VoIP + NAT

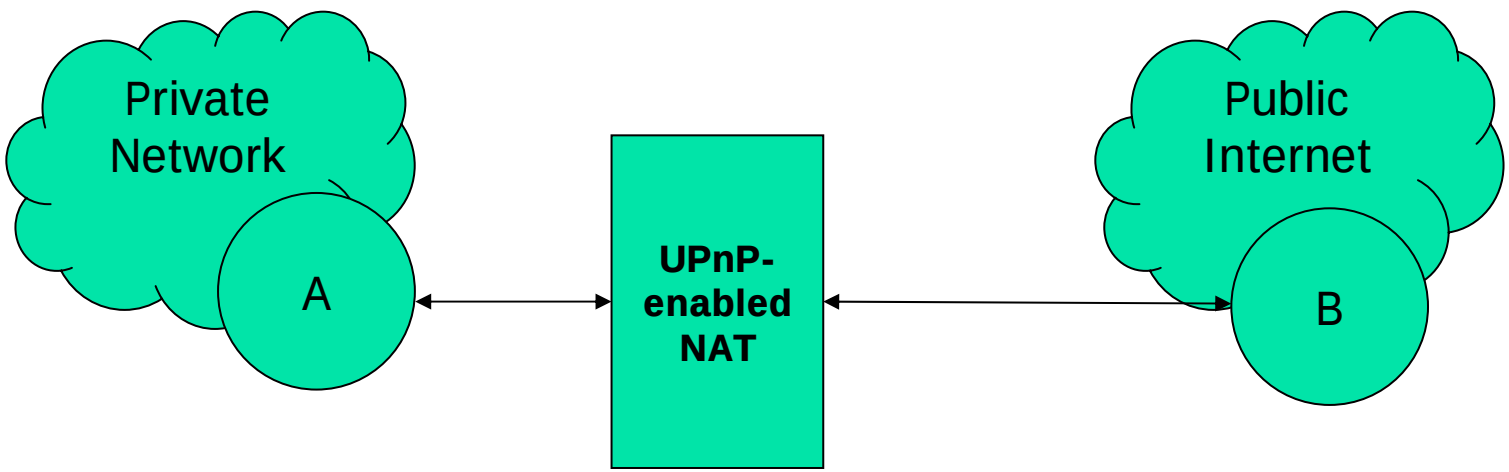
UPnP [1/2]

http://www.upnp.org/

- Universal Plug and Play
- It is being pushed by Microsoft
  - Windows® Messenger
- A UPnP-aware client can ask the UPnP-enabled NAT how it would map a particular IP:port through UPnP
- It will not work in the case of cascading NATs

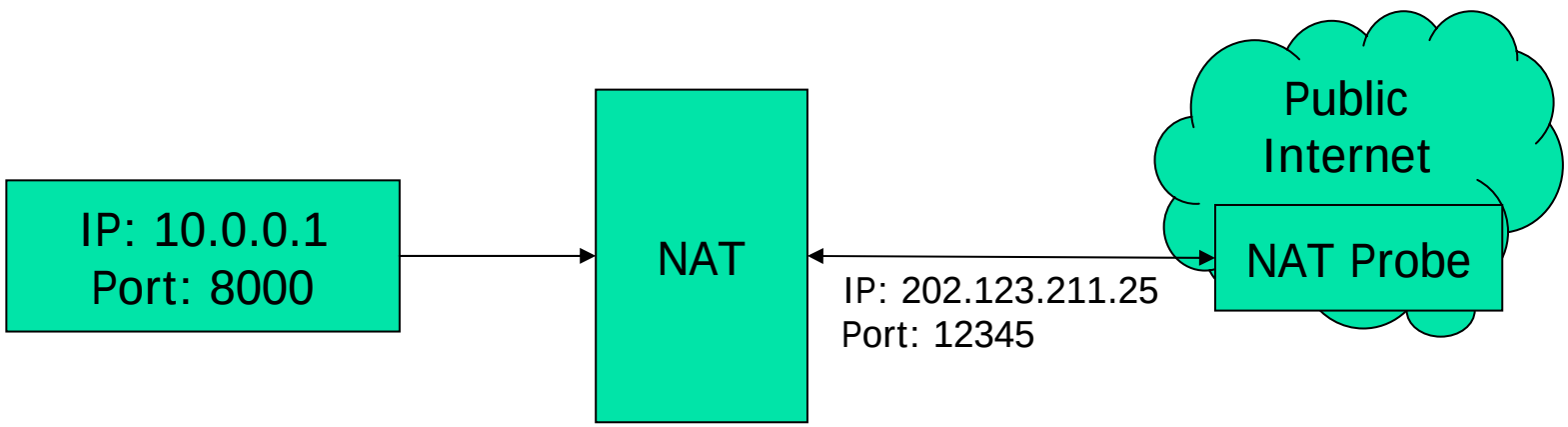
UPnP [2/2]

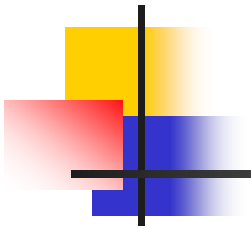
- A: Private Network
  - UPnP-aware Internet gateway device
  - The UPnP-enabled NAT allows “A” to be aware of its external IP
- B: Public Internet
  - “B” and “A” can communicate with each other



