Native IPv6 across NAT44-only CPEs (6a44)

draft-despres-softwire-6a44-01

Rémi Després – RD-IPtech
Brian Carpenter – Univ. of Oakland
Sheng Jiang – Huawei

IETF 79 - Softwire - November 8, 2010

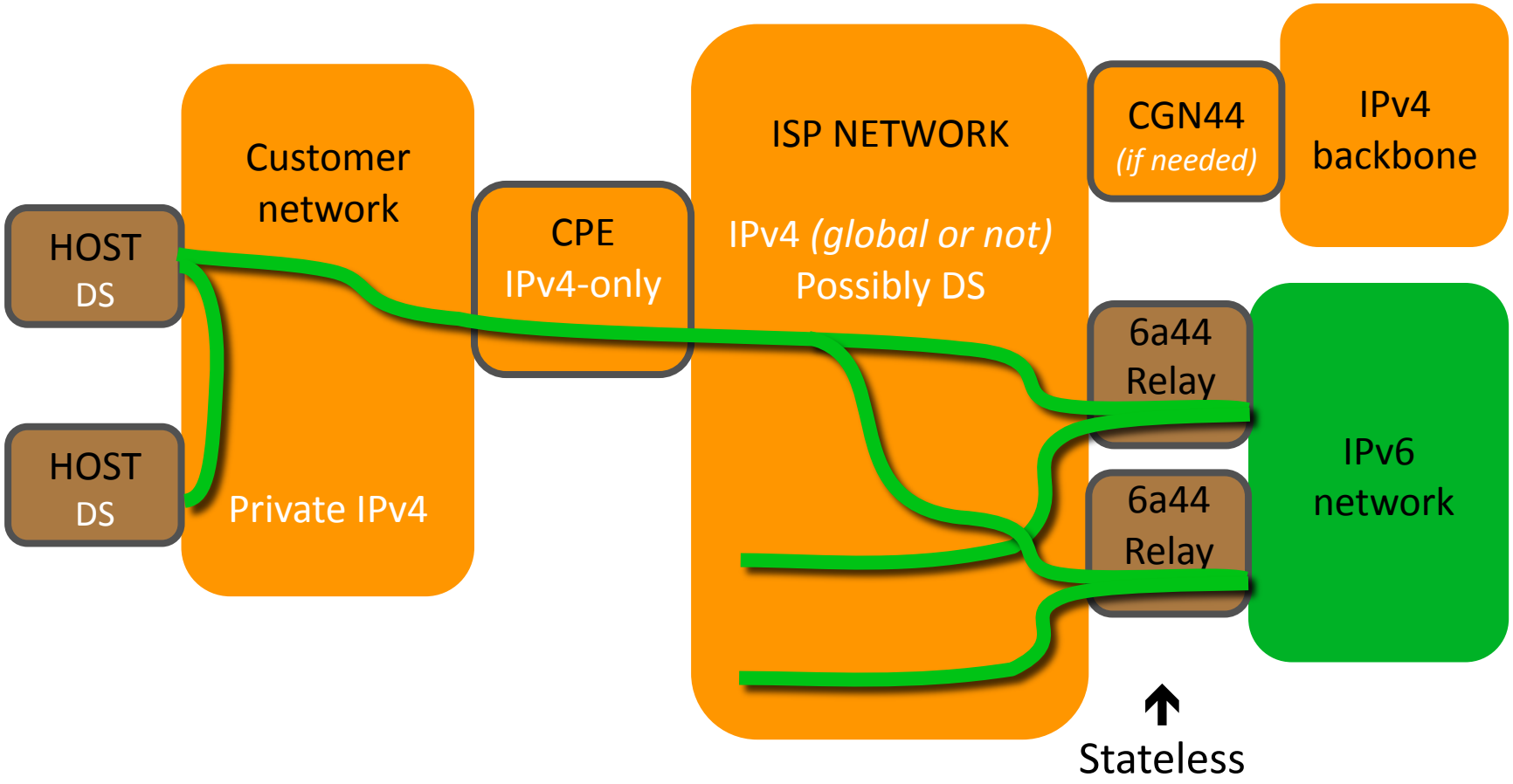
The need for 6a44

- IPv4-only CPEs are in great number
- More and more ISPs assign non-global IPv4 addresses to customers
- Some applications need incoming connectivity
- Outgoing connectivity must be reliable
- Operation must be Plug-and-Play

