Introduction to the IETF ICE/TURN/STUN set of RFCs

Emil Ivov, Pal Martinsen,
Justin Uberti & Brandon Williams

IETF 92

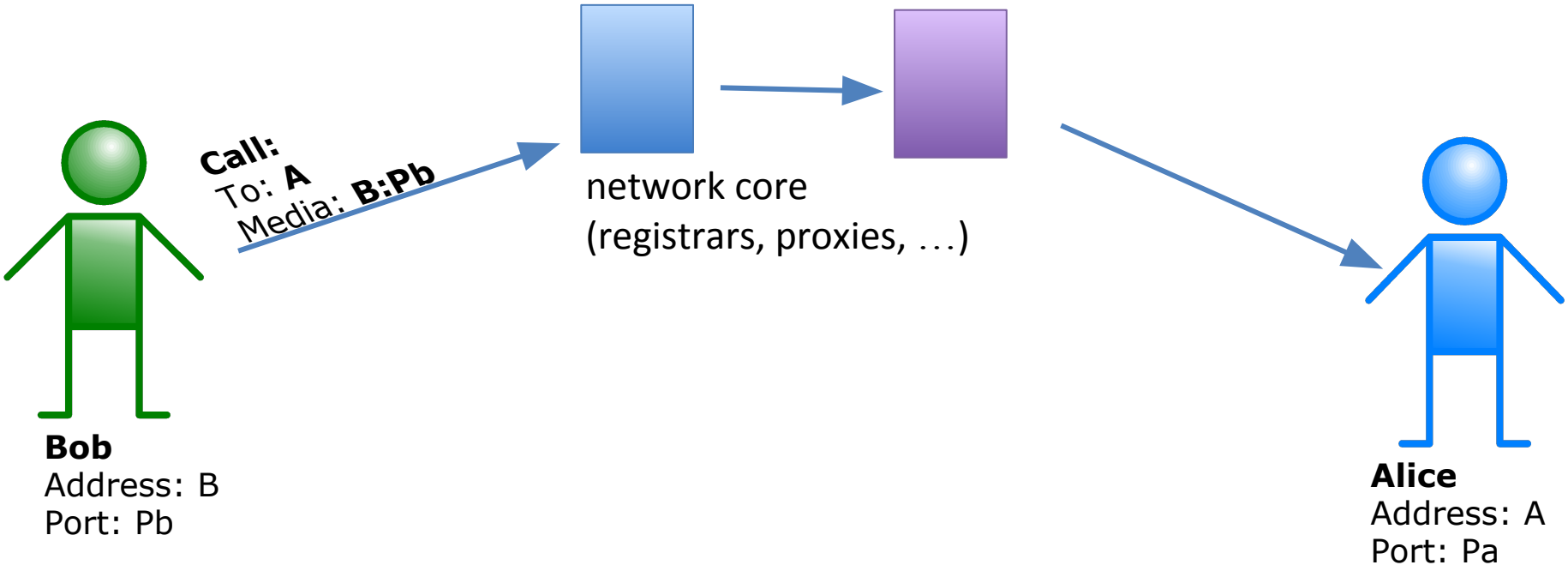
Content

Q and A
SHOULD happen
during the session

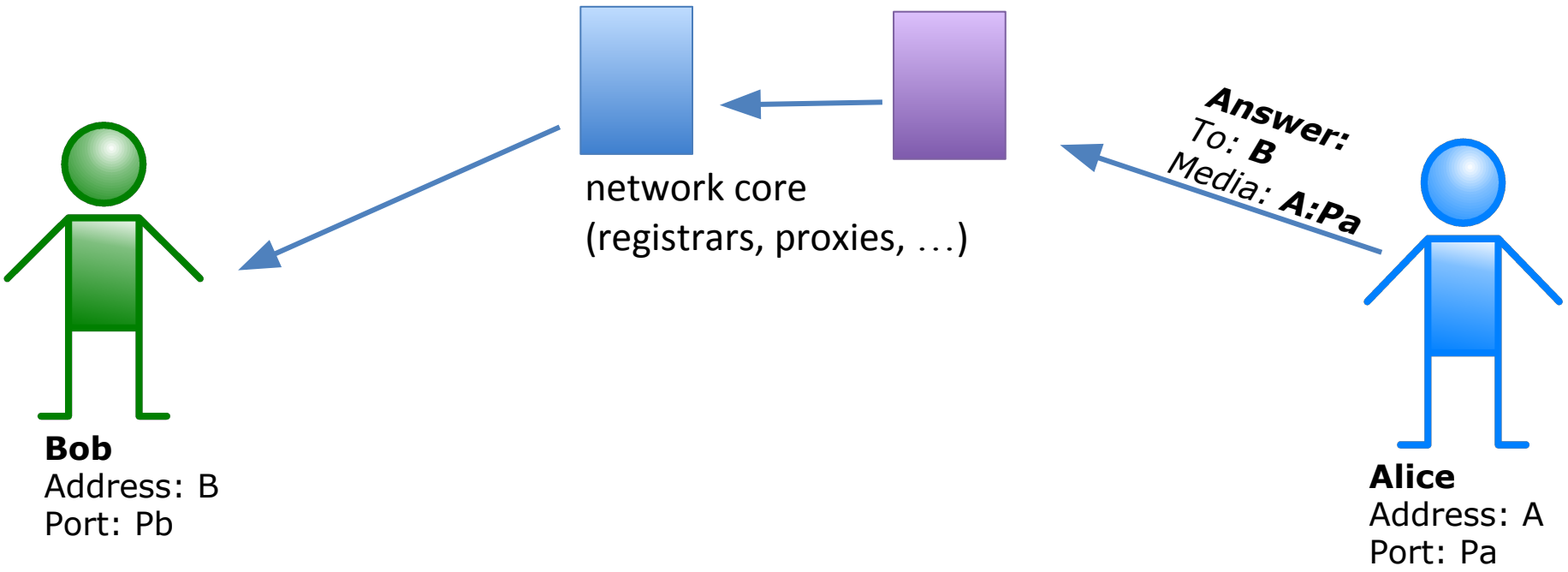
- What is the Problem?
  - Basics of IP telephony
  - How NAT works
- Core ICE functionality
  - What is a Candidate
  - Candidate Gathering
  - Connectivity Checks
  - Concluding
- IETF RFCs, drafts and I-Ds
- Summary

WHAT IS THE PROBLEM?

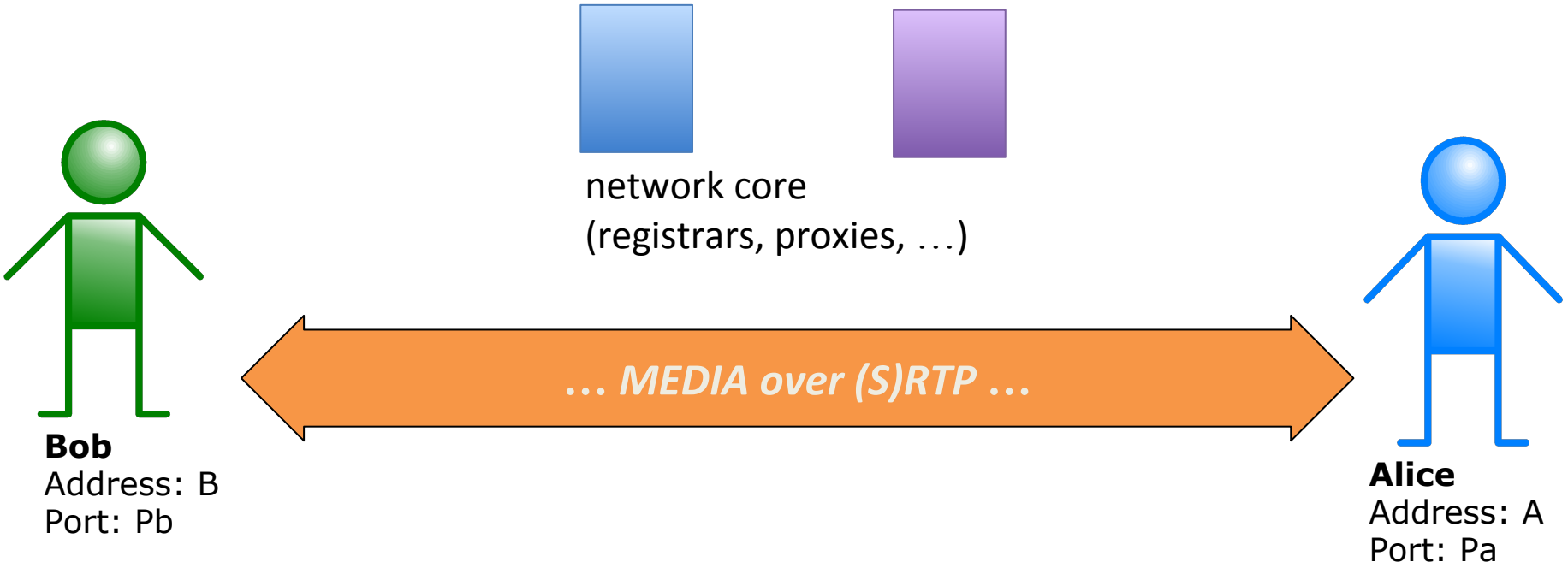
The basics of IP telephony
A sample call



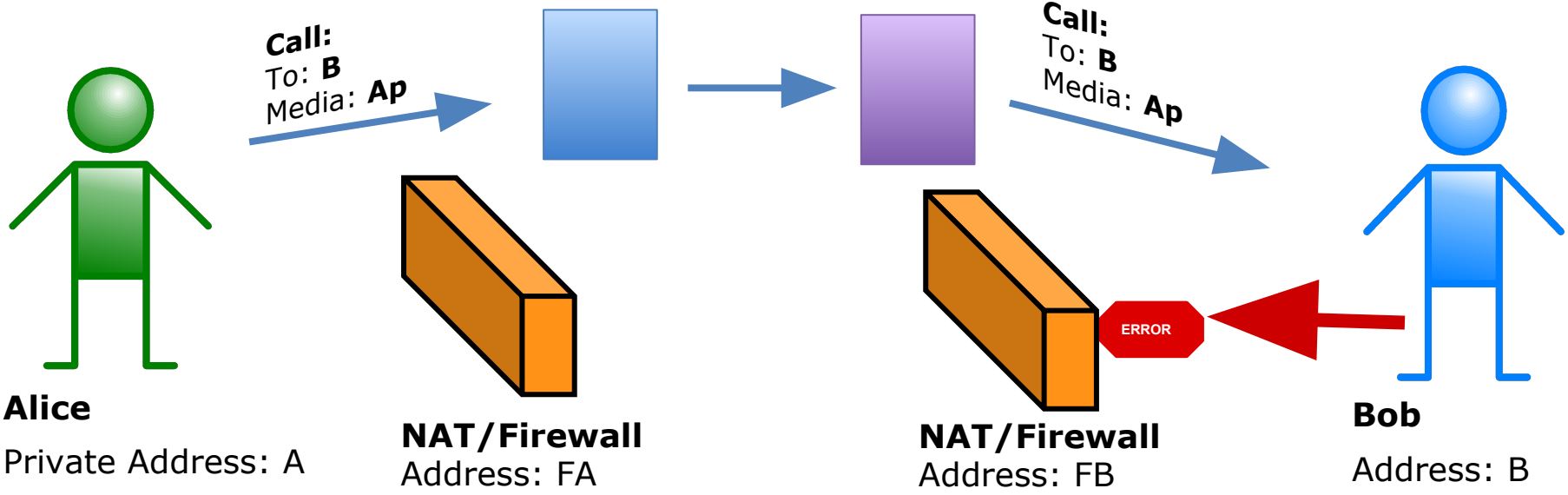
The basics of IP telephony
A sample call



The basics of IP telephony.



