HIP Rendezvous Extensions

draft-ietf-hip-rvs-01.txt

Julien Laganier, Lars Eggert

HIP WG, 62th IETF
Minneapolis, MN, USA

Wednesday, March 9th, 2005

HIP Rendezvous Basics

- A HIP node might frequently change its IP address
- How to maintain reachability with new correspondents at 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 -00

- Removed RVS registration sub-protocol
- Simplify RVS Types
  - *I1_TUNNEL*
  - *I1_REWRITE*
  - *BIDIRECTIONAL*
- Rewritten introduction and usage scenarios

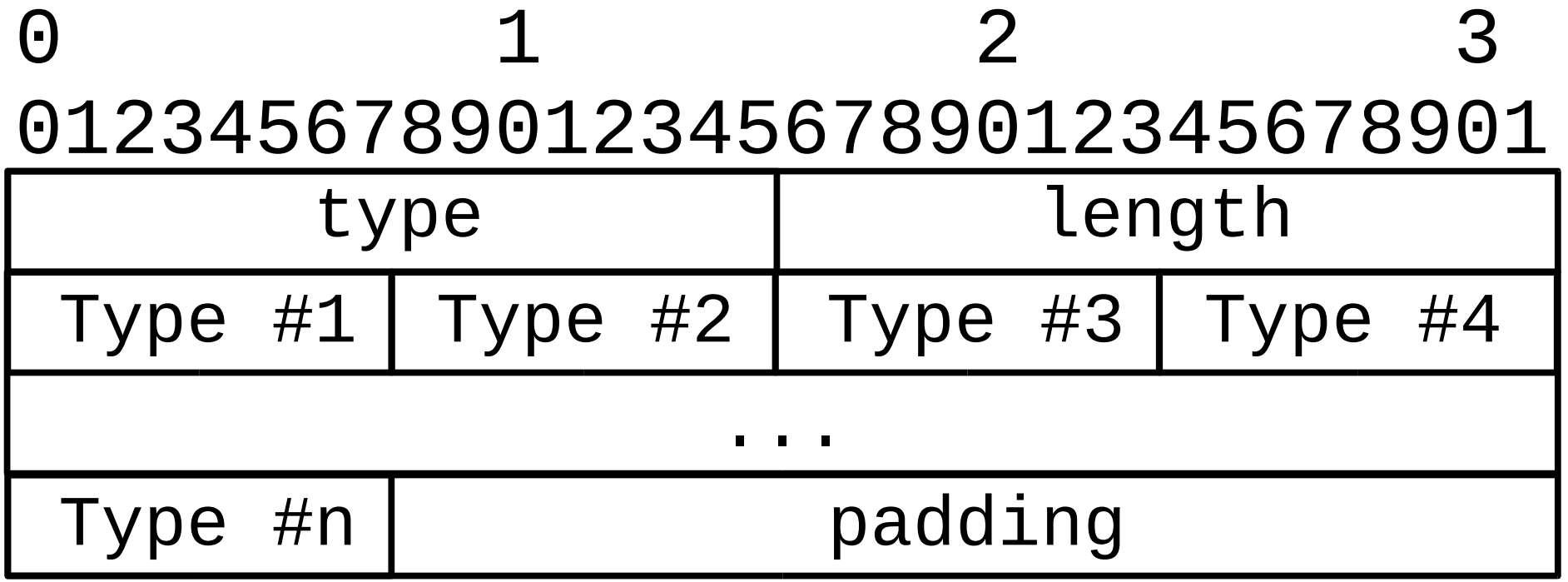
Rendezvous Extensions

- Establish a Rendezvous Registration *with* a RVS
  - Registration Protocol extensions
  - New HIP Registration Type: *RENDEZVOUS*
  - New HIP Parameter: *RVR_TYPE*
- Establish a HIP Association *via* a RVS
  - HIP Base Exchange extensions
  - New HIP Parameters: *FROM*, *TO*, *VIA_RVS*

