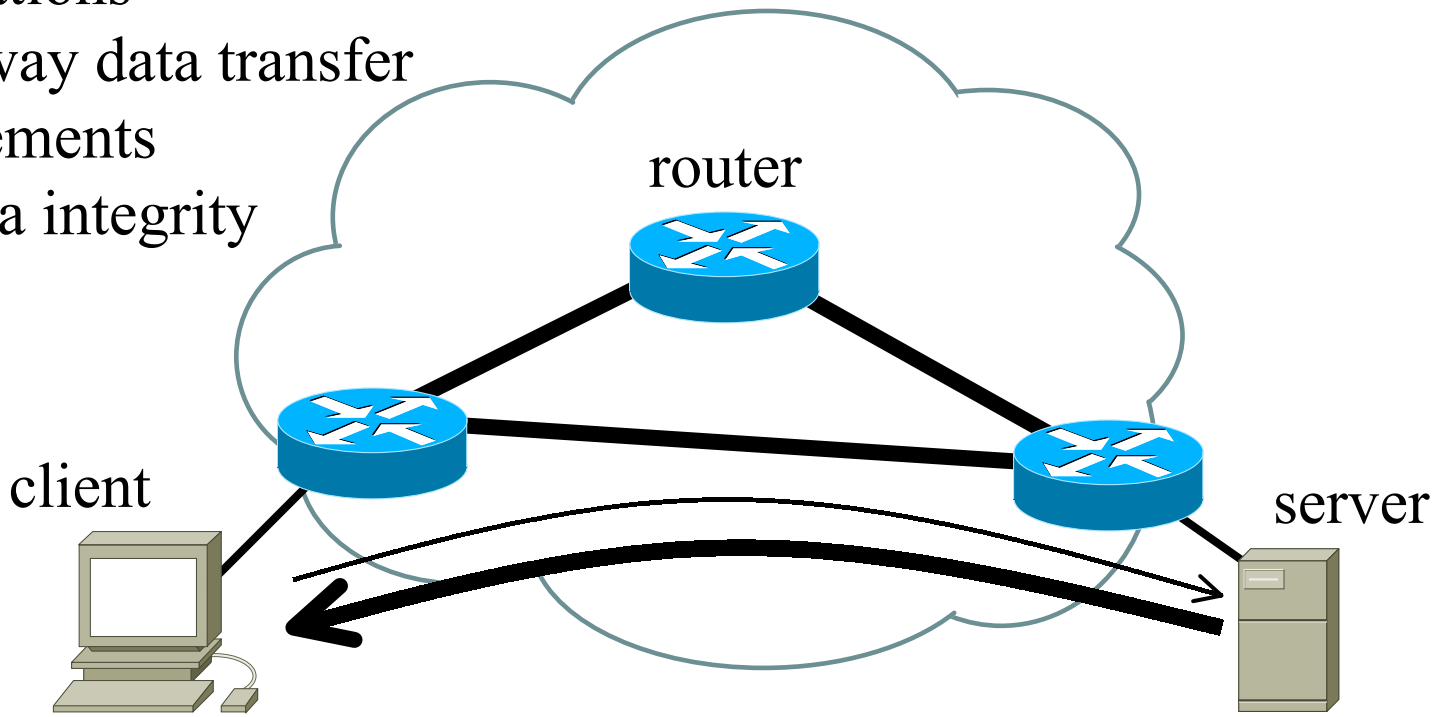
SIP-assisted NAT Traversal

Jianping Pan
web.uvic.ca/~pan
October 25, 2005

Internet was ...

- infrastructures
  - routers, end-hosts
- applications
  - 1-way data transfer
- requirements
  - data integrity

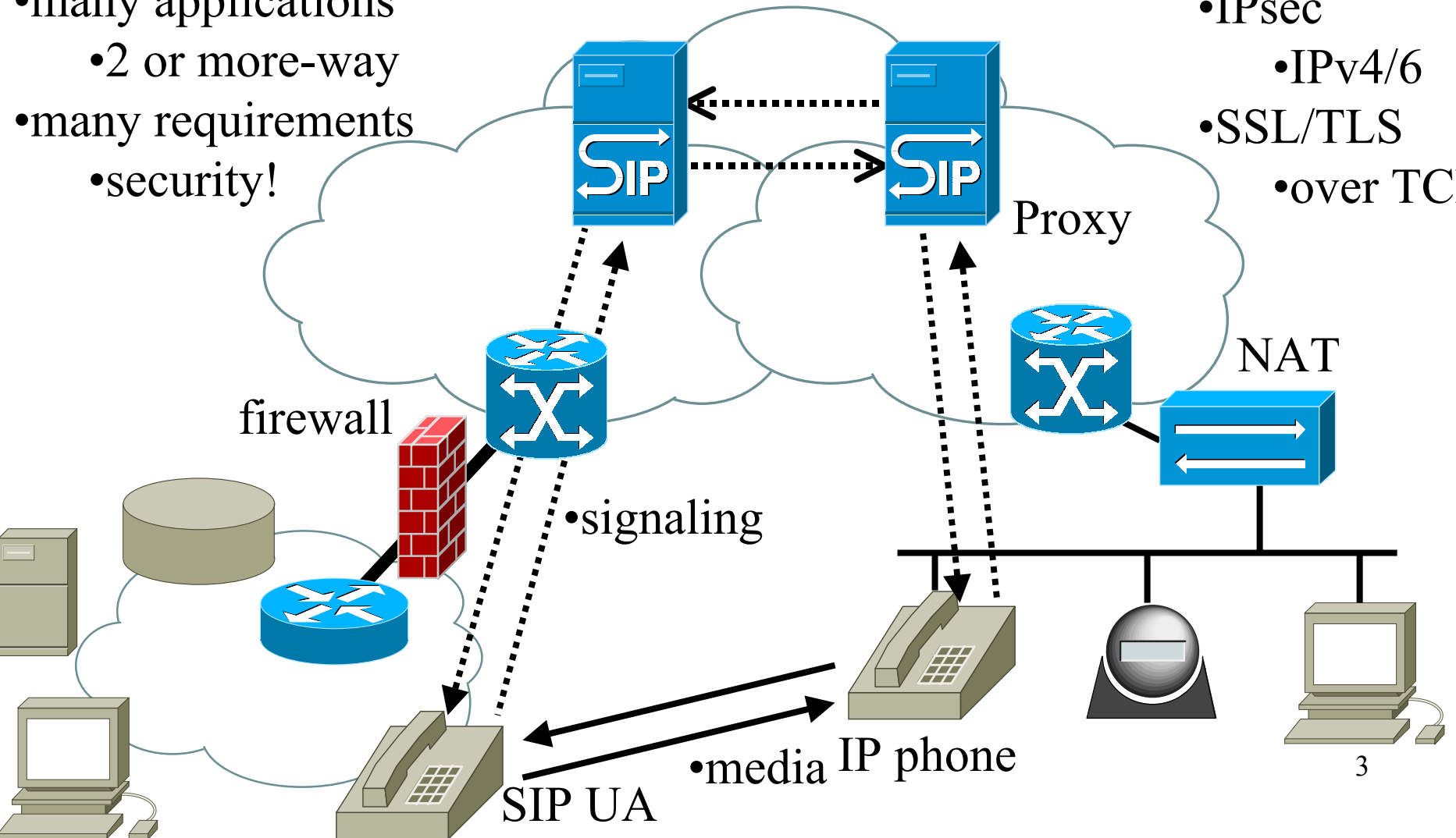


- global addressable and end-to-end reachable

"Internet" now …

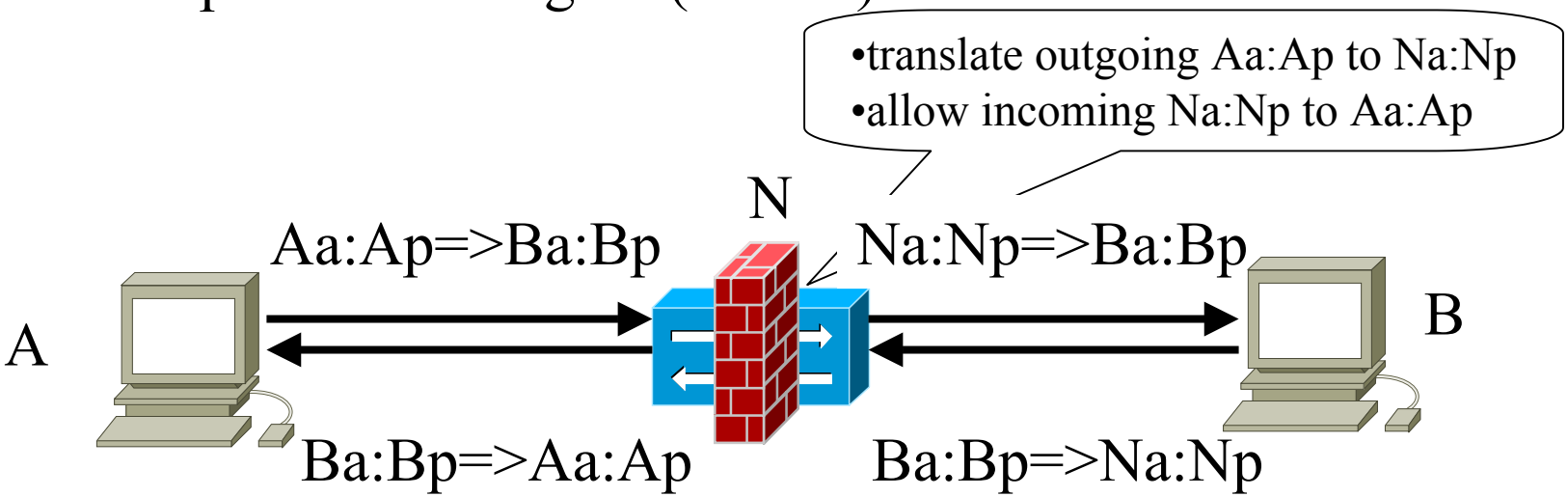
- many mid-boxes
  - firewalls, NATs
- many applications
  - 2 or more-way
- many requirements
  - security!

- SIP
  - ~SS7?
- IPsec
  - IPv4/6
- SSL/TLS
  - over TCP



Firewalls and NATs

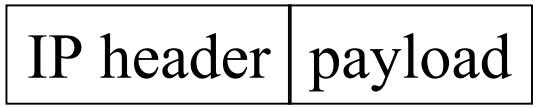
- firewalls and NATs usually work hand-to-hand
- firewalls: packet filtering w/ (known) rules



- NATs: initially as a *quick-fix* to IPv4 address shortage
- now pervasive in every networking scenario
- translate source/destination address/port
- update other related information (checksum etc.)

