פרק 11

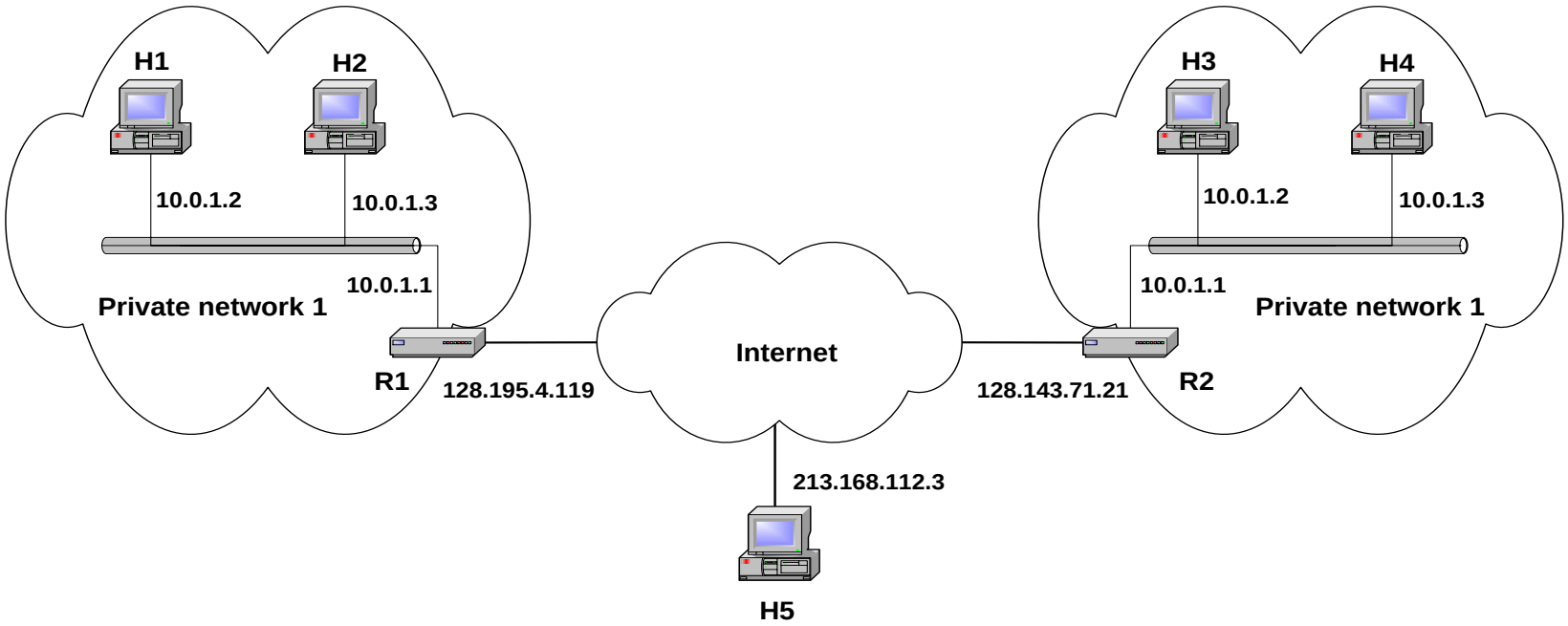
- Private Networks
- What is NAT?
- NAT types
- NAT and VoIP Challenges
- NAT Traversal solutions and positioning
- UPnP (Universal Plug and Play)
- External Query Method
- STUN, TURN and ICE

Private Network

- Private IP network - an IP network which is **not directly connected** to the Internet
- IP addresses in a private network can be **assigned arbitrarily**
  - Not registered and not guaranteed to be globally unique
- Private networks use non-routable addresses

10.0.0.0 – 10.255.255.255	**10.x.x.x**
172.16.0.0 – 172.31.255.255	**172.16.x.x-172.31.x.x**
192.168.0.0 – 192.168.255.255	**192.168.x.x**

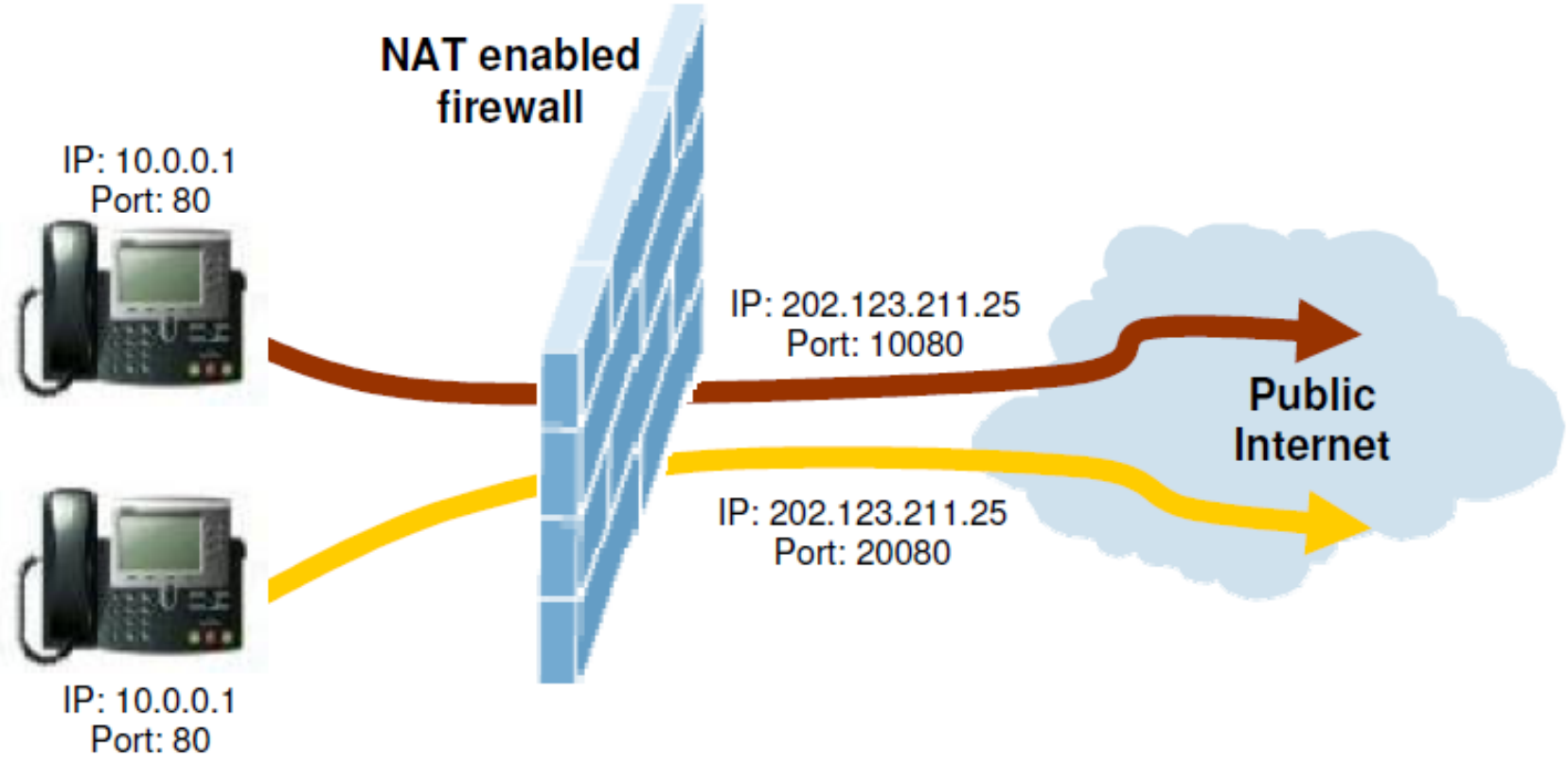
Private Addresses



NAT- Network Address Translation

- In the mid-1990s NAT became a popular tool for overcome the IPv4 address exhaustion
- It has become a standard, indispensable feature in routers for home and small-office Internet connections
- Enables multiple hosts on a private network to access the Internet using a single public IP address