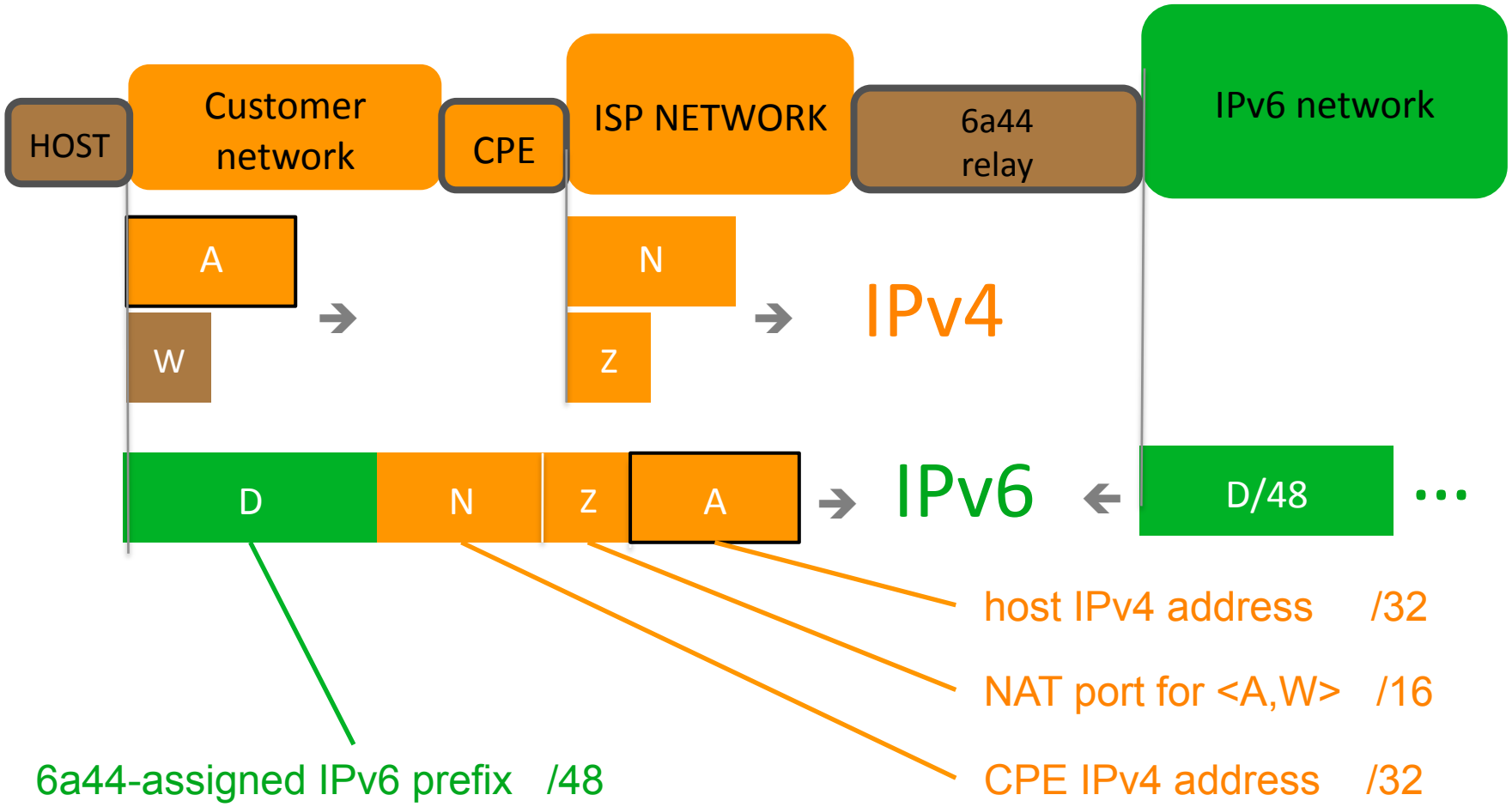
Limitations of other solutions

- NAT44 cascades
  - Still miss reliable incoming connectivity
  - Will be rather complex to operate (PCP, …)
- IPv6 Tunnel Brokers
  - Are not plug-and-play
  - Intra-site traffic goes via external server
- Teredo
  - Fails with some NAT-type combinations
  - Can’t provide ISP-controlled QoS

6a44 Overview



6a44 Address Format



Deployment

- An ISP can start with 1 or 2 relays
  - very small entry cost
  - If need for more: user service is real (intense IPv6 use behind NAT44 CPEs)
- Hosts can include the 6a44 add-on