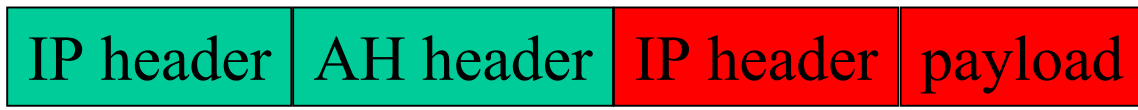
IPsec and NAT

- authenticated
- encrypted+auth*ed*

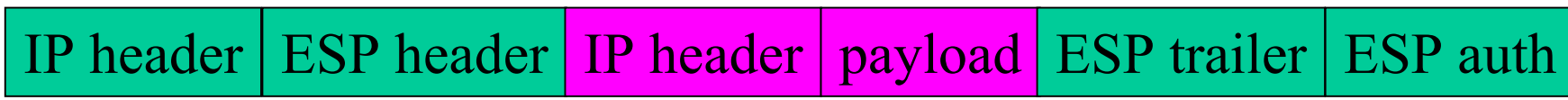


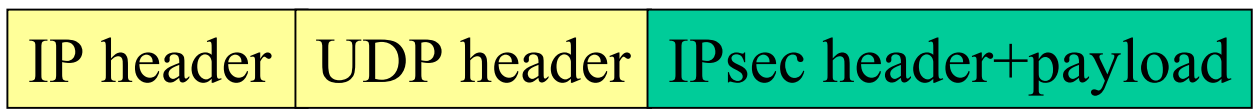
transport mode

- upper-layer header inaccessible
- IP header cannot be modified



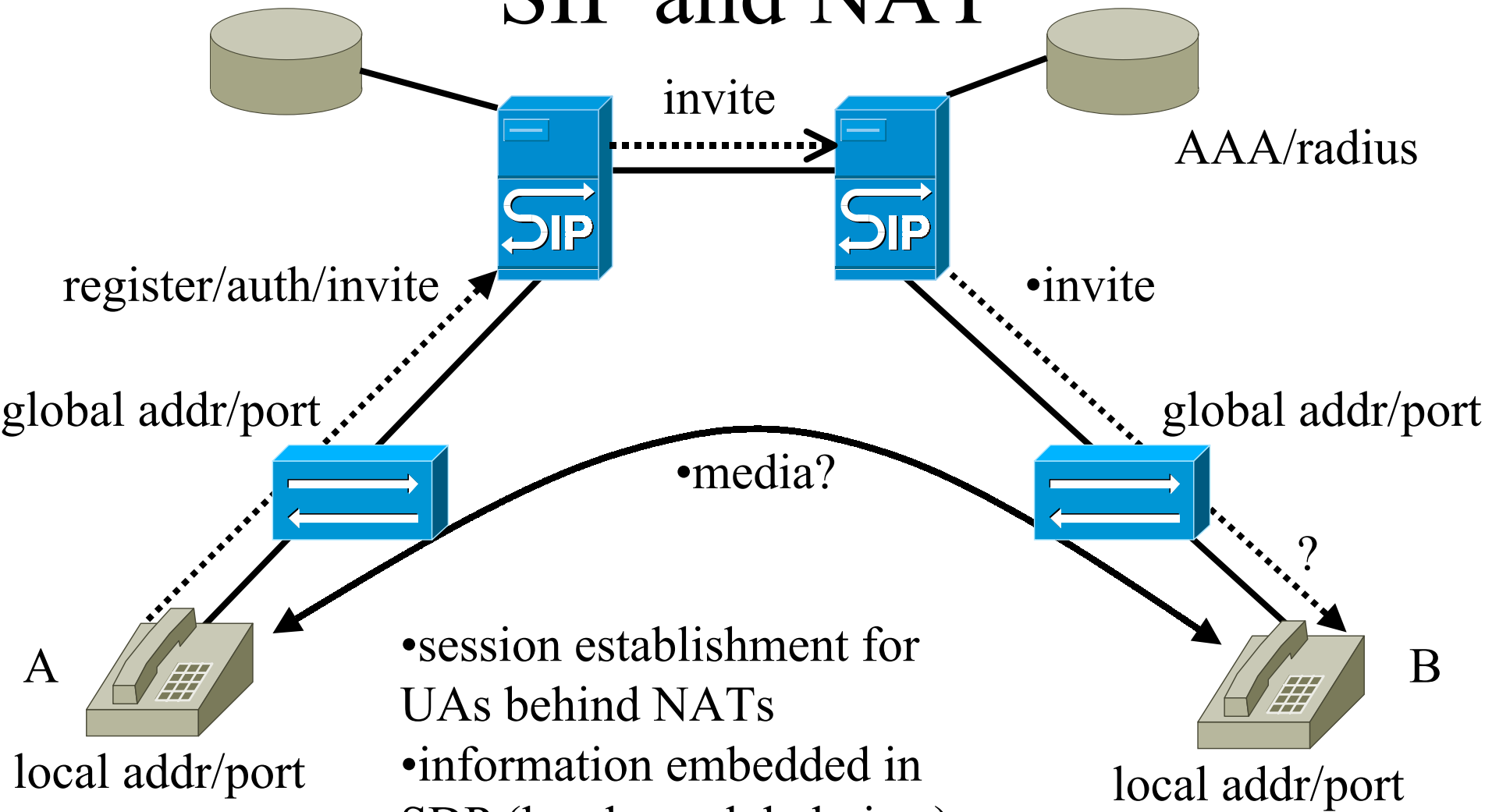
tunnel mode





- UDP-encapsulated IPsec NAT traversal
- MTU discovery?

SIP and NAT



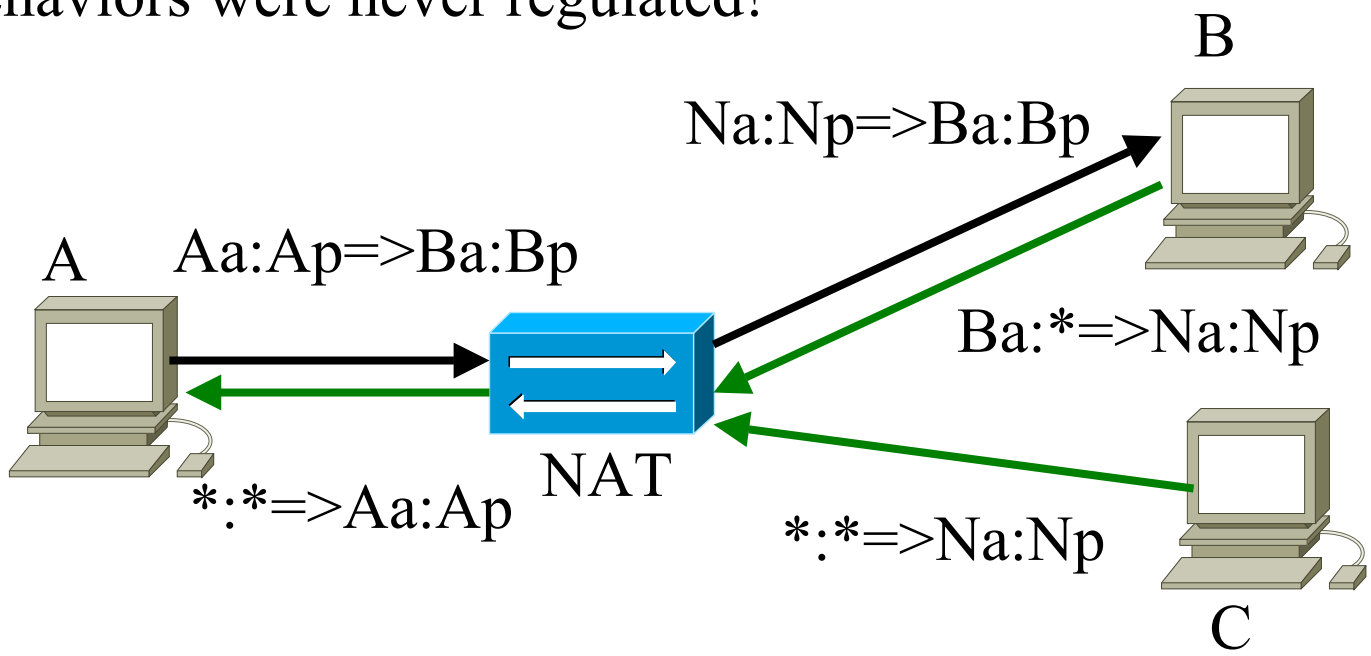
- •session establishment for UAs behind NATs
- •information embedded in SDP (local vs. global view)
- •NAT traversal is still an *open* problem!

Roadmap

- Introduction
  - why IPsec, SIP, and NAT cannot work together
- Why NAT traversal is so difficult?
- NAT traversal approaches
- SIP-assisted NAT traversal
  - with ***ordinary*** applications and NATs and IPsec
- Network reliability & security in a big picture

Types of NATs: full cone

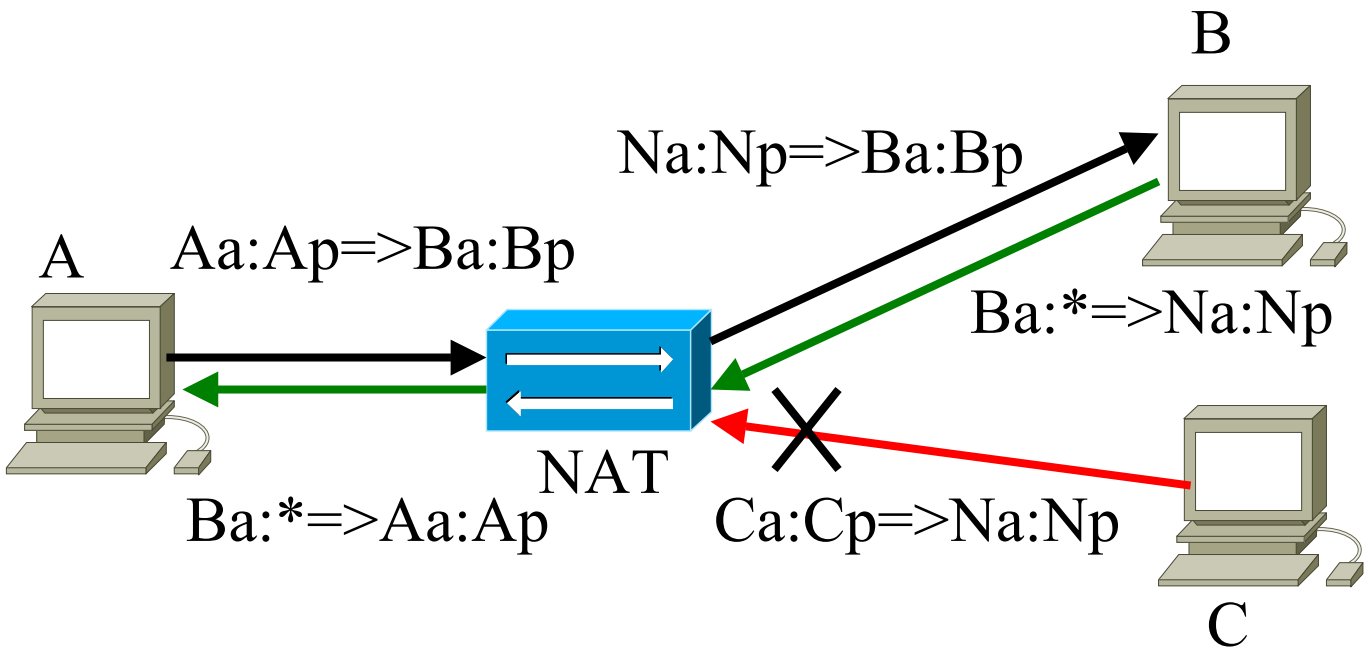
•NAT behaviors were never regulated!