External Query

- A server sits listening for packets (call this a **NAT probe**)
- When it receives a packet, it returns a message from the same port to the source containing the IP:port that it sees



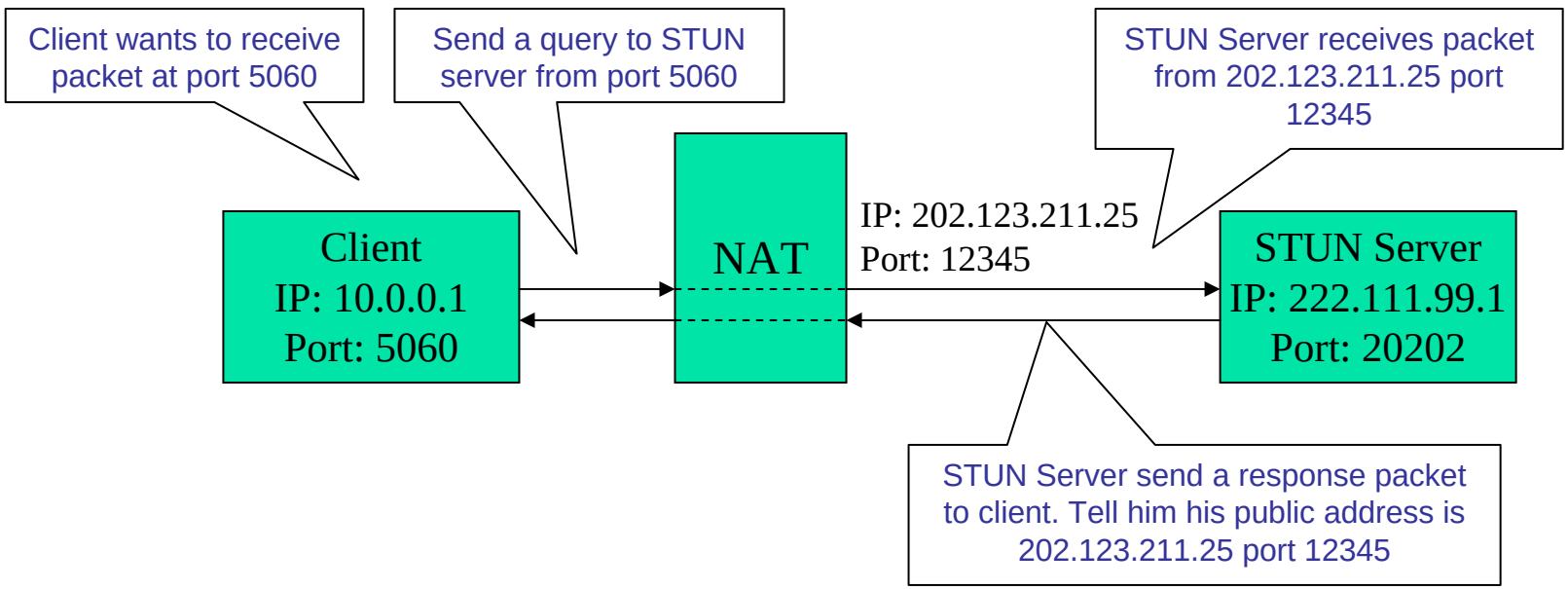


STUN

- Simple Traversal of UDP Through NAT
- RFC 3489
- In Working Group IETF MIDCOM Group
- Simple Protocol
- Works with existing NATs
- Main features
  - Allow Client to Discover Presence of NAT
  - Works in Multi-NAT Environments
  - Allow Client Discover Type of NAT
  - Allows Client to Discover the Binding Lifetimes
  - Stateless Servers