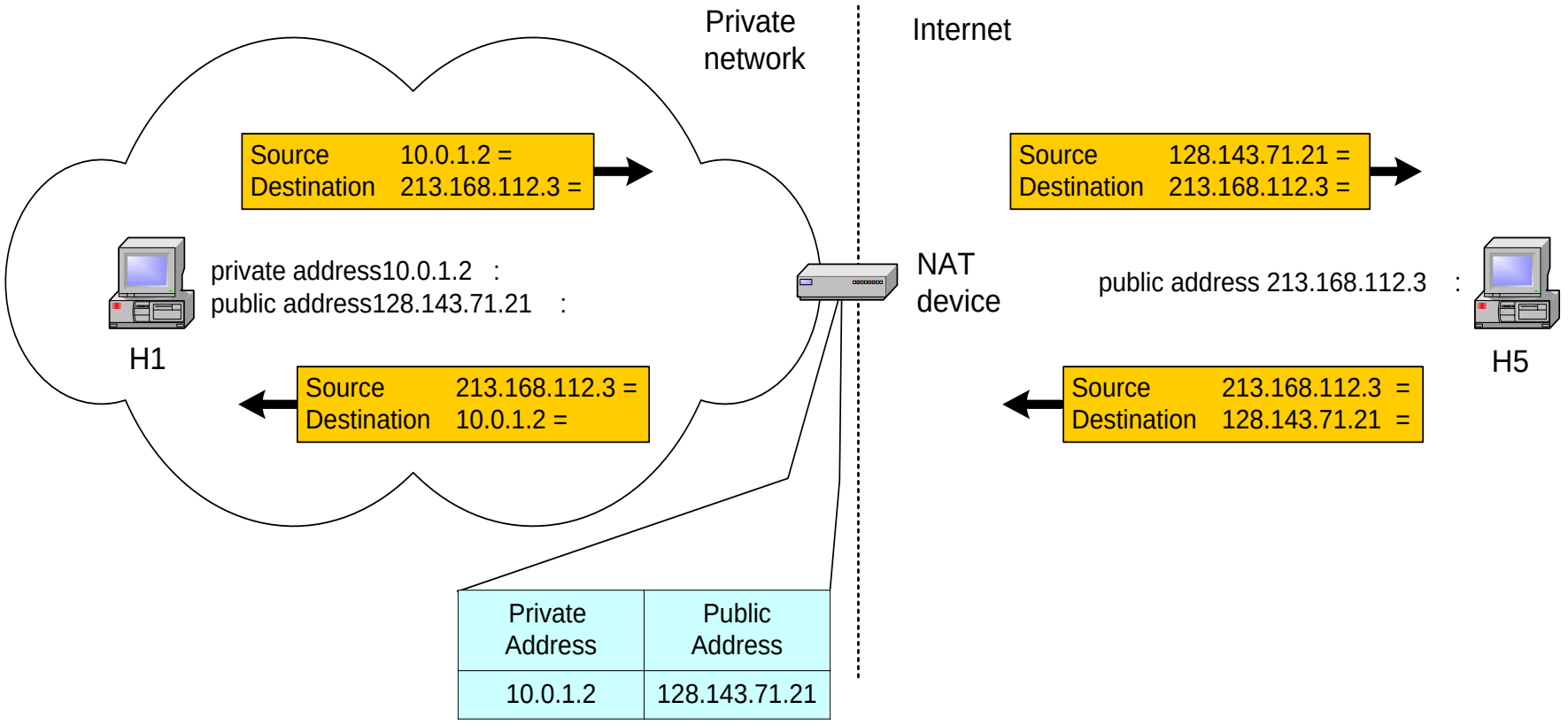
NAT Schematic



NAT functionality

- IP addresses and/or port numbers of IP datagrams are replaced at the boundary of a private network
- Manipulates the source or destination IP address and usually also the TCP/UDP port numbers of IP packets
- Checksums (both IP and TCP/UDP) must also be rewritten to take account of the changes

Basic operation of NAT



- **NAT device has address translation table**

Basic NAT and PAT

- Two levels of network address translation
  - Basic NAT. This involves IP address translation only, not port mapping
- PAT (Port Address Translation) or Network Address Port Translation, NAPT
  - Translation of both IP addresses and port numbers
- All Internet packets have a source IP address and a destination IP address
  - Both or either of the source and destination addresses may be translated

Port Manipulation

- Some Internet packets do not have port numbers
  - For example, ICMP packets have no port numbers
- The vast bulk of Internet traffic is TCP and UDP packets, which do have port numbers
  - Packets which do have port numbers have both a source port number and a destination port number
  - Both or either of the source and destination ports may be translated

NAT Types

SNAT and DNAT

- **SNAT** - translats the source IP address and/or source port
  - Re-writes the IP address and/or port number of the IP-Device which originated the packet
- **DNAT** - translats the destination IP address and/or destination port number
  - Re-writes the IP address and/or port number corresponding to the destination IP-Device
- SNAT and DNAT may be applied simultaneously to Internet packets

NAT Types

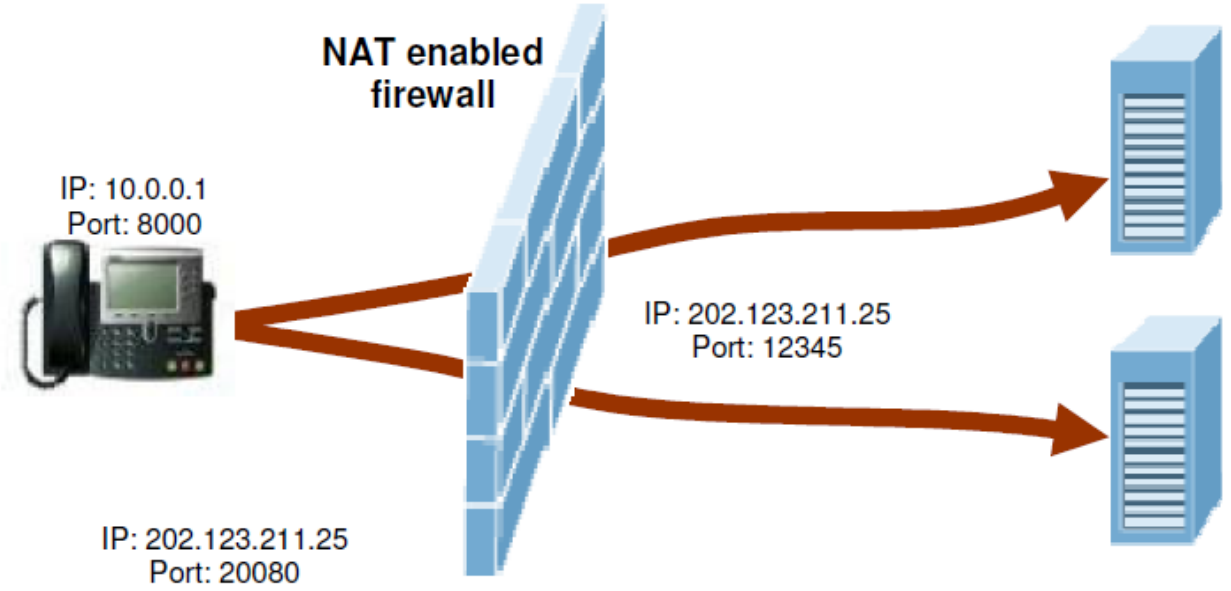
- There are four types of NATs
  1. Full Cone
  2. Restricted Cone
  3. Port Restricted Cone
  4. Symmetric