•outgoing mapping: Aa:Ap=>*:* to Na:Np=>*:*

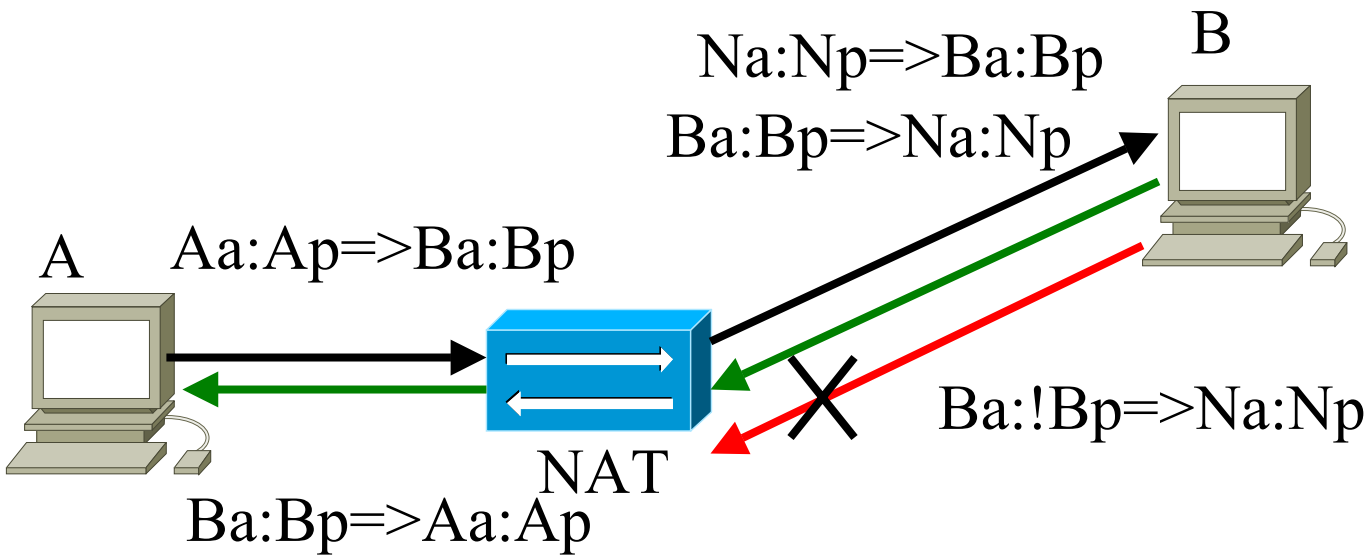
•incoming filtering: *:*=>Na:Np to *:*=>Aa:Ap

(IP) restricted cone



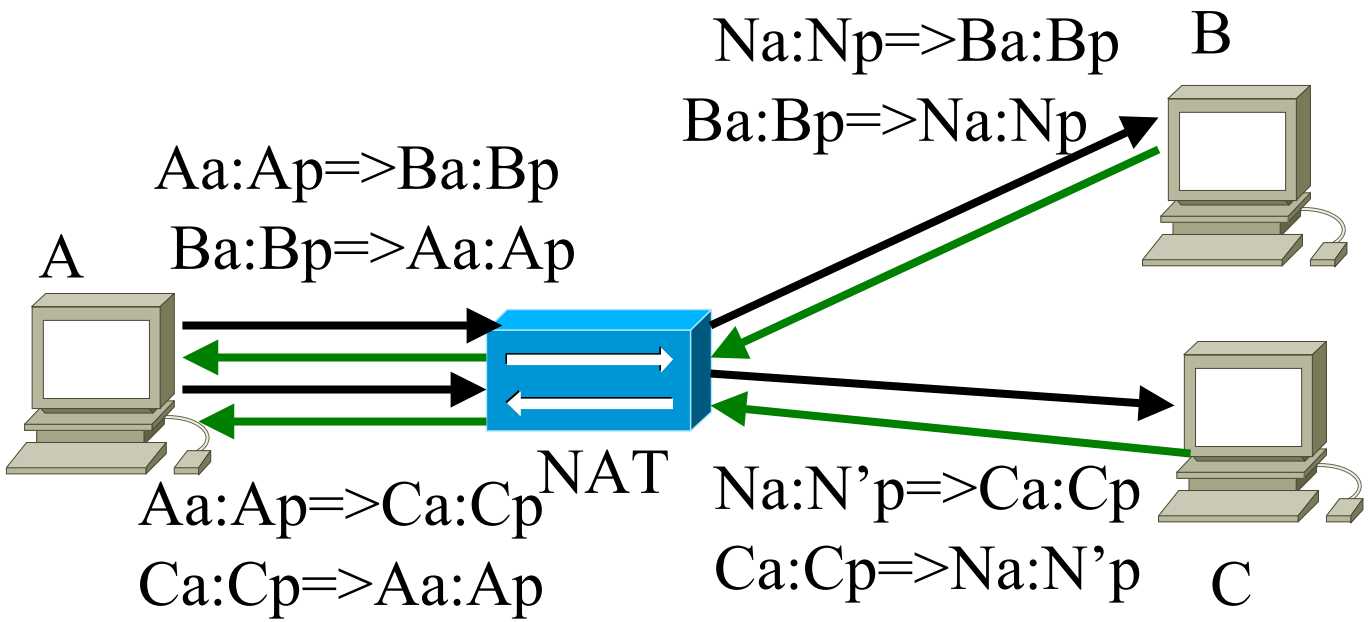
- outgoing mapping: Aa:Ap=>*:* to Na:Np=>x:* (remember x)
- incoming filtering: x:*=>Na:Np to x:*=>Aa:Ap

(IP and) port restricted cone



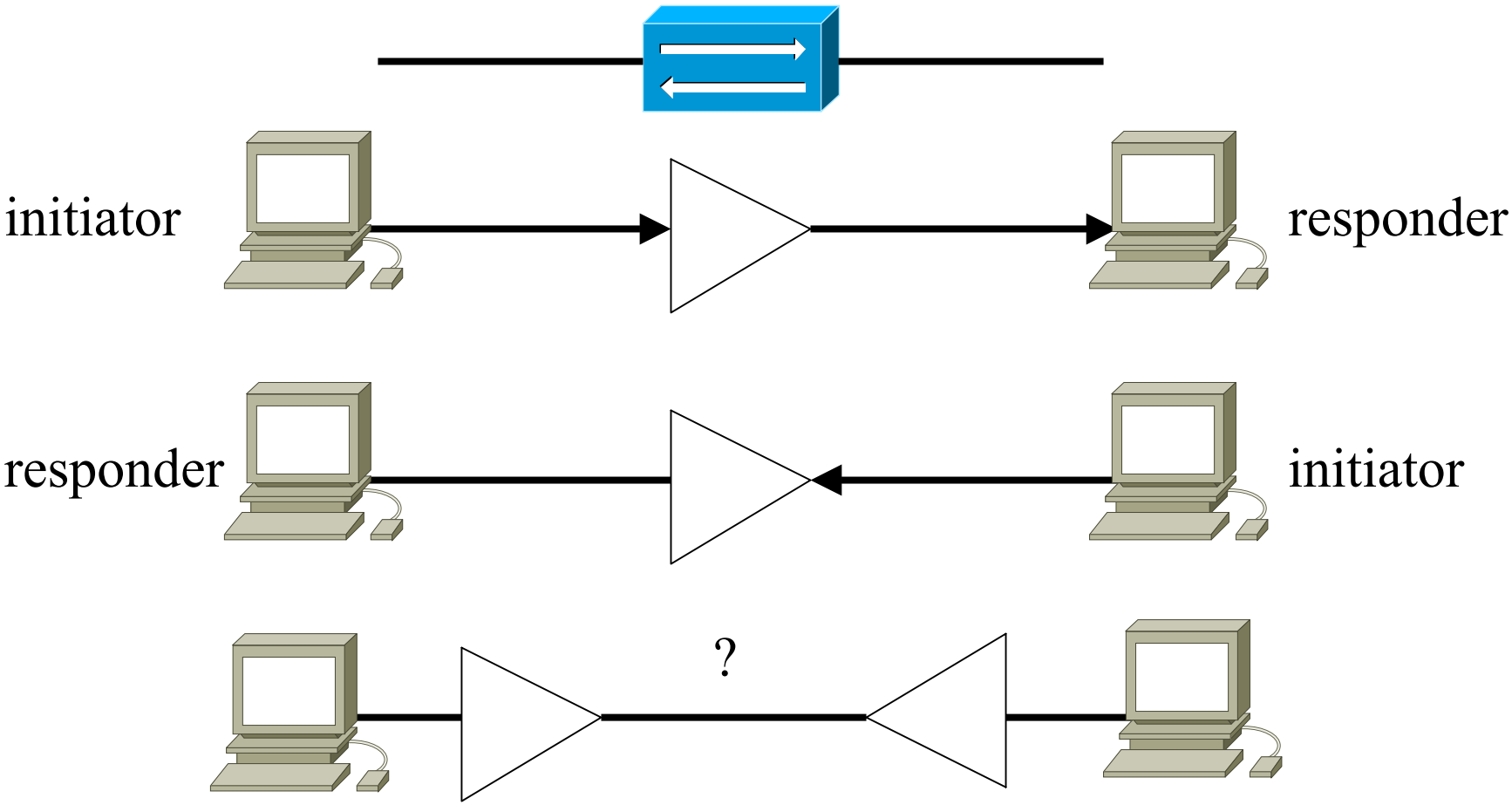
- outgoing mapping: Aa:Ap=>*:* to Na:Np=>x:y (rem x and y)
- incoming filtering: x:y=>Na:Np to x:y=>Aa:Ap

Symmetric NAT



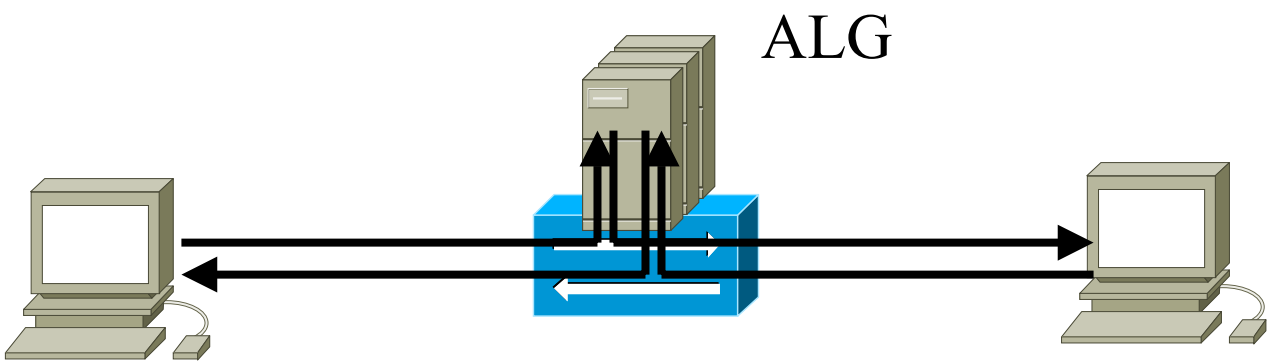
- outgoing mapping: Aa:Ap=>Ba:Bp to Na:Np=>Ba:Bp
- incoming filtering: Ba:Bp=>Na:Np to Ba:Bp=>Aa:Ap

Why NAT breaks things?