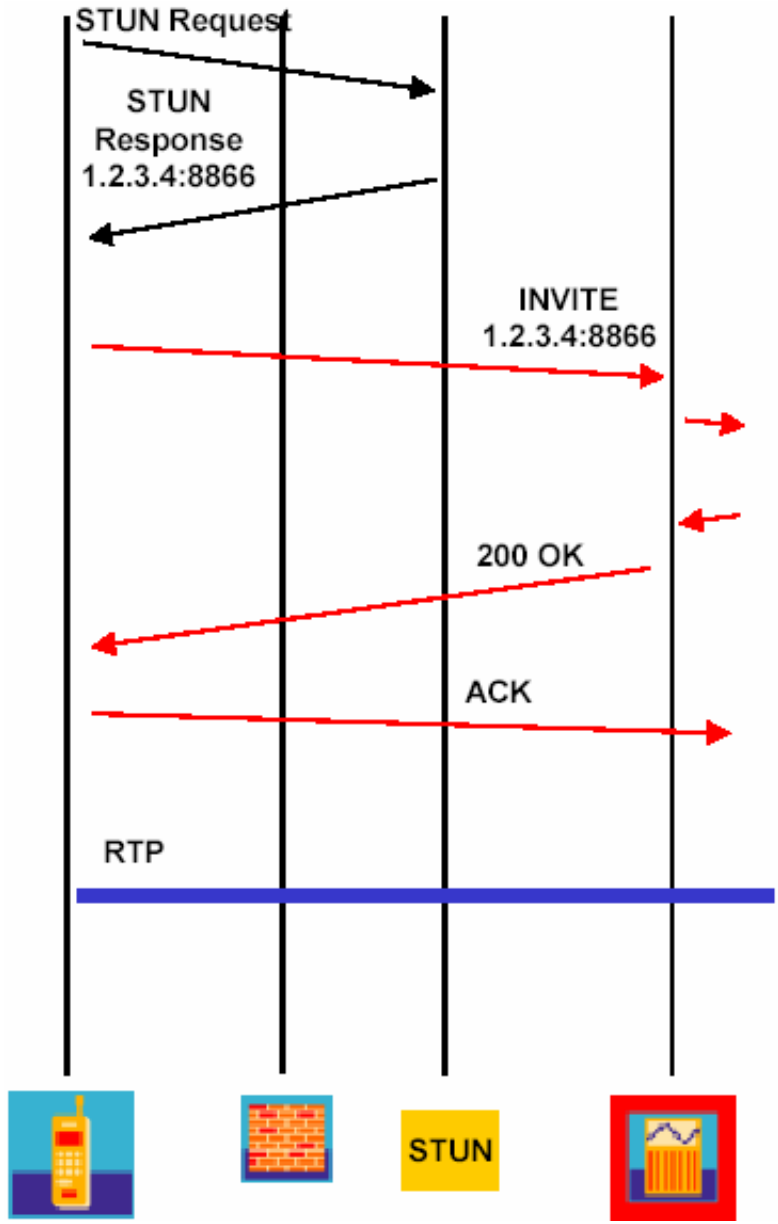
STUN Server

- Allow client to discover if it is behind a NAT, what type of NAT it is, and the public address & port NAT will use.
- Very Simple Protocol, Easy to implement, Little load



Binding Acquisition

- STUN Server can be ANYWHERE on Public Internet
- Call Flow Proceeds Normally

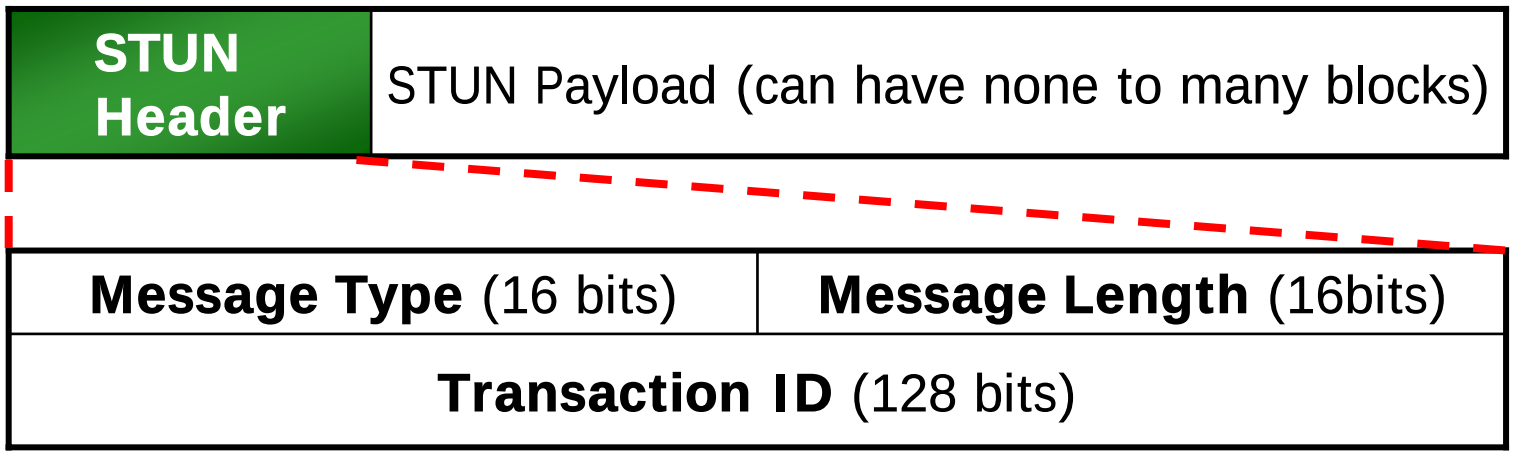


STUN Message [1/3]

- TLV (type-length-value)
- Start with a STUN header, followed by a STUN payload (which is a series of STUN attributes depending on the message type)
- Format

STUN Header	STUN Payload (can have none to many blocks)

STUN Message [2/3]