  - ➔ Where other native IPv6 addresses are available => No harm
  - ➔ Where ISPs don't support 6a44 => no harm
  - ➔ Where ISP's support 6a44:
    - native IPv6 works (plug an play)
    - Intra-site IPv6 doesn't go the ISP

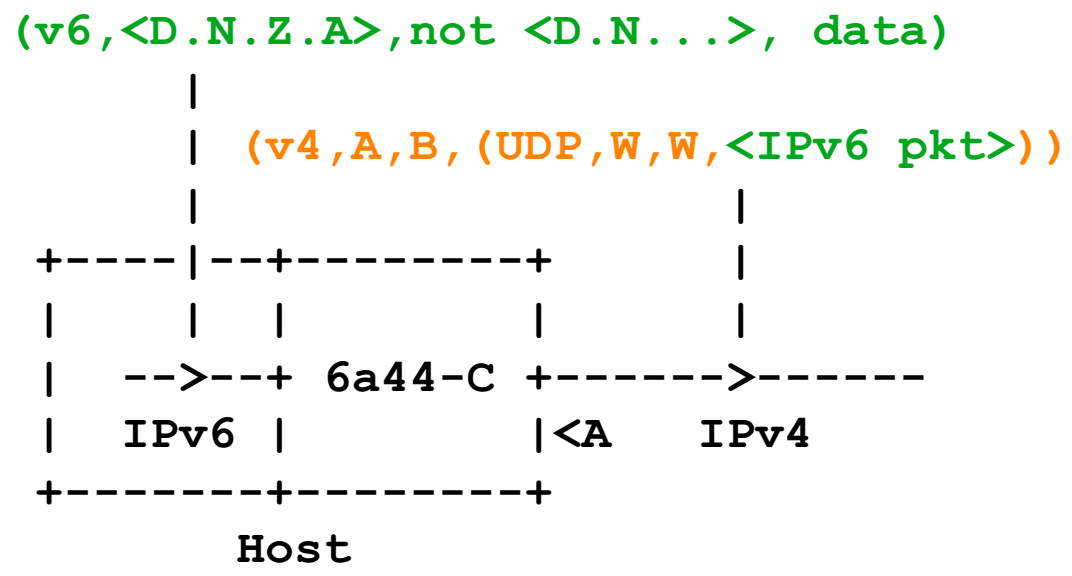
ANNEXES

Address construction

- **6a44 address = D.N.Z.A, where:**
  - **D** = the /48 IPv6 prefix assigned by the ISP to 6a44 for the considered network
  - **A** = the IPv4 local address of the host (private IPv4)
  - **N** and **Z** are the NAT address and NAT port that are bound to the [A, W] couple (W is the well-known port of 6a44)

