HIP Rendezvous Extensions

draft-ietf-hip-rvs-00.txt

Lars Eggert, Julien Laganier

HIP WG, 61th IETF
Washington, DC, USA

Monday, November 8th, 2004

HIP Rendezvous Basics

- A HIP node might frequently change its IP address
- Such a node might maintain reachability:
  - Using its Rendezvous Server IP address

  - Then *possibly* store in DNS its RVS IP address or FQDN

foo.bar.com HIPRVS foo_rvs.bar.com

foo.bar.com HIPRVS 123.213.132.231

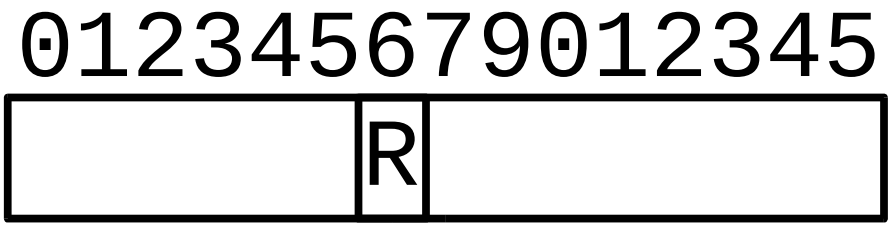
Changelog

Since WG adoption

- Removed IP concealing extensions
  - Simpler
- Add support for Opportustic Initiators
  - Relaying I1 *and* R1
- Add Security and IANA Considerations
- Complete *REDIRECT* packet description

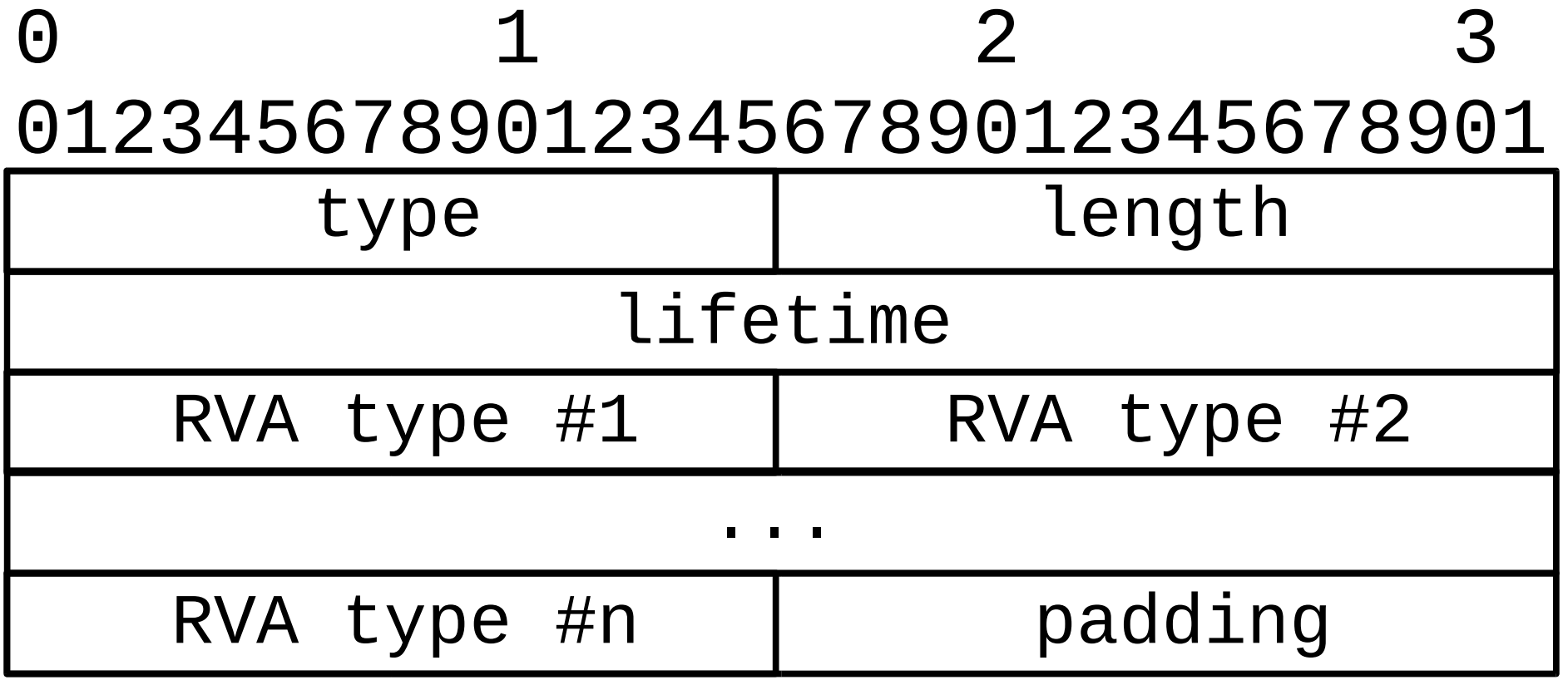
Rendezvous Extensions

- Header extensions
  - New HIP parameters
    - *RVA_REQUEST, RVA_REPLY, FROM, TO, VIA_RVS*
  - New HIP control fields
    - *RVS_CAPABLE*