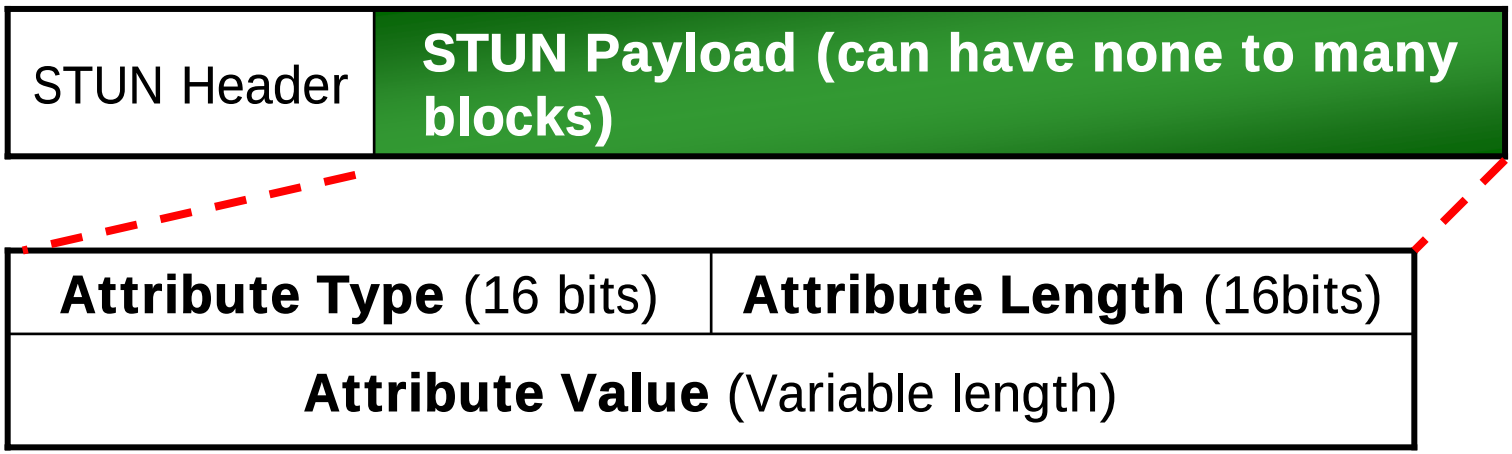


Message Types

0x0001: Binding Request
0x0101: Binding Response
0x0111: Binding Error Response

0x0002: Shared Secret Request
0x0102: Shared Secret Response
0x0112: Shared Secret Error Response

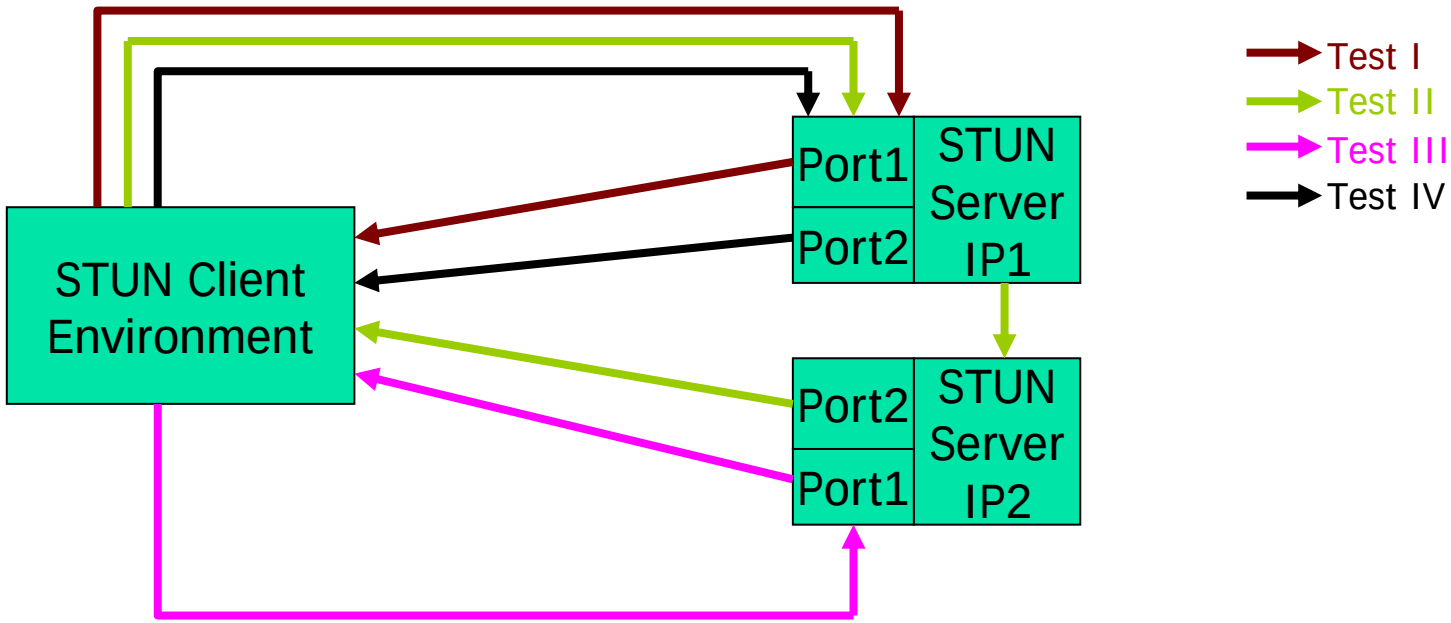
STUN Message [3/3]



