HIP Rendezvous Extensions

draft-eggert-hip-rvs-00.txt

Lars Eggert, Julien Laganier

HIP WG, 60th IETF
San Diego, CA, USA

Thurday, August 5th, 2004

HIP Rendezvous Basics

- A HIP node might frequently change its IP address
- To maintain reachability, such node might either:
  - Update DNS with its current IP address

Or

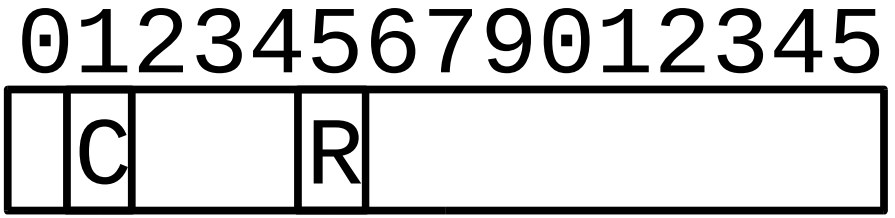
  - Put its Rendezvous Server's IP address in DNS
  - Update its RVS with its current IP address

HIP Rendezvous Requirements

- Needs two new HIP sub-protocols
  - A node updates its RVS with its current IP address
  - A RVS relays HIP packets to the responder

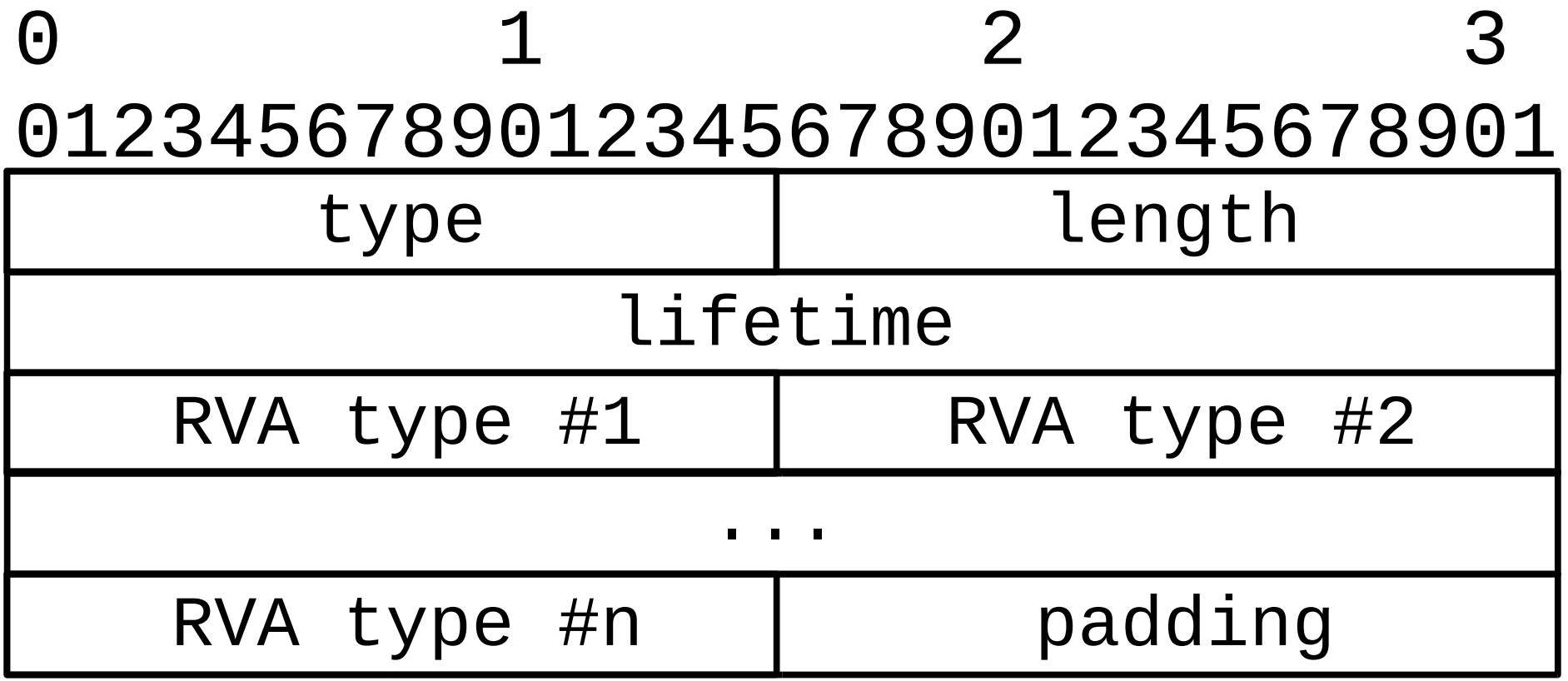
Rendezvous Extensions

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

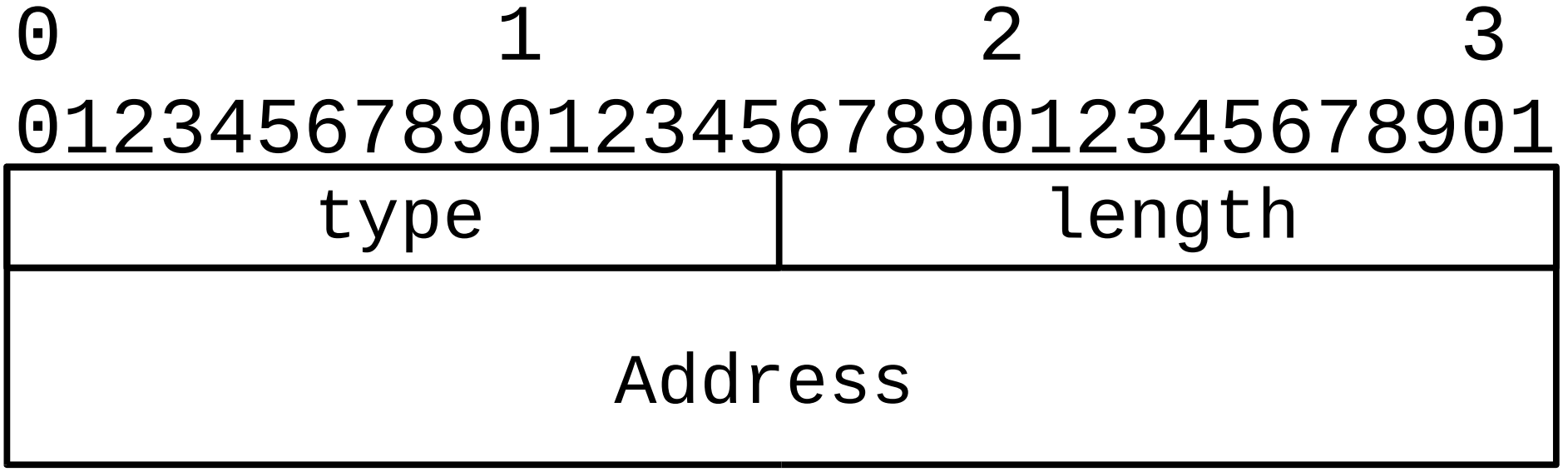


- Protocol extensions
  - Create a Rendezvous Association (RVA)
  - Establish a HIP Association (HA) through a RVS