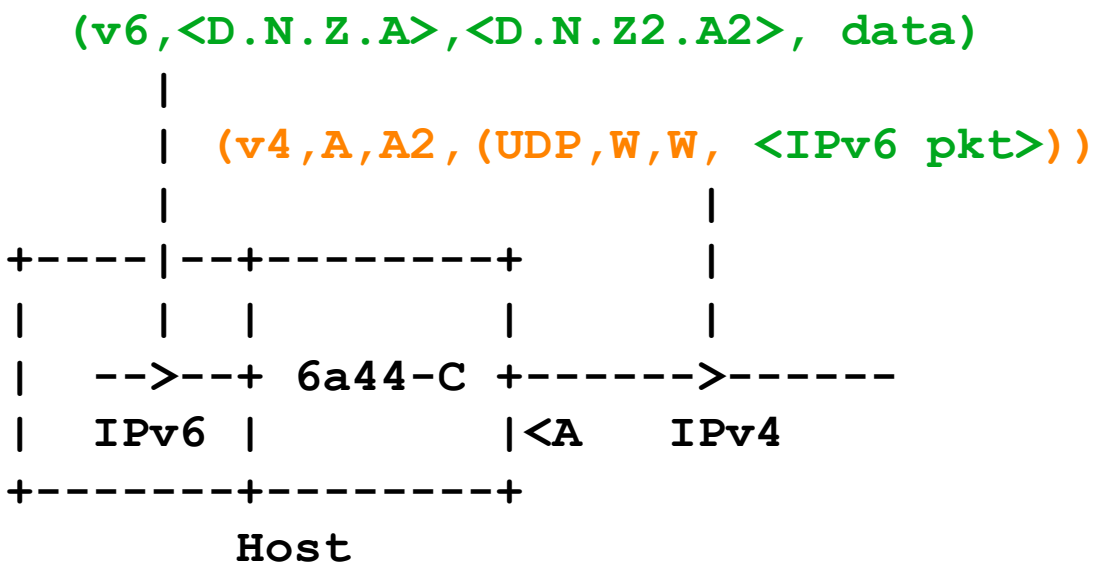
Mappings and Encapsulations Rules

Host to Relay

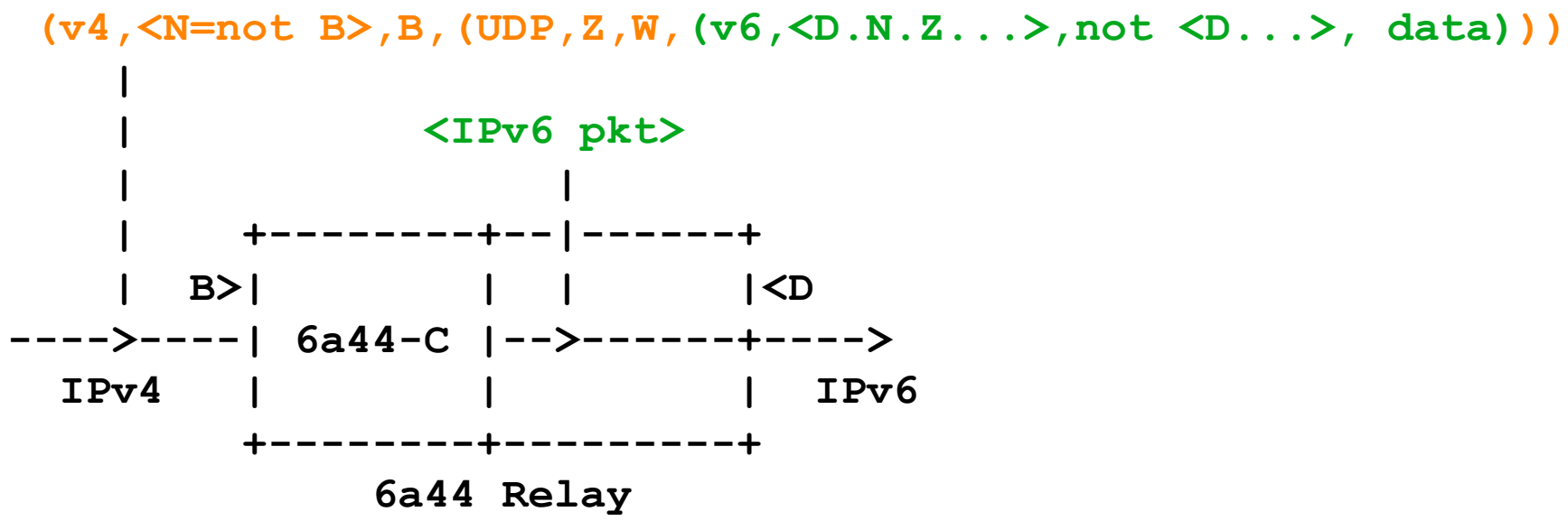


Mappings and Encapsulations Rules

Host to Host (intra-site)