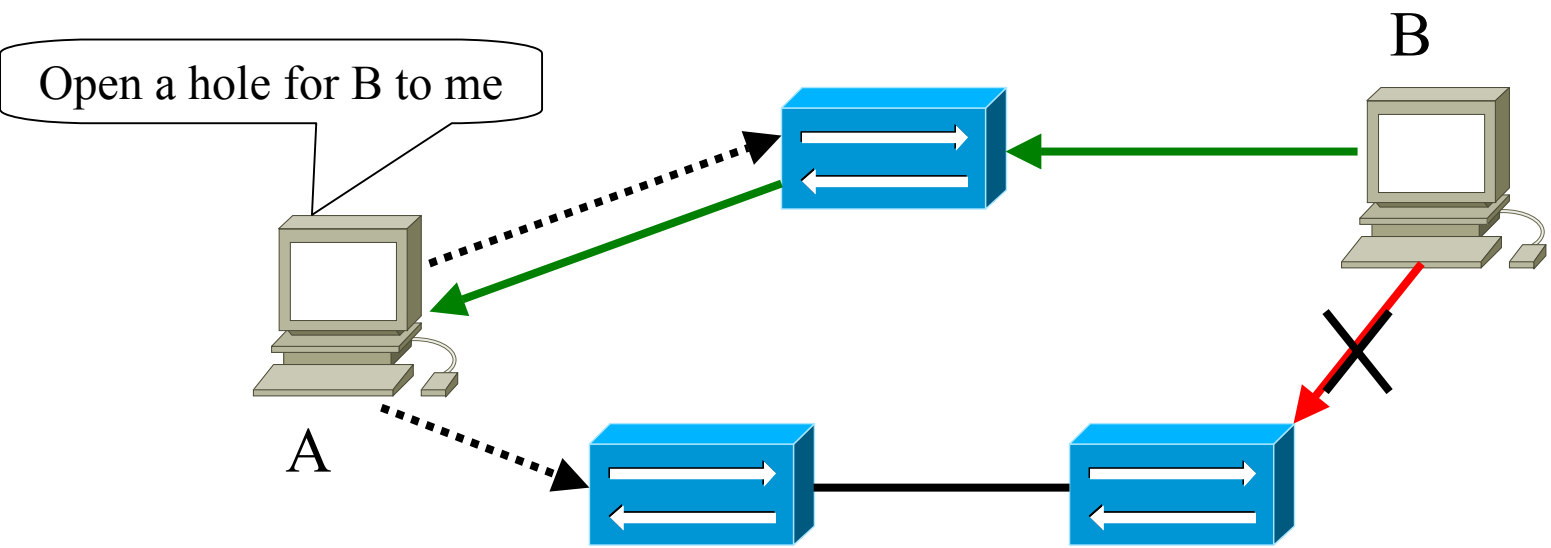
NAT traversal approaches

- Manual configuration
  - static port forwarding at NATs (*always open*)
- Application layer gateway (ALG)
  - proxy or snoop at NATs
  - *application-specific*



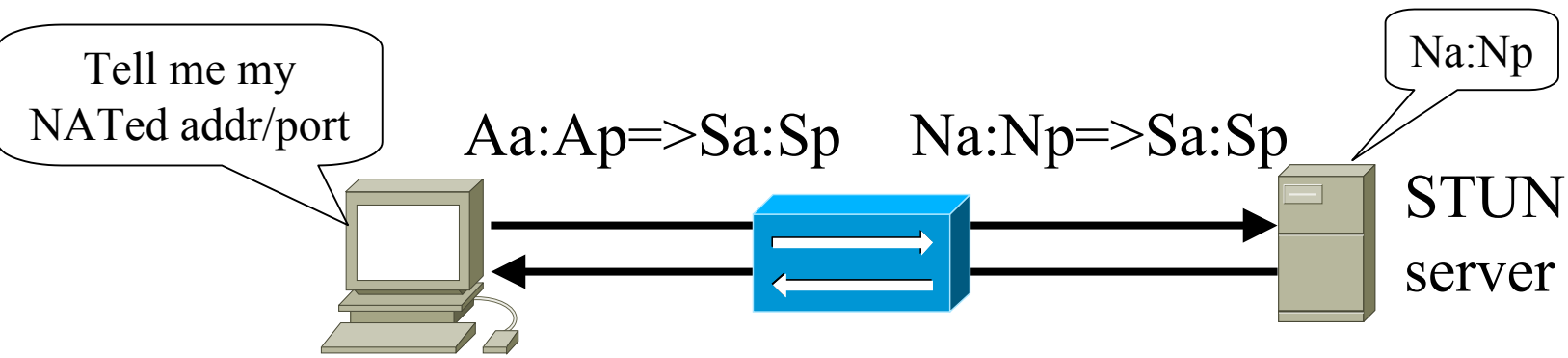
With NAT cooperation

- Universal Plug 'N Play (UPnP)
  - UPnP-aware NATs and clients
  - *security, cascaded NAT, etc.*



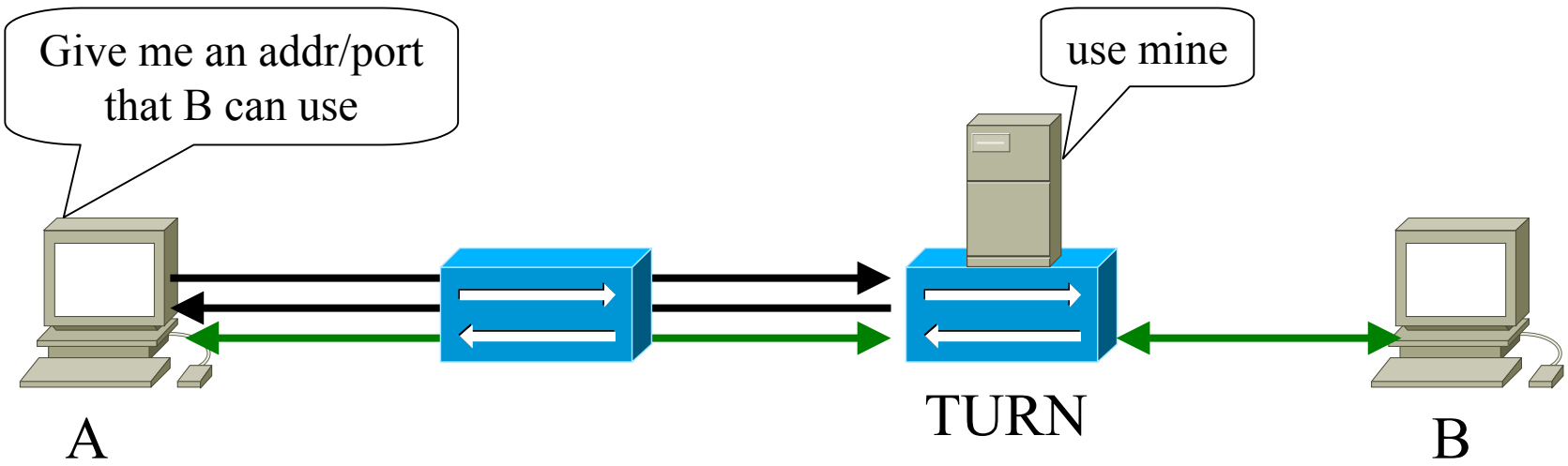
Without NAT cooperation

- Simple Traversal of UDP thru NATs (STUN)
  - probe and learn allocated address/port at NATs
  - work with *many* but not all NATs



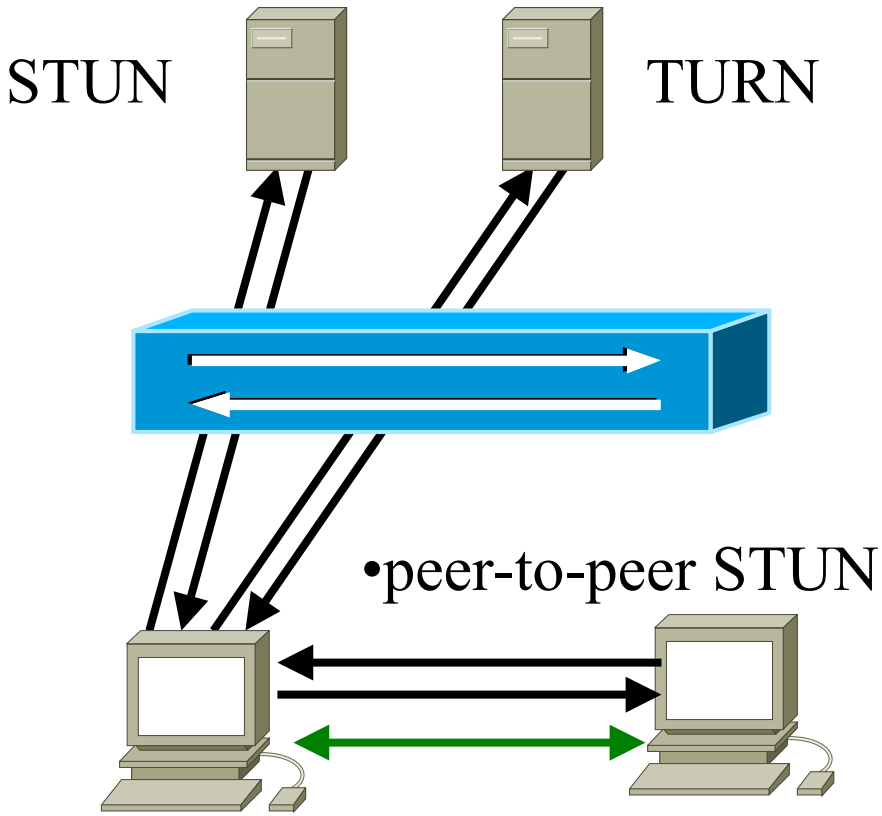
How about one more NAT?