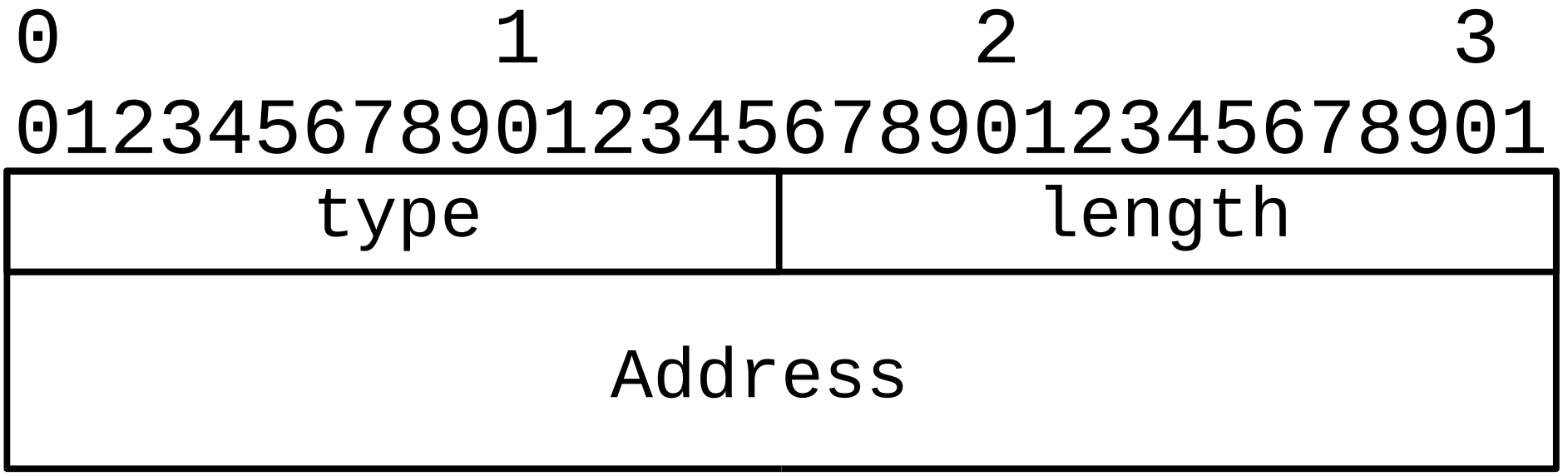


- Protocol extensions
  - Create a Rendezvous Association (RVA)
  - Establish a HIP Association (HA) using a RVS