Attribute Types

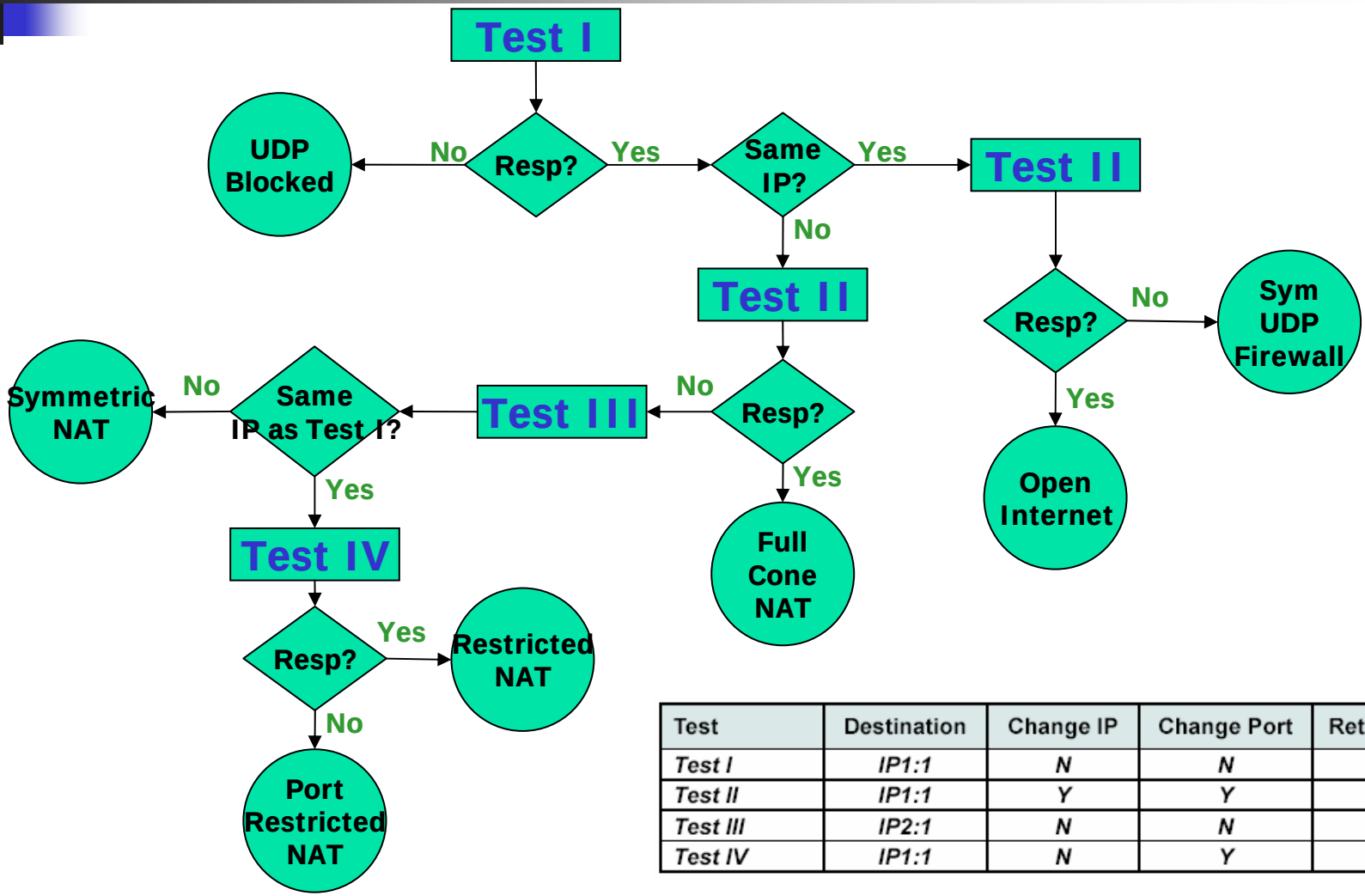
0x0001: MAPPED-ADDRESS
0x0002: RESPONSE-ADDRESS
0x0003: CHANGE-REQUEST
0x0004: SOURCE-ADDRESS
0x0005: CHANGED-ADDRESS
0x0006: USERNAME
0x0007: PASSWORD
0x0008: MESSAGE-INTEGRITY
0x0009: ERROR-CODE
0x000a: UNKNOWN-ATTRIBUTES
0x000b: REFLECTED-FROM

Automatic Detection of NAT Environment [1/2]