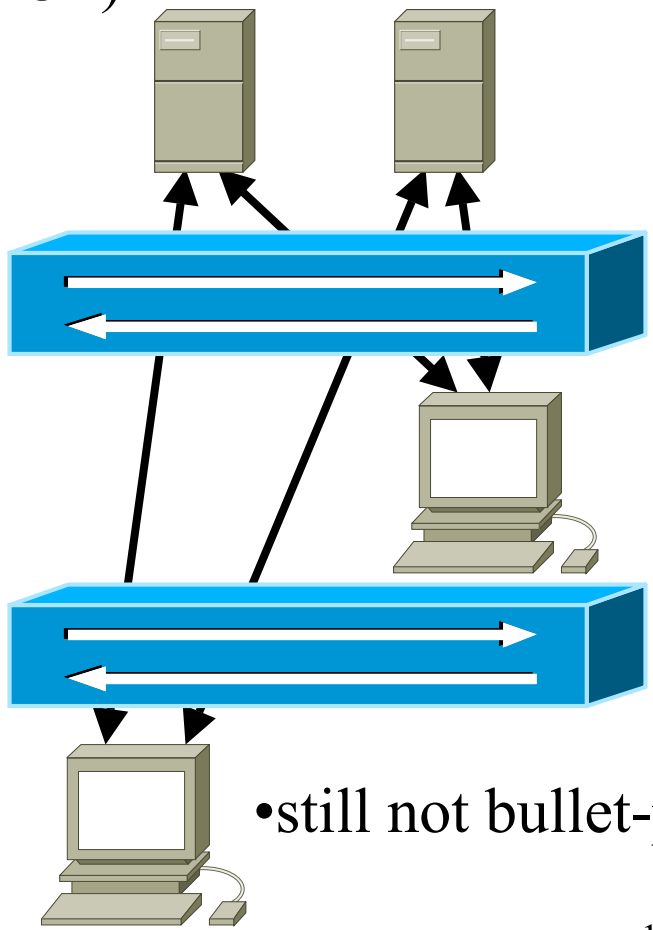
- Traversal Using Relay NATs (TURN)
  - request to allocate address/port at this NAT
  - act as a masquerade relay



Trial and error ...

•Interactive Connectivity Establishment (ICE)



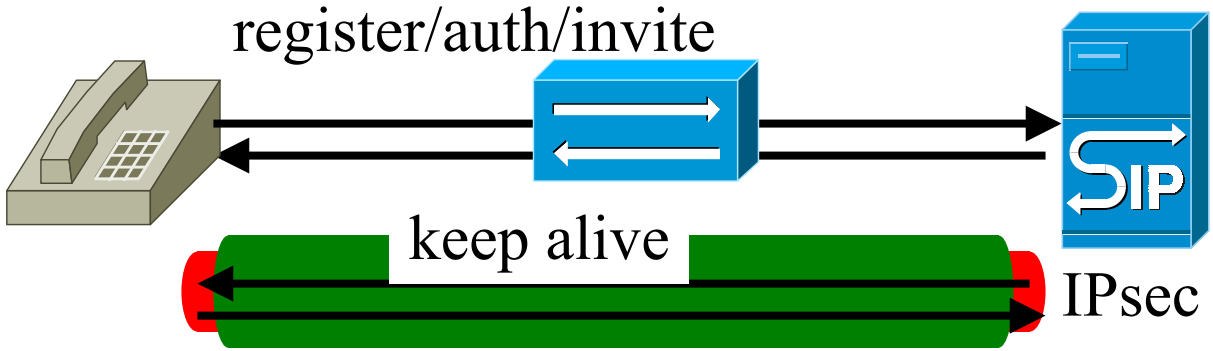


SIP-assisted NAT traversal

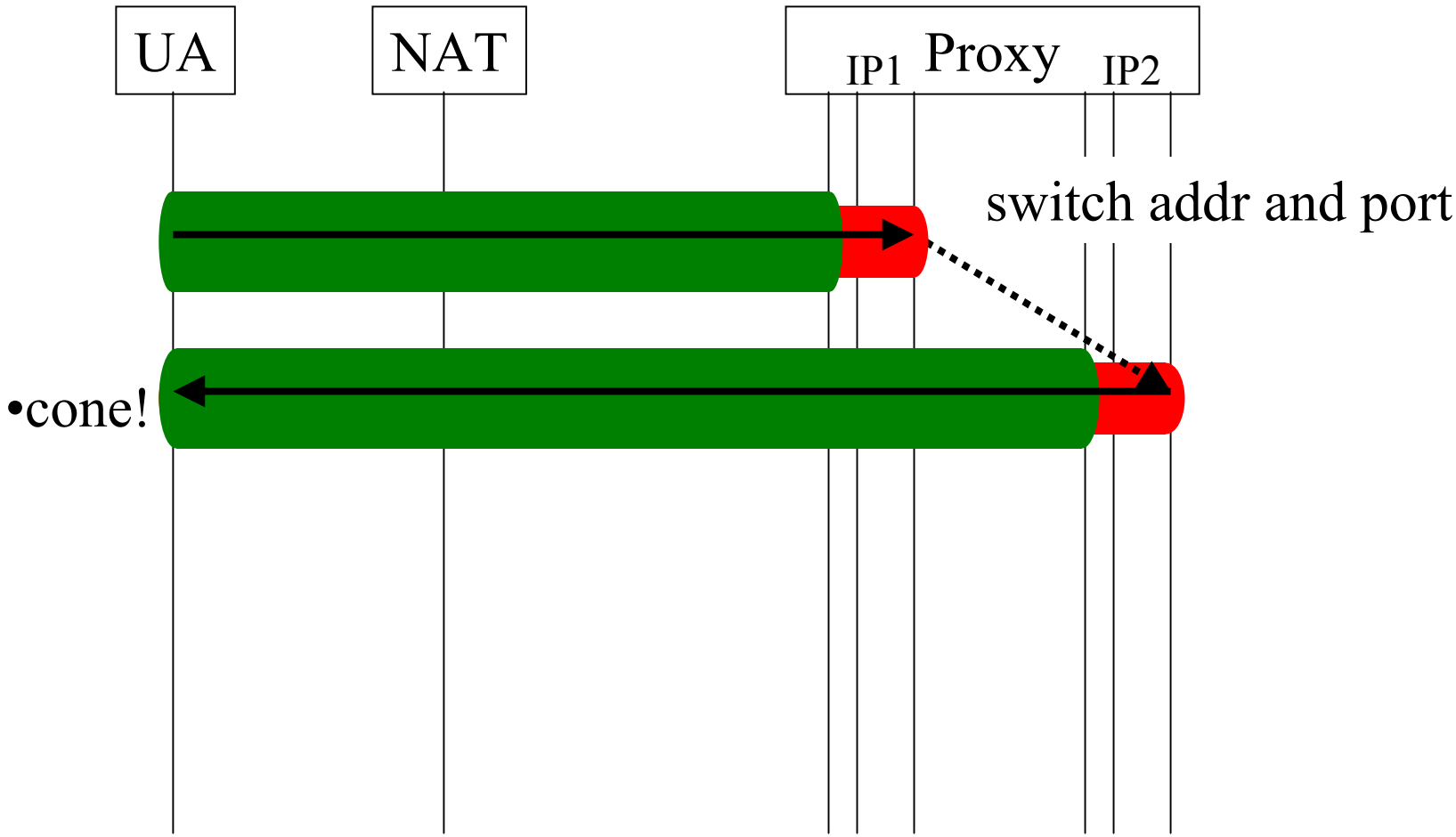
- Why SIP
  - SIP is otherwise NAT-challenged
  - SIP is flexible and extensible
  - SIP may become pervasive
- How NAT traversal with SIP
  - be aware of the existence of NATs
  - determine the type of NATs of the most interest
  - establish sessions btw UAs w/ the help of proxy

UA-Proxy NAT traversal

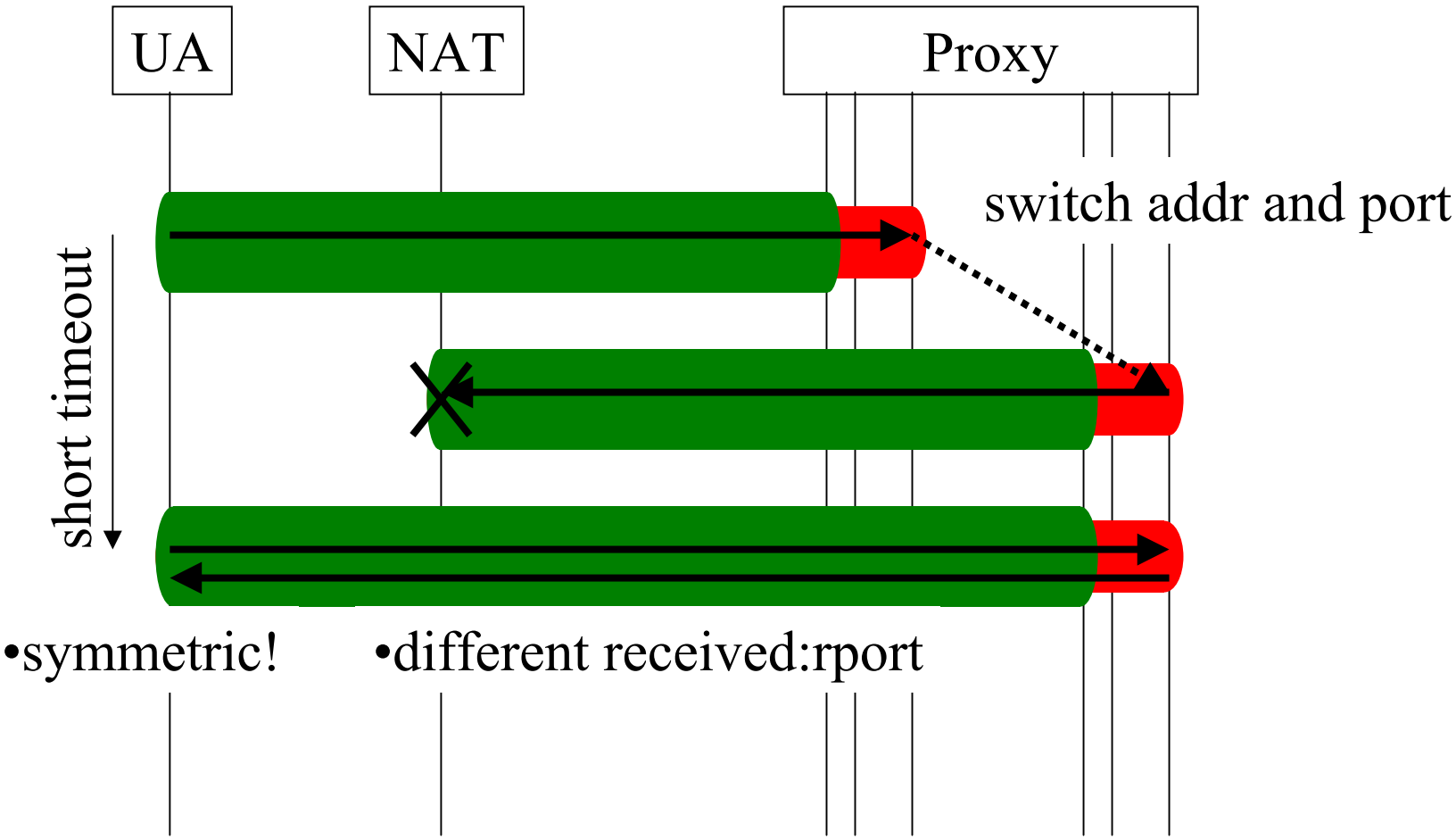
- Symmetric Response Routing (SRR)
  - UA (x.x.x.x:x)
  - Proxy
    - return received=y.y.y.y;rport=y in SIP attributes
  - UA: if x!=y, there is NAT(s)!