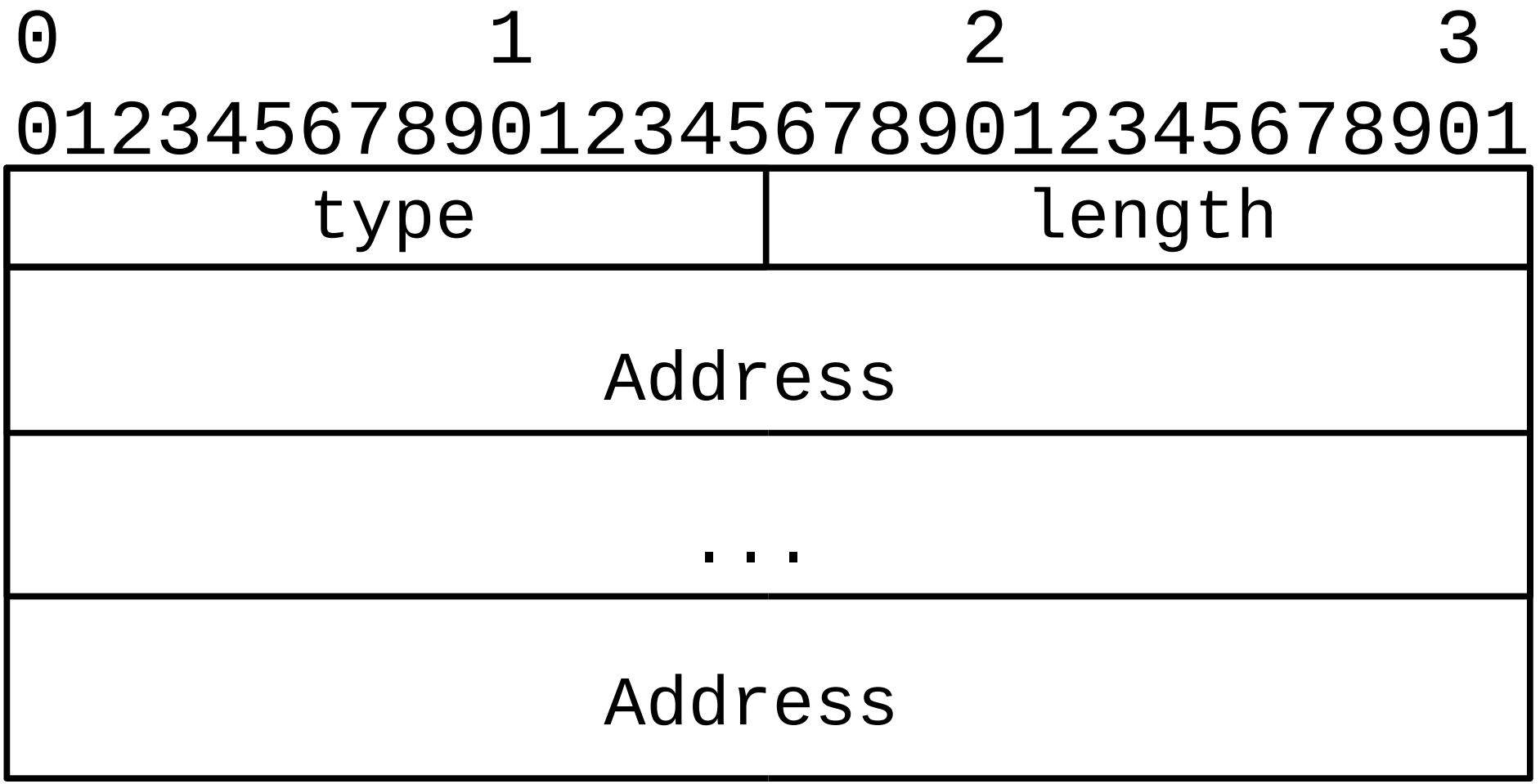
RVA_{REQUEST / REPLY}



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 Association

- A soft association between a RVS and its client
- Allows the RVS to relay HIP packets
  - Without maintaining full blown HA
- Created by adding 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

Establishing an HA through a RVS (1)

- New HIP parameters
  - Protect integrity between RVS and client (*RVA_HMAC*)
  - RVS preserve original source IP address (*FROM*)
  - Responder loose source-routes R1/R2 via RVSs (*TO*)
  - Signal the IP addresses of traversed RVSs (*VIA_RVS*)

Establishing a HA through a RVS (2)

RVS relays only I1

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

Establishing a HA through a RVS (3)

RVS relays further HIP packets

- Responder MAY answer via the RVS with *TO*
  - *TO* contains the IP address included in *FROM*
- New *CONCEAL_IP* control field
  - Initiator and/or responder can conceal IP address(es)
  - RVS rewrites all source IP addresses
  - End-nodes disclose IP addresses after authentication
    - Using REA after getting an I2 or an R2
- RVS authenticates all packets relayed further I1
  - *ECHO_REQUEST* in I1 and possibly I2
  - *ECHO_REPLY* in R1 and possibly R2

Next Steps

- Get (more ;) feedback from the WG
- Implementation
  - HIPL team already has a preliminary one
- Adopt this I-D as a WG item?

Questions or comments...

ju@sun.com