- The First three types of NAT maintain a mapping that is independent of the destination address

- The fourth type allocates a new mapping for each independent destination address

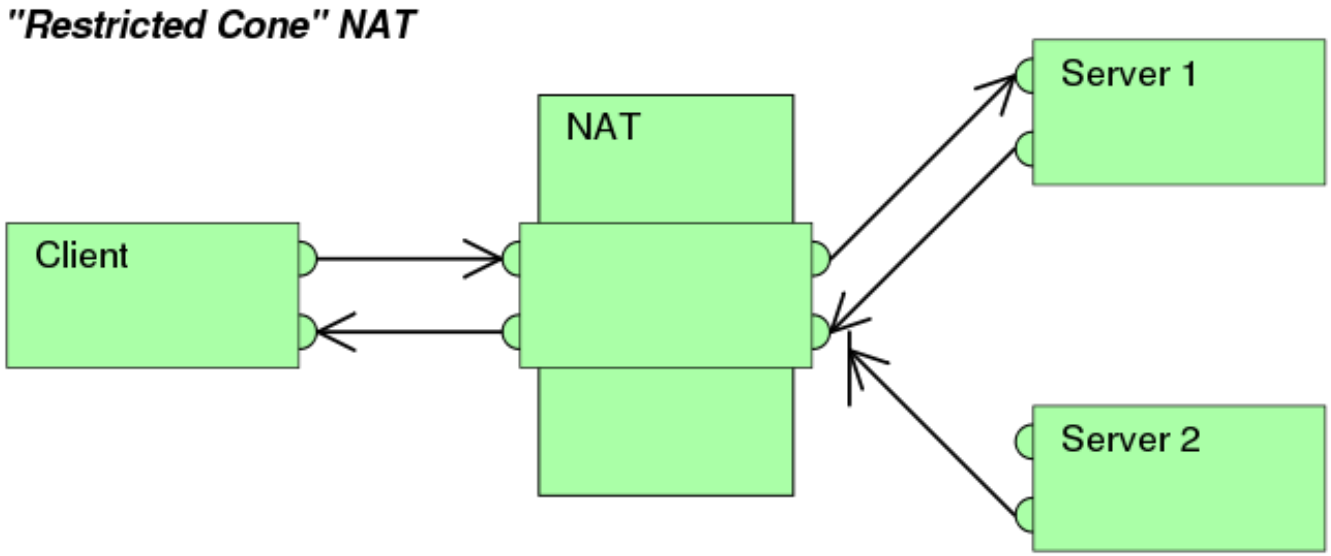
Full Cone NAT

- Once an internal address (iAddr: iPort) is mapped to an external address (eAddr: ePort)
  - any packets from iAddr: iPort will be sent through eAddr: ePort
- **Any external host** can send packets to iAddr: iPort by sending packets to eAddr: ePort



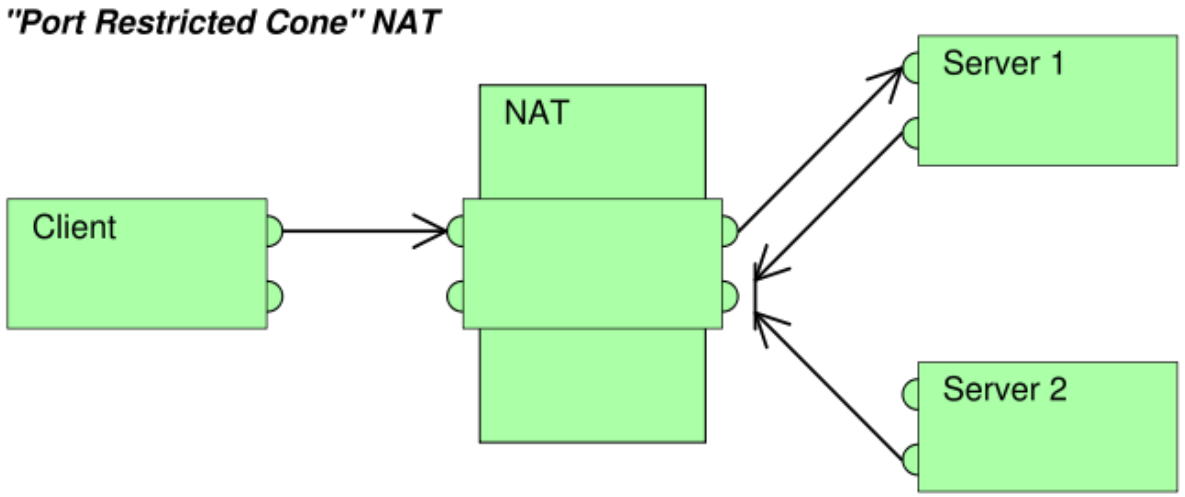
Restricted Cone NAT

- An external host (**hAddr: any**) can send packets to iAddr: iPort
  - by sending packets to eAddr: ePort only if iAddr: iPort had previously sent a packet to hAddr: *any*
  - "any" means the port number doesn't matter



Port-Restricted Cone NAT

- Like a **Restricted cone NAT**, but the restriction includes port numbers
- An external host (**hAddr: hPort**) can send packets to iAddr: iPort
  - by sending packets to eAddr: ePort only if iAddr: iPort had previously sent a packet to hAddr: hPort