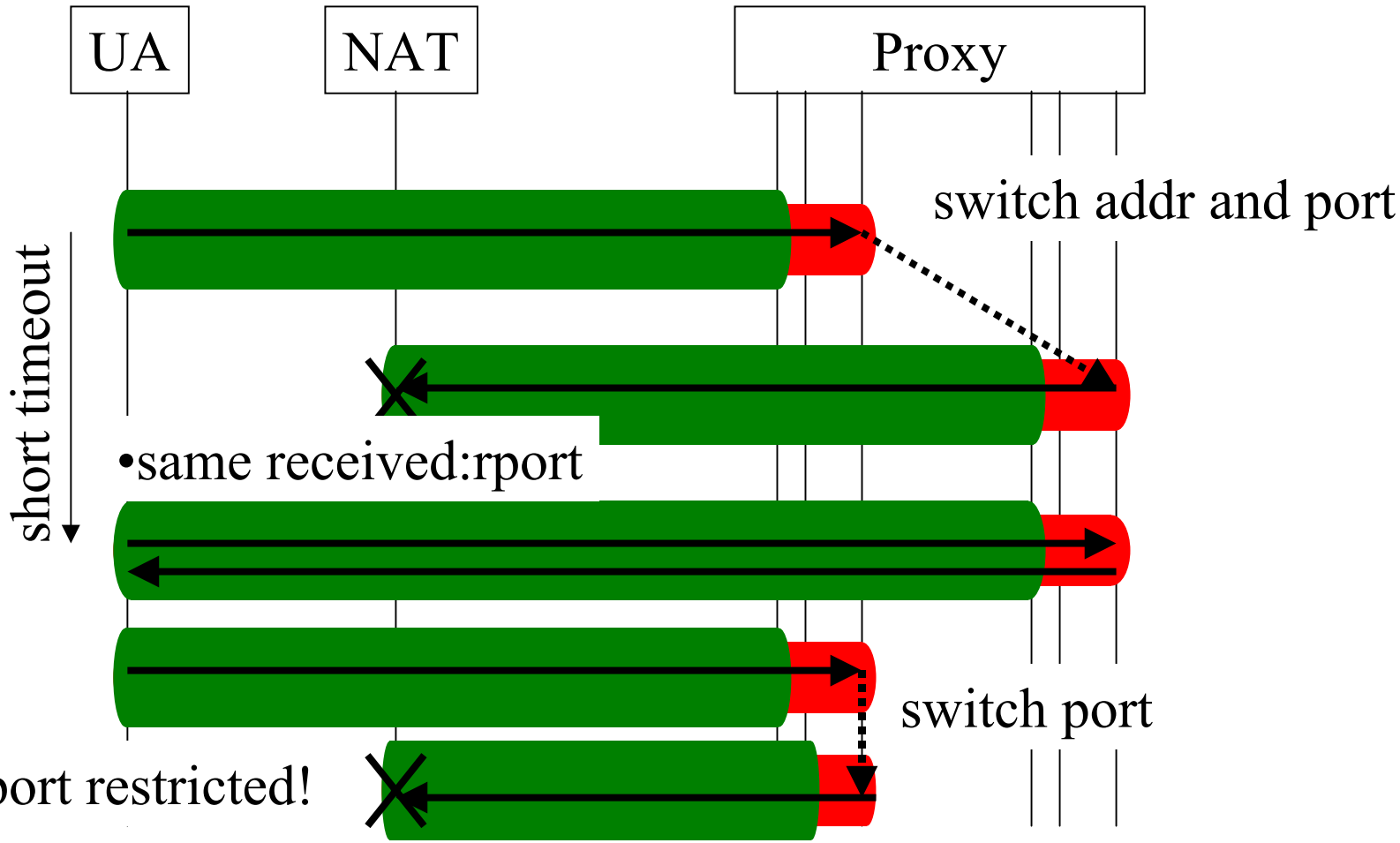
UA-Proxy STUN: cone



UA-Proxy STUN: symmetric



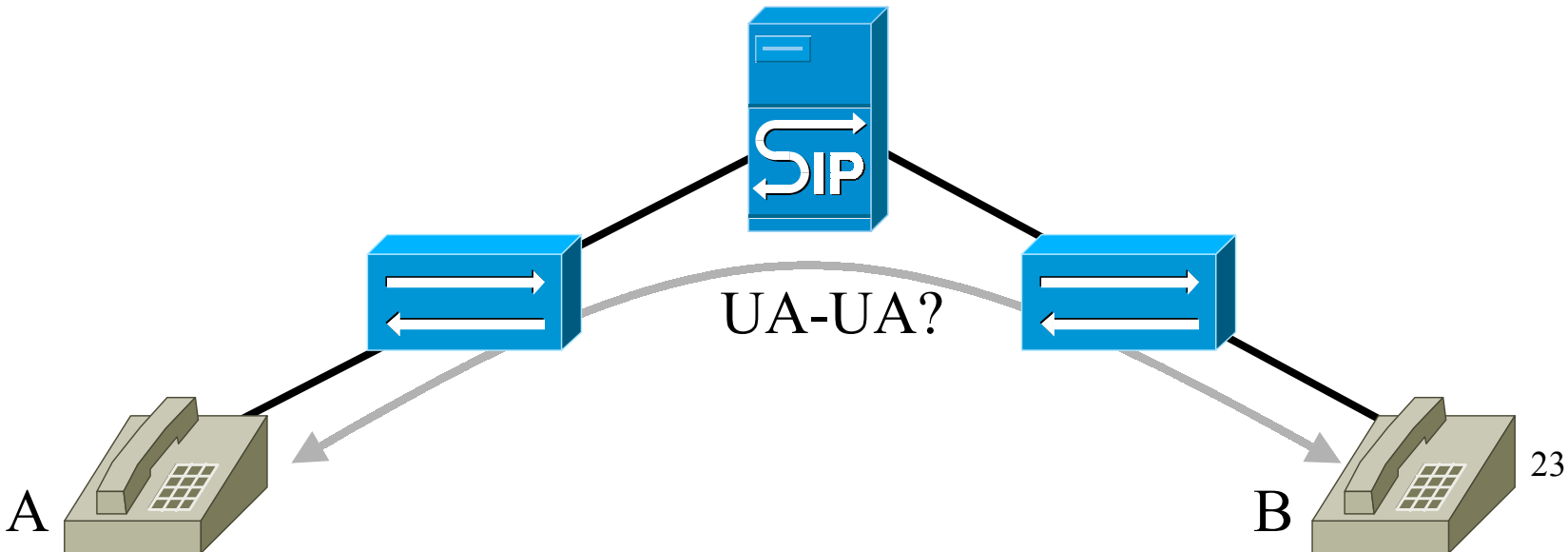
UA-Proxy STUN: restricted



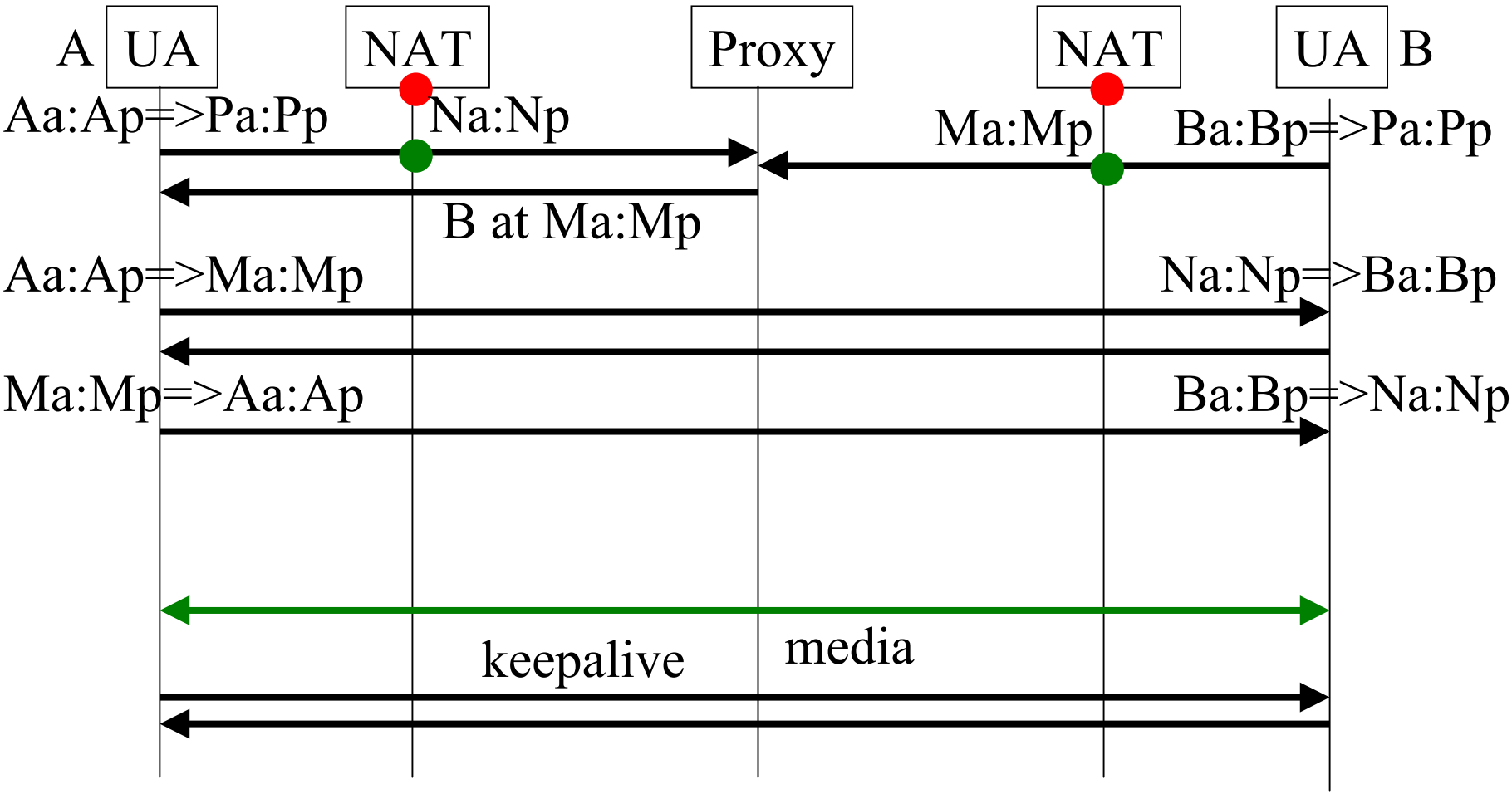
•otherwise, (IP) restricted!

