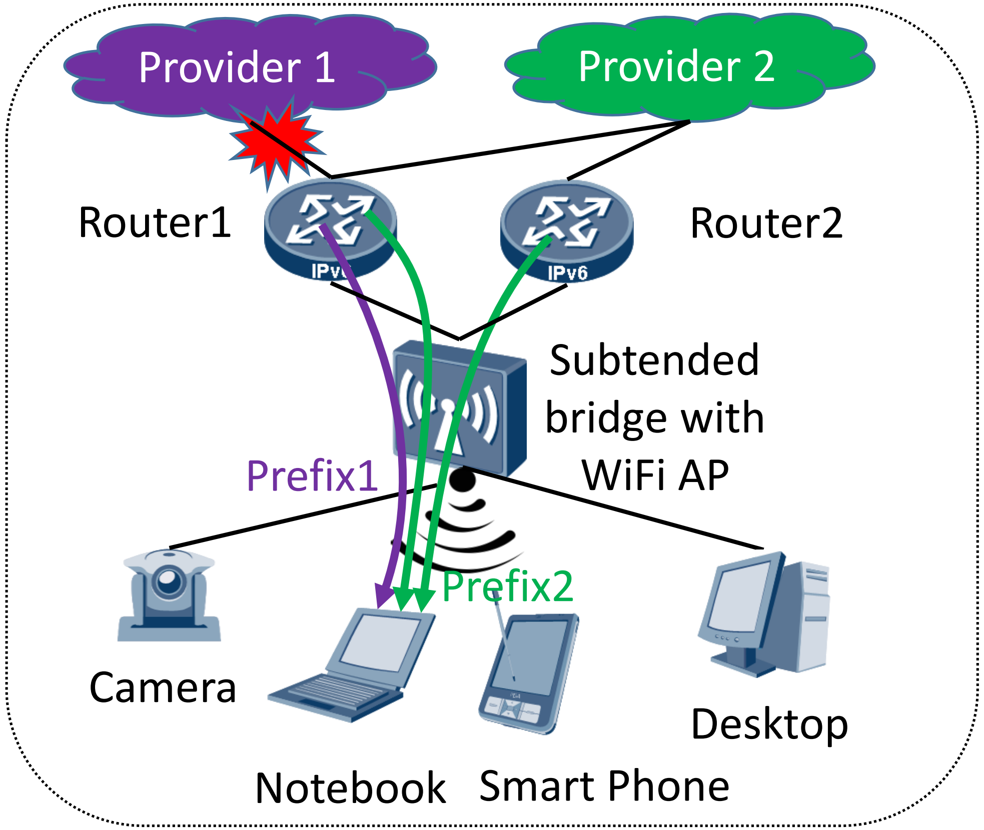
Neighbor Discovery Support for Multi-Home Multi-Prefix

draft-vv-6man-nd-support-mhmp-00

Eduard Vasilenko vasilenko.eduard@huawei.com

Paolo Volpato paolo.volpato@huawei.com

MHMP environment



- Site topology may be very complex – see RFC 7157 and RFC 8678
- Hosts have PA addresses from many Carriers
- Solution needs to solve 3 problems:
  1. Choose the proper source address (Internet filtering may restrict what is possible to connect for a particular source address; “walled garden” example)
  2. Choose the proper next hop on the path to the source address owner (re-routing by source routing on-site may release this requirement at the expense of redundant hop)
  3. Do source routing on-site with complex topology to forward traffic to proper Carrier (Carrier would drop packets with source addresses of another Carrier)
- Almost all problems are resolved by RFC 8028 + RFC 8678
- This draft is concerned with the solution for the first two problems, as discussed in the next slides:
  1. Improvement to ND (RFC 4861), SLAAC (RFC 4862) and Default Address Selection (RFC 6724)
  2. The last problem is properly discussed by Multihoming in Enterprise (RFC 8678).

MHMP Scenarios

1. Scenario **“equal prefixes”**: Announced prefixes are fully equal by scope and value, all resources interested for hosts could be reachable through any announced PA prefix. Additionally, traffic distribution between carriers could be non-predictable (no traffic engineering or policy).
   Solutions:
   - Rule 5 or 5.5 of RFC 6724 – choose source address only advertised by already chosen next hop
   - Conditional PIO of RFC 8475 – does not leave the choice for the host that does not support Rule 5.5

2. Scenario **“non-equal prefixes”**: Announced prefixes are not equal because (1) some resources could be accessed only through a particular prefix (for example “walled garden” of one carrier) or (2) it is desirable to have some policy for traffic distribution between PA prefixes (cost of traffic, delay, packet loss, jitter, proportional load, etc.).
   Solutions:
   - The only solution available is “The same policies could be formatted differently and fed to the host by two mechanisms at the same time: 1) “Routing Information Options” of RFC 4191 and 2) RFC 7078 to modify policies in RFC 6724 selection algorithm” (via DHCPv6). It has a low probability to be accepted because RFC 7078 is not supported by hosts and CPEs.

New Solutions for Case “non-equal prefixes”

1. Choose **Source Address first,** only then **Next-Hop**.
2. It would open many new possibilities:
   A. Only policies could be supplied by RFC 7078 to the RFC 6724 selection algorithm (no need for RIO). This method has a low probability of implementation because of not wide support of DHCPv6 in the industry. Maybe this method would have more acceptance in the future.
   B. It is possible to check the longest match between the source and the destination address to choose the potentially closest address. This method looks most promising, it is partially discussed in RFC 6724 section 7.
   C. The host could use DNS requests with different source addresses to understand what is visible for a particular source address.
   D. URL for configuration information could be supplied in RA – see RFC 8801 (Provisioning domains).
   E. The host may have local performance management capabilities (packet loss, delay, jitter, etc.) to choose the best source for the application.

Standards modifications

#	Standard modifications	Change/Extension
6.1	Preference to choose source address before the next-hop	Section 7 of RFC 6724
6.2	Prefer default routers that advertise prefix used for source address already chosen	Section 6.3.6 of RFC 4861
6.3	Deprecate PIOs if source prefix is lost (with optional dampening)	Section 4.2, 5.1 of RFC 4862
6.4	Do not deprecate default routers, deprecate PIOs	Requirement G-4/5 of RFC 7084 (CPE requirements)
6.5	Clean orphaned prefixes (PIOs) after default router list change	Section 6.3.5 of ND

MHMP is supported on IPv4 by Private Addresses + NAT.

We need a good MHMP solution or we have a danger
that ULA+NPT would become the primary solution for IPv6.

Next Steps

- Any reviews, criticism, missing aspect?
- Co-authoring is welcome

- Thank you