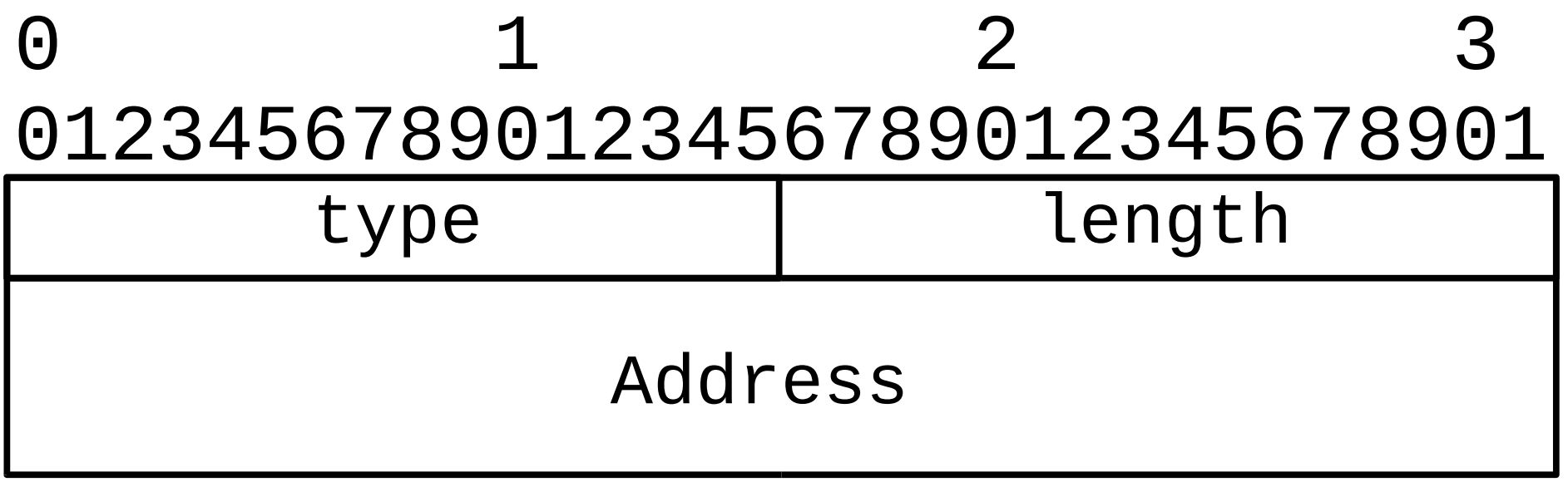
New HIP parameters

- *RVR_TYPE* specifies the type of the Rendezvous registration
- *RVR_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