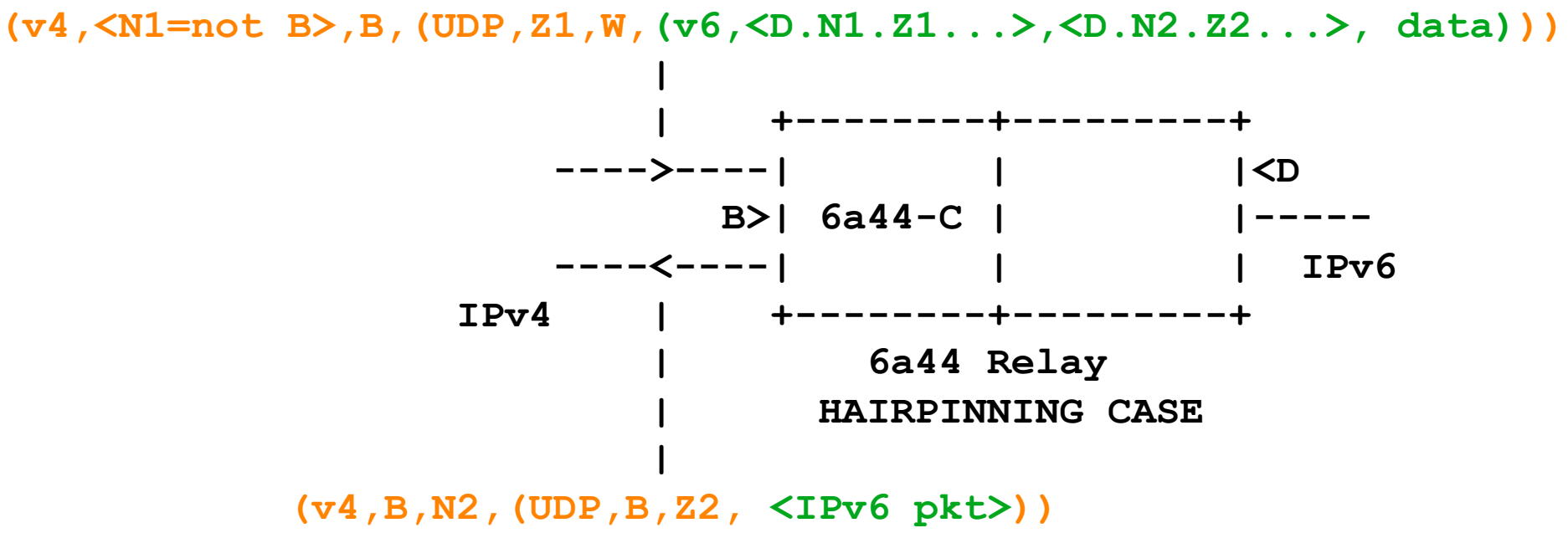


Mappings and Encapsulations Rules
Relay Traversal



Mapping and Encapsulation Rules

Relay Hairpinning

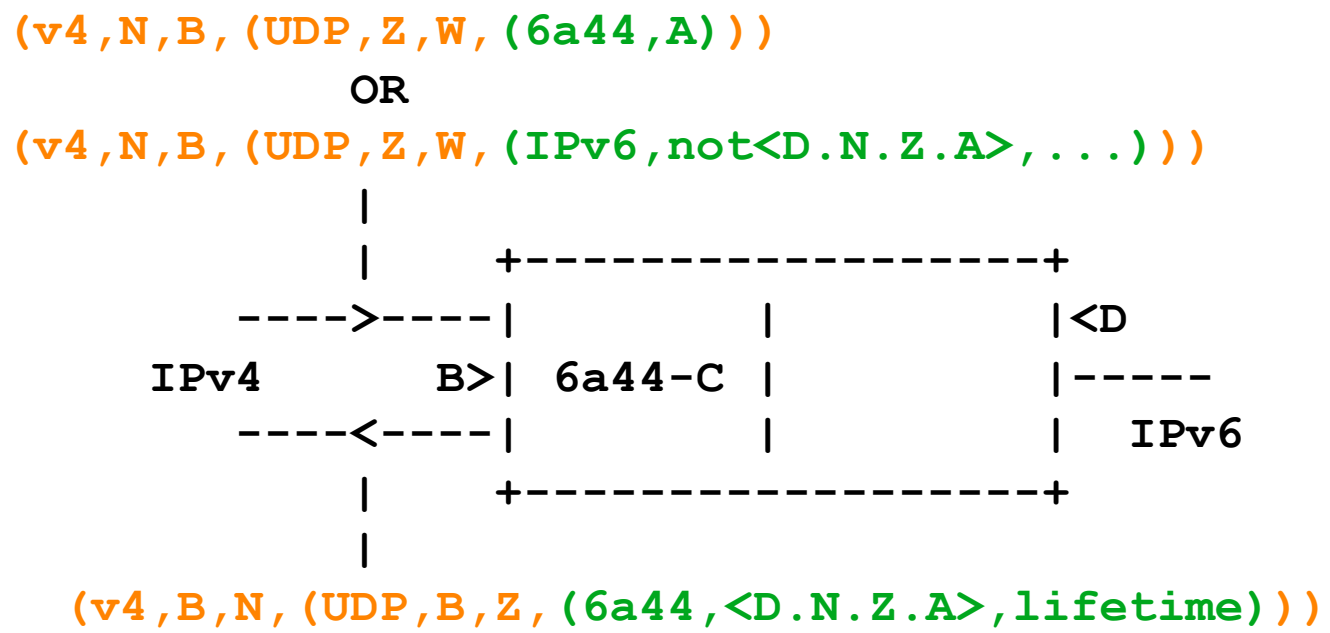


Parameter Acquisition by Hosts

- A **Host** sends a "Parameter Request" to Relays:
  - At init
  - Periodically in the absence of host to relay traffic (NAT binding refresh)
  - If the local IPv4 address changes (CPE reset)
  - With its local IPv4 address as data
- A **Relay** transmits a "Parameter Indications" to a host:
  - When it receives a parameter request
  - If it receives from the host a packet with IPv6 and IPv4+port that are inconsistent (CPE reset)
  - With the host IPv6 address and a lifetime

Parameter Acquisition by Hosts

Message Processing in 6a44 Relays



Open Issues

- Is the lifetime necessary?
  - The NAT binding refresh initiated by hosts at least every every 29 s (as for SIP) could be sufficient
- Is an additional security protection needed
  - With ISP networks that don't have ingress filtering, DOS attacks could be launched (false Parameter Indications usurping the 6a44 well-known source address)
  - Add a *nonce* for host-relay exchanges?
- What to do next in IETF?