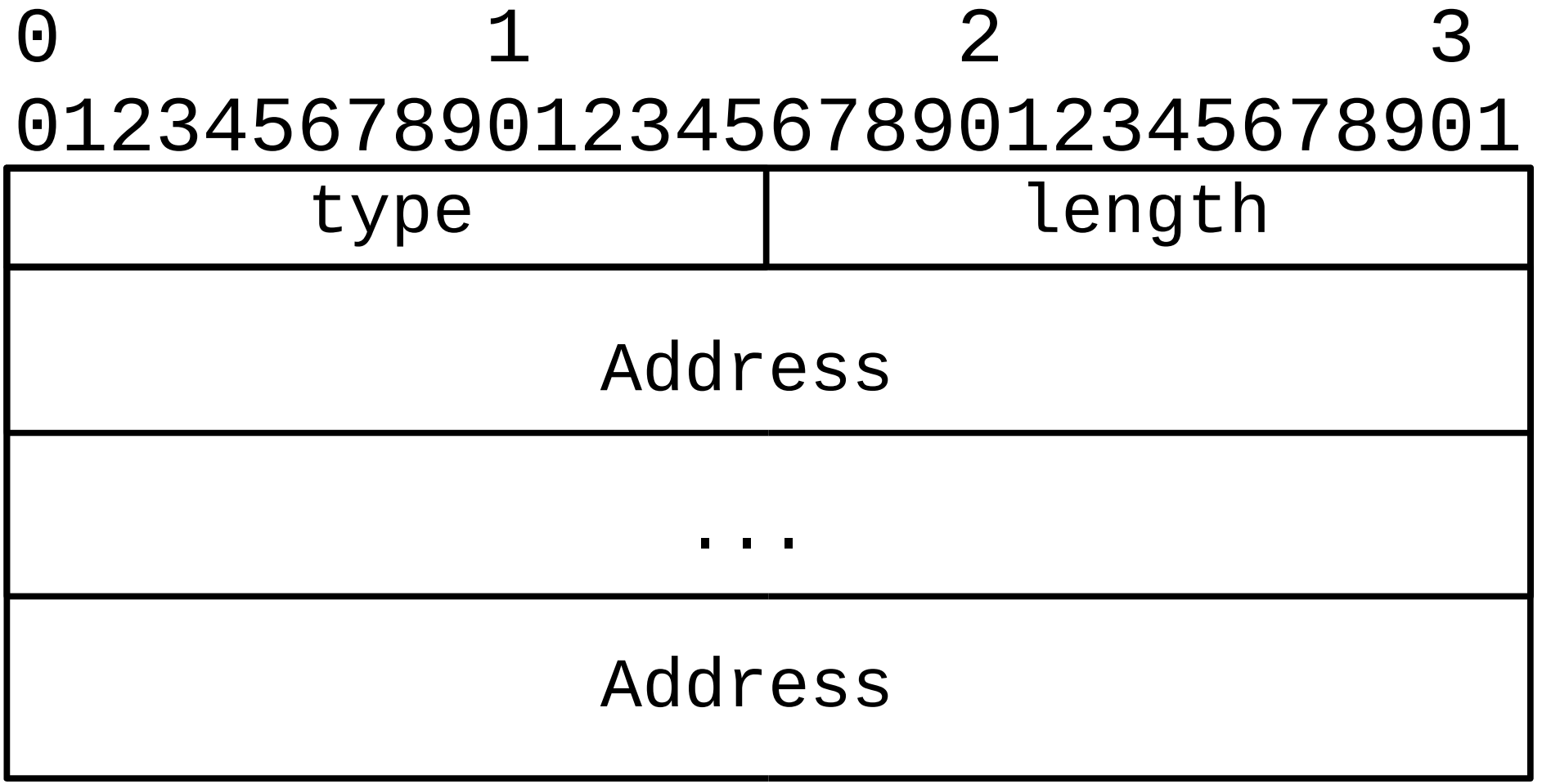
RVA_{REQUEST / REPLY}



FROM / TO / REDIR



VIA_RVS


0 1 2 3
0123456789012345678901234567890 1
type
length
Address
...
Address

Establishing a Rendezvous Association

A soft association between client and RVS

- Allows the RVS to relay/redirect HIP packets
  - Without maintaining full blown HA
  - Better scalability
- Established like a HA, with two new parameters:
  - *RVA_REQUEST* added on I2
  - *RVA_REPLY* added on R2
- Then, most of the HA state can be deleted
  - Retain only client HIT, IP address, RVA lifetime and HIP integrity keys for *RVA_HMAC* keying

New HIP parameters

- *RVA_HMAC* protects packet integrity between RVS and client
- *FROM* preserves original source IP address
- *TO* loose source-routes R1 via RVSs
- *VIA_RVS* signals the IP addresses of traversed RVSs
- *REDIR* signals an Initiator the current IP address of Responder