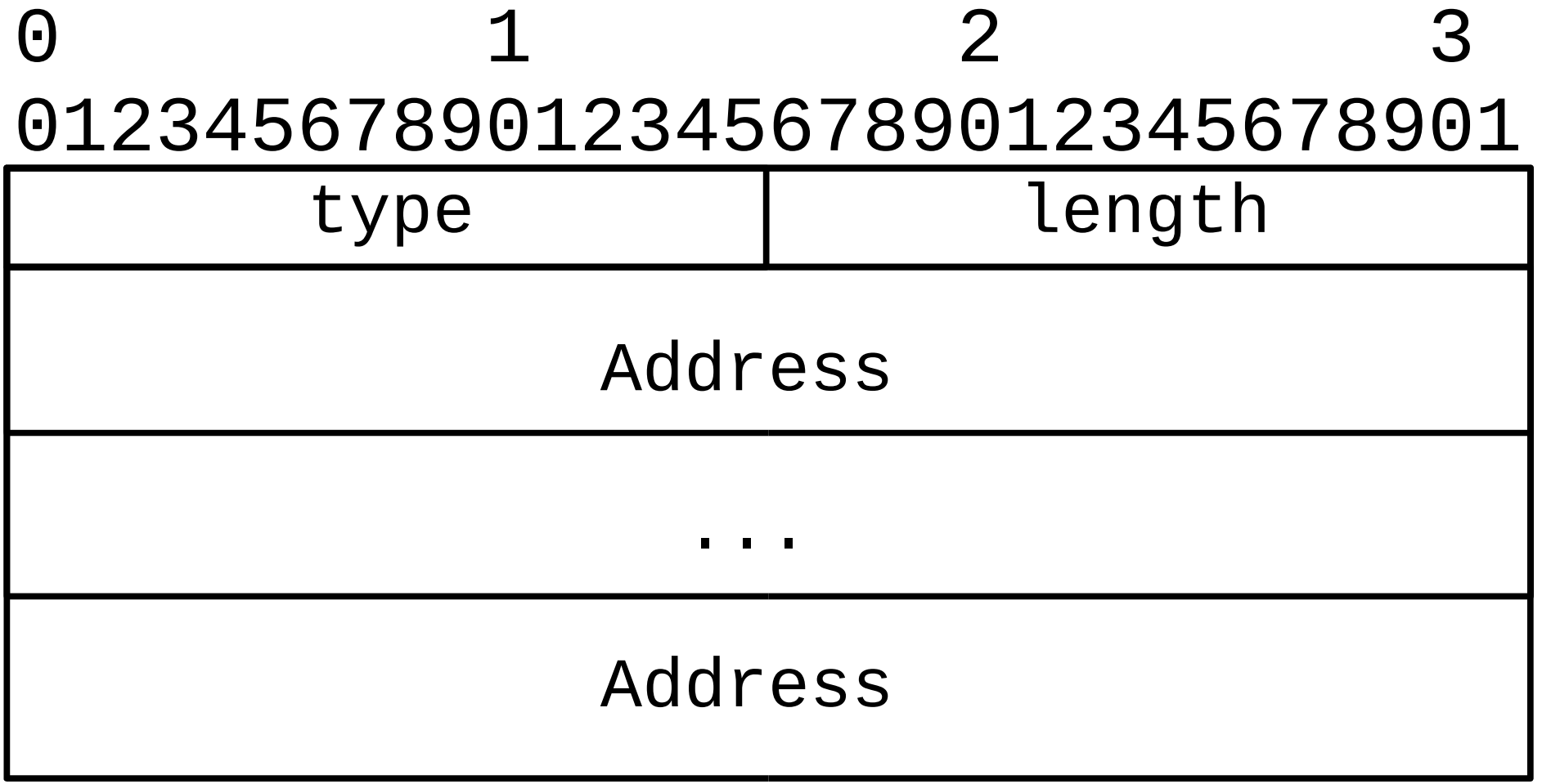
RVR_TYPE


0 1 2 3
0123456789012345678901234567890 1
type
length
Type #1
Type #2
Type #3
Type #4
...
Type #n
padding