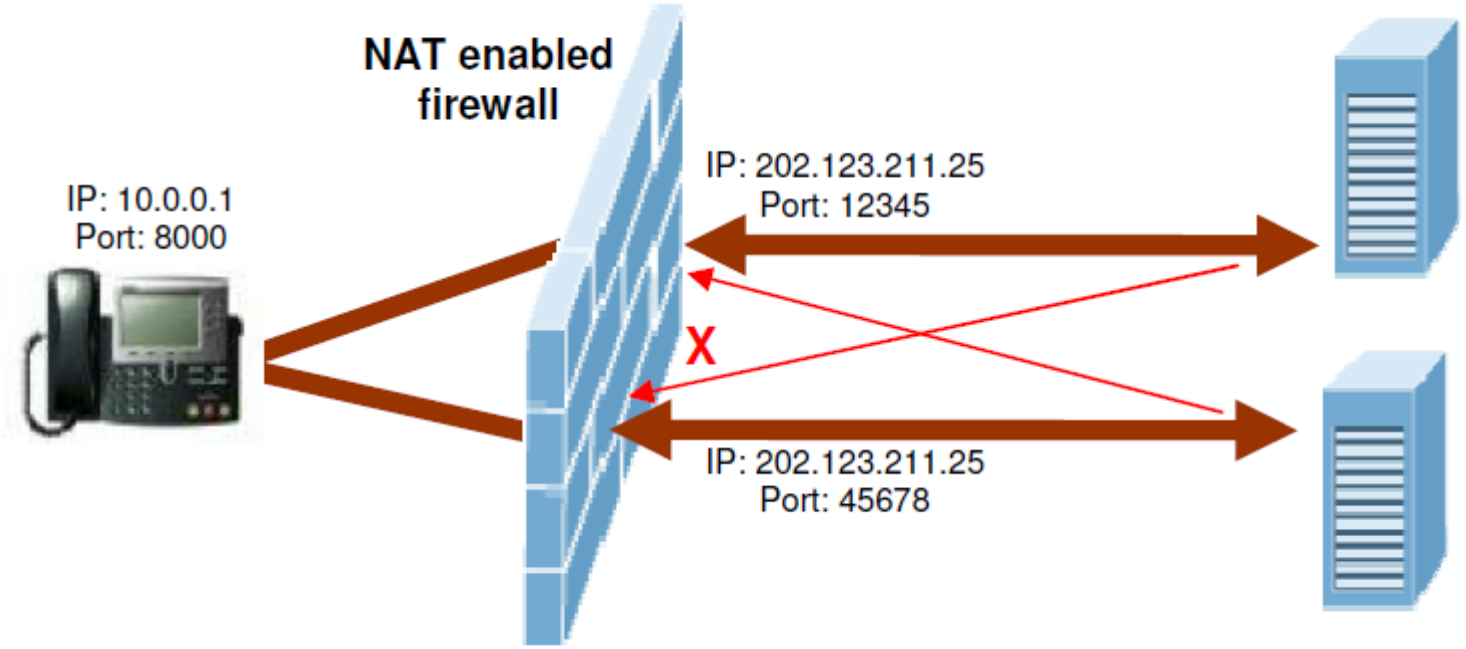


Symmetric NAT

- Each request from the same iAddr: iPort to a specific destination IP address and port
  - Is mapped to a unique external source IP address and port (this is ambiguous)
  - If the same internal host sends a packet even with the same source address and port but to a different destination, a different mapping is used

Symmetric NAT (cont.)

- Only an external host that receives a packet from an internal host can send a packet back



SIP and NAT Challenge

- NAT breaks the originally envisioned model of IP end-to-end connectivity across the Internet
  - Introduces complications in communication between hosts, and affects performance
- Two parts in a SIP based call
  - Signalling
  - Media stream

SIP Signalling

- SIP signaling messages can easily traverse NAT
  - SIP proxy needs to return SIP packets on the same port it received from the client
- Special tags in SIP message header: **received tag** and **rport**
- The “received” tag tells the proxy to return a packet to a specific IP and the “rport” tag keeps the port to return to

RTP – media stream

- The SIP message body contains the information that the endpoints need in order to communicate directly with each other
  - This information is contained in the SDP message
  - A client sitting behind a NAT knows only its internal address: port pair
- When the destination endpoint wants to start sending packets to the originating endpoint
  - It will use the received SDP information containing the internal address: port pair of the originating endpoint
    - The packets never get there

Example header

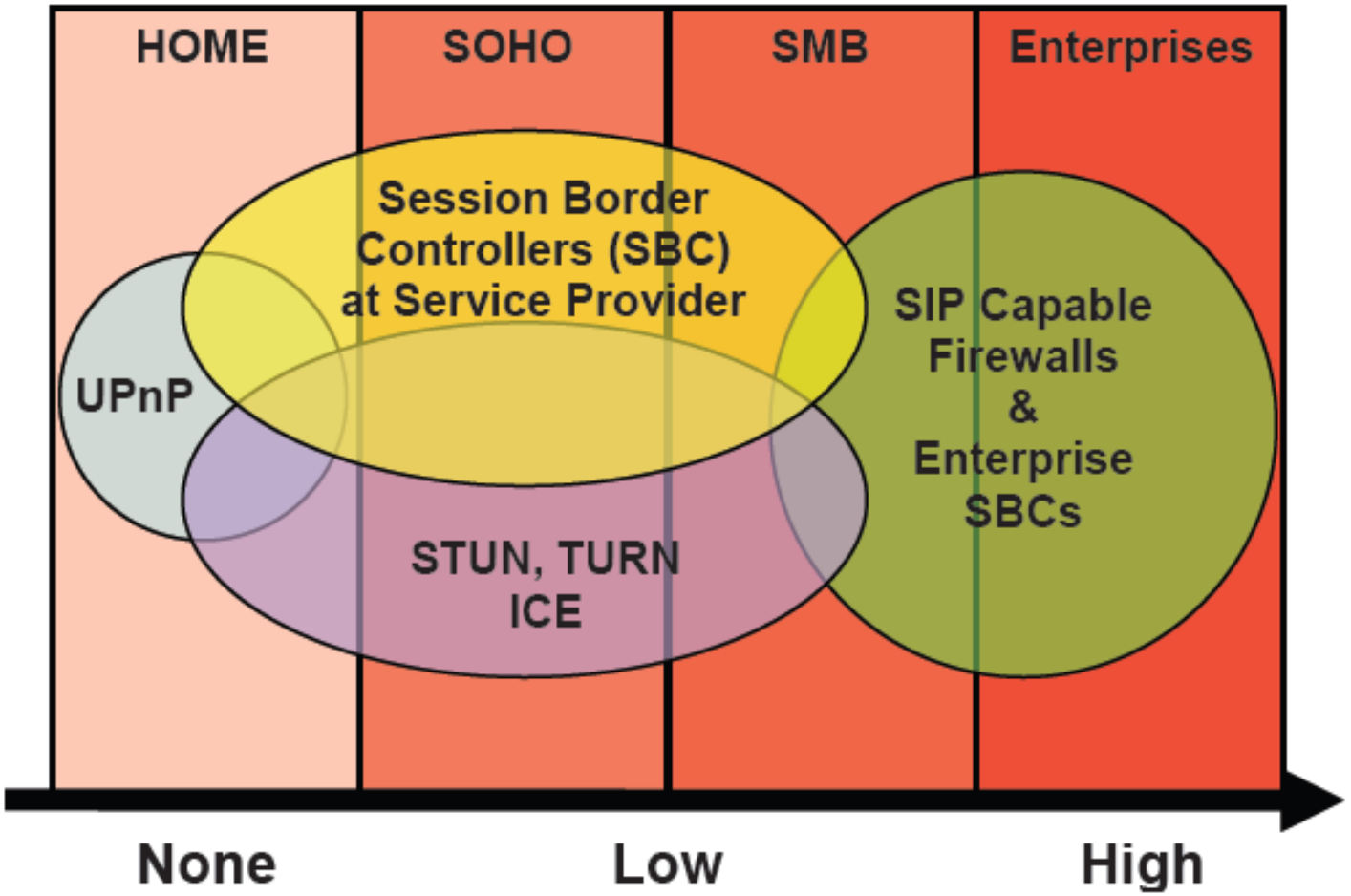
```
INVITE sip:1000@203.143.0.120 SIP/2.0
Via: SIP/2.0/UDP 203.143.0.121:5060;branch=a43u4h42-507c77f2
Via: SIP/2.0/UDP
   192.168.0.1:5060;reveived=202.124.211.25;rport=10000
From: <sip: 1001@ 203.143.0.121>tag=108bcd14
To: sip: 1000@203.143.0.120
   .
   .
V=0
o=123467777 123467777 IN IPV4 192.168.0.2
s= abc Session
c=IN IPV4 192.168.0.1
t=1253886592 0
m=audio 23456 RTP/AVP 4
a=rtpmap:0 PCMU/8000
A=ptime:20
```