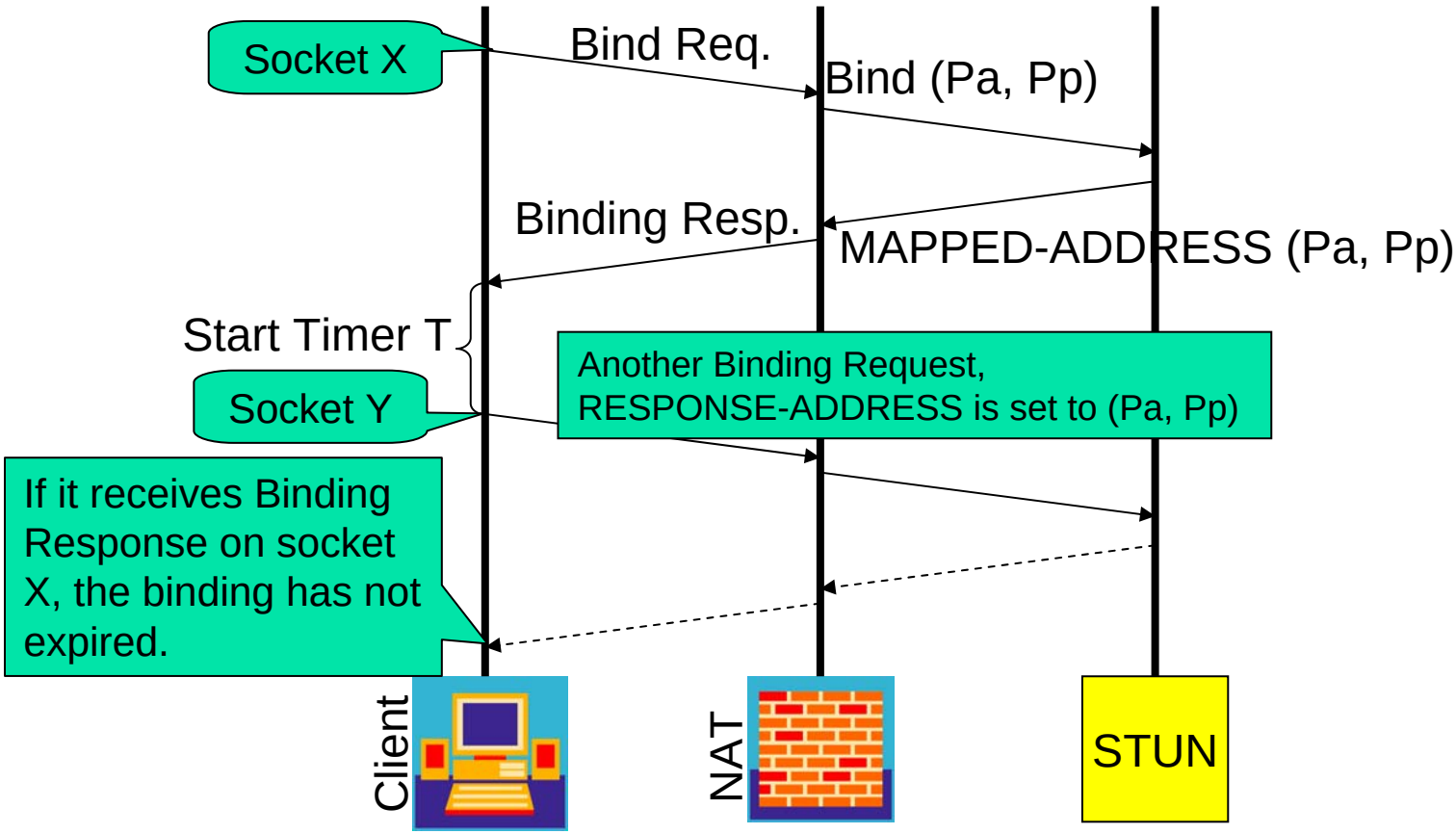
Test	Destination	Change IP	Change Port	Return IP:port
Test I	*IP1:1*	*N*	*N*	*IP1:1*
Test II	*IP1:1*	*Y*	*Y*	*IP2:2*
Test III	*IP2:1*	*N*	*N*	*IP2:1*
Test IV	*IP1:1*	*N*	*Y*	*IP1:2*

Automatic Detection of NAT Environment [2/2]

