DHT-01

Jeffrey Ahrenholz

Clarifications to MM-05

Samu Varjonen

23.3.2007
68th IETF
Prague

dht-01

- draft-ahrenholz-hiprg-dht-01
- Common interface for using HIP with a Distributed Hash Table service
- Uses OpenDHT PlanetLab service
  - Bamboo open source DHT software
  - XML RPC calls
  - put(), get() and rm() operations

dht-01

Defines these HIP services:

- HIP address lookup
  - address = get(HIT)
- Secure HIP address lookup
  - (address,time,HI,sig) = get(HIT)
  - server enforced (requires mods) or client verified
- HIP name to HIT lookup
  - HIT = get(SHA1(“name”))
  - why? no authority, unsupported RR, non-DNS names

dht-01

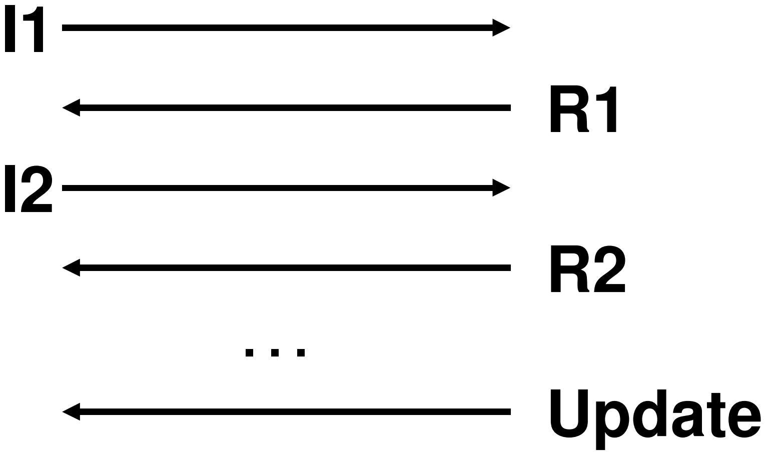
Suggested usage:

put(HIT-I, addr1), put(HIT-I, “initiator”)

HIT-R = get(“responder”)

addr1 = get(HIT-R)

put(HIT-R, addr2)
put(HIT-R, “responder”)



I1

R1

I2

R2

…

Update

put(HIT-R, addr3)

dht-01

Changes from -00 to -01:

- added HIT lookup service using names, removed LSI
  - HIT = get(SHA1(“name”))
- support for OpenDHT remove
  - put(HIT, addr, SHA1(secret)) rm(HIT, secret)
- secure address lookup
  - (address,time,HI,sig) = get(HIT)

Clarifications to mm-05

- Addresses change and possibly also the family
- If the base exchange is done over IPv4 the connection is lost when either end moves to IPv6 only network
- The other end could have valid IPv6 address but its not known to the other end

Base exchange with LOCATORs

```
Initiator                                        Responder
                      I1: trigger exchange
          -------------------------------->
                                                 select pre-computed R1
                   R1: puzzle, D-H, key,
                   LOCATOR(P=0, addr*), sig
          <--------------------------------
check sig                                        remain stateless
solve puzzle
**
                 I2: solution, D-H, {key},
                 LOCATOR(P=0, addr*), sig
          -------------------------------->
compute D-H                                      check puzzle
                                                 check sig
                                                    **
                            R2: sig
          <--------------------------------
check sig                                        compute D-H
```