FROM / TO


0 1 2 3
0123456789012345678901234567890 1
type
length
Address

VIA_RVS


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

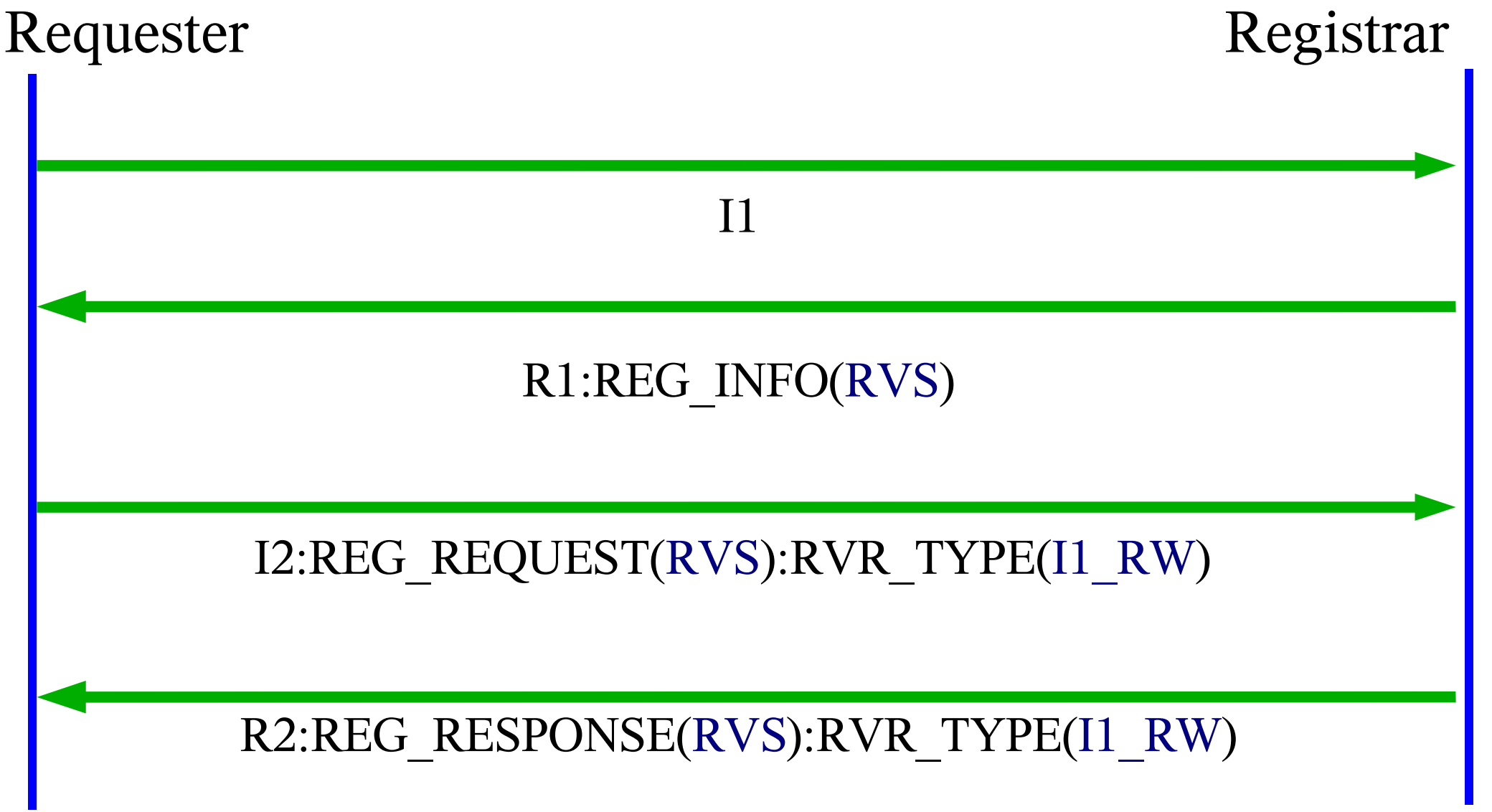
Establishing a Rendezvous Registration

An association between client and RVS

- Allows the RVS to relay some HIP packets
- Established using the registration protocol with:
  - *RENDEZVOUS* registration type
  - *RVR_TYPE* parameter in I2 and R2