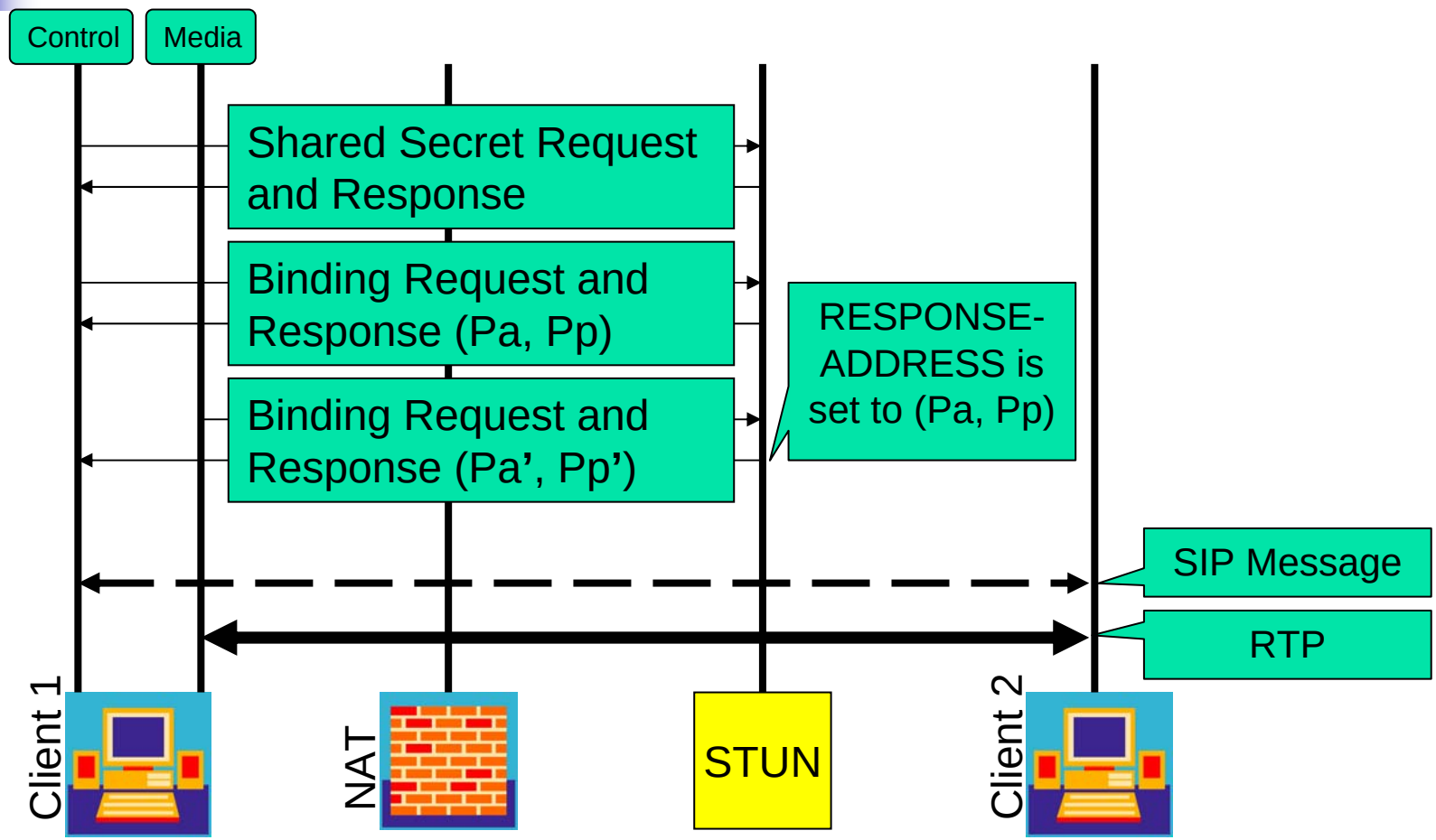


Test	Destination	Change IP	Change Port	Return IP:port
Test I	*IP1:1*	*N*	*N*	*IP1:1*
Test II	*IP1:1*	*Y*	*Y*	*IP2:2*
Test III	*IP2:1*	*N*	*N*	*IP2:1*
Test IV	*IP1:1*	*N*	*Y*	*IP1:2*

Binding Lifetime Determination



Binding Acquisition Procedure

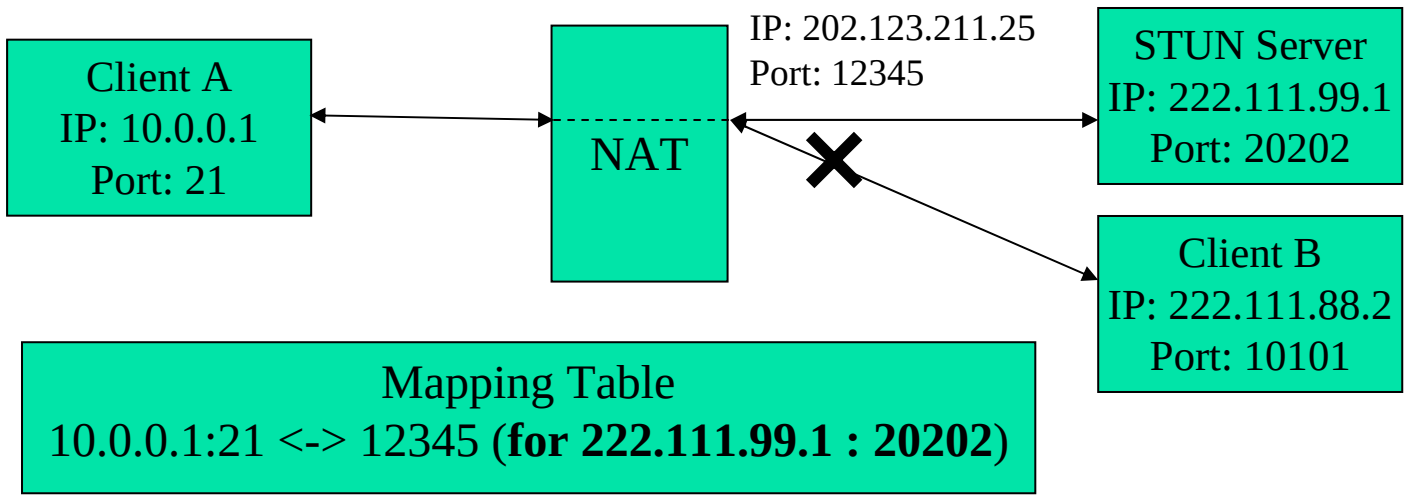


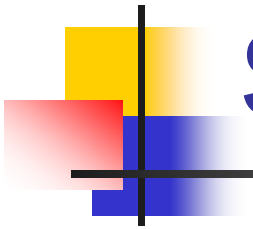
STUN - Pros and Cons

- Benefits
  - No changes required in NAT
  - No changes required in Proxy
  - Works through most residential NAT
- Drawbacks
  - Doesn’t allow VoIP to work through Symmetric NAT
  - RTCP may not work
  - Need to keep media flowing to keep bindings alive