Solutions for NAT Traversal

- Two main methods for determining mapping information

1. Ask from the NAT device
2. Ask someone outside the NAT device

Positioning of NAT traversal solutions



- Who should be in control of security infrastructure
  - The firewall administrator, the user or the service provider?

UPnP

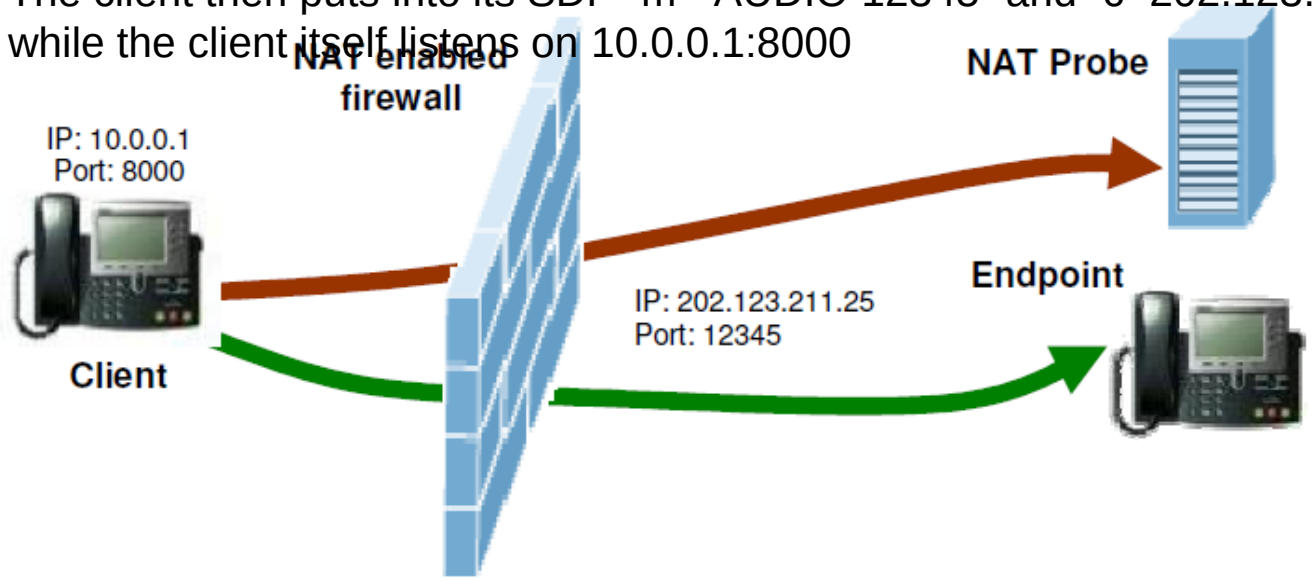
- UPnP (Universal Plug and Play)
- Mainly is pushed by Microsoft
- Client queries the NAT device via UPnP
- NAT device responds with the IP:port on the public internet
- Cannot use with cascading NATs

External Query Method

- Used when it's not possible to communicate with NAT device
- Ask a server, outside the NAT on the internet how it sees the source packets
- The NAT Probe is listening (NAT probing)
- NAT Probe replies from the same port of the received packet, containing IP: port as the server sees
- Then client can determine
  - If it's behind the NAT
  - Public IP:port that should be used in SDP message

External Query Example

- If the client wants to be reached on 10.0.0.1:8000
  - It will first send out a query to the NAT probe from port 8000
  - The NAT probe will actually receive the query packet from 202.123.211.25:12345
  - It will respond to that address:port pair with a packet containing 202.123.211.25:12345
  - The client then puts into its SDP “m= AUDIO 12345” and “c=202.123.211.25” while the client itself listens on 10.0.0.1:8000



External Query Guidelines

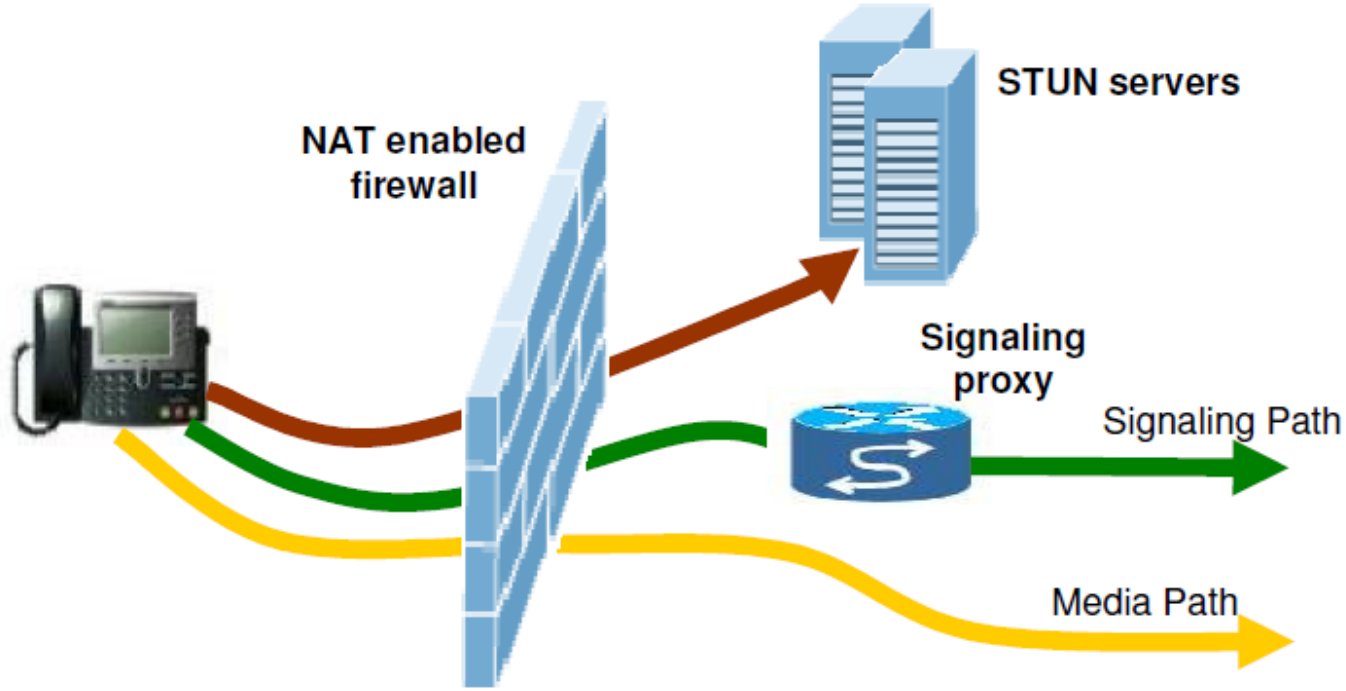
1. The client must send and receive RTP on the same port