** Family is opposite of the family used in BEX*
*** LOCATOR status = UNVERIFIED*

UPDATE

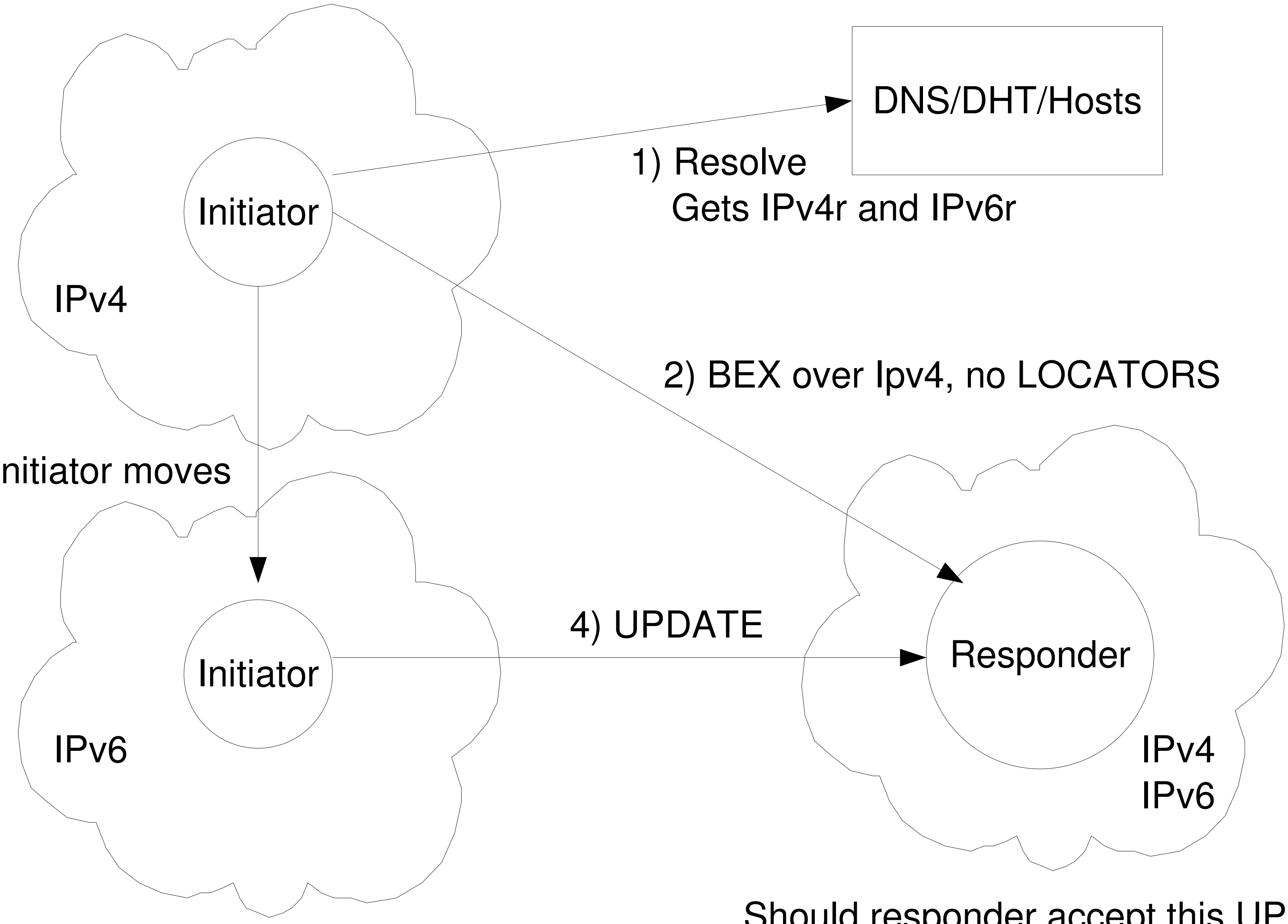
- If host moves and both the used and the alternative addresses change

```
UPDATE(ESP_INFO, LOCATOR(P=1,addr), SEQ, [DIFFIE_HELLMAN])
---------------------------------------------------------->
UPDATE(ESP_INFO, SEQ, ACK, [DIFFIE_HELLMAN,] ECHO_REQUEST)
<----------------------------------------------------------
UPDATE(ACK, ECHO_RESPONSE)
---------------------------------------------------------->
                                    LOCATOR status = ACTIVE

UPDATE(ESP_INFO, LOCATOR(P=0,addr*), SEQ, [DIFFIE_HELLMAN])
---------------------------------------------------------->
UPDATE(ACK**)
<----------------------------------------------------------
                                LOCATOR status = UNVERIFIED

                        * other family than currently used
                        ** or sent later
```

Double jump



DNS/DHT/Hosts

1) Resolve
Gets IPv4r and IPv6r

Initiator

IPv4

2) BEX over Ipv4, no LOCATORS

3) Initiator moves

Initiator

IPv6

4) UPDATE

Responder

IPv4
IPv6

Should responder accept this UPDATE?

Other considerations

- No need for revoking the alternative address because they are not used before verification
- Succeeding UPDATEs override previous one
- NAT and others
- Should this be in mm-06 or its own draft?

Thanks