And then NATs were born …



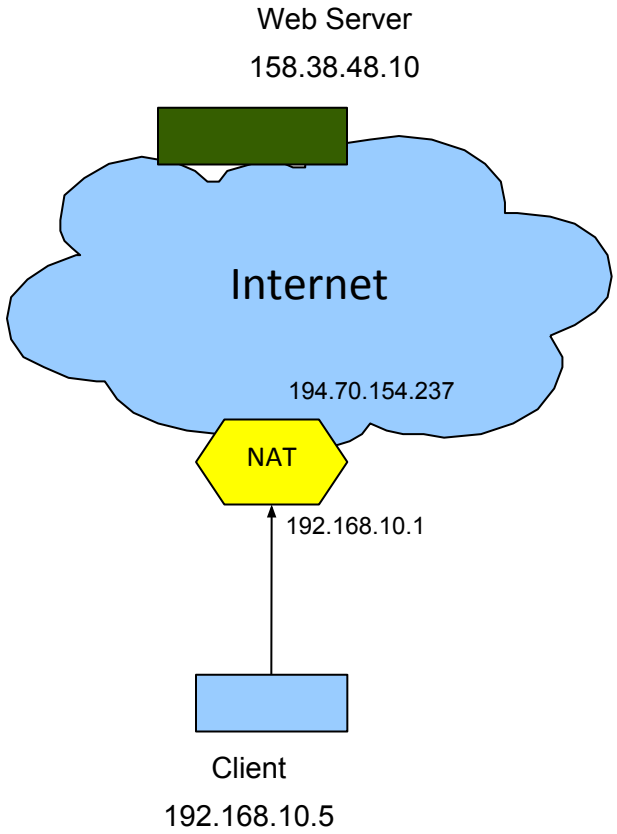
Impossible for Bob to initiate a media connection to Alice

Impossible for Alice to initiate a media connection to Bob

How NAT boxes work

NAT Mappings

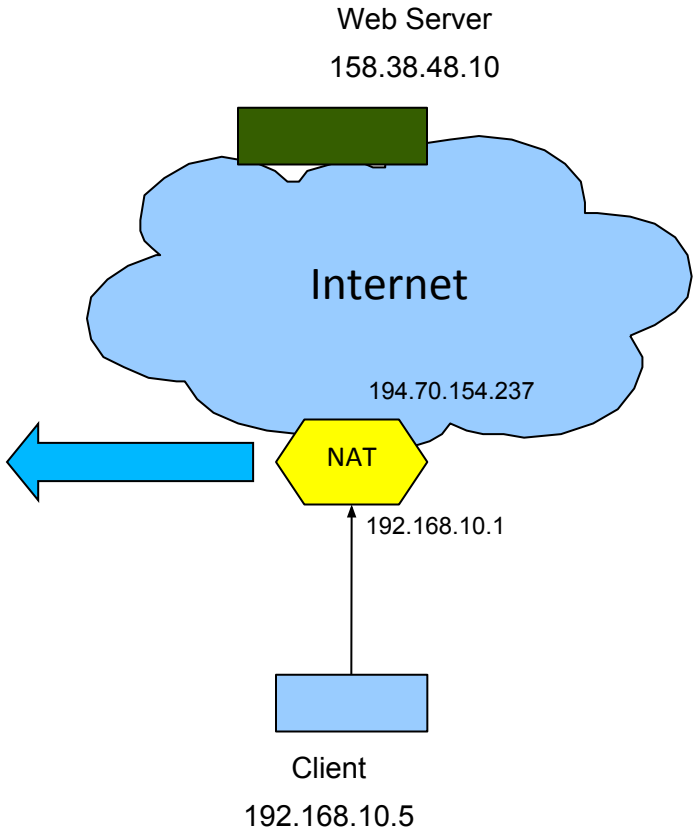
Src addr	Src port	Dst addr	Dst port	Rewritten src port



How NAT boxes work

NAT Mappings

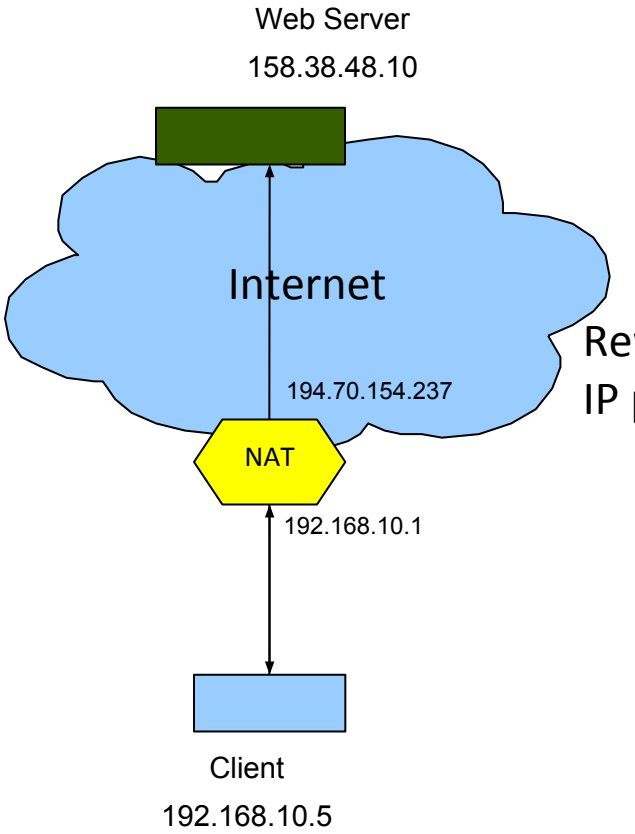
Src addr	Src port	Dst addr	Dst port	Rewritten src port
192.168.10.5	23045	158.38.48.10	80	34567



How NAT boxes work

NAT Mappings

Src addr	Src port	Dst addr	Dst port	Rewritten src port
192.168.10.5	23045	158.38.48.10	80	34567

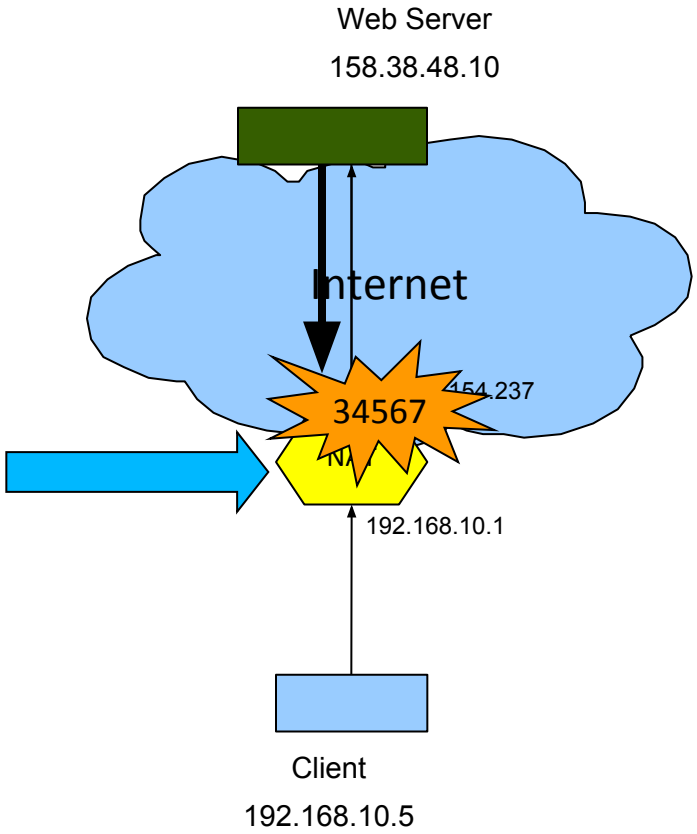


Rewrite outgoing IP packet

How NAT boxes work

NAT Mappings

Src addr	Src port	Dst addr	Dst port	Rewritten src port
192.168.10.5	23045	158.38.48.10	80	34567

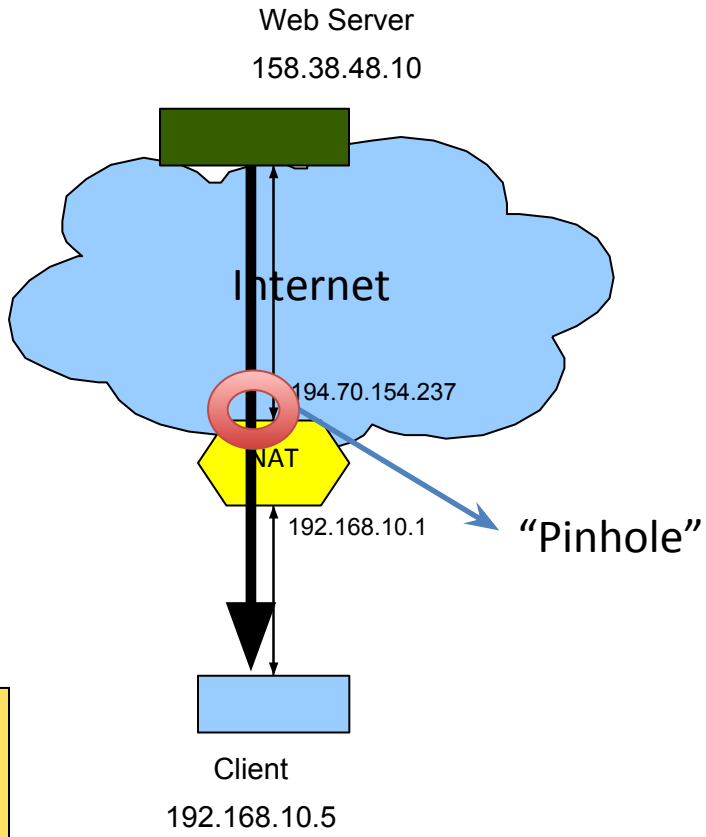


How NAT boxes work

NAT Mappings

Src addr	Src port	Dst addr	Dst port	Rewritten src port
192.168.10.5	23045	158.38.48.10	80	34567

A client request is required to open the pinhole, but the mapping is usually active for at least 30 sec, so subsequent packets get through.



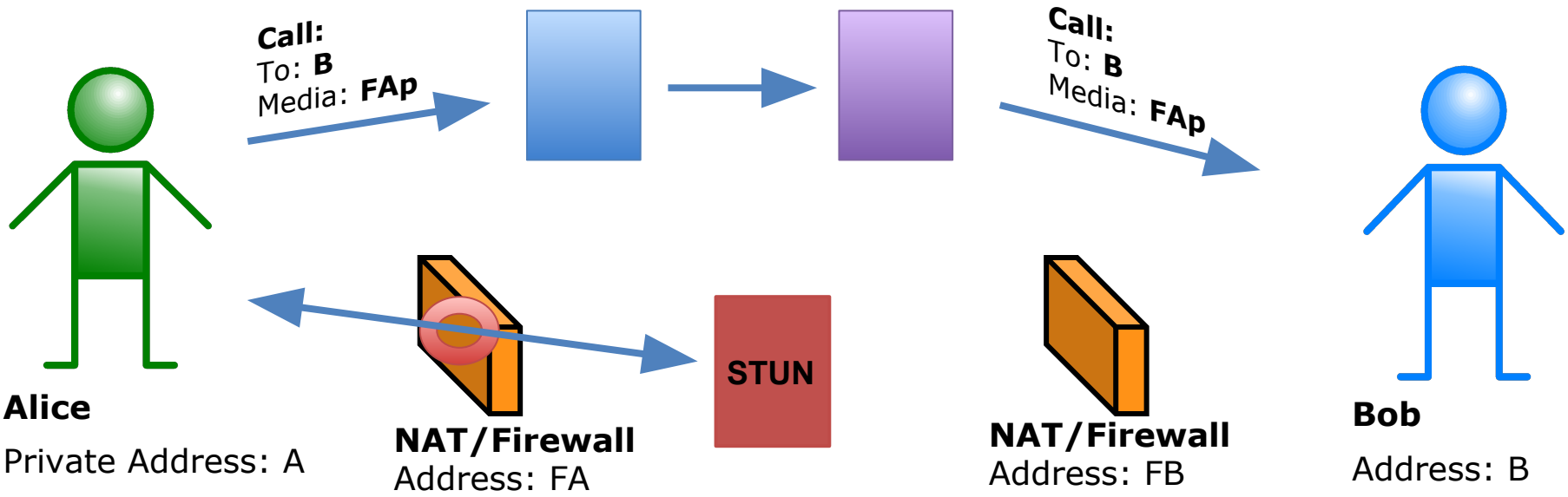
Problem Summary

- The signaling path works because the server has a known publicly routable IP address.
- The media path breaks because the peers have private non-routable IP addresses.
- IPv6 could solve the problem, except firewalls/NATs still exist there.

STUN to the Rescue

- STUN binding request exchanged with the server opens a NAT pinhole.
- Client learns the NAT mapping from the STUN server in the binding response.
- Remote peer can send to this address.
- Doesn't work for all NATs. Some NATs only accept from the original server.

STUN to the Rescue



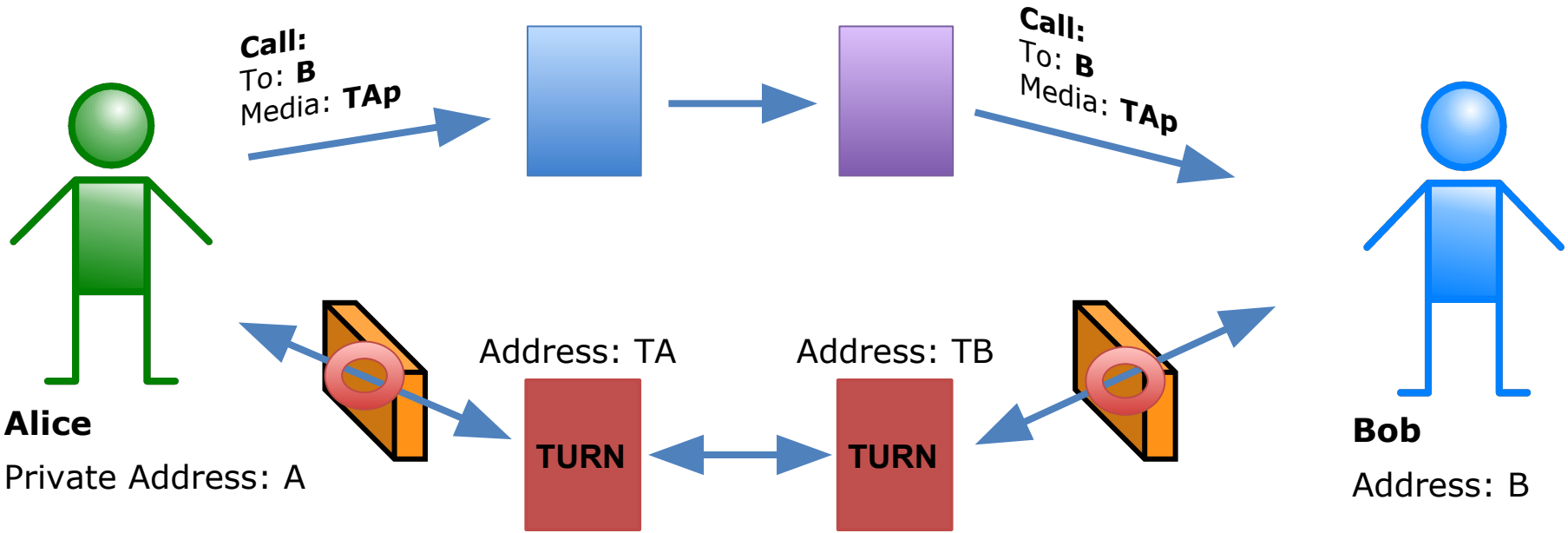
Alice learns FAp from the STUN server, and sends it to Bob.

Bob can initiate a media connection to Alice via FAp.

TURN to the Rescue

- TURN server allocates a public address for the client to advertise.
- All p2p data is relayed via the TURN server, so restrictive NAT pinhole works.
- Often more overhead than direct: processing time on relay, additional latency.

TURN to the Rescue



Alice and Bob get addresses from their TURN servers.

The media connection is relayed via TA and TB.

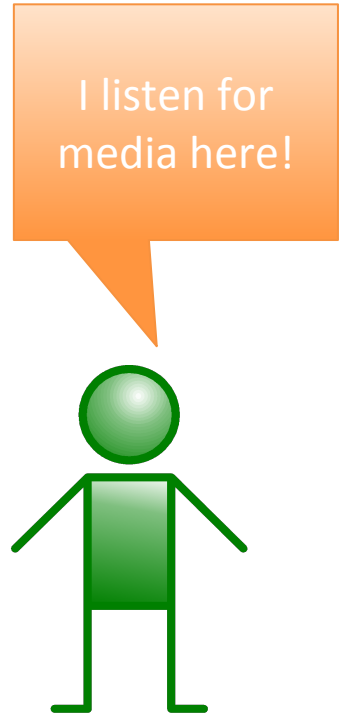
CORE ICE FUNCTIONALITY

What is ICE?

- Each peer can have multiple "candidate" addresses.
- Interactive Connectivity Establishment is how the peers pick a candidate pair to use.
- Basically, test connectivity for all pairs and pick the best* pair that works.

What is a Candidate?

What is a Candidate?

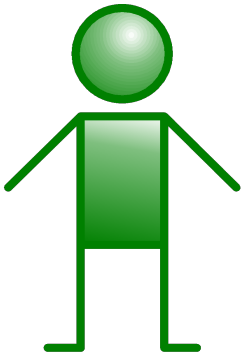


Bob
IP: 192.168.1.34
Port: 4567

HOST

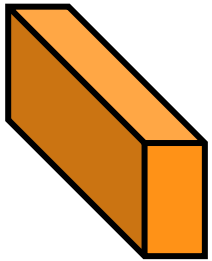
What is a Candidate?

And here!



Bob
IP: 192.168.1.34
Port: 4567

HOST



NAT/Firewall
IP: 1.4.7.4

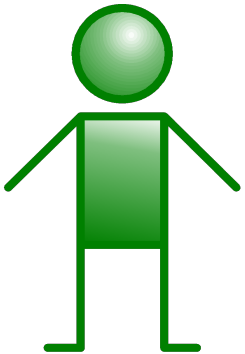
Port: 7865

RFLX

What is a Candidate?

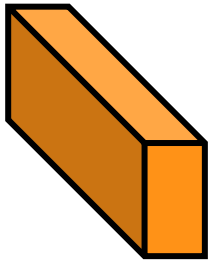
And even here!

TURN Server



Bob
IP: 192.168.1.34
Port: 4567

HOST



NAT/Firewall
IP: 1.4.7.4

Port: 7865

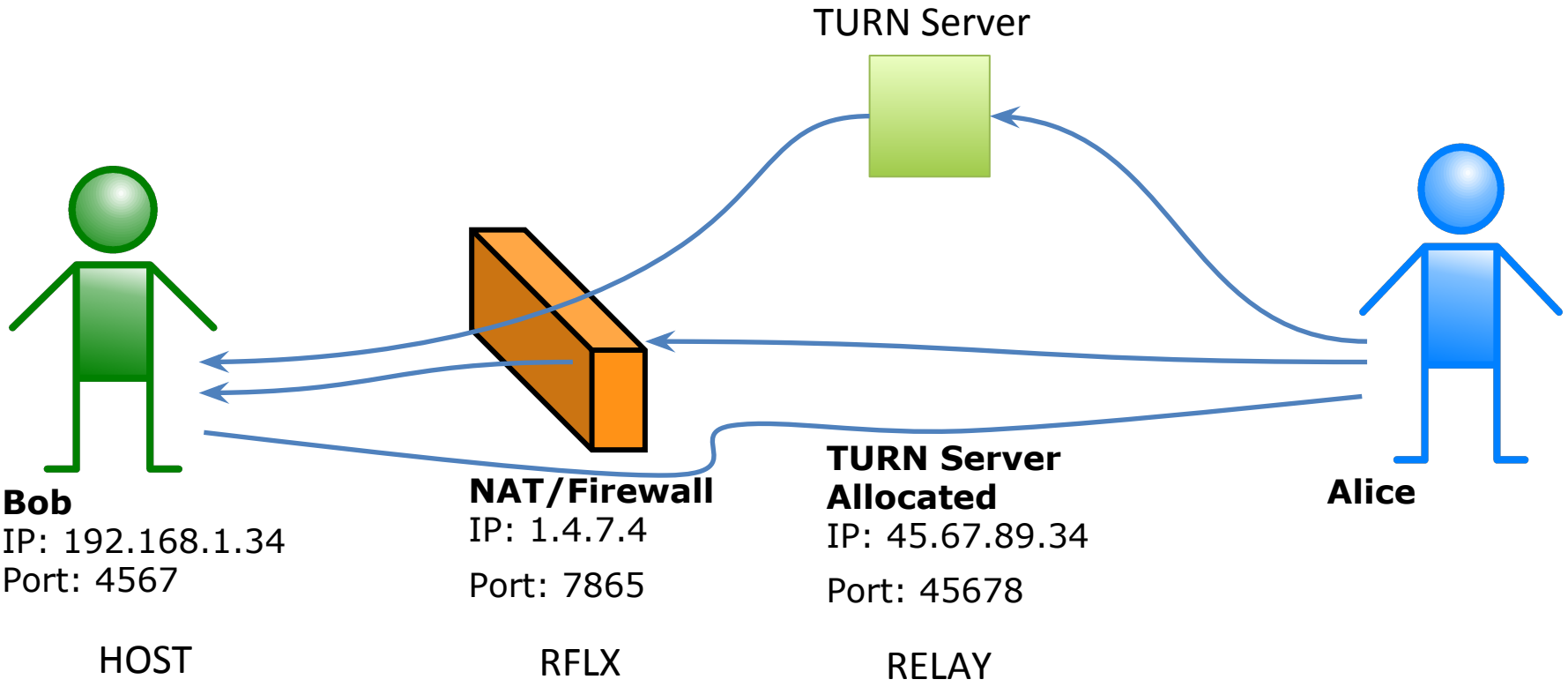
RFLX

TURN Server Allocated
IP: 45.67.89.34

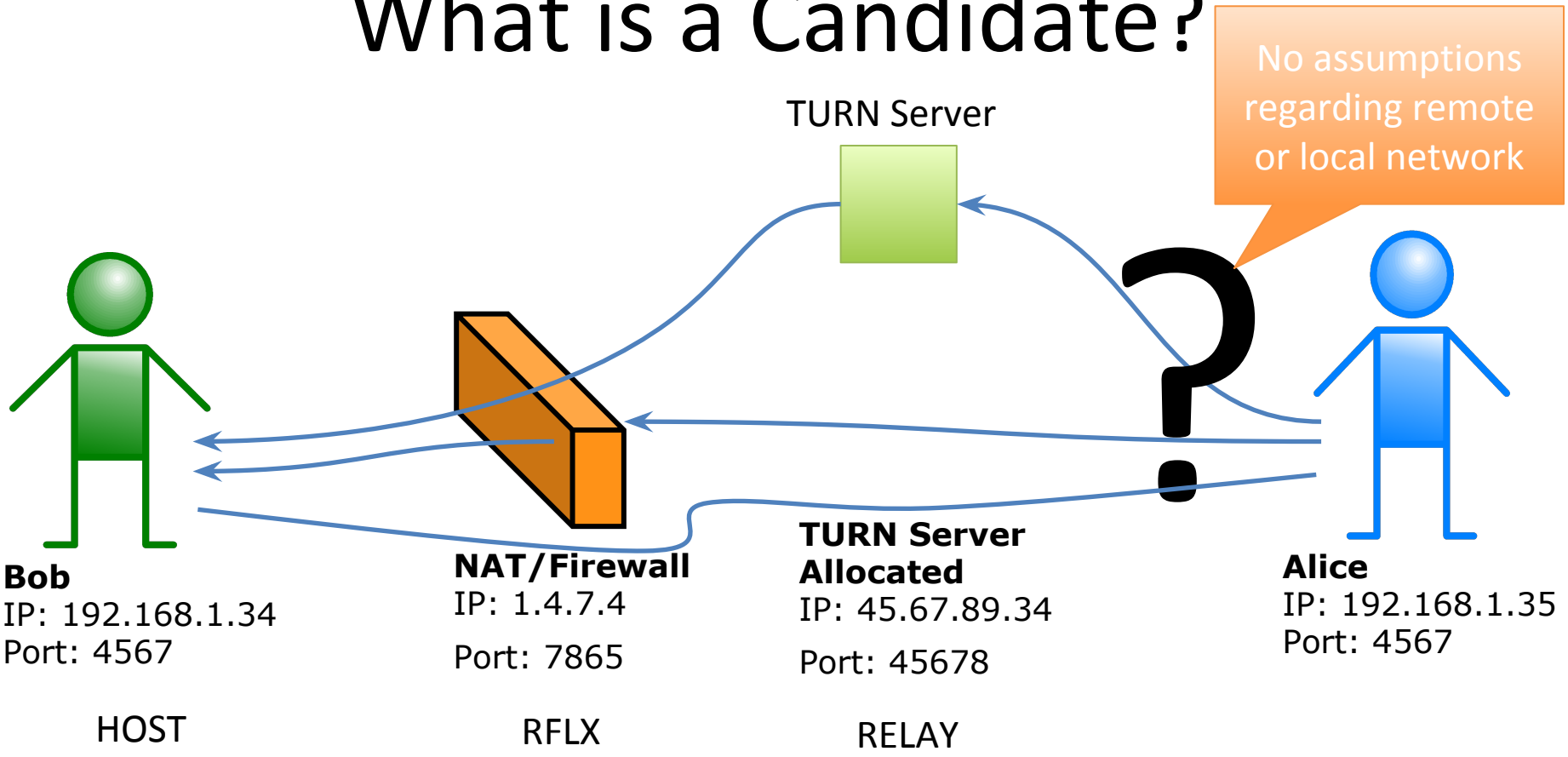
Port: 45678

RELAY

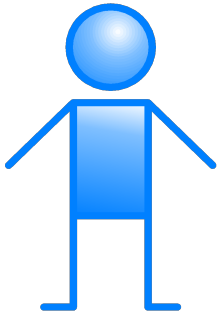
What is a Candidate?

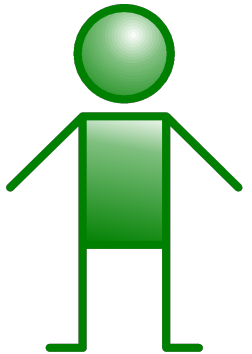


What is a Candidate?

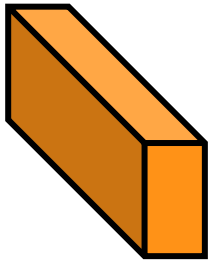


What is a Candidate?





Alice can even be on the desk next to Bob..



Bob
IP: 192.168.1.34
Port: 4567

HOST

NAT/Firewall
IP: 1.4.7.4

Port: 7865

RFLX

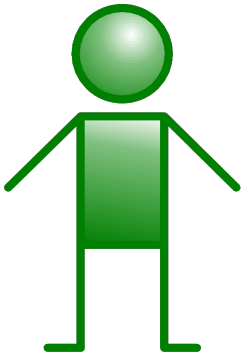
TURN Server Allocated
IP: 45.67.89.34

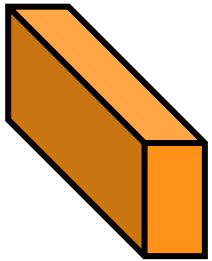
Port: 45678

RELAY

Candidate Gathering

TURN Server

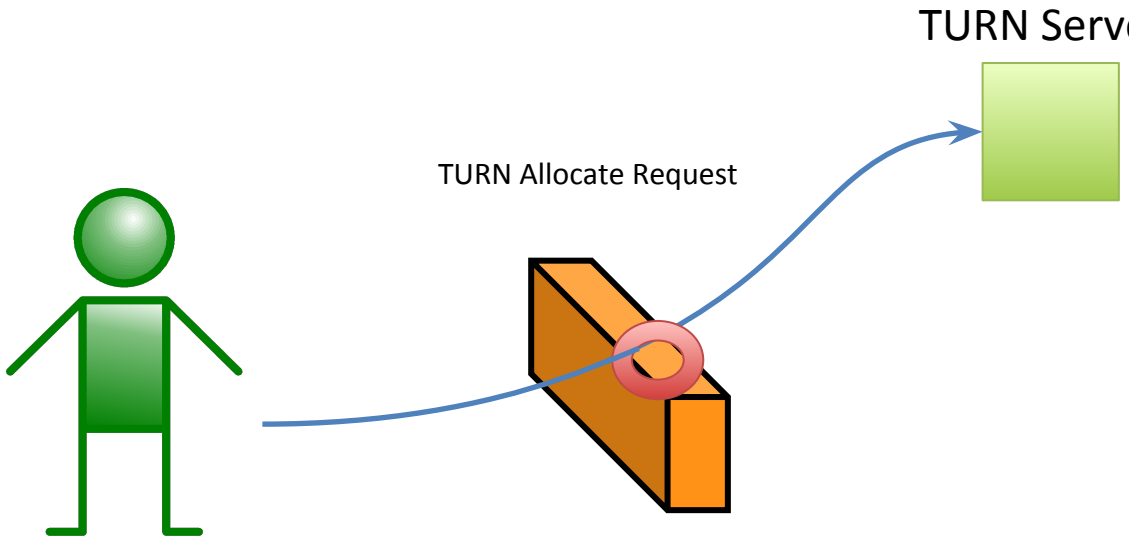




Bob
IP: 192.168.1.34
Port: 4567

HOST

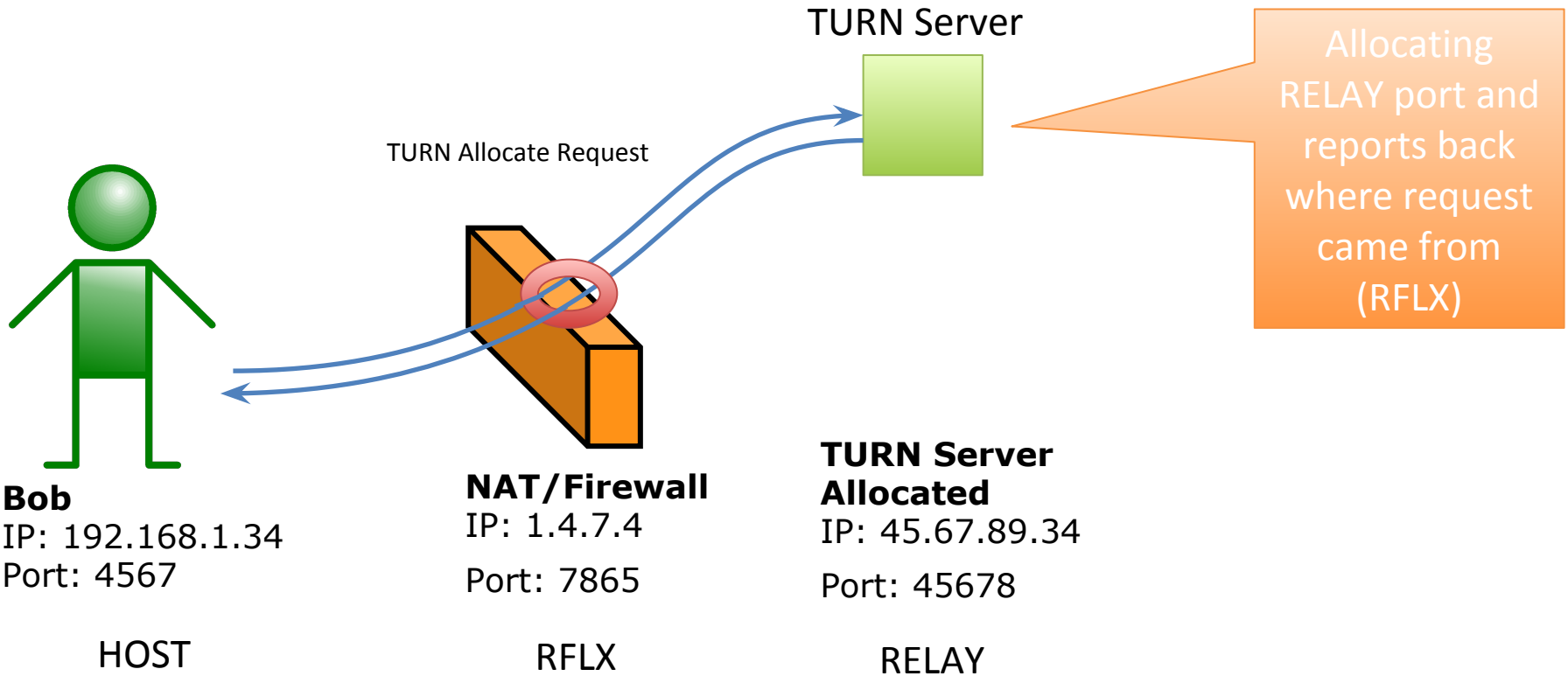
Candidate Gathering



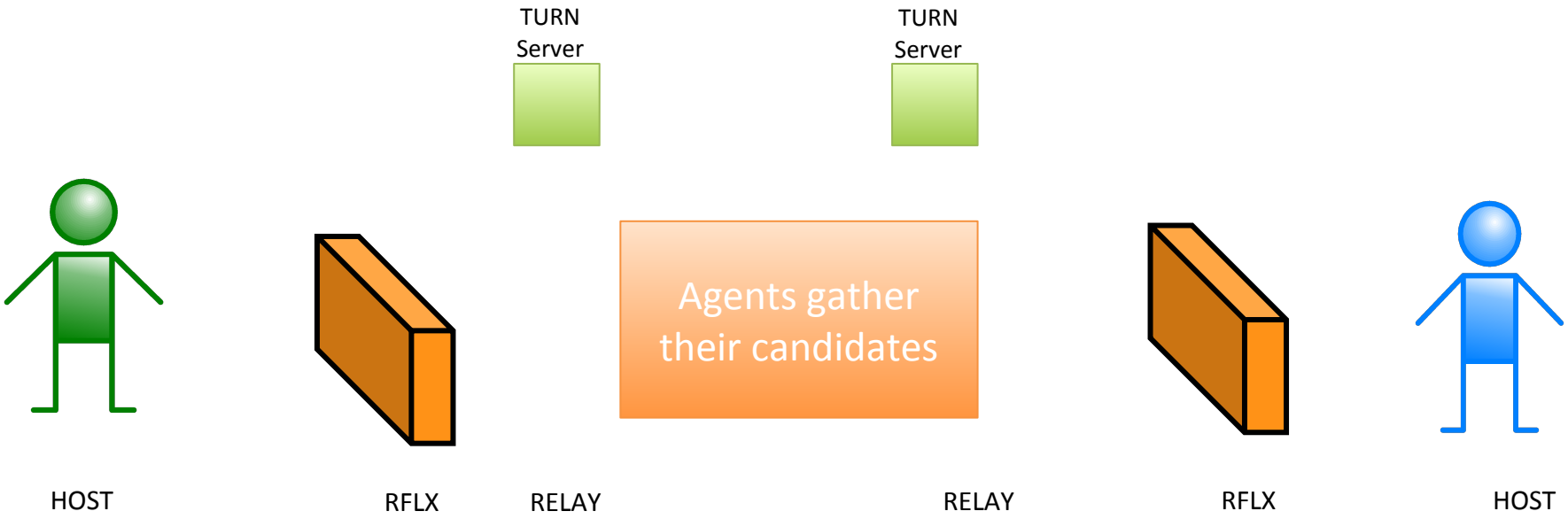
Bob
IP: 192.168.1.34
Port: 4567

HOST

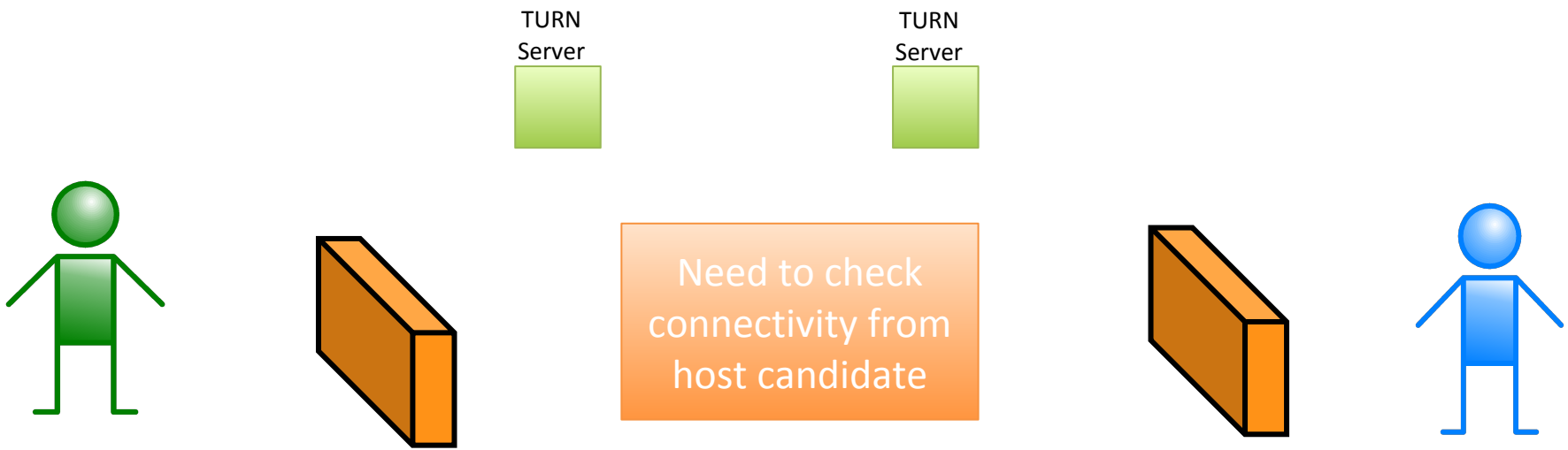
Candidate Gathering

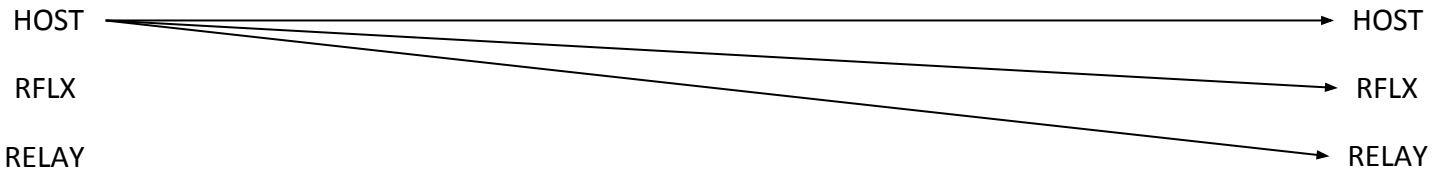


Checklist

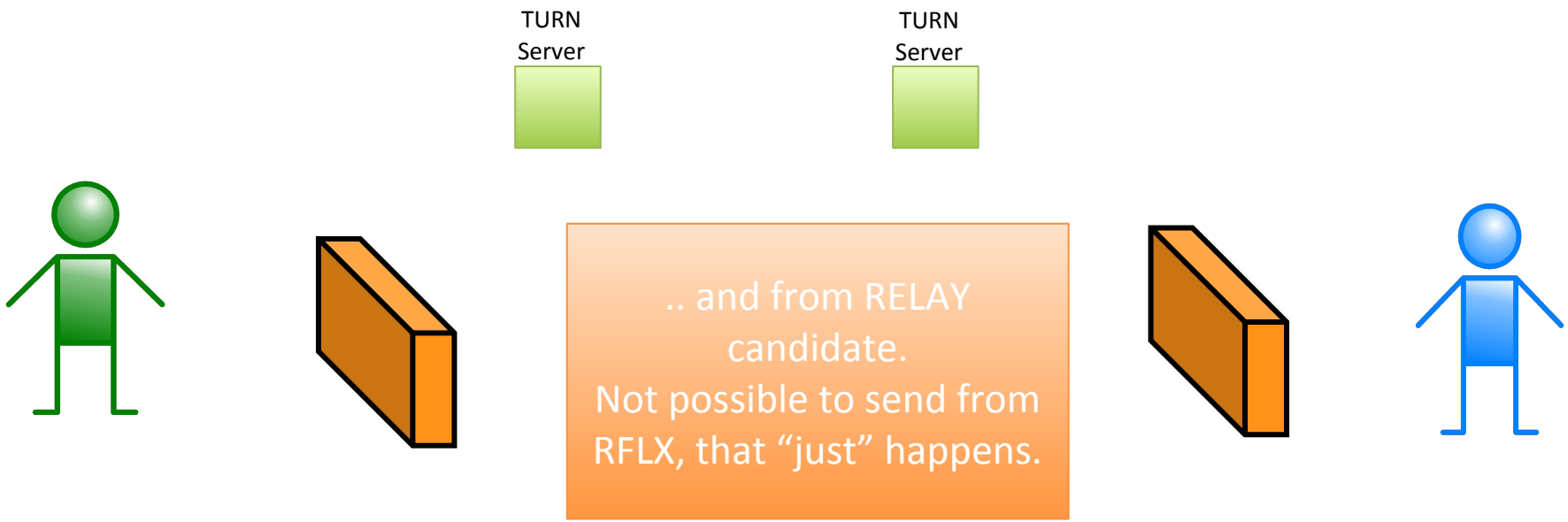

TURN Server
TURN Server
Agents gather their candidates
HOST
RFLX
RELAY
RELAY
RFLX
HOST

Checklist

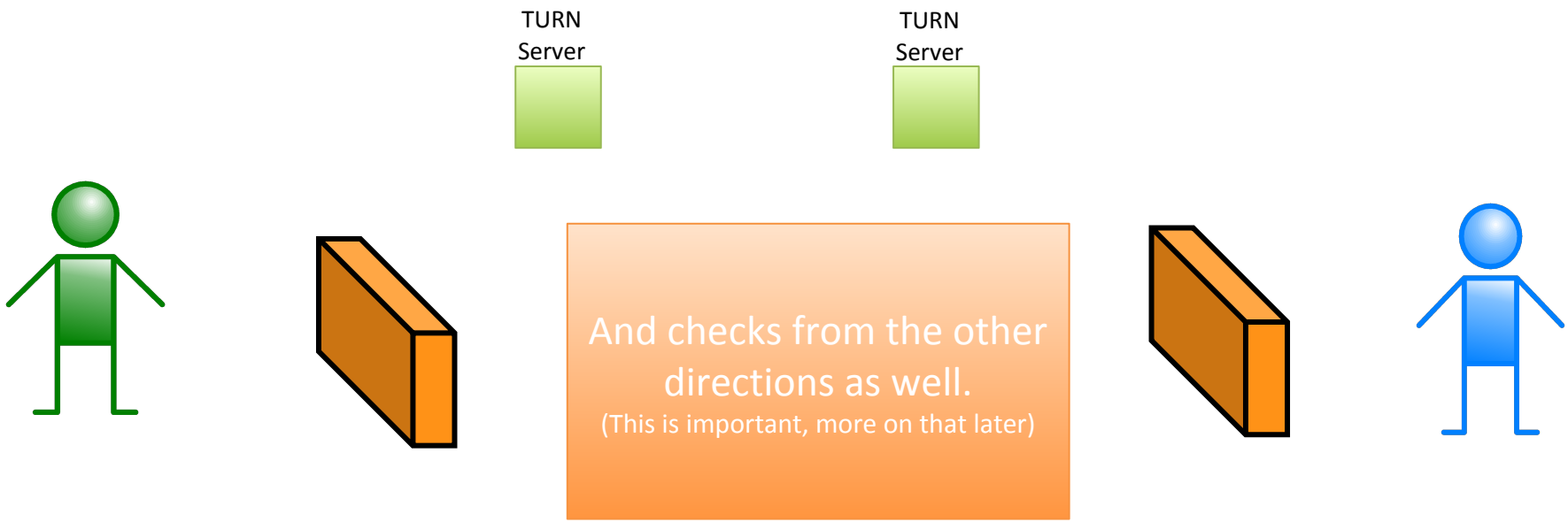

TURN Server
TURN Server
Need to check connectivity from host candidate


HOST
RFLX
RELAY
HOST
RFLX
RELAY

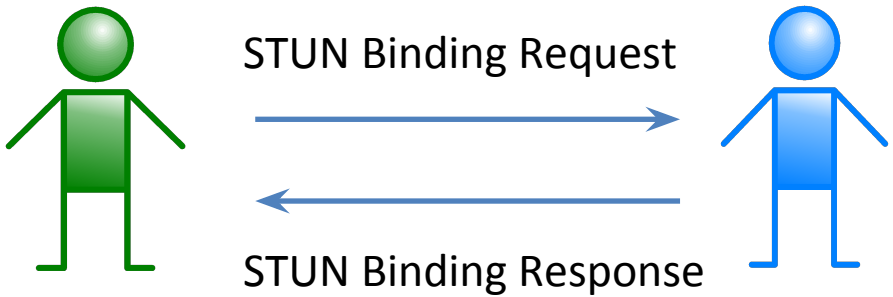
Checklist


TURN
Server
TURN
Server
.. and from RELAY
candidate.
Not possible to send from
RFLX, that “just” happens.
HOST
RFLX
RELAY
HOST
RFLX
RELAY

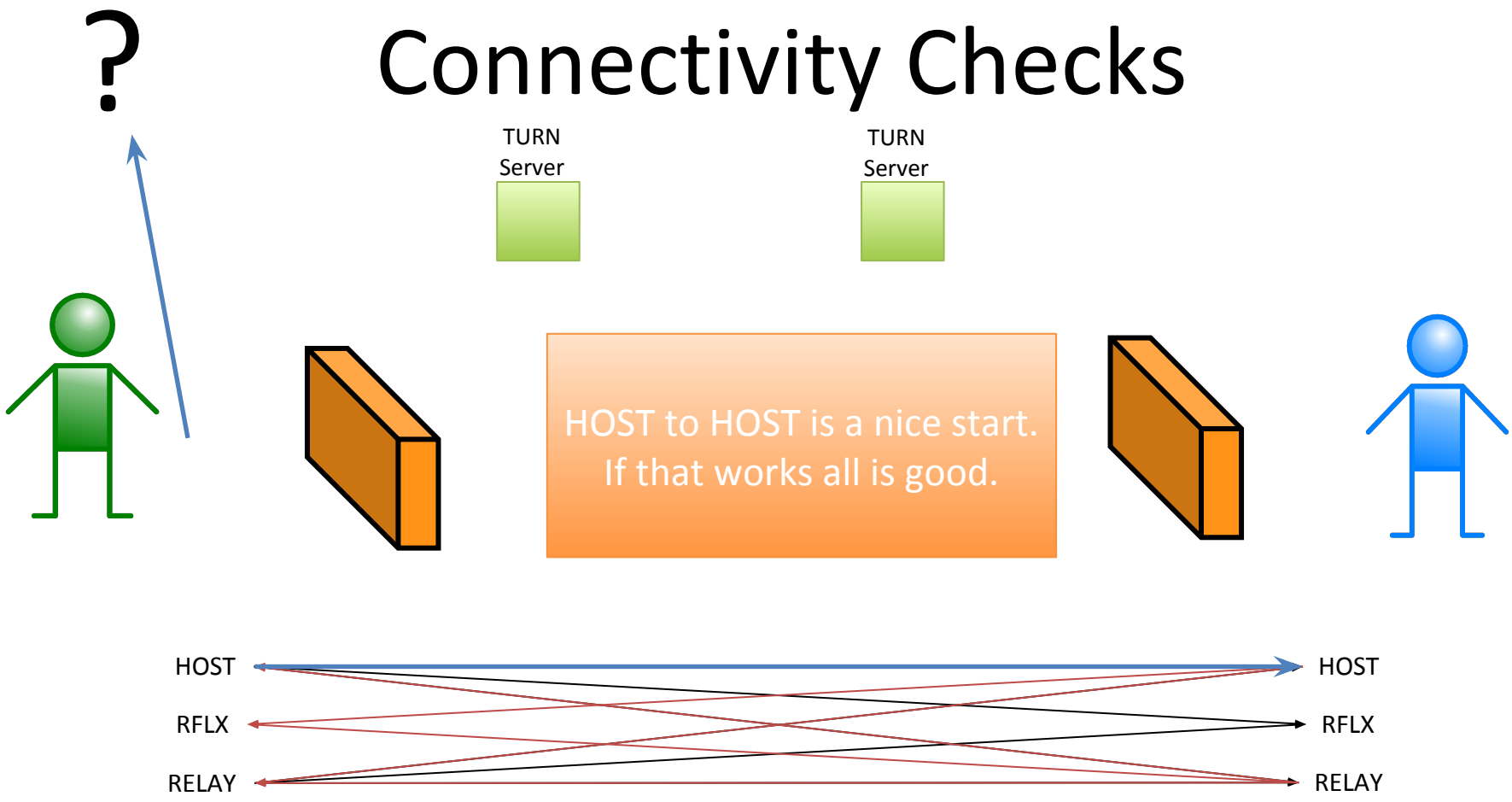
Checklist


TURN
Server
TURN
Server
And checks from the other directions as well.
(This is important, more on that later)
HOST
RFLX
RELAY
HOST
RFLX
RELAY

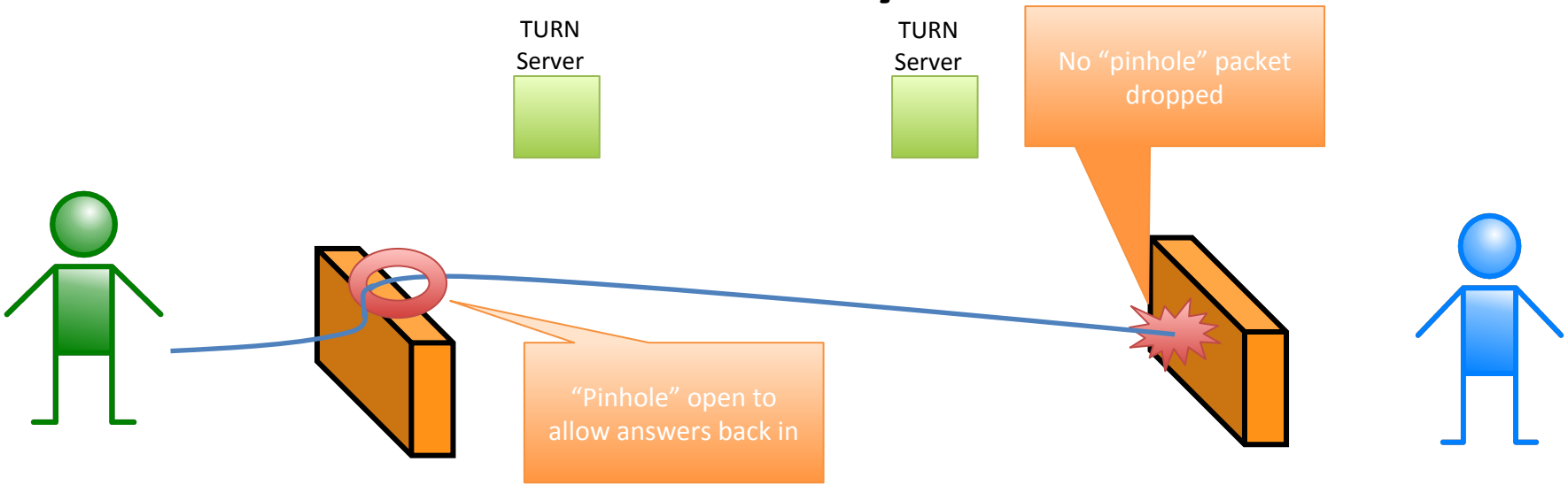
Connectivity Check

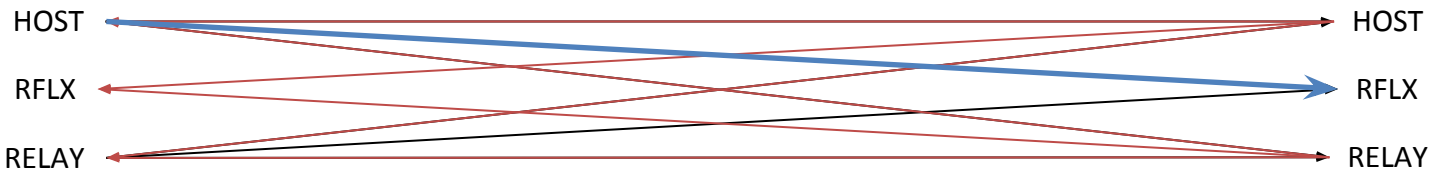


Connectivity Checks

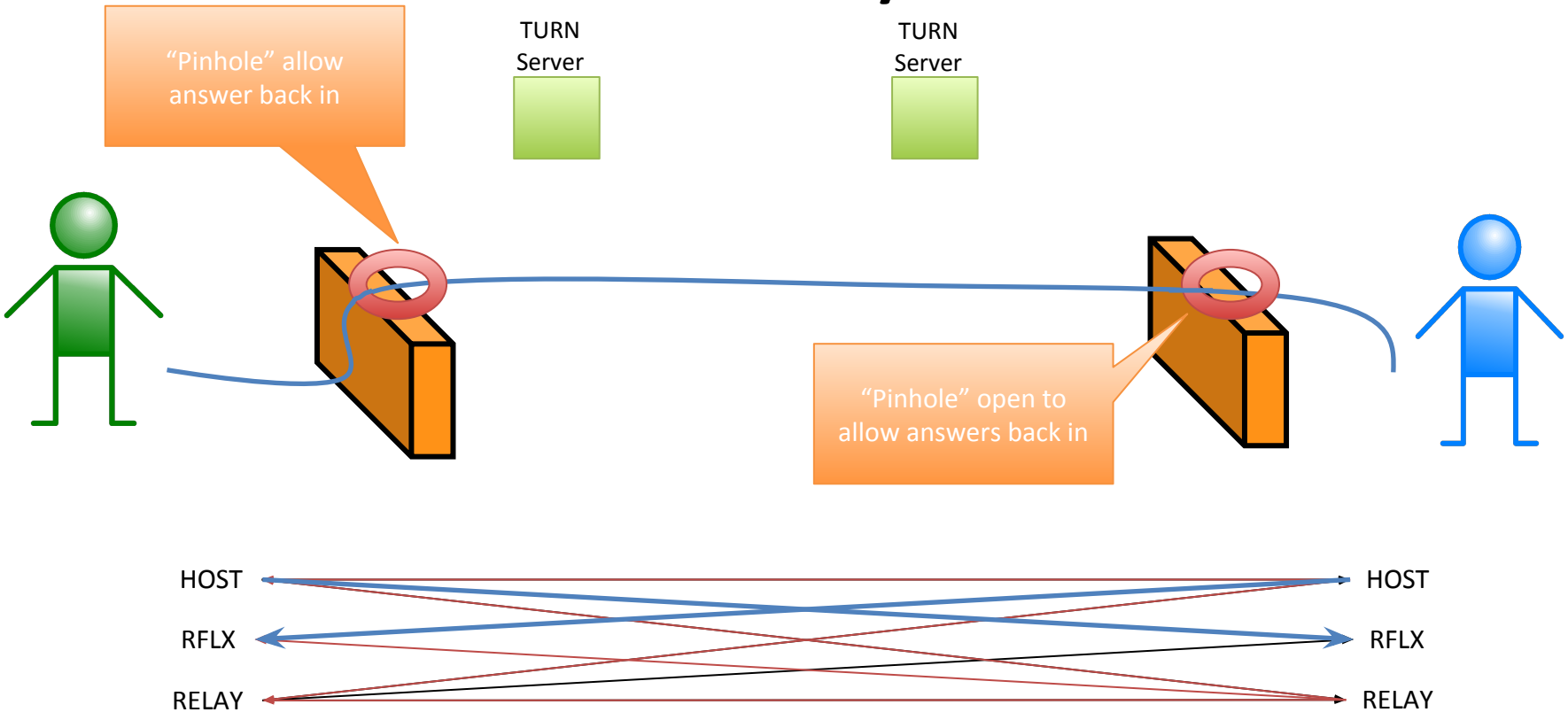


Connectivity Checks

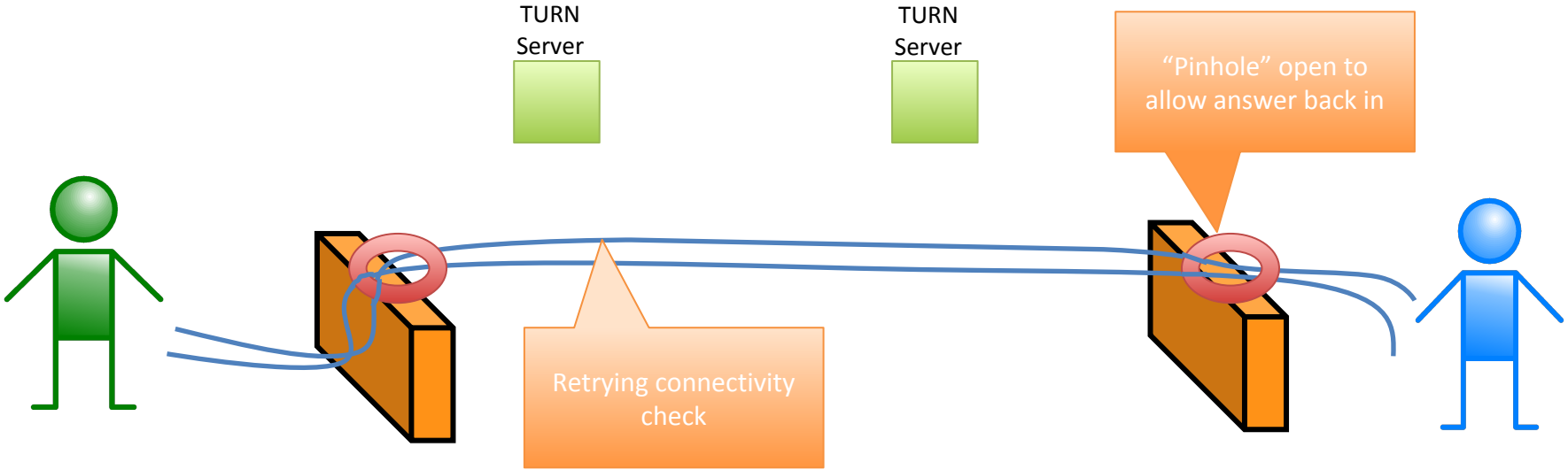


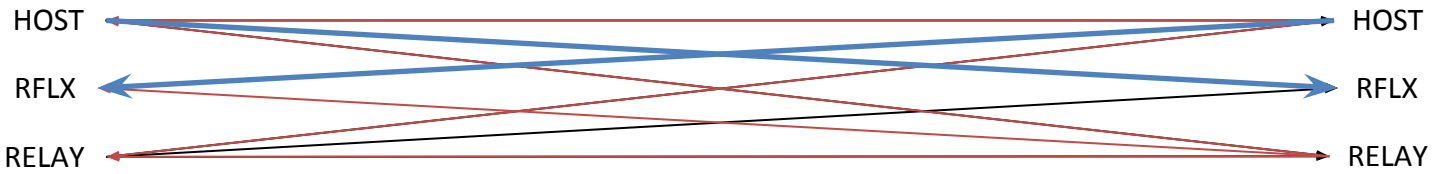


Connectivity Checks

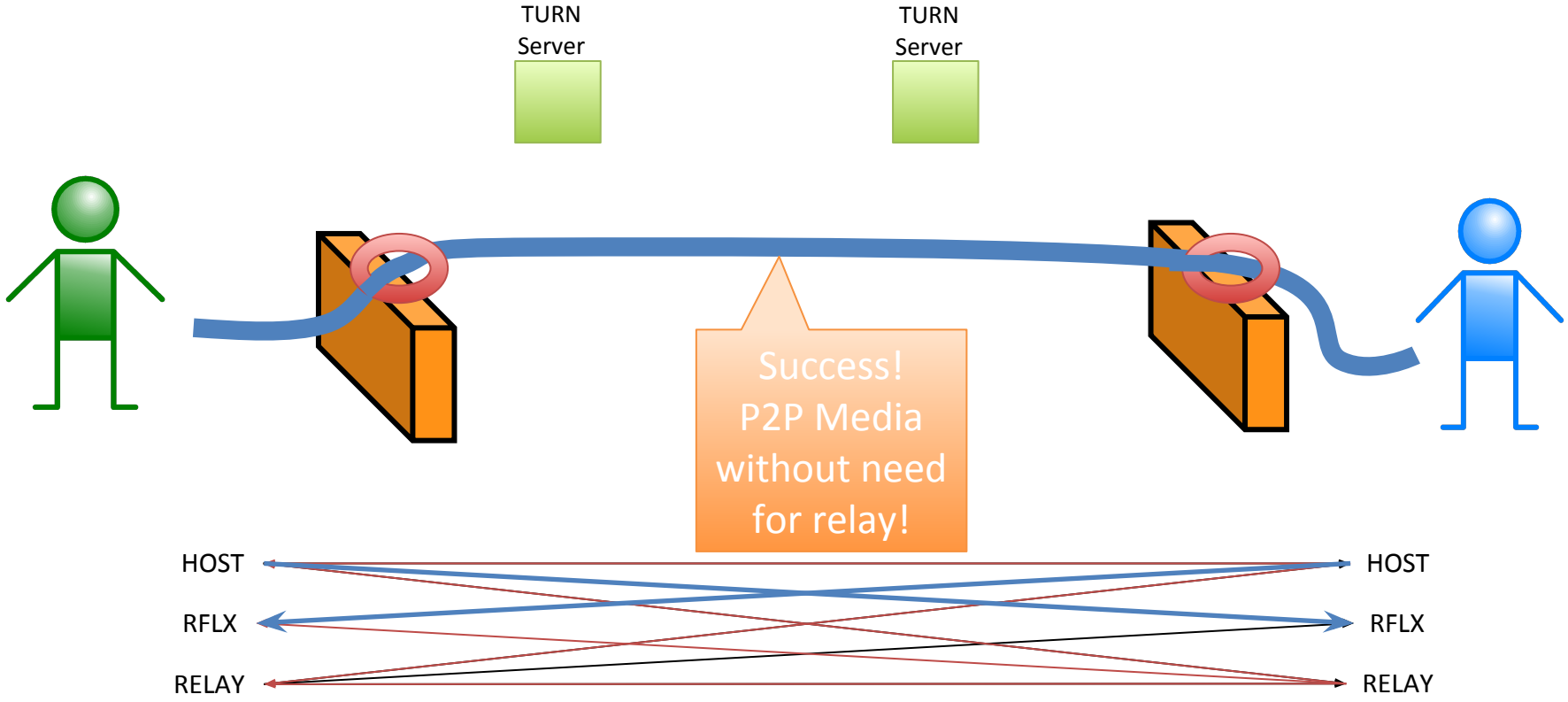


Connectivity Checks

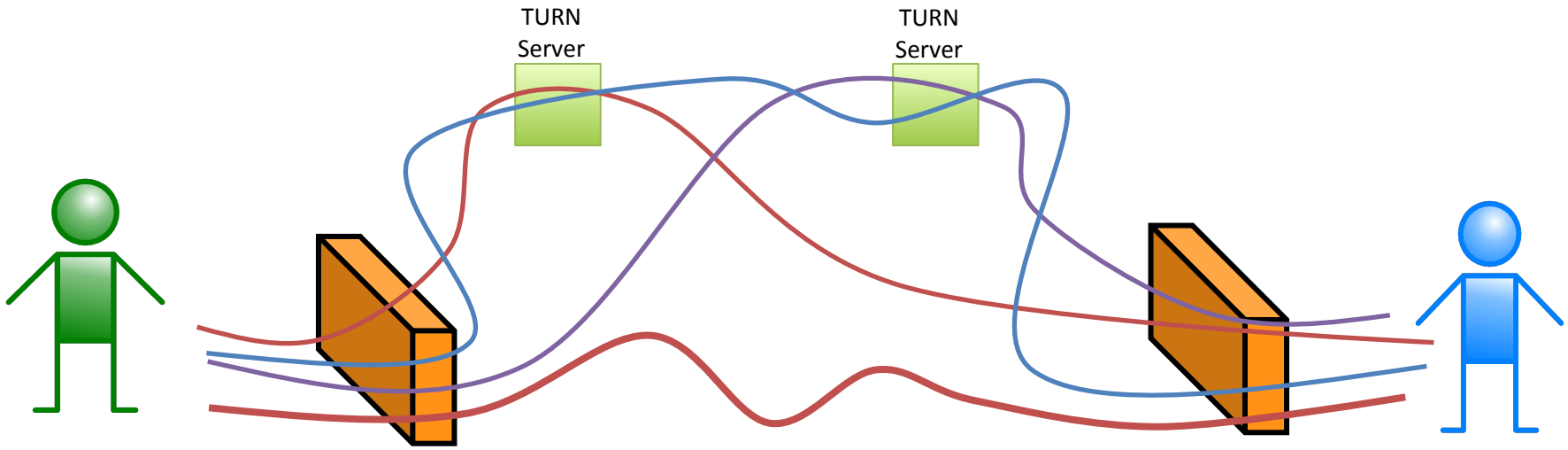




Concluding


TURN Server
TURN Server
Success! P2P Media without need for relay!
HOST
RFLX
RELAY
HOST
RFLX
RELAY

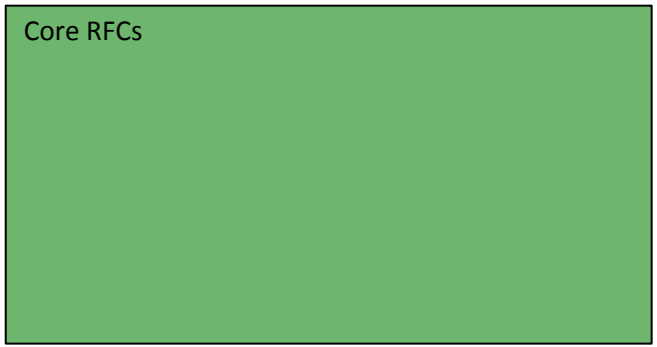
Concluding



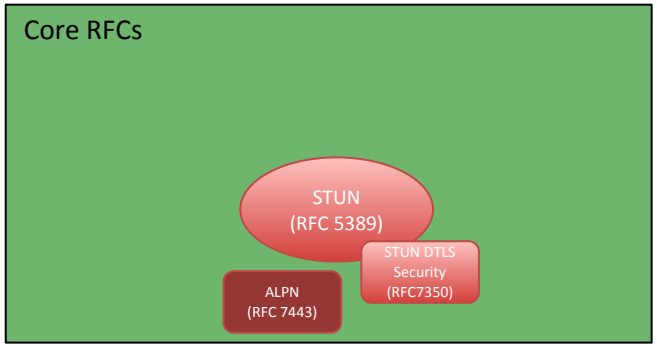
Dependent on the NAT/FW media might take many paths

IETF RFCS, DRAFTS AND I-DS

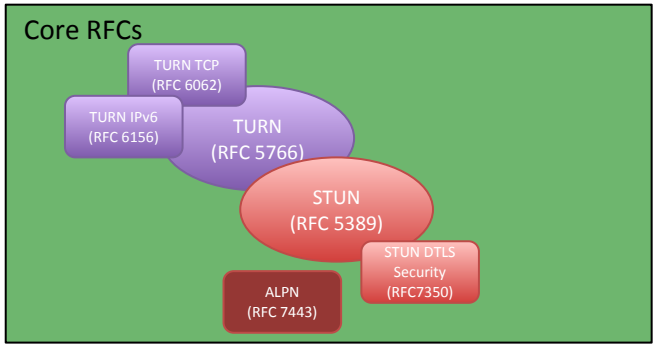
RFCs, drafts and I-Ds



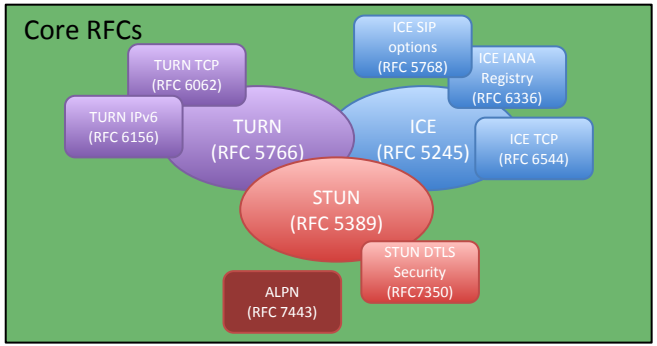
RFCs, drafts and I-Ds



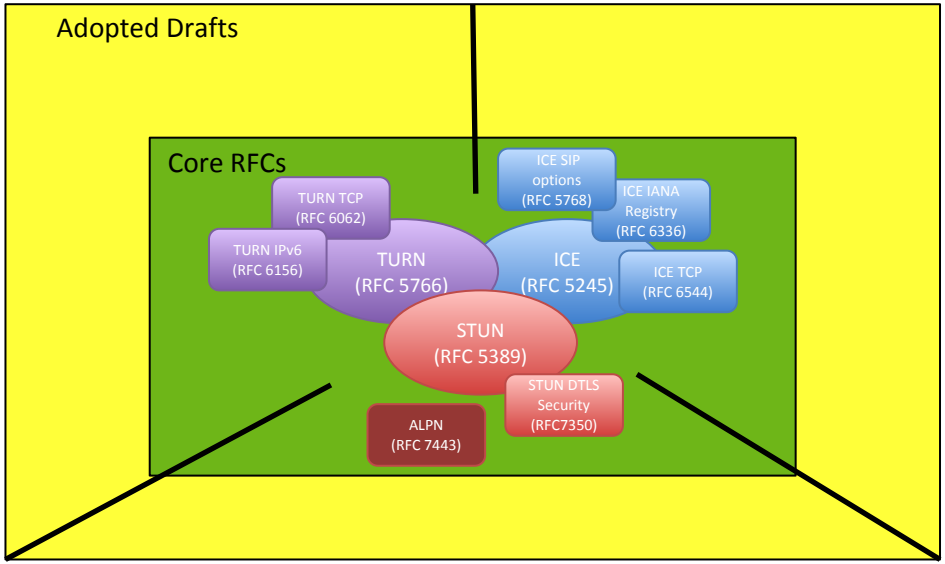
RFCs, drafts and I-Ds



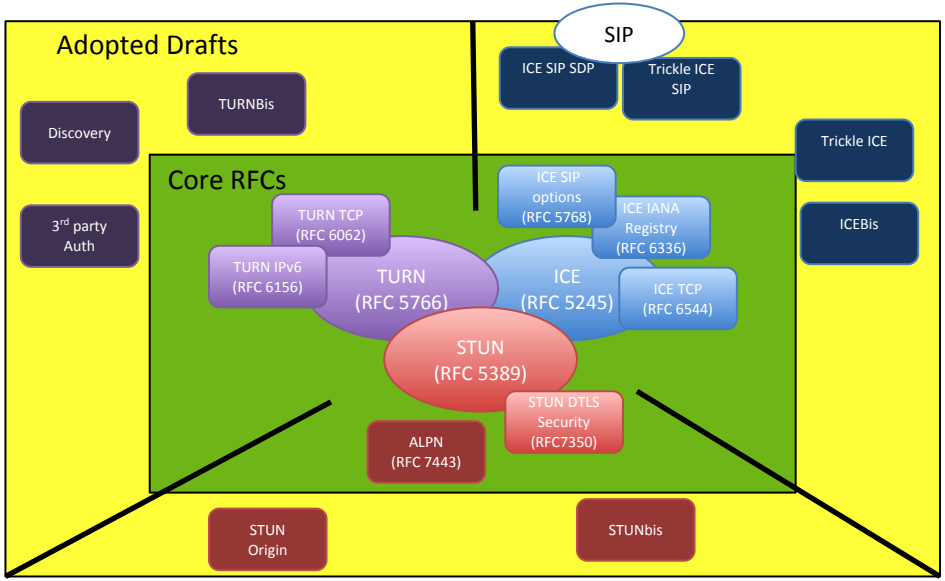
RFCs, drafts and I-Ds



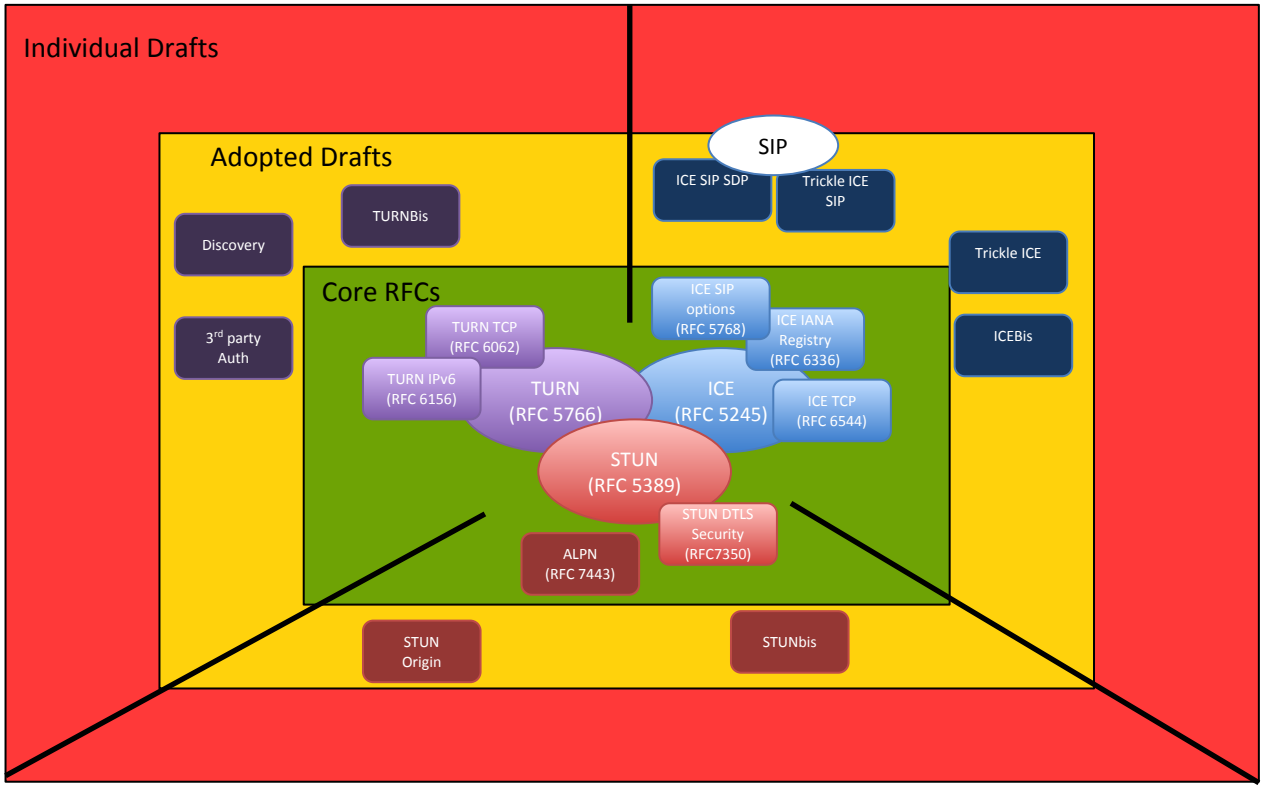
RFCs, drafts and I-Ds



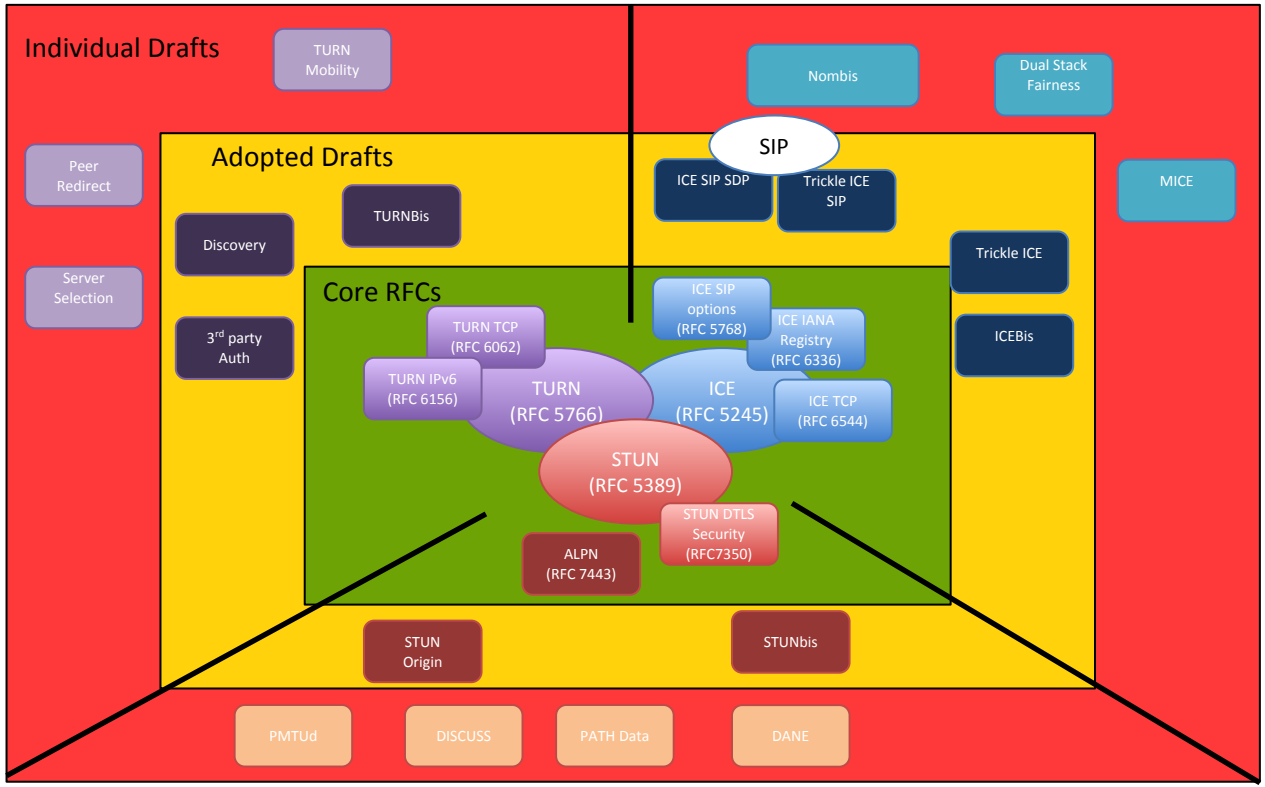
RFCs, drafts and I-Ds



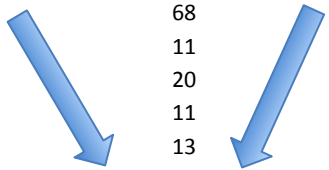
RFCs, drafts and I-Ds



RFCs, drafts and I-Ds



RFC/Draft	Category	Name	Pages
ICE	RFC	RFC 5245	117
ICE SIP Options	RFC	RFC 5768	6
ICE IANA Registry	RFC		5
ICE TCP	RFC	RFC 6544	31
ICEBis	Adopted Draft	draft-ietf-mmusic-trickle-ice	89
ICE SIP SDP	Adopted Draft	draft-ietf-mmusic-ice-sip-sdp	41
Trickle ICE	Adopted Draft	draft-ietf-mmusic-trickle-ice	25
Trickle ICE SIP	Adopted Draft	draft-ietf-mmusic-trickle-ice-sip	22
Dual Stack Fairness	I-D	draft-martinsen-mmusic-ice-dualstack-fairness	8
MICE	I-D	draft-wing-mmusic-ice-mobility	16
Continious Nomination	?		0
STUN	RFC	RFC 5389	51
STUN DTLS	RFC	RFC 7350	16
STUN Origin	Adopted Draft	draft-ietf-tram-stun-origin	12
ALPN	RFC	RFC 7443	5
STUNbis	Adopted Draft	draft-ietf-tram-stunbis	51
PMTUd	I-D	draft-petithuguenin-tram-stun-pmtud	10
DISCUSS	I-D	draft-martinsen-tram-discuss	15
DANE	I-D	draft-petithuguenin-tram-stun-dane	7
PATH Data	I-D	draft-reddy-tram-stun-path-data	9
TURN	RFC	RFC 5766	67
TURN TCP	RFC	RFC 6062	13
TURN IPv6	RFC	RFC 6156	14
TURNbis	Adopted Draft	draft-ietf-tram-turnbis	68
Discovery	Adopted Draft	draft-ietf-tram-turn-server-discovery	11
3rd Party Auth	Adopted Draft	draft-ietf-tram-turn-third-party-authz	20
TURN Mobility	I-D	draft-wing-tram-turn-mobility	11
Peer Redirect	I-D	draft-williams-peer-redirect	13
Server Selection	I-D	draft-patil-tram-turn-serv-selection	7
			760

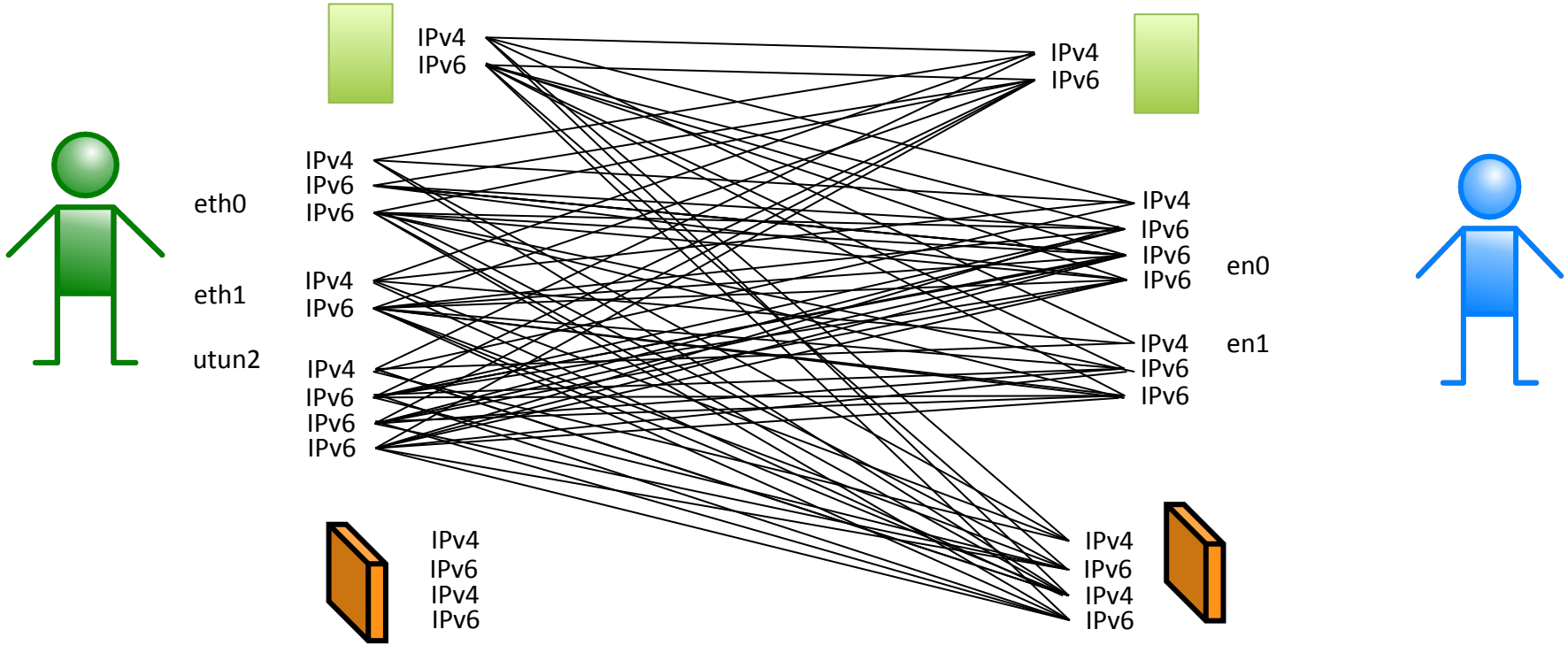


SUMMARY

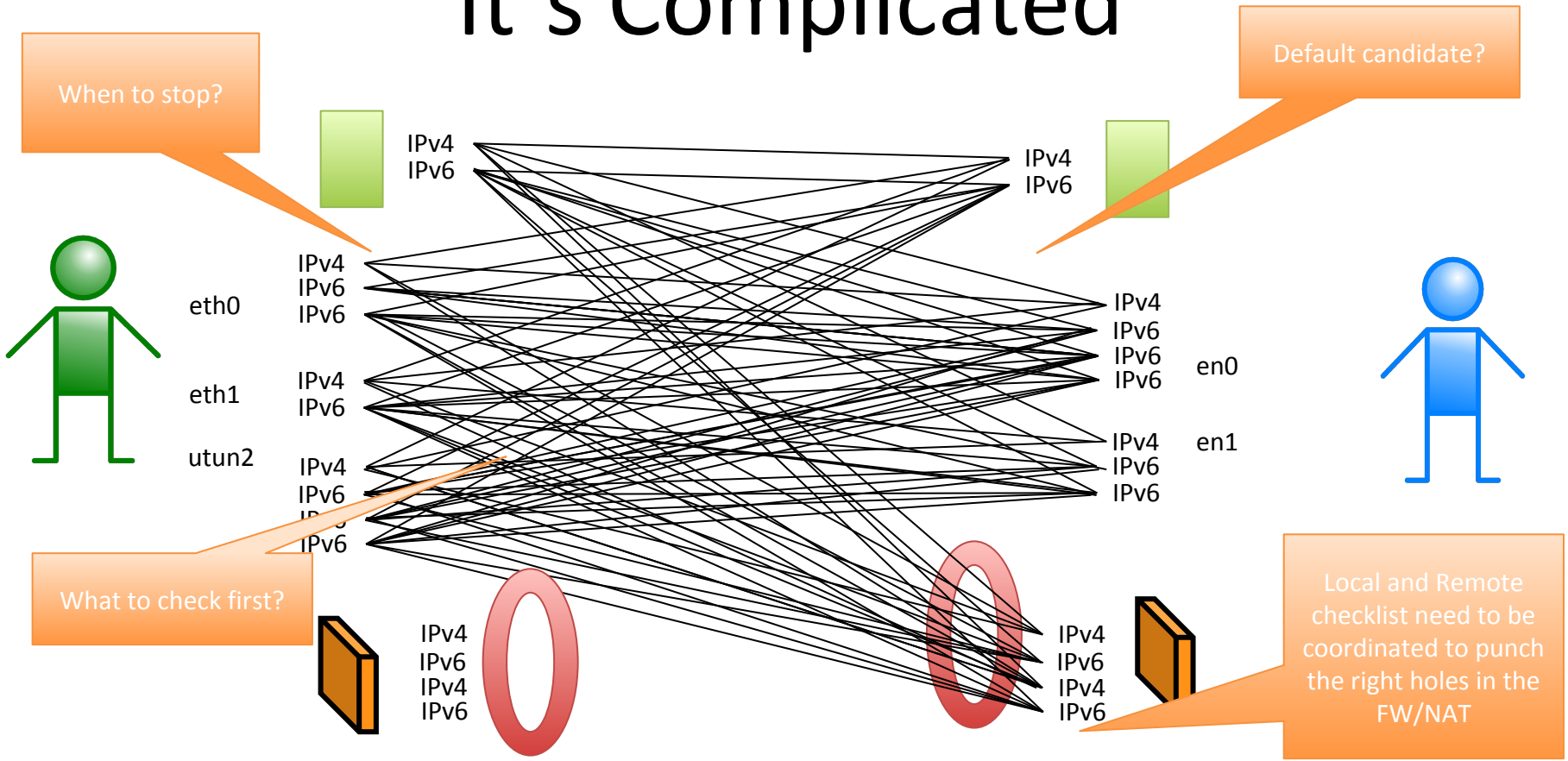
Main Steps

- Gather candidates
- Exchange candidates
  (Signaling path, SIP/XMPP, etc.)
- Create checklist and do connectivity checks
- Stop, conclude and send media

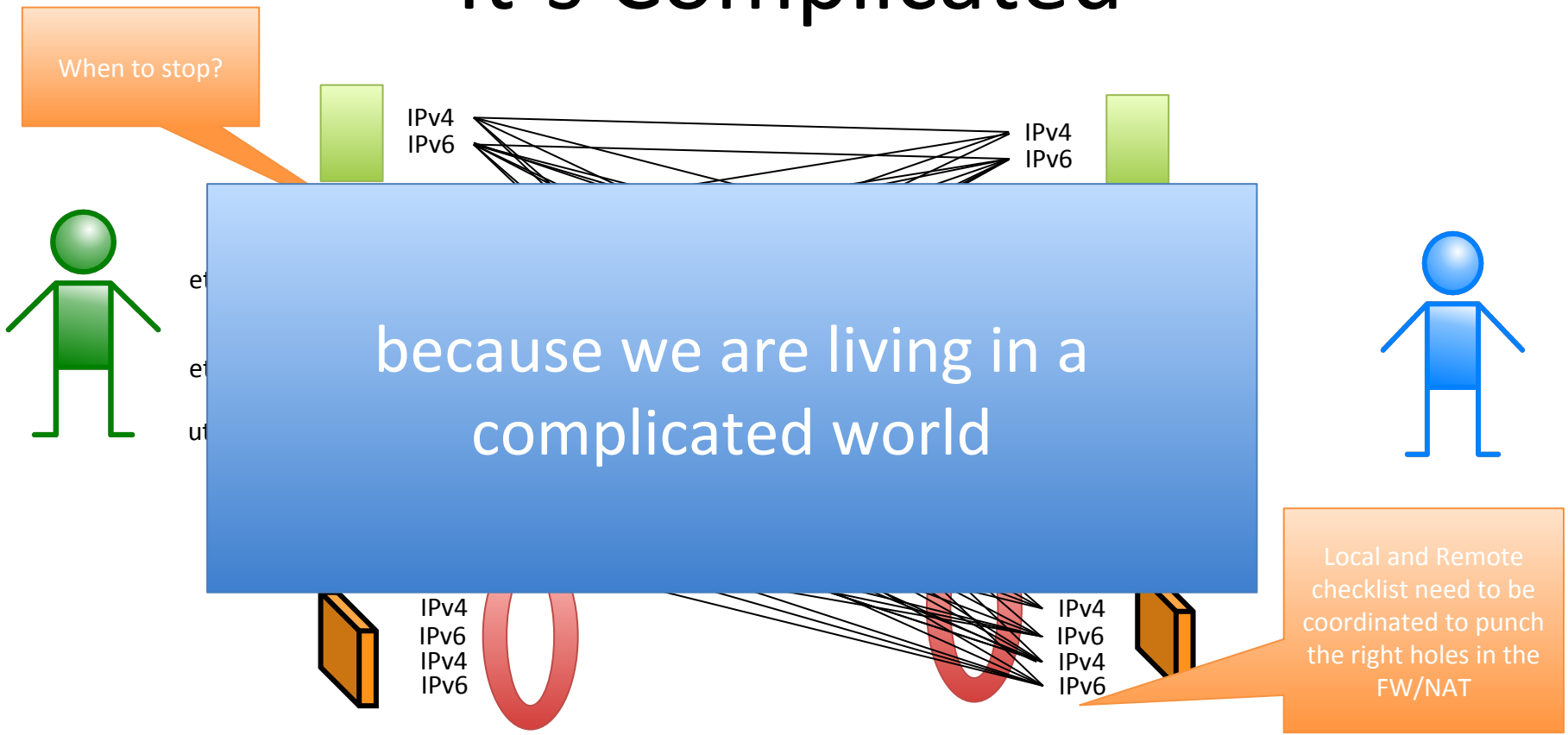
It´s Complicated



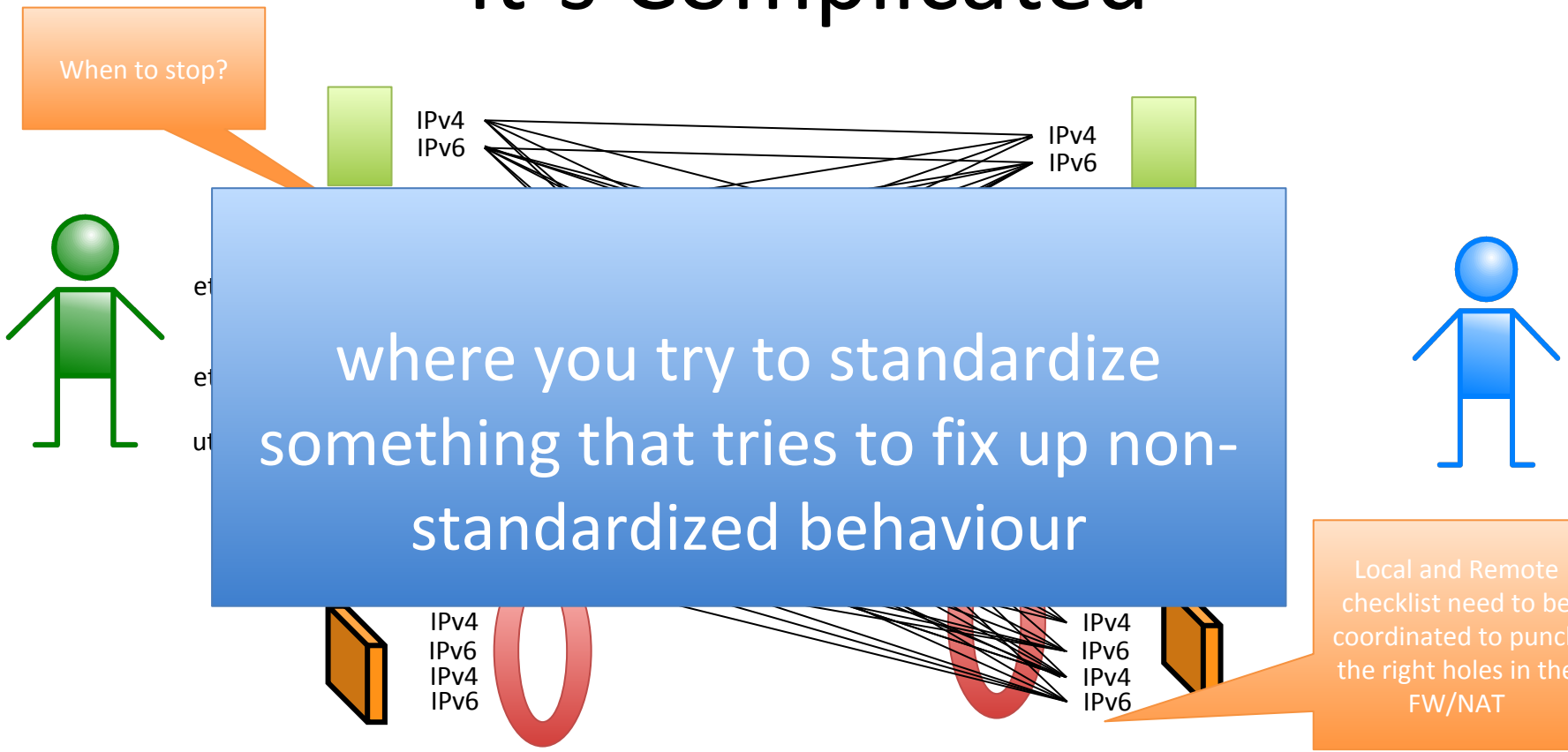
It´s Complicated



It´s Complicated



It´s Complicated



… the end

Authors / Presenters

Pål-Erik Martinsen (Cisco)

Emil Ivov (Jitsi)

Justin Uberti (Google)

Brandon Williams (Akamai)