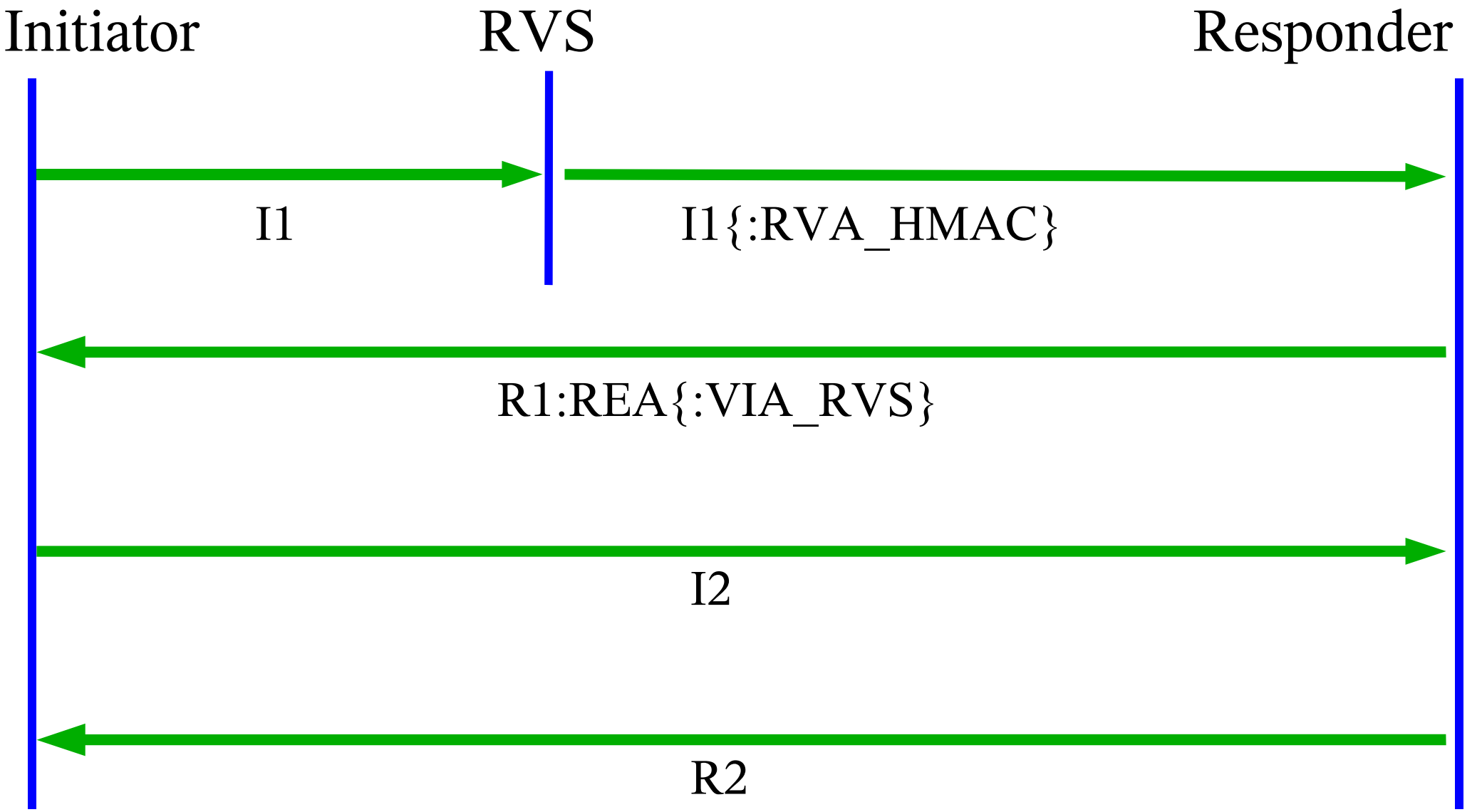
RVS relays only I1

Further packets flows directly

- RVS merely rewrite I1 destination IP address
  - Egress filtering on RVS's network might prevent that
- So RVS may also rewrites I1 source IP address
  - *FROM* parameter preserves original source IP address
- *FROM* requires authentication
  - Spoofed RVS => Reflection / amplification attacks
- *RVA_HMAC* authenticates relayed I1s