UA-UA: 4x4

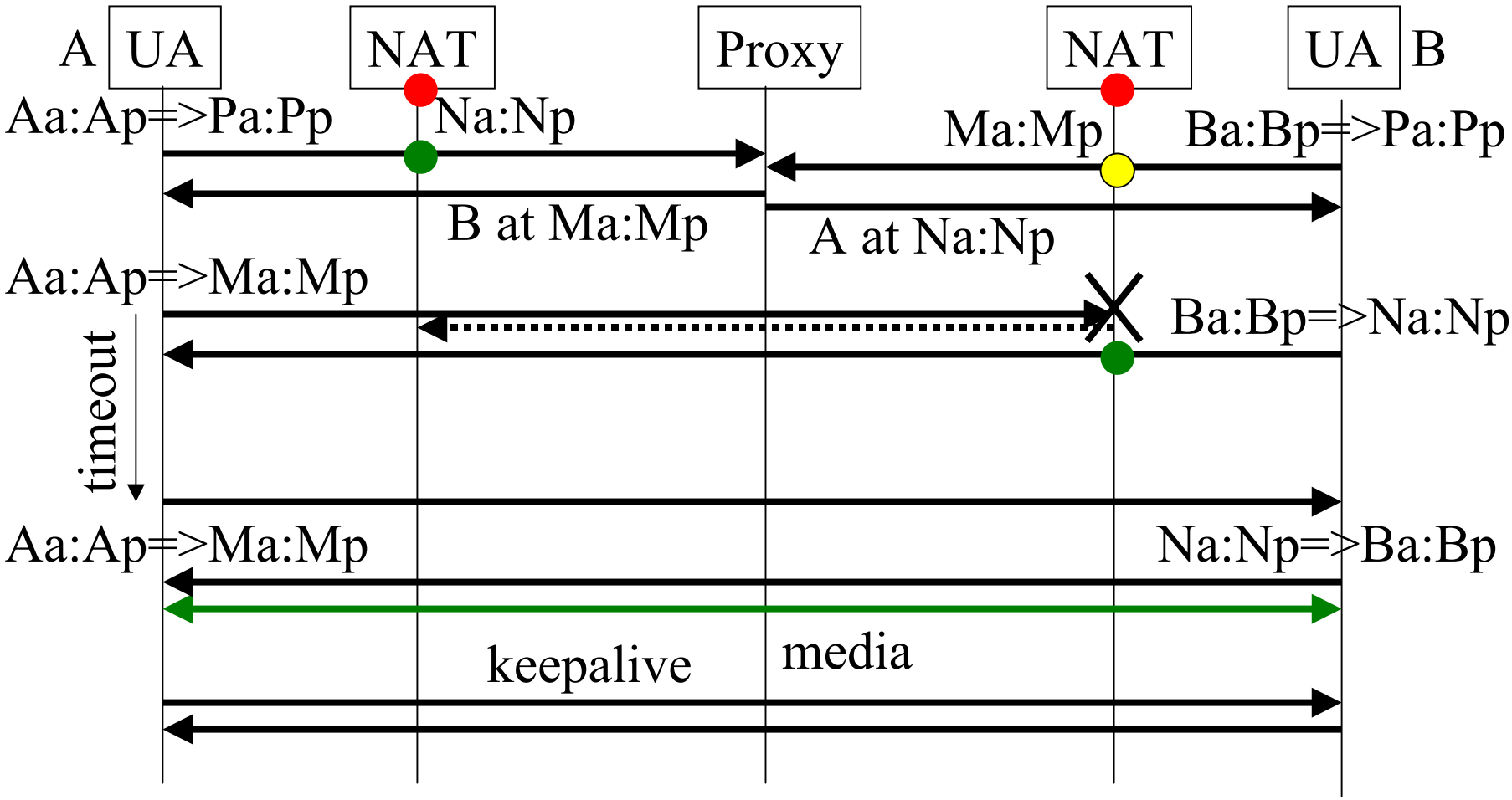
A \ B	cone	IP restricted	port restricted	symmetric
cone	√	√	√	√
IP restricted		√	√	√
port restricted			√	√
symmetric				?



UA-UA: cone-cone

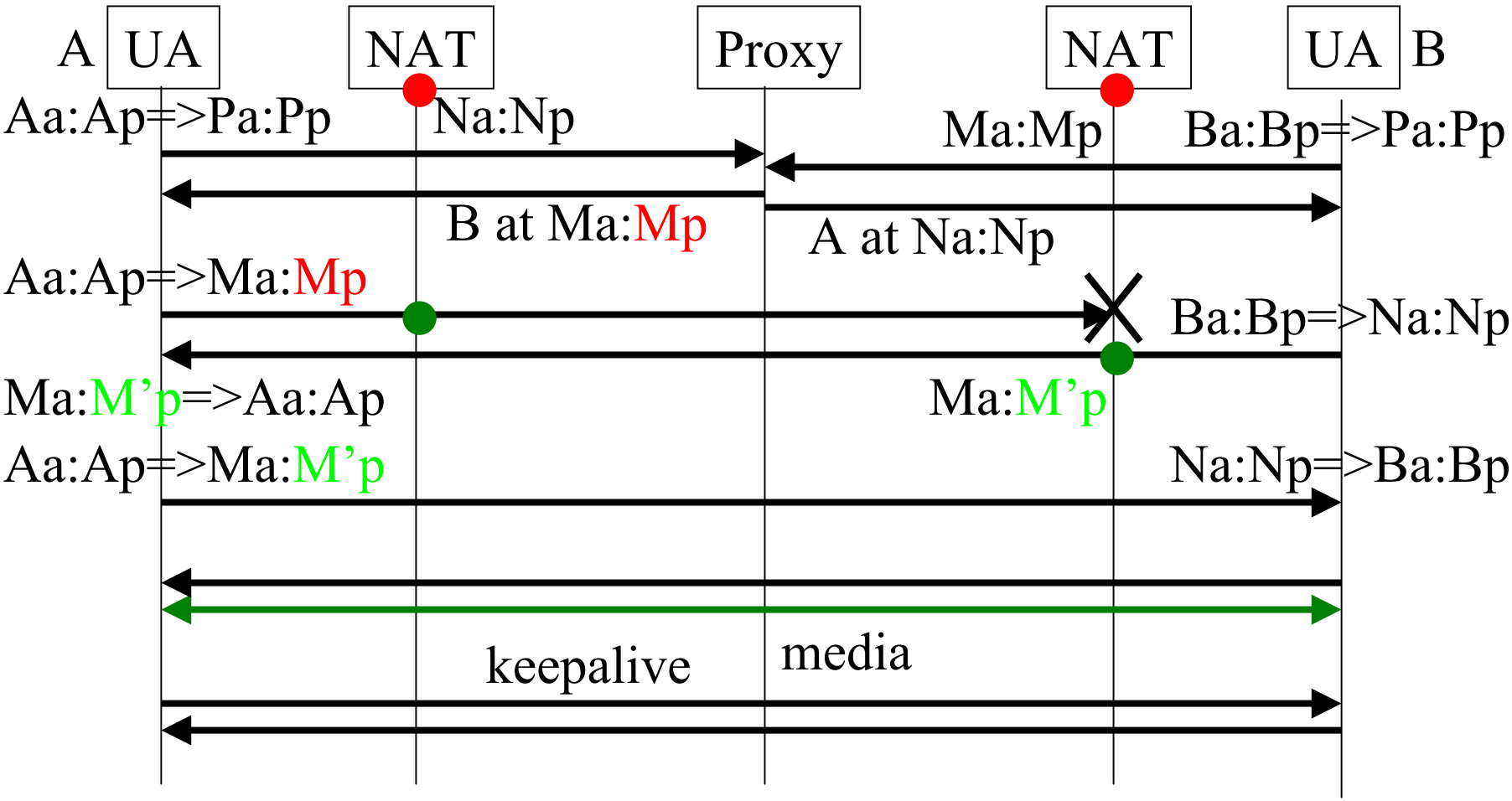


UA-UA: cone/restricted-restricted

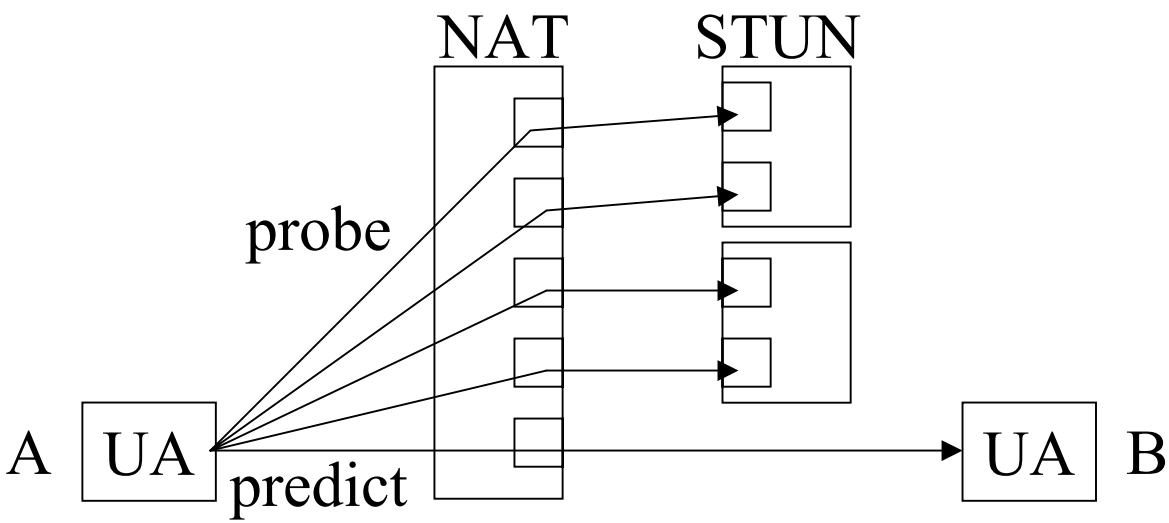


•ICMP messages?