Typical Rendezvous Registration

Protocol sketch



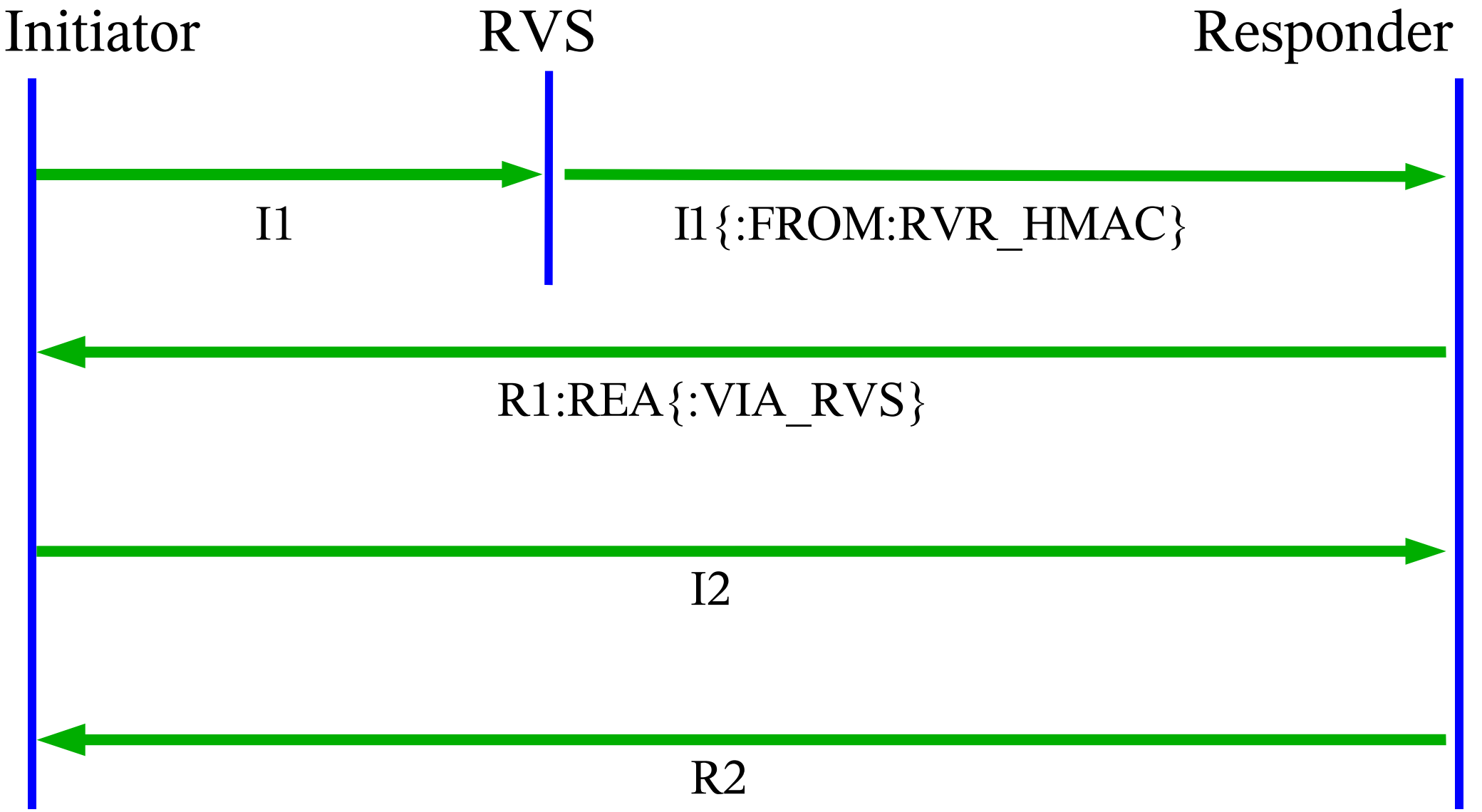
RVS relays only I1

Further packets flows directly

- Two solutions:
  - RVS rewrite I1 destination IP address
  - RVS tunnels I1 to its client
- if egress filtering on RVS's network
  - RVS also rewrites I1 source IP address
  - *FROM* parameter preserves original source IP address
  - *FROM* requires authentication
    - Spoofed RVS => Reflection / amplification attacks
- *RVR_HMAC* authenticates *FROM*