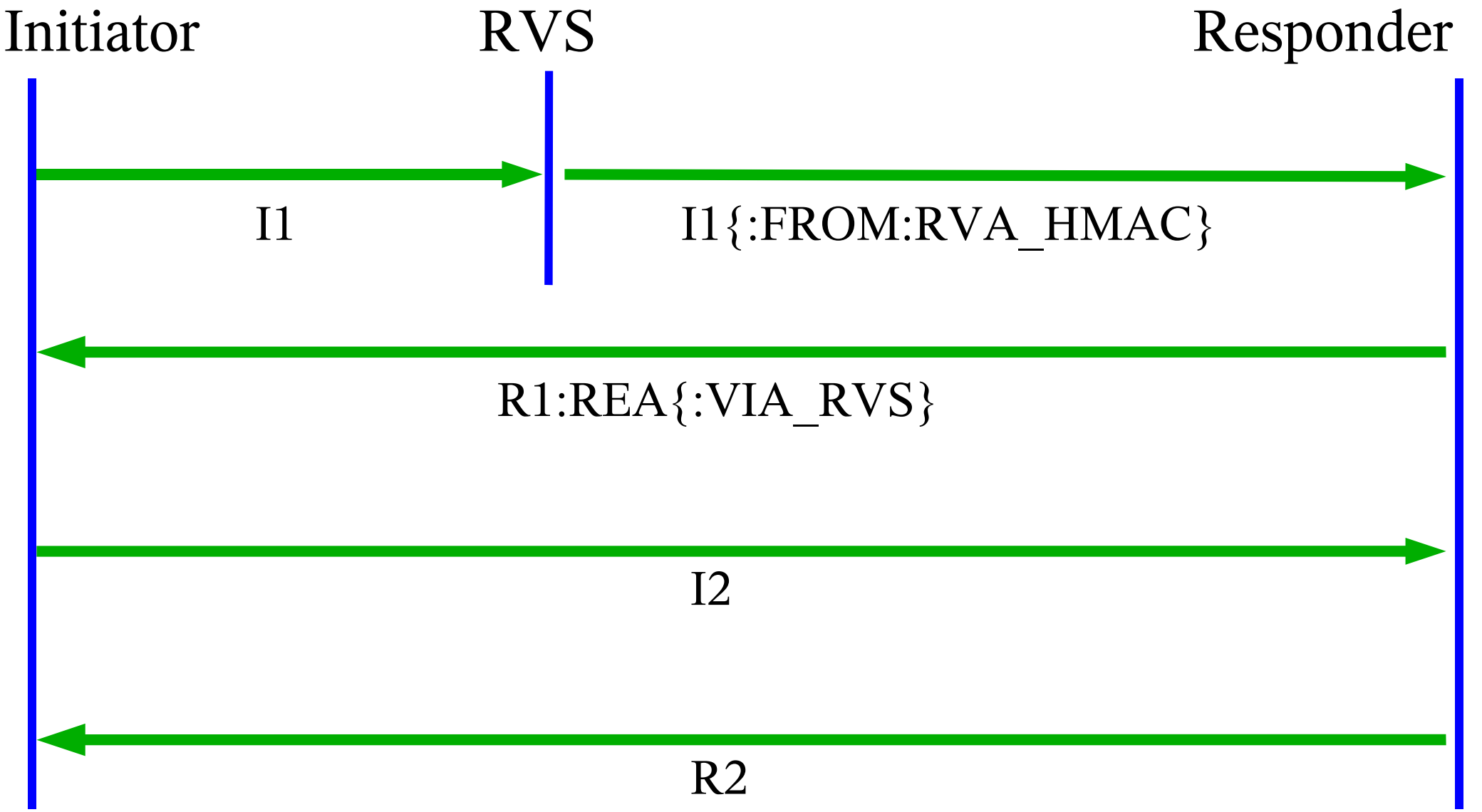
I1_REWRITE_DST

Protocol sketch



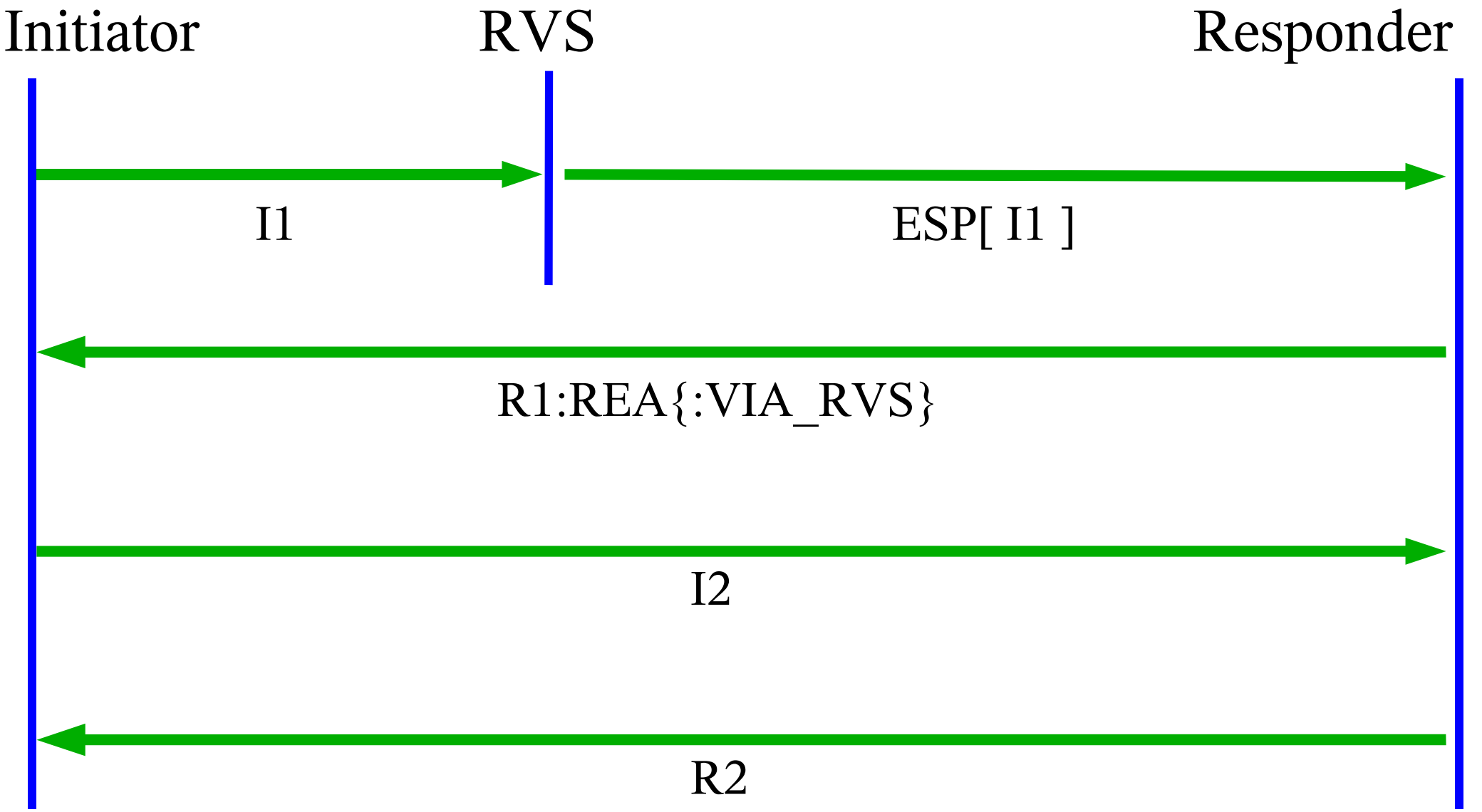
I1_REWRITE_SRCDST

Protocol sketch



I1_RELAY_ESP

Protocol sketch



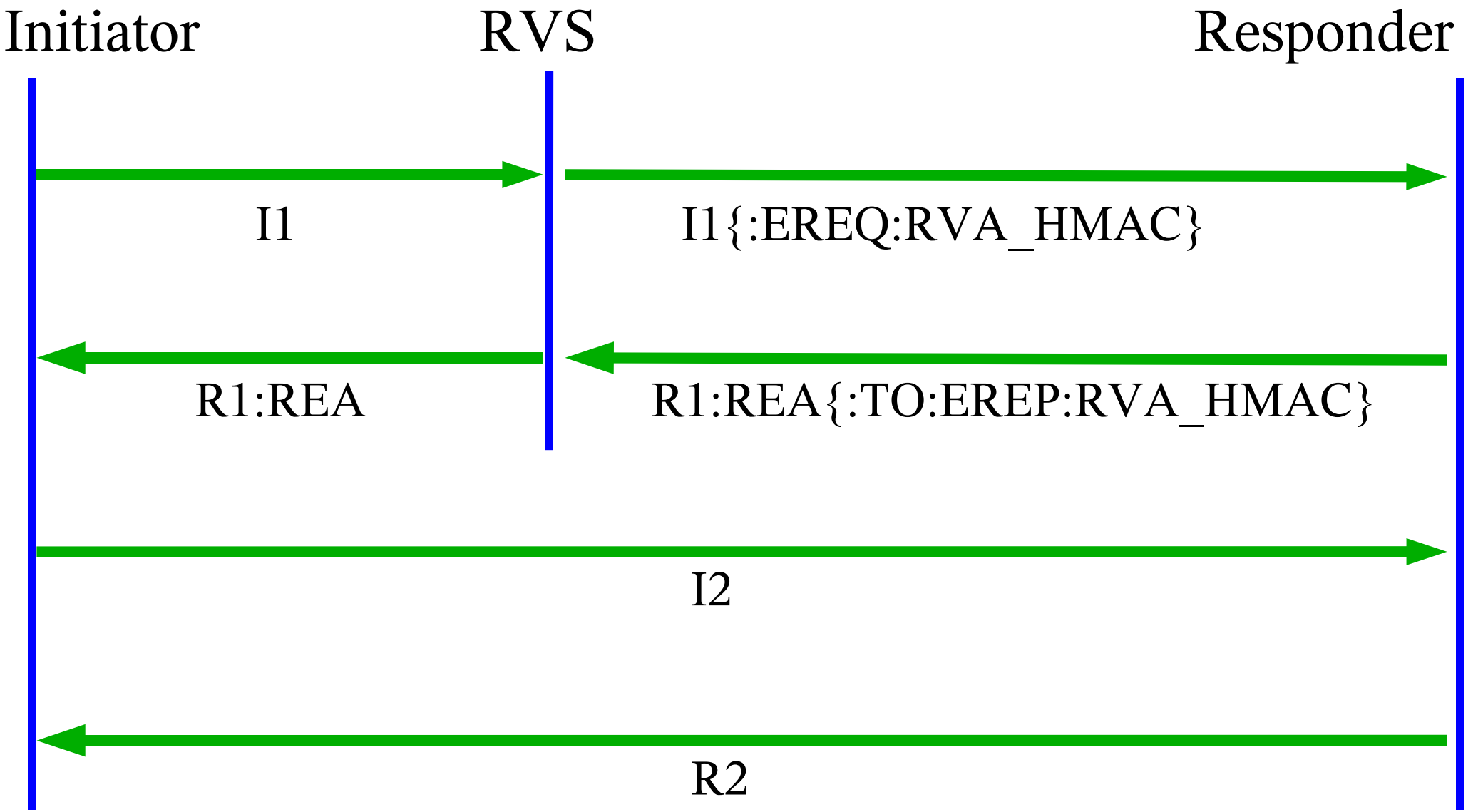
RVS relays I1 *and* R1

Opportunistic Initiators Support

- Responder MAY answer R1 via RVS
  - If I1 was Opportunistic, R1 embeds
    - *REA* contains the Responder IP address (draft-ietf-hip-mm)
    - *TO* contains the Initiator IP address taken fromI1 *FROM*
  - Initiator get an R1 from the IP address they sent I1
    - Mitigates spoofing and hijacking attacks
    - Initiator sends I2 directly to Responder address in*REA*
  - RVS MUST validates *TO* IP address
    - Opaque data encoding the Initiator*FROM* IP address
    - RVS adds *ECHO_REQUEST* onto I1
    - Responder adds *ECHO_REPLY* onto R1, removed by RVS