Is STUN suitable for Symmetric NAT

- Absolutely not





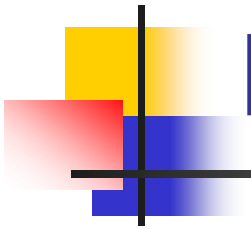
Solutions for Symmetric NATs

- Connection Oriented Media
- RTP-Relay

Connection Oriented Media

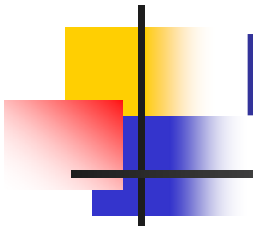
- The endpoint outside the NAT must wait until it receives a packet from the client before it can know where to reply
- Add a line to the SDP message (coming from the client behind the NAT)

  a=direction:active
- The initiating client will “actively” set up the IP:port to which the endpoint should return RTP
  - The IP:port found in the SDP message should be ignored



Problem?

1) If the endpoint does not support the **a=direction:active** tag
2) If both endpoints are behind Symmetric NATs

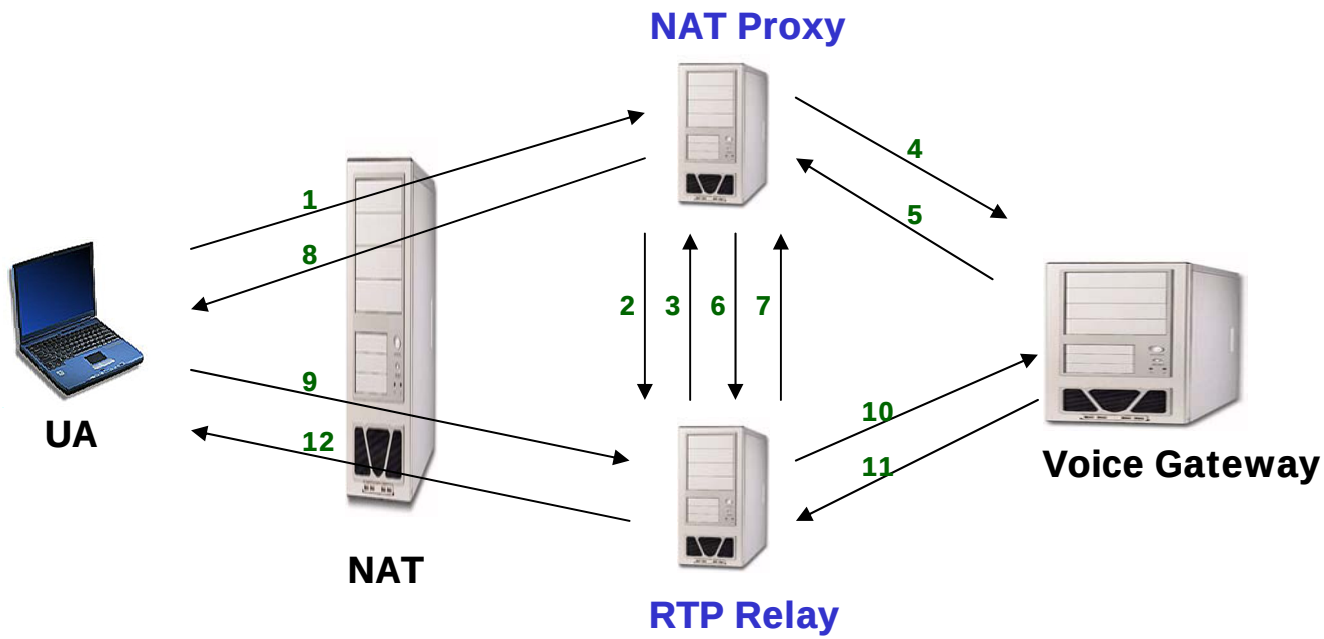


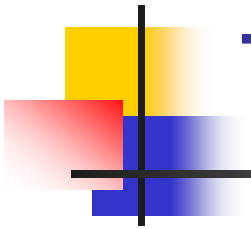
RTP-Relay

- In either of the cases considered in the previous slide, one solution is to have an RTP Relay in the middle of the RTP flow between endpoints.
- The RTP Relay acts as the second endpoint to each of the actual endpoints that are attempting to communicate with each other.

Example

The following is a typical call flow that might be instantiated between a User Agent behind a symmetric NAT and a voice gateway on the open Internet:





TURN

- Traversal Using Relay NAT
- draft-rosenberg-midcom-turn-04.txt
- Expires: August 16, 2004