UA-UA: cone/restricted-symmetric

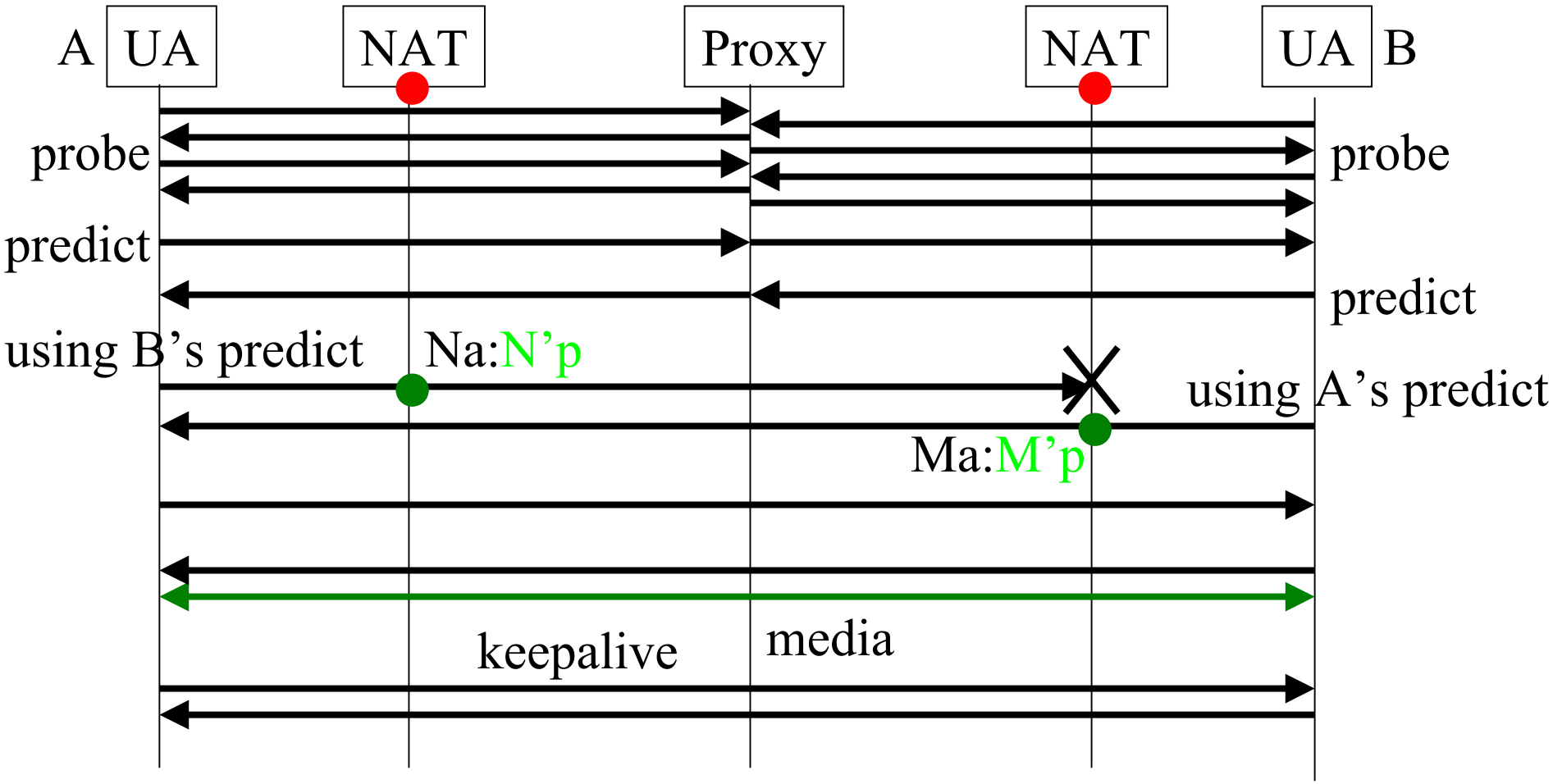


A close look at symmetric NATs

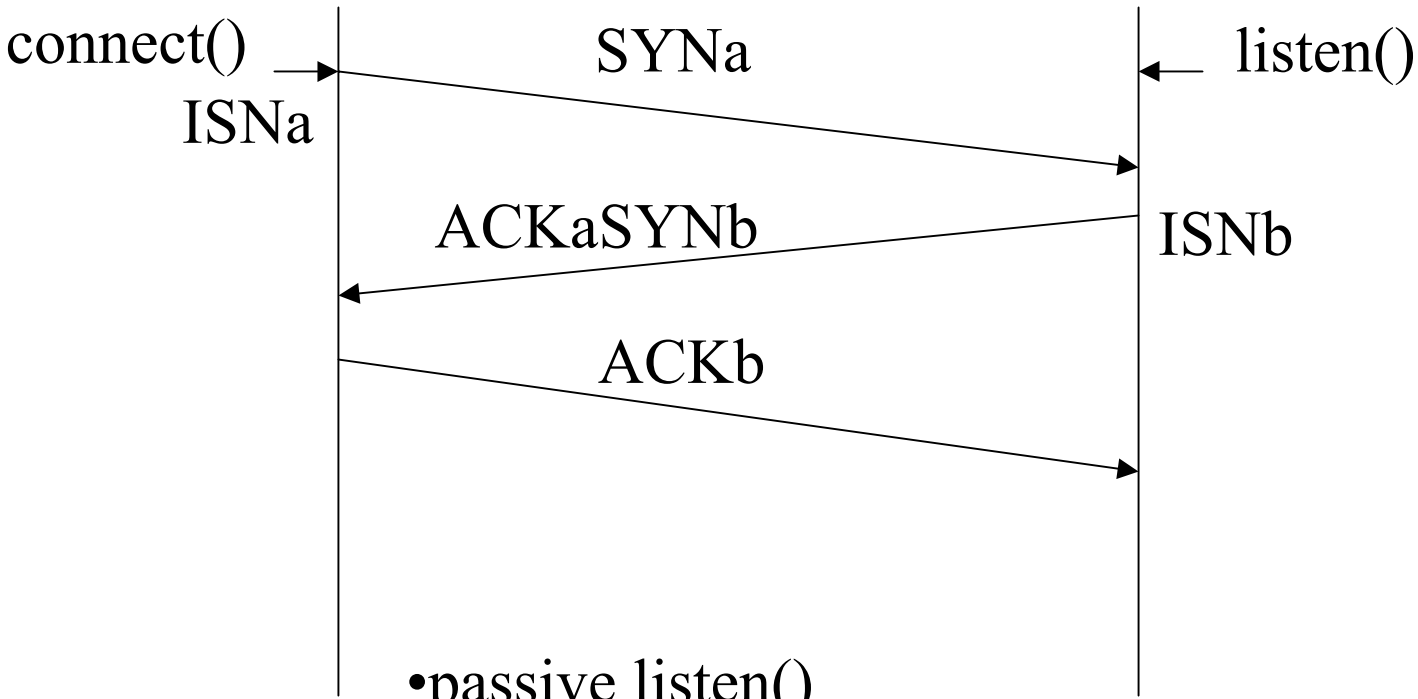


- many symmetric NATs have predictable port allocation

UA-UA: symmetric-symmetric

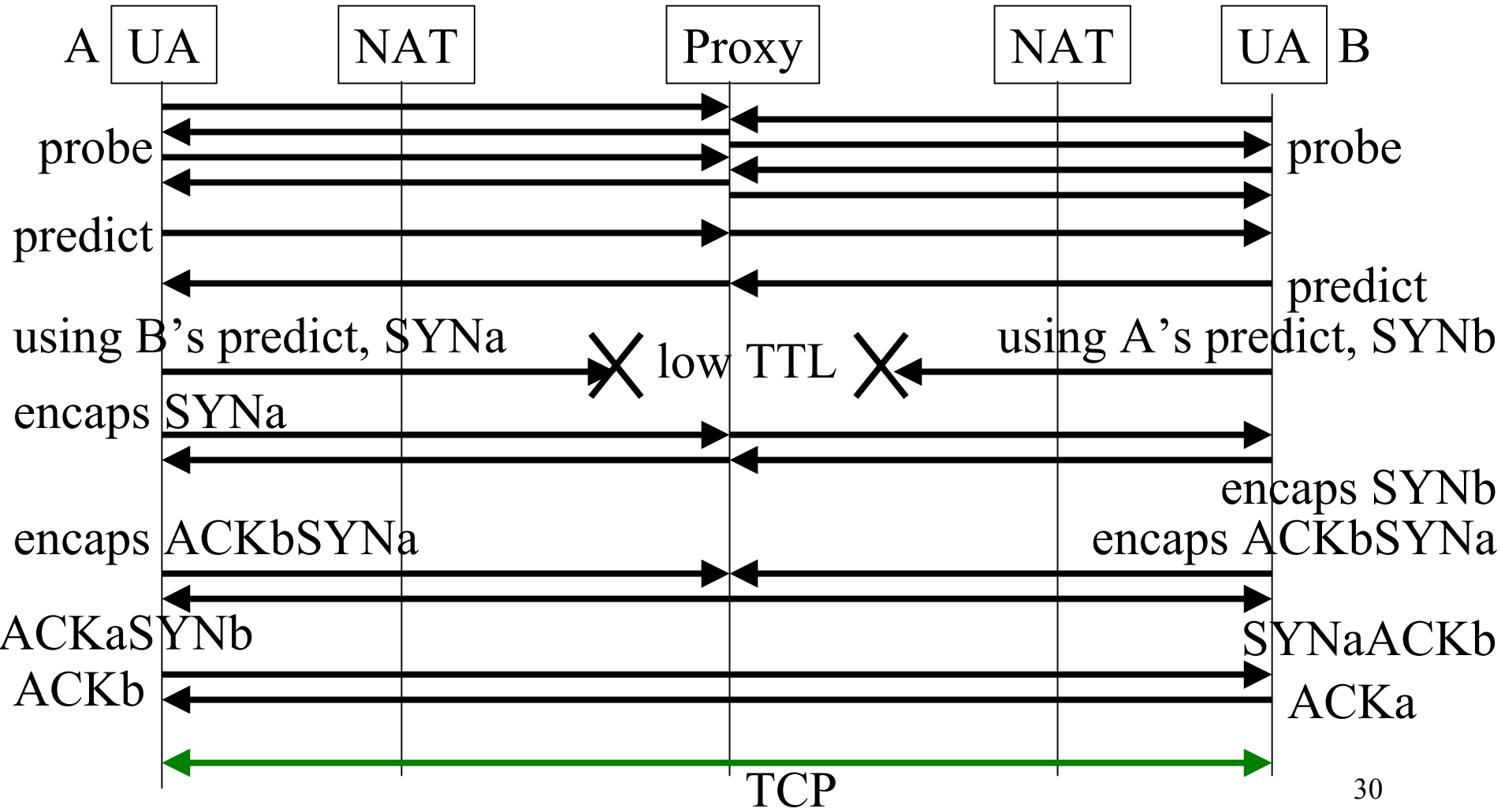


How about TCP



- passive listen()
- active connect()
- sequence number matters!

UA-UA: TCP/NUTSS



TCP: more issues

- UDP-encapsulated TCP/IPsec NAT traversal
  - port uniqueness
- Port allocation at UA
  - TCP-based
- Port allocation at NAT
  - UDP-based
- mix and match
  - multi-UA behind the same NAT

SIP-assisted NAT traversal

- SIP becomes versatile
  - such as XML/HTTP for data transfer
- SIP protocol can be extended to support NAT traversal
  - more signaling attributes
- SIP proxy can play an important role in assisting NAT traversal
  - already exists; may become ubiquitous; why not use it for extra purpose?

Thanks!

- Q&A?