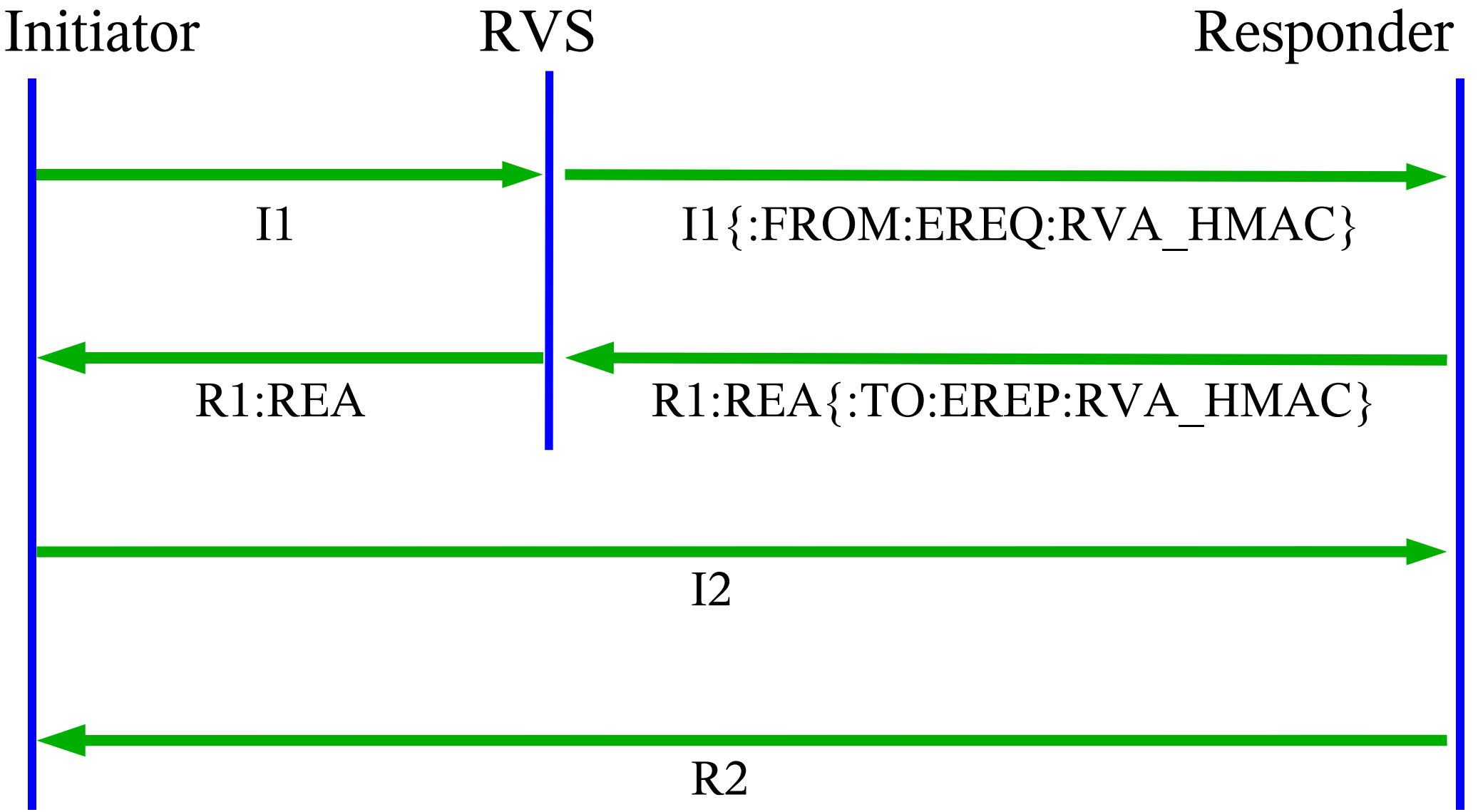
I1R1_REWRITE_DST

Protocol sketch



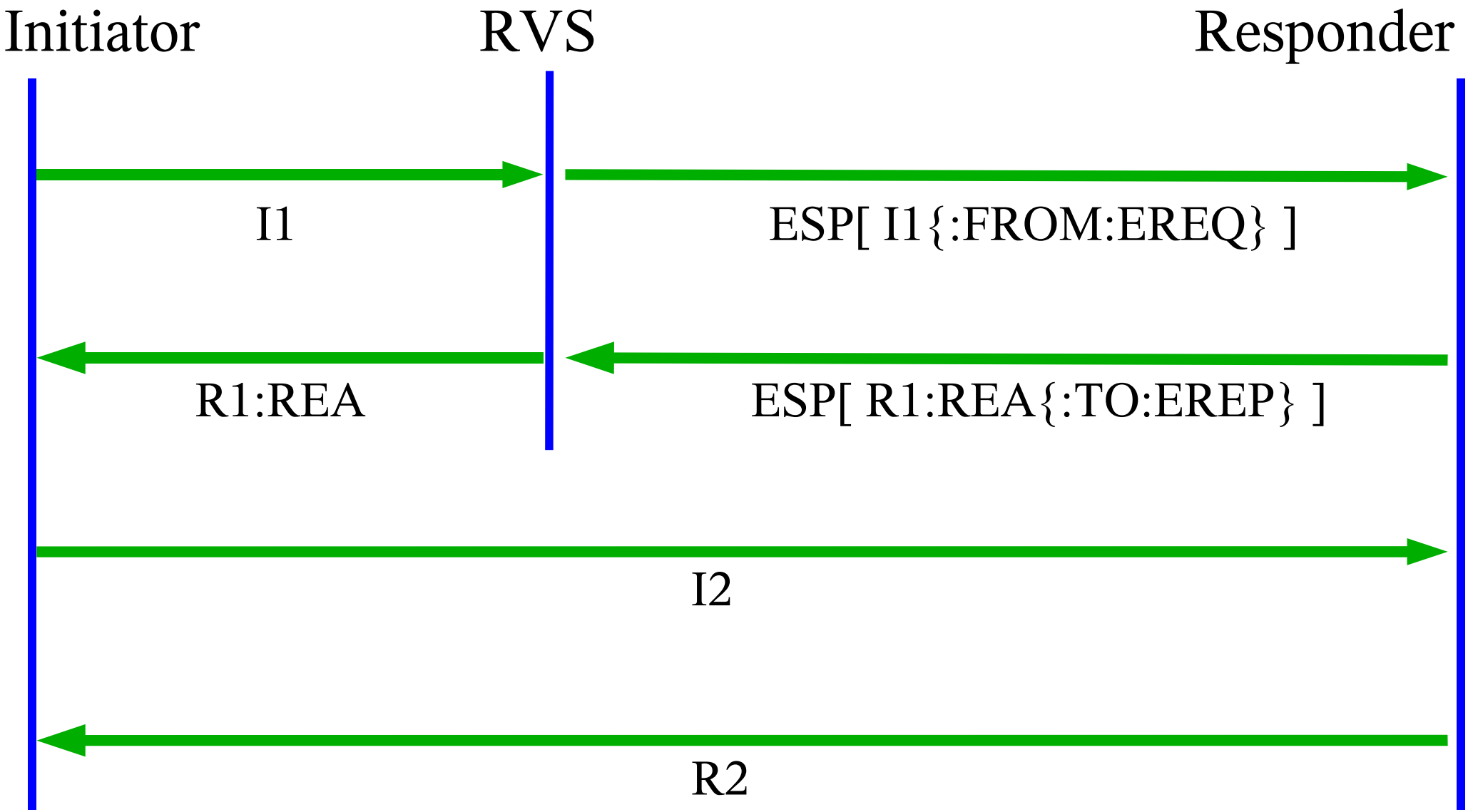
I1R1_REWRITE_SRCDST

Protocol sketch



I1R1_RELAY_ESP

Protocol sketch



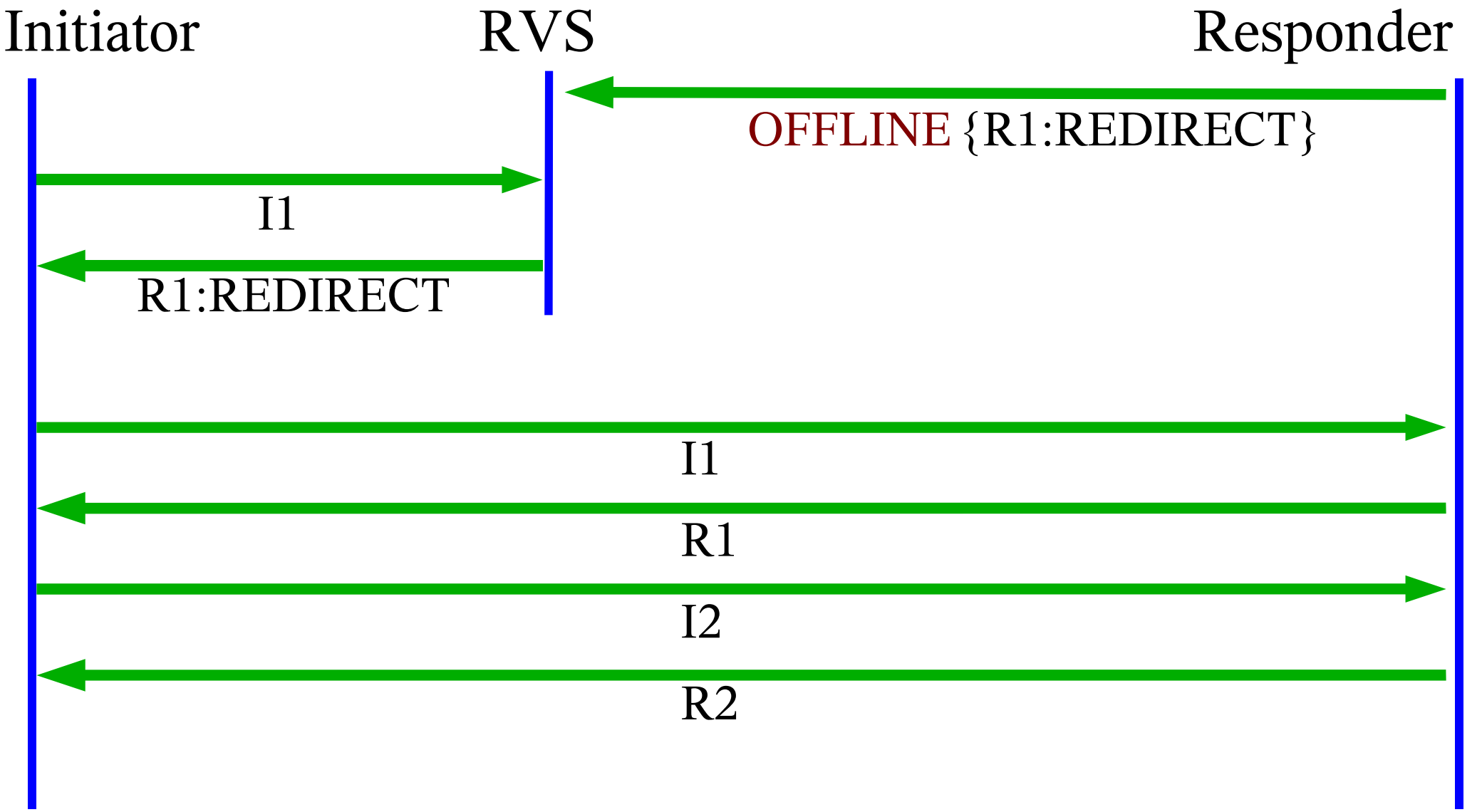
RVS redirects Initiator

Sending REDIRECT packet

- Responder provisions RVS with REDIRECT packet
  - While creating RVA
  - Contains the Responder IP address in *REDIR* parameter
  - Signed by Responder
  - Perhaps validity dates?
- RVS answers I1s with REDIRECT
  - Initiator validates signatures and validity dates
- Then Initiator re-initiate an HIP exchange
  - Directly towards Responder IP address

REDIRECT

Protocol sketch



Next Steps

- Does the protocol need:
  - All these relaying/redirect modes?
    - Pekka Nikander suggests:
      - TUNNEL_I1, REWRITE_I1 and BIDIRECTIONAL
    - Drop REDIRECT?
  - *TO* parameter?
    - *ECHO_REPLY* required anyway to authentify *TO*
- Should we split the current specification:
  - Generic HIP registration with Rendezvous Server
  - Rendezvous Service

Questions or comments...

ju@sun.com