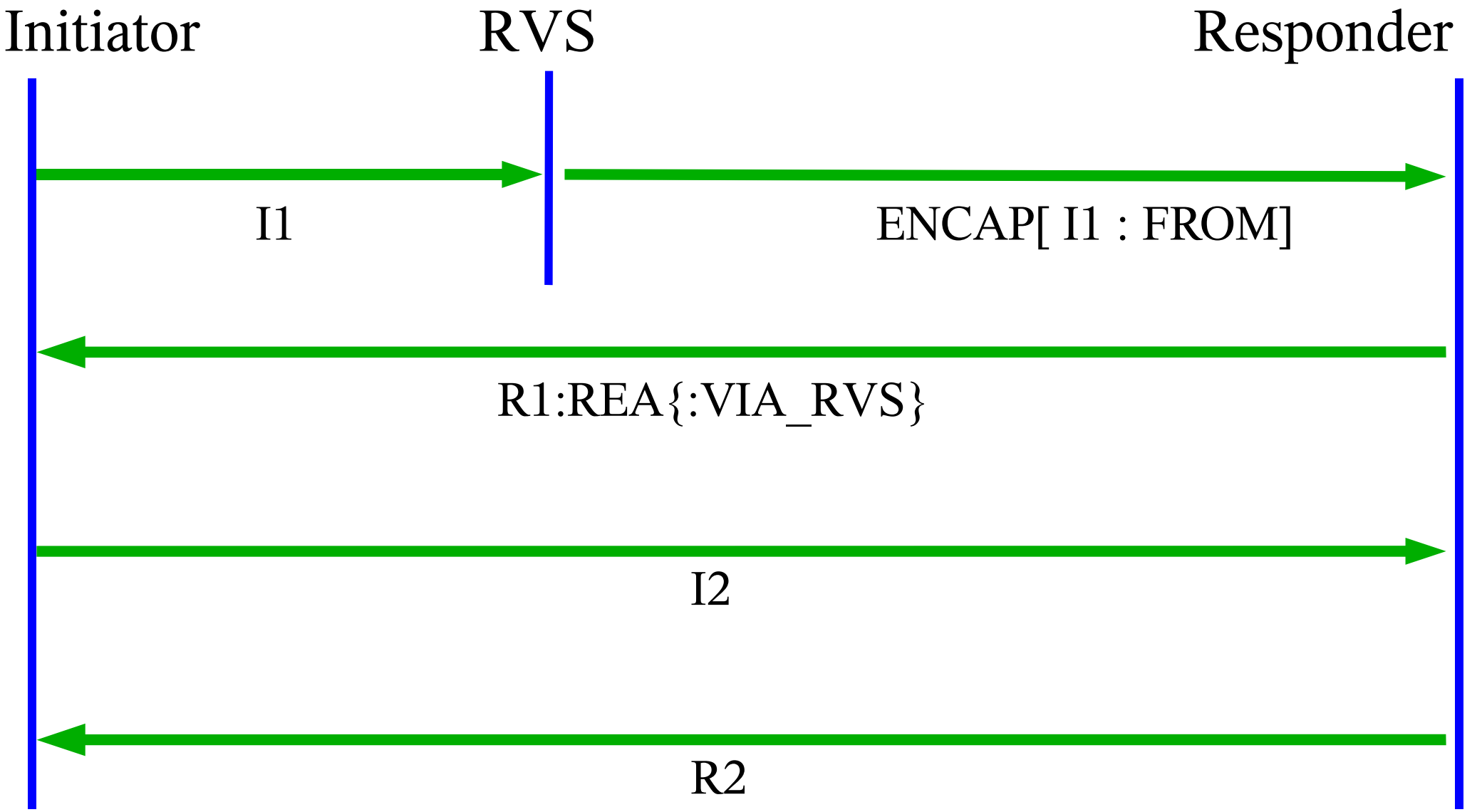
I1_REWRITE

Protocol sketch



I1_TUNNEL

Protocol sketch

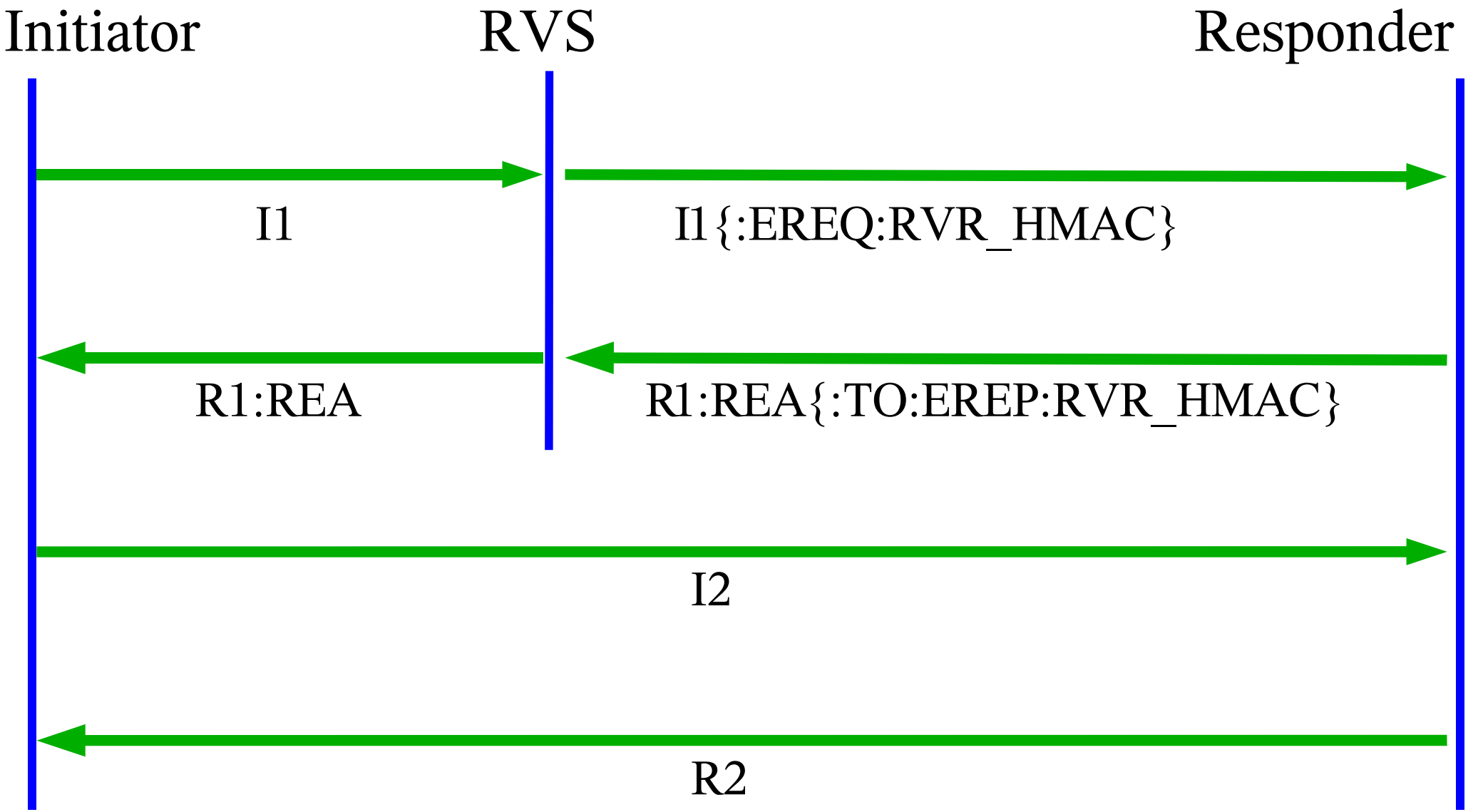


RVS relays I1, R1...
and further HIP packets?

- Responder MAY answer R1 via RVS
- Such R1 includes:
  - *REA* with the Responder IP address
  - *TO* with the Initiator address taken from I1 *FROM*
  - Initiator get an R1 from the IP address they sent I1
  - Initiator sends I2 directly to Responder address
- 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, RVS removes it

BIDIRECTIONAL

Protocol sketch



Open Questions

- What types of tunnel encapsulation do we support
  - IP-in-IP, ESP, UDP...
  - And how it is negotiated if multiples types coexist
- Should we specify UPDATE relaying (as for I1)
  - Useful for double movement in mobility scenarios
  - Or does it belongs to draft-ietf-hip-mm

Questions or comments...

ju@sun.com
lars.eggert@netlab.nec.de