2. The client must send out the SIP message shortly after sending out a query to the NAT probe
   - If there is a long delay, the mapping may change

3. This will not work in the case of symmetric NATs
   - The IP address of the NAT probe is different than that of the endpoint
     a. The mapping that the NAT probe sees is different than the mapping that the endpoint uses (address:port pair)

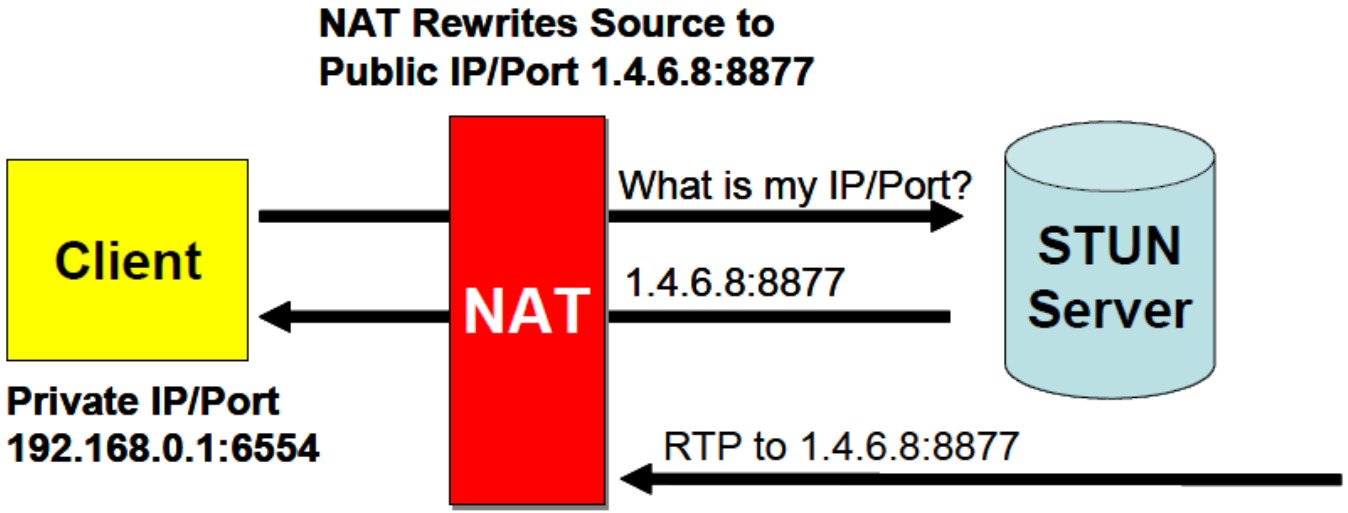
STUN

- Simple Traversal of UDP Through NAT
- A protocol for setting up the kind of NAT Probe
  - Extra functionality- it can also help determine which kind of NAT the client is behind
  - STUN Aware Client- Clients can set their SDP messages accordingly

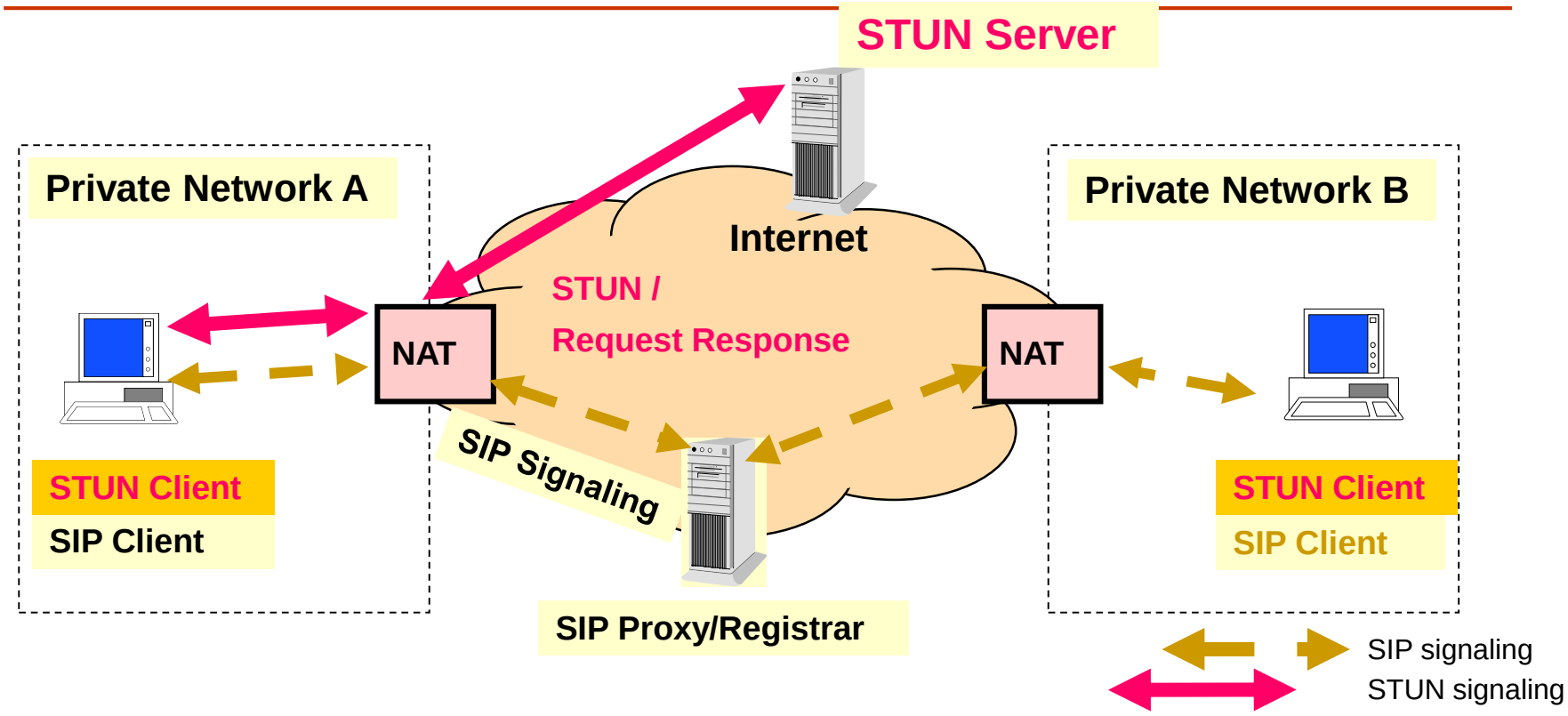


STUN (cont.)

