Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 02, 2016

M.G.D.Sumanta
IMTEC
March 02 , 2016

IPv6 Multihoming with transparent End-to-End connectivity
draft-sumanta-ipv6-multihoming-solution-00

Abstract

Ipv6 Multihoming for Host could be implemented using Ipv6-to-Ipv6 Network prefix translation (NPTv6), however NPTv6 not ideal as this solution not achieve End-to-End transparency of connectivity. Basic issues with End host Multihoming architecture without NPTv6 are:
1. Source address selection, 2. Next hop selection and 3. DNS resolution.
One other approach to solve above mention all three issues with End-to-End transparent connectivity would be using policy at End host to enforce source address and next hop selection. In this document,a solution being propose to solve all above mention three problem enhancing policy based enforcement on host directed by router using its router advertisement.This document not obsolete any of the previous work,only propose how policy on End-host can be enforce from router by mapping destination prefix with DNS via Router Advertisement.

Status of This Memo

Table of Contents

1. Introduction

Multi Homing has been architect to exchange IP packet uninterruptedly from local host to remote host or vice versa even when underlying connectivity change dynamically. It is being designed to support change in path without knocking session of the application.

```
                           +------+
                           |remote|
                           | host |
                           |  R   |
                           +------+
                              |
                    + - - - - - - - - - - - - +
                    | Internet Connectivity |
                    + - - - - - - - - - - - - +
                         /            \
                   +---------+    +---------+
                   | ISP A   |    |  ISP B  |
                   +---------+    +---------+
                       | Path A         | Path B
         + - - - - - - - - - - - - - - - - - - - - +
         | multi-      |               |           |
           homed   +------+         +------+
         | site    | site-|         | site-|       |
                   | exit |         | exit |
         |         |router|         |router|       |
                   |  A   |         |  B   |
         |         +------+         +------+       |
                      |                |
         |         local site connectivity         |
                           |
         |           +-----------+                 |
                     |multi-homed|
         |           |   host    |                 |
                     +-----------+
         + - - - - - - - - - - - - - - - - - - - - +
```

Fig 1 : Complete figure of ipv6 multiHoming.

Network Address and port Translation (NAPT) one of the solution which being used in Ipv4 Multihoming scenario also can be used in Ipv6. Ipv6-to-Ipv6 network prefix translation (NPTV6) work on basic principle, End host address being mapped with a global address and confined End host address visibility from outside network. Non visibility nature of Network address translation prevent End-to-end transparency. Unlike Ipv6, in Ipv4 where global address are scarce resource, Network Address Translation could be ideal solution. That unlikely the case on IPv6. Hence, end host address visibility is the primary goal in Ipv6 solution space. As Network address translation confined address visibility, make it obvious not to consider as No1 solution in Ipv6. End host configure with multiple Ipv6 address from each service provider address space and use of Ipv6 specification to achieve switch over among service provider and drop free forwarding consider to be best solution. Adequate number of Ipv6 global unique address make easy to implement end host with multiple unique service provider dependent global IPv6 address for each connected different service provider.This further ensure end-to-end transparent connection unlike NAT.However there are several issue in this kind of implementation or design, Herein summarizing all issues with different use case topologies:

A. Wrong Source address selection.
B. Wrong Next hop selection.
C. Private and public RDNSS co-existence.

On way to get ride off above mention issues on multi address assigned end host implementation would be using policy on end host to select Source address and Next hop.

Depends on different uses case, end host policy define may a burden some activity and difficult to achieve complete error free.Complexity arise due to multiple next hop, source address and DNS presence and any wrong combination will raise reachability issue or ingress filtering on service provider ingress end. It further complicate on deployment where local destination reachable via a particular site and remote destination reachable via multiple sites. Further, manual policy configuration on end host subjected to changeable whenever service provider's or local site's DNS,default gate way router and numerous destination changes.

1.1. Reserved Words

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Terminology

NPTv6 **IPv6-to-IPv6 Network Prefix Translation as described in** [RFC6296].

NAPT Network Address Port Translation as described in [RFC3022]. In other contexts, NAPT is often pronounced "NAT" or written as "NAT".

MHMP Multihomed with multi-prefix. A host implementation that supports the mechanisms described in this document; selection, and DNS selection policy.

namely, source address selection policy, next hop

3. Problem Statement

```
                                +------+       ___________
                                |      |      /           \
                            +---| rtr1 |=====/   network   \
                            |   |      |     \    1 ISP A  /
               +------+     |   +------+      \___________/
               |      |     |
               |host  |-----+
               |      |     |
               +------+     |   +------+       ___________
                            |   |      |      /           \
                            +---| rtr2 |=====/   network   \
                                |      |     \  2 ISP B    /
                                +------+      \___________/
```

Fig 2: Ipv6 Multi homing Part figure.

3.1 Wrong Source address selection.

When multiple address assigned on End host, End host may select different Source address compare to right source address need to reach via a service provider. Wrong source address selection does not alarming without service provider have ingress filter applied as packet with any global address perfect to travel global scope. However, uncertainty on service provider ingress filter presence impose packet's source address should be particular service provider dependent address. Otherwise, will be filter out on service provider network by ingress rule.Having different service provider dependent source address compare to service provider packet being forwarded consider as wrong source address selection.

3.2 Wrong Next hop selection.

End host for all off-link prefix, consider default router address as next hop.Default routers are being advertise using dynamic router advertisement process. Selection of default router is either by round robin or by preference setting. Further, end host could be router capable and have routing table entry corresponding to different destination. However, practice of having routing info limited on End host, due to memory and computation requirement.In the case of default router scