Preferred Alternatives for Tunnelling HIP (PATH)

Pekka Nikander

61st IETF, Thursday Nov 11th, 2004

Presentation outline

- Goals and non-goals
- Proposed approach
- Details

Goals and non-goals

- Make HIP work through legacy NATs
  - Maybe also some firewalls, but not all
- Make HIP hosts reachable behind NATs
- Lean as much as possible to the ugly work done elsewhere; don't reinvent the wheel

Proposed approach

- Integrate a HIP rendezvous and a STUN server
- Refer to:
  - draft-ietf-behave-rfc3489bis-00.txt
  - draft-ietf-hip-registration-00.txt
  - draft-ietf-hip-rvs-00.txt
  - draft-ietf-hip-mm-00.txt
  - draft-ietf-ipsec-udp-encaps-09.txt
- UDP REA parameter for m

Details

- HIP over UDP
- UDP-REA parameter
- HIP registration to a STUN/RVS server
- Contacting a HIP host behind a NAT
- Deriving STUN username and key from HIP

HIP over UDP

<table>
<tr><td colspan="3">IP header</td></tr>
<tr><td>Source port</td><td colspan="2">Destination port</td></tr>
<tr><td>Length</td><td colspan="2">Checksum</td></tr>
<tr><td>Controls</td><td>Type</td><td>Nxt Hdr</td></tr>
<tr><td colspan="3">Sender’s HIT</td></tr>
<tr><td colspan="3">Receiver’s HIT</td></tr>
<tr><td colspan="3">HIP parameters, if any</td></tr>
</table>

Details

- Checksum and Length in the UDP header
  - Not repeated in the HIP header
- HIP version determined by the destination port used when sending the `I1` packet
- SIG / HMAC computed over the *original* format
  - First construct "normal" HIP packet, compute HMAC and SIG, then convert to HIP over UDP format

NAT-T ESP packet format

<table>
<tr><td colspan="2">IP header</td></tr>
<tr><td>Source port</td><td>Destination port</td></tr>
<tr><td>Length</td><td>Checksum = 0</td></tr>
<tr><td colspan="2">ESP SPI</td></tr>
<tr><td colspan="2">ESP packet content</td></tr>
</table>

NAT-T IKE packet format

<table>
<tr><td colspan="2">IP header</td></tr>
<tr><td>Source port</td><td>Destination port</td></tr>
<tr><td>Length</td><td>Checksum</td></tr>
<tr><td colspan="2">zero</td></tr>
<tr><td colspan="2">IKE packet content</td></tr>
</table>

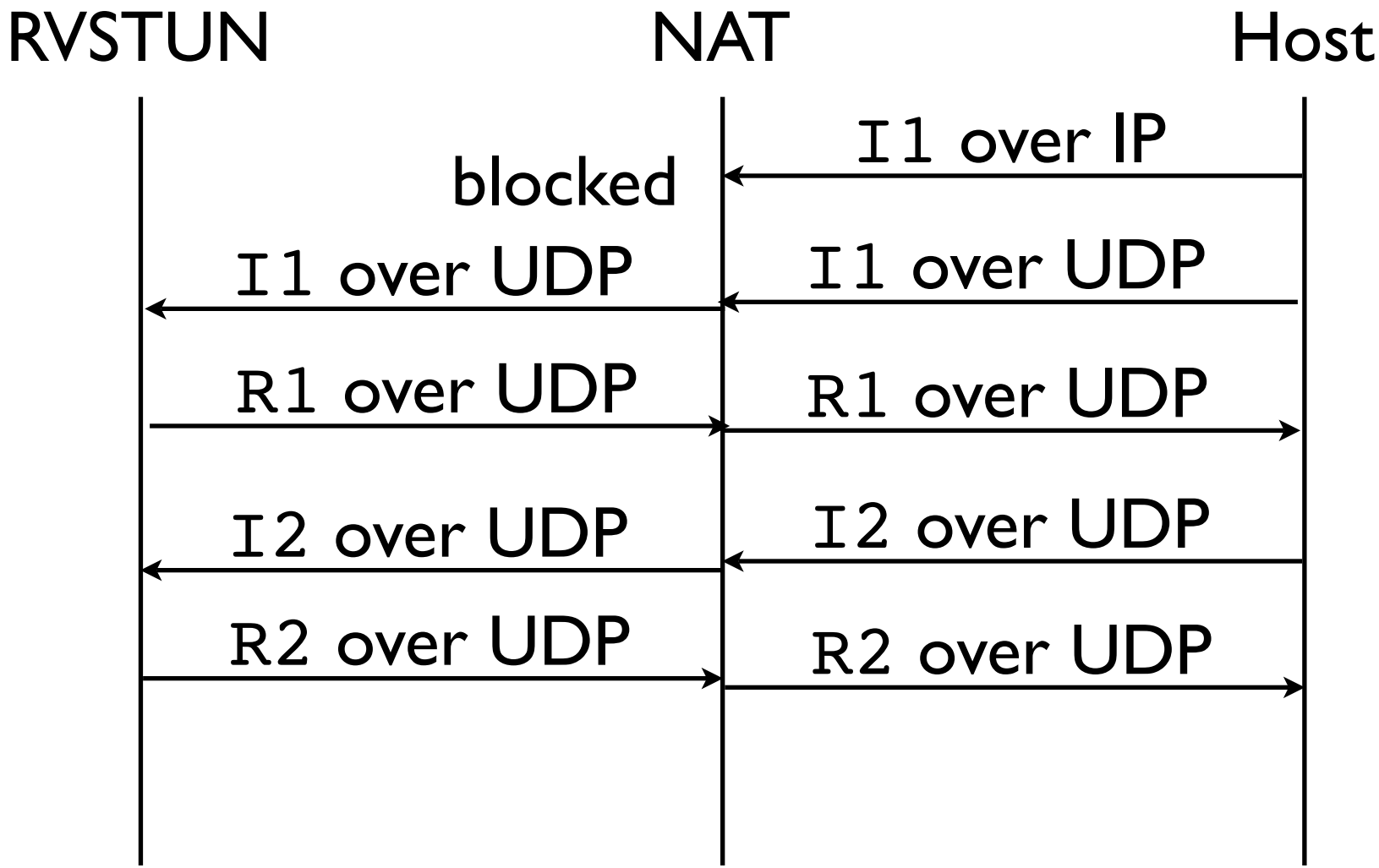
UDP-REA parameter

Type	Length
SPI	
Address Lifetime	
NAT keep alive frequency	
Sender's private IPv4 address	
Sender's private port	Receiver's port

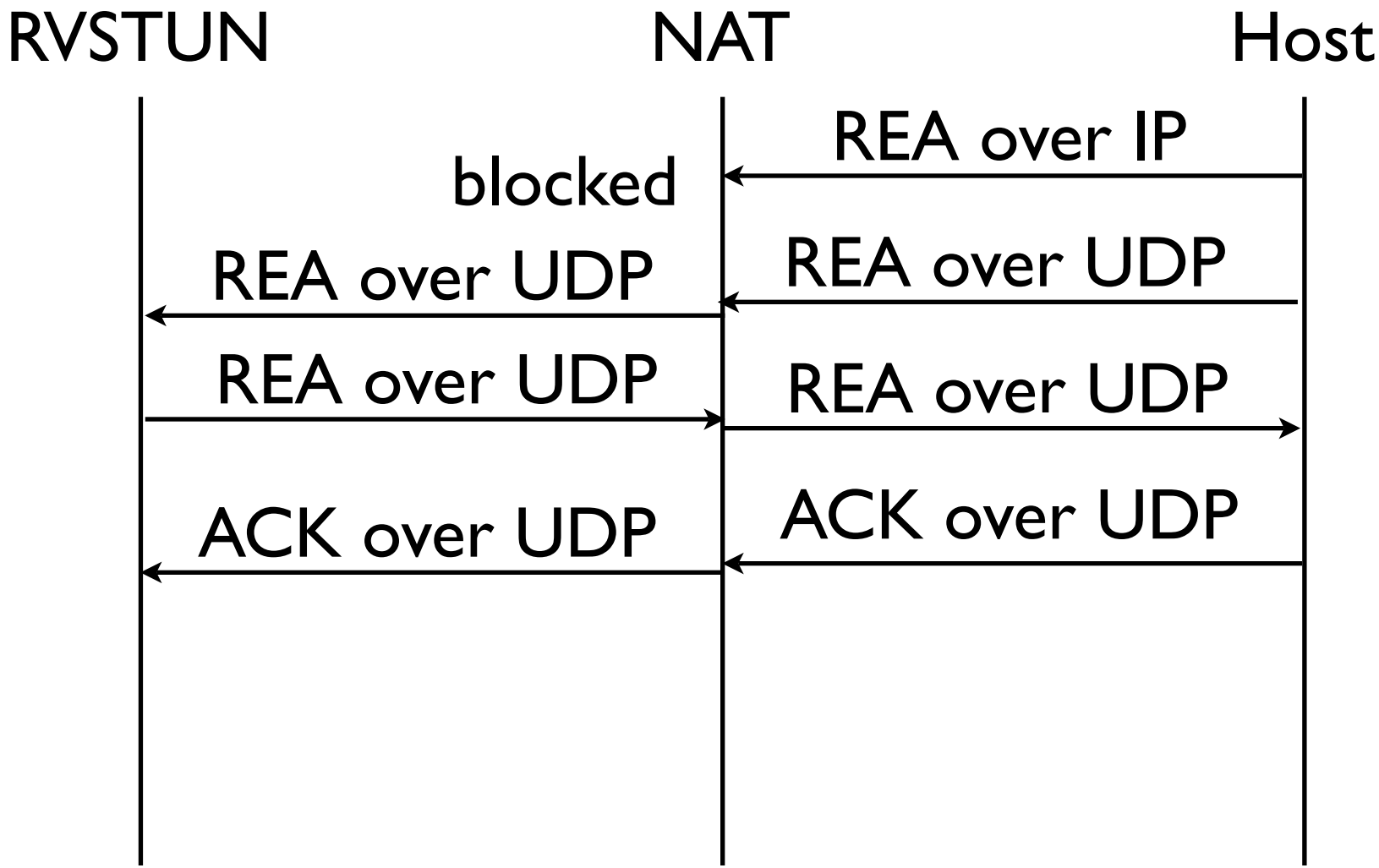
Details

- Perform NAT detection similar to STUN
- Send source address and ports as they are at the time of creating the packet
- Addresses and ports masked with something?
  - XORed with SPI?
    - What if SPI is moved to separate payload?

Running HIP registration



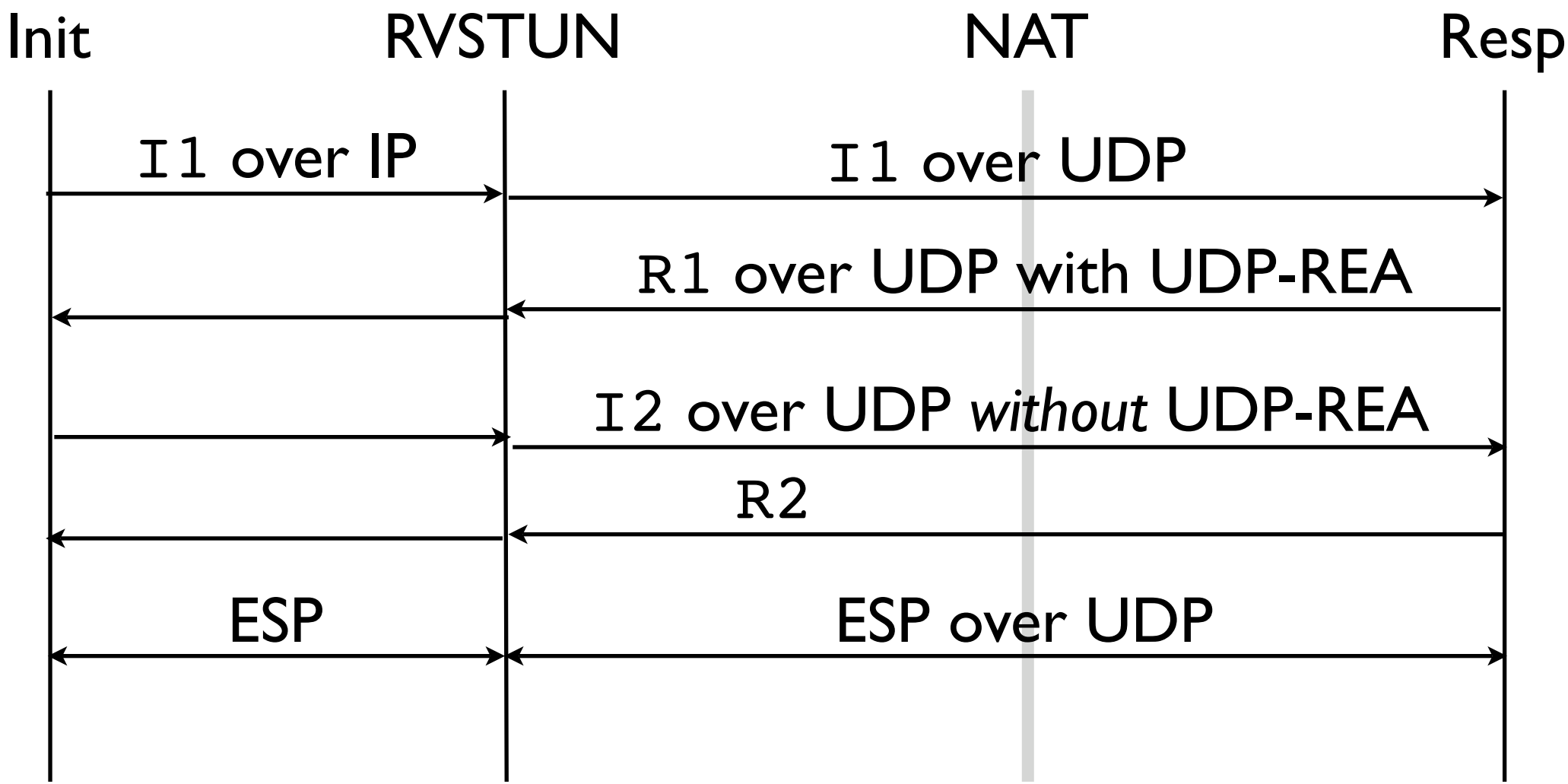
HIP mobility



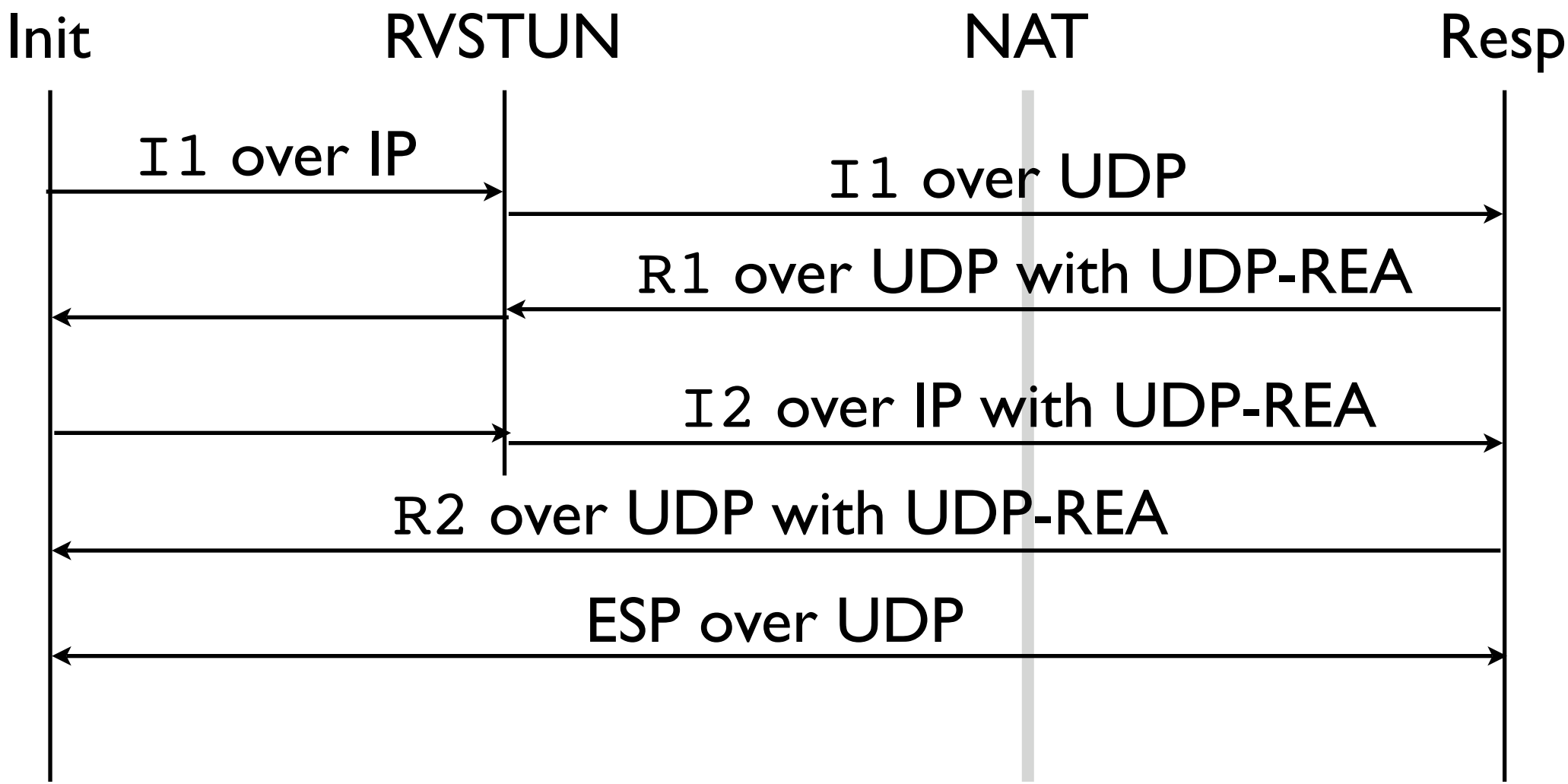
Details

- Short timeout (200ms) after first packet
  - Encourage NAT-less operation!
- Bypass timeout if in RFC1918 address space
  - Send `I1` over IP and `I1` over UDP a few milliseconds apart
- UDP-REA payload
  - Public IP and port
  - Information for ESP

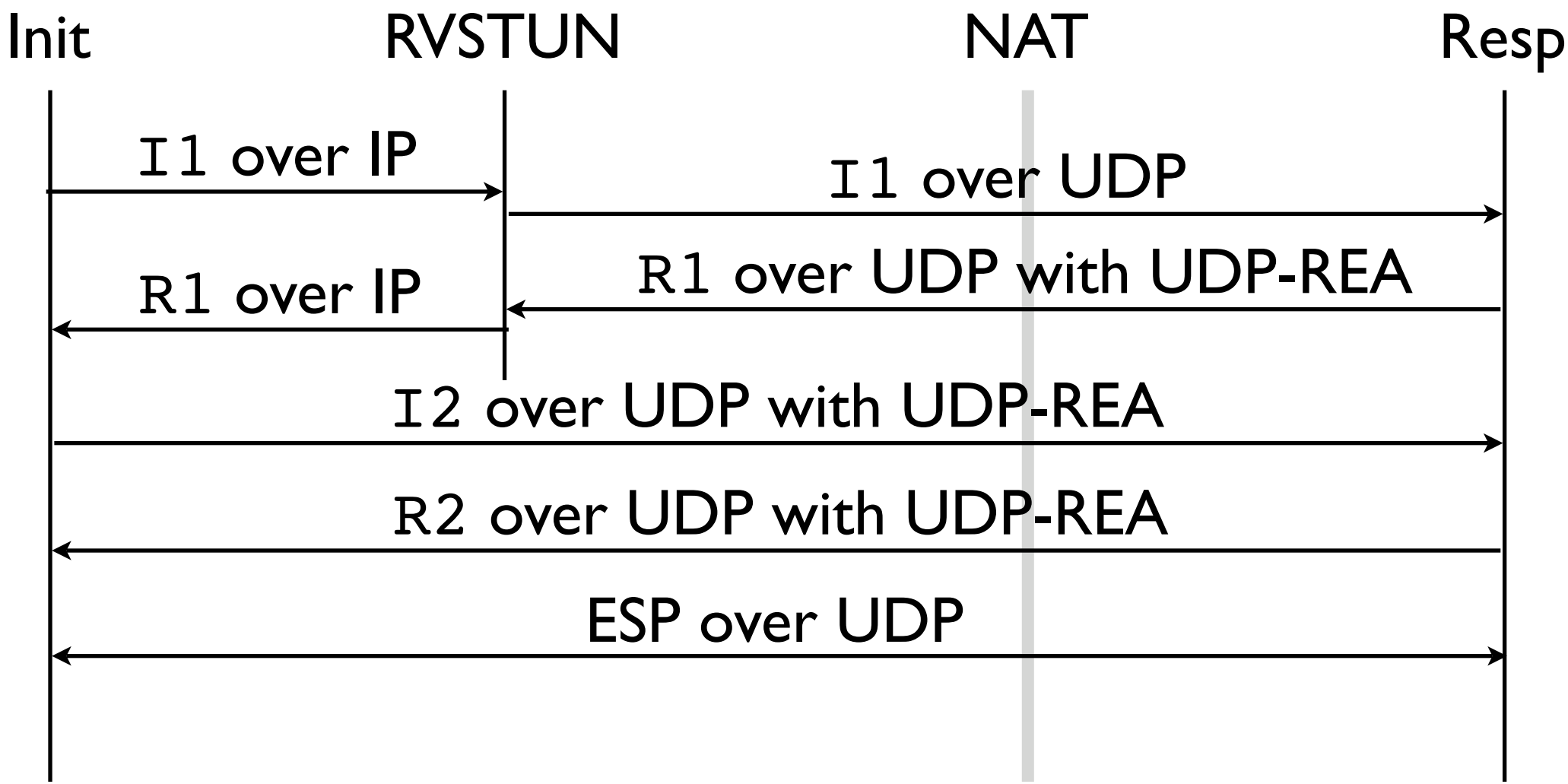
Making a contact 1/3



Making a contact 2/3



Making a contact 3/3



Next steps

- Draft about packet formats
  - HIP over UDP
  - New locator type
  - Authors: Martin, Julien
- Draft about UDP rendezvous servers
  - Rely on the the packet formats
  - Authors: Hannes, Lars, Tom, Pekka