- The STUN server does not sit in the signaling or media data path
- STUN can work for the first 3 types of NAT
  - Symmetric NAT is not supported
    - Different mappings depending on the target IP
    - The mapping that the NAT assigns between the client and the NAT probe is different than that assigned between the client and the gateway

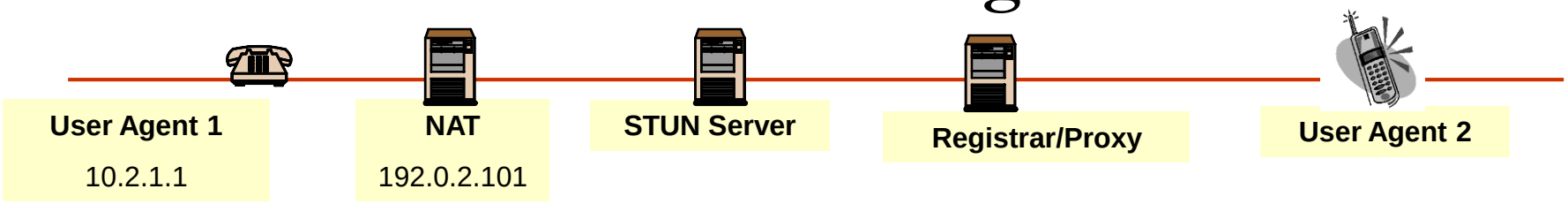


STUN (cont.)



- STUN client contacts STUN server, discovers NAT, address translation
- SIP client uses “external” address in signaling for setup of media streams

