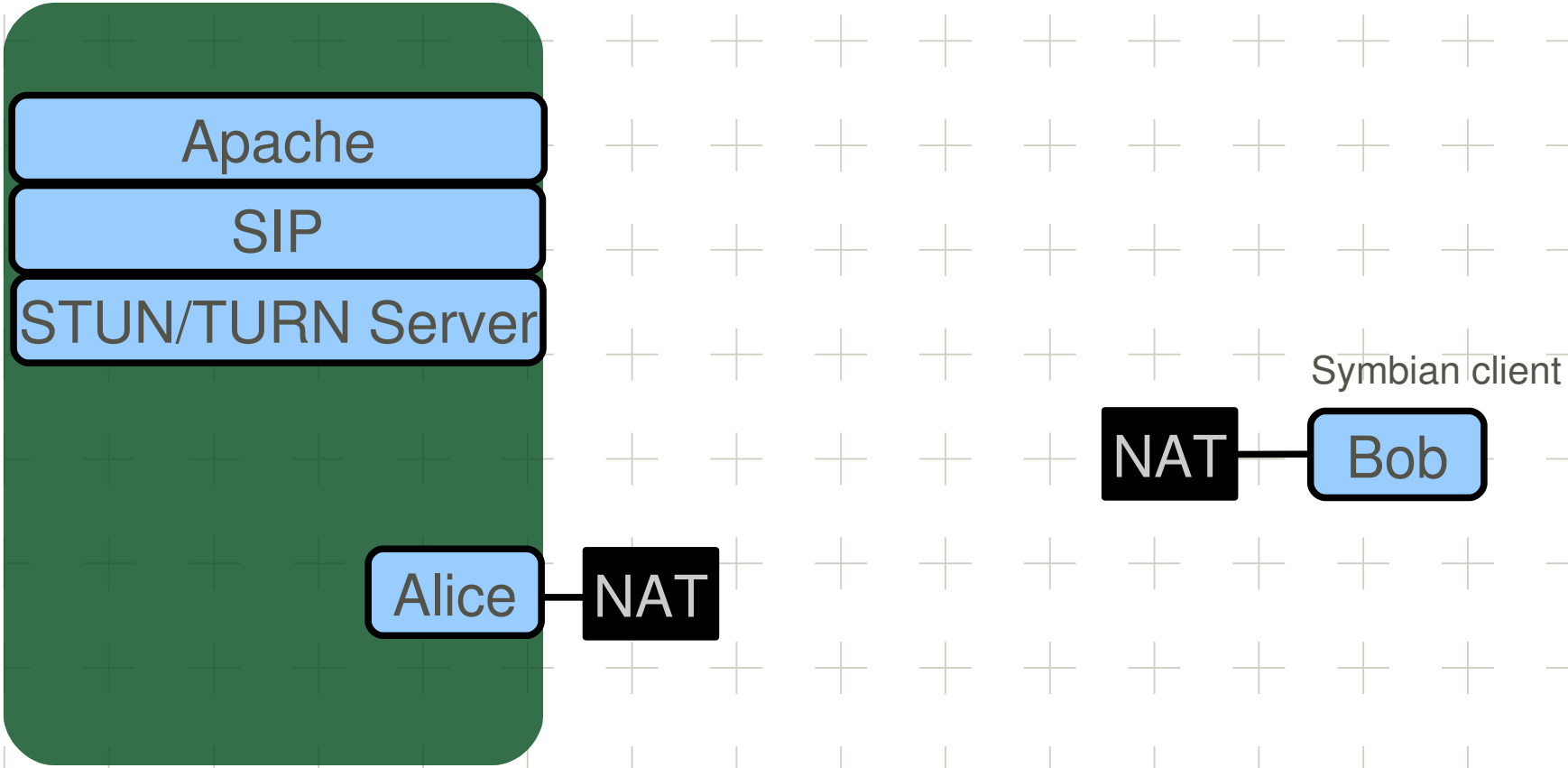


What don't we know?

- People are building software using these protocols, or similar ideas, but we have little quantifiable data on their real-life behaviour
  - Success rates for ICE
  - How well does it *actually* work? Quality of chosen candidates?
  - Throttling of connectivity checks?
- ... and then there's the possibility of collecting information on the type of NATs widely deployed in the Internet

What are we building?

- Measurement platform



We need *you*...

- There's a lot of work here which can be done... For starters:
  - Web front-end
  - Linux client
- We would like to take on
- interested students for special assignments to help us implement some of this work...

Resources

- ICE: http://tools.ietf.org/html/draft-ietf-mmusic-ice
- STUN: http://tools.ietf.org/html/draft-ietf-behave-rfc3489bis
- TURN: http://tools.ietf.org/html/draft-ietf-behave-turn

Questions?
stephen.strowes@nokia.com