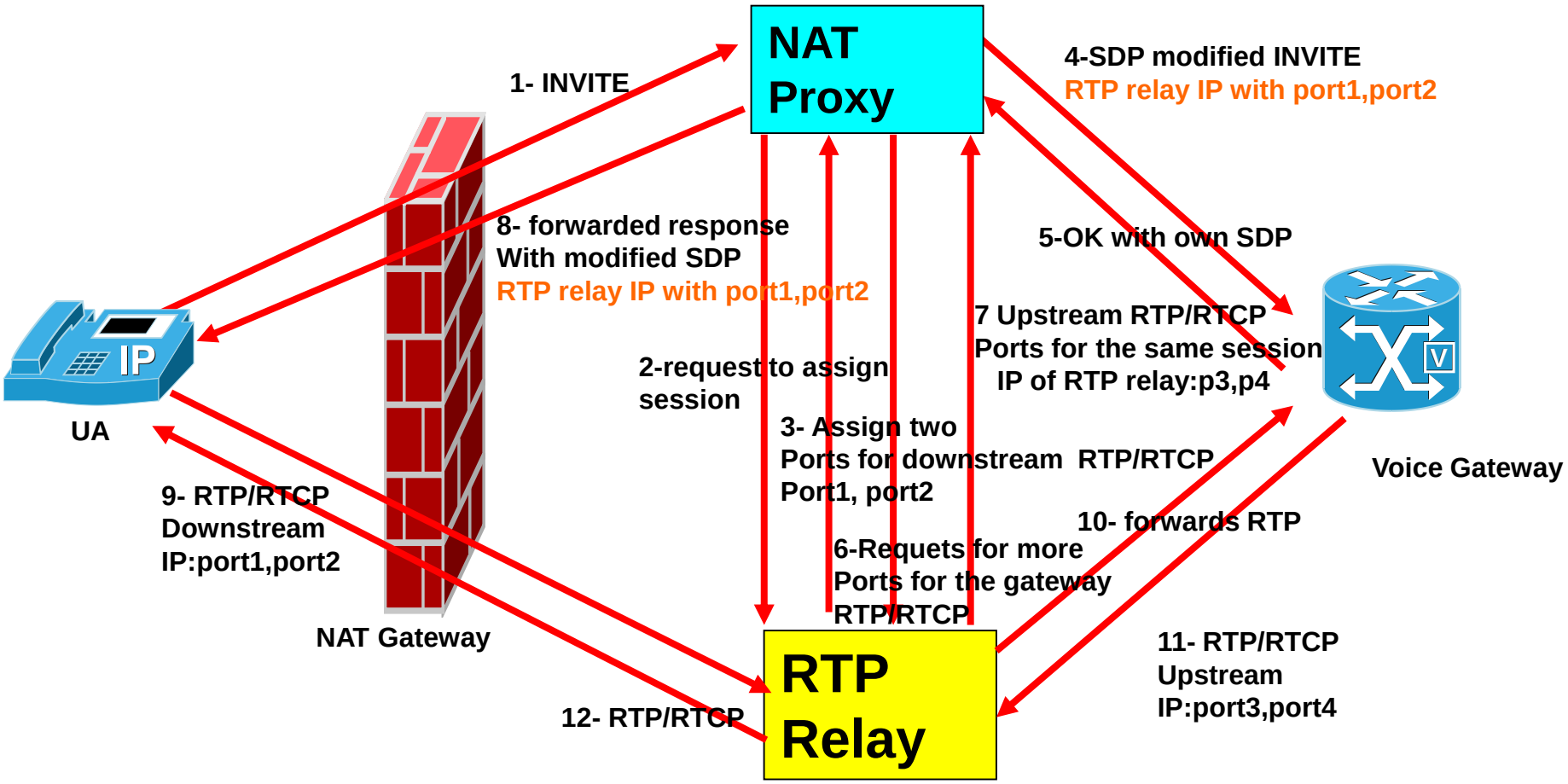
NAT Traversal Using STUN



Connection Oriented Media

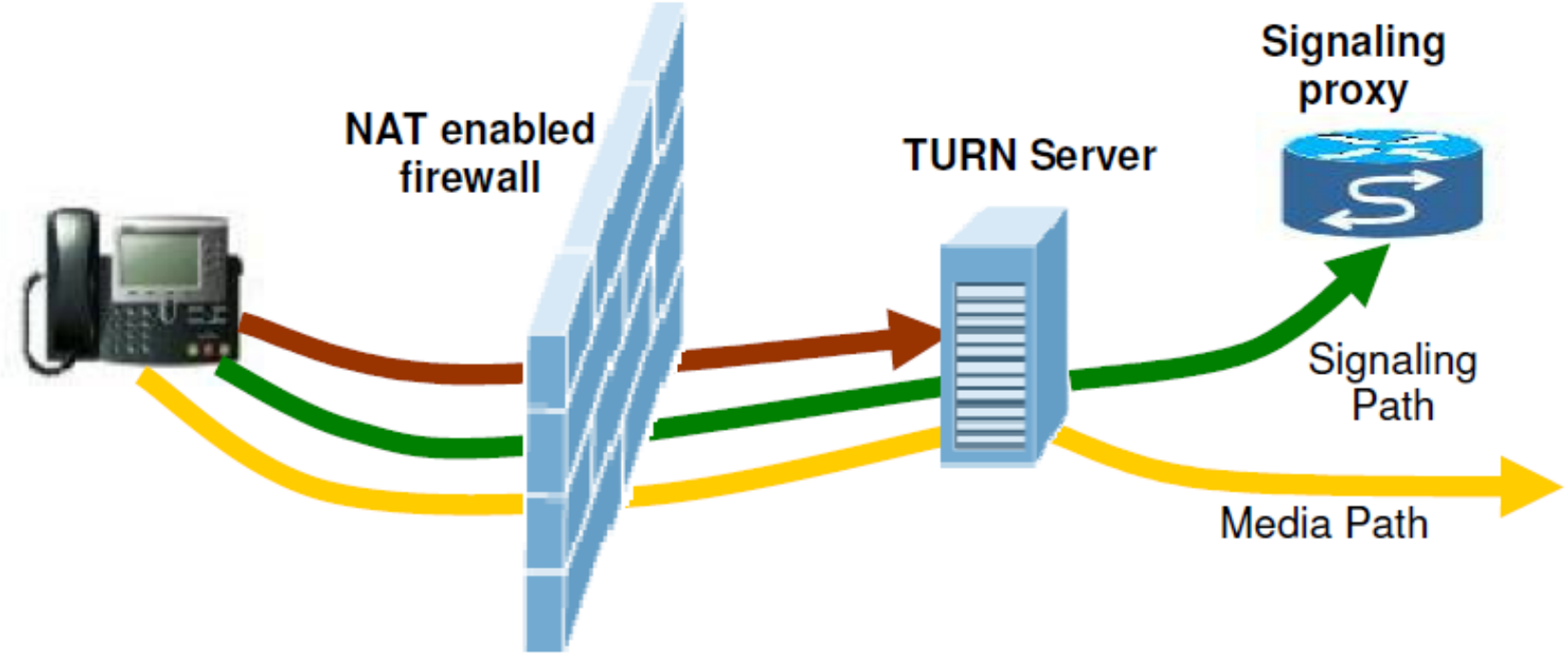
- STUN and UPnP works only with the first 3 types of NATs
- Symmetric NAT case
  - the client must send out RTP to, and receive RTP back from the same IP address
- Any RTP connection between an endpoint outside a NAT and one inside a NAT must be established point to point
  - The endpoint outside the NAT must wait until it receives a packet from the client before it can know where to reply

Solution for Symmetric NAT



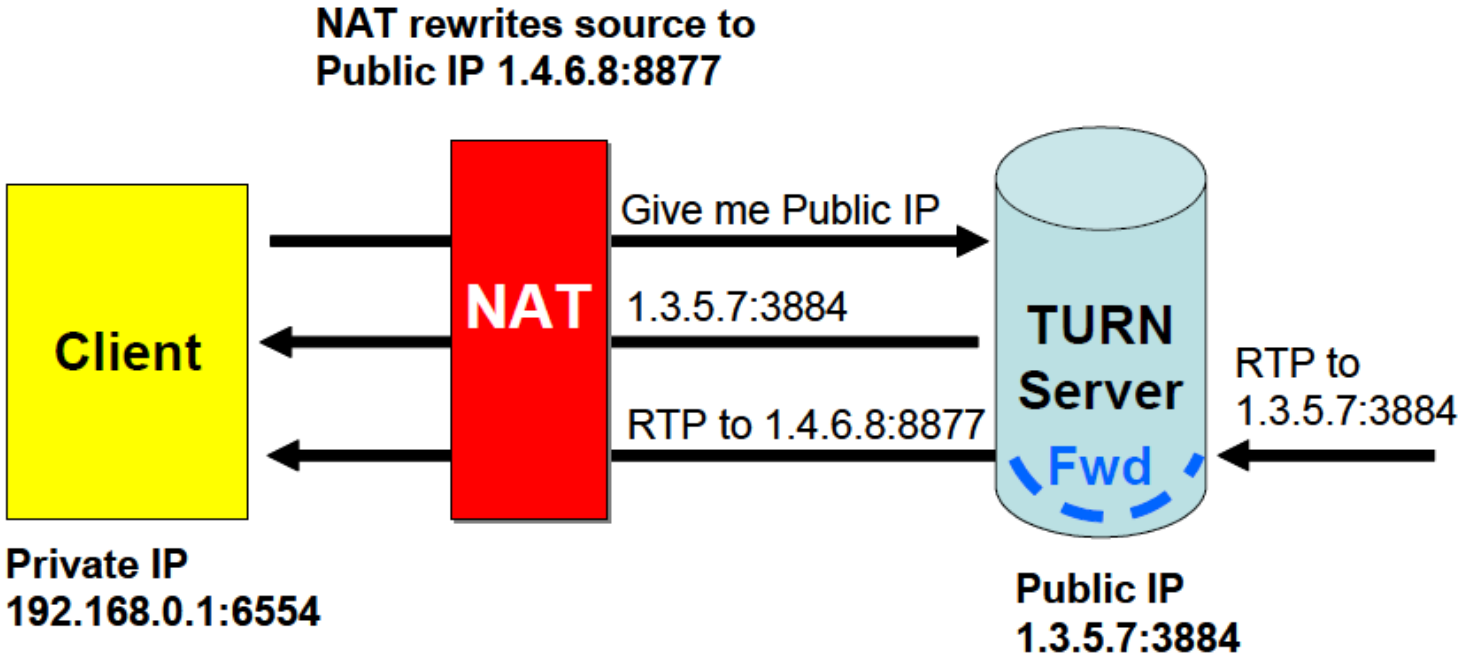
TURN

- **T**raversal **U**sing **R**elay **N**ATs (TURN) complements STUN
  - Places the probe in the signalling and media path
  - TURN (Traversal Using Relay NAT) allows an end point behind a firewall to receive SIP traffic on either TCP or UDP ports



TURN (cont.)

- This solves the problems of clients behind symmetric NATs
- TURN connects clients behind a NAT to a single peer
- The TURN server acts as a relay
  - Any data received is forwarded



ICE – Interactive Connectivity Establishment

- ICE uses STUN, TURN and other methods to solve the NAT traversal issue
- ICE allows end points to discover other peers and then establish a connection
- ICE essentially incorporates all of the methods proposed for NAT traversal of SIP that do not rely on the firewall or NAT device
- ICE is a complex solution to the problem of NAT traversal
  - Encompasses multiple solutions- always enable the connection, regardless of the number of NATs involved

ICE (cont.)

- ICE still relies on client-server based approaches, and removes control from the enterprise
- Due to its complexity - limited clients support ICE
- STUN, TURN and ICE are methods that assume certain behaviour from th NAT/firewall
  - Do not work in all scenarios
  - The control is removed from the firewall
    - FW has to be sufficiently opened to allow users to create the pinholes needed to let the communication through

References

- RFC 1631 NAT
- RFC 2391 NAT for Load Sharing
- RFC 2663 NAT Terminology and Usages
- RFC 2709 IPsec for NAT
- RFC 2766 NAT-PT
- RFC 2993 NAT Architectural Implications
- RFC 3022 Traditional IP-NAT
- RFC 3235 NAT Friendly Application Design
- RFC 3489 UDP through NAT - STUN
- RFC 3519 Mobile IP though NAT
- RFC 3715 IPsec NAT compatibility
- RFC 3947 IKE NAT Traversal
- RFC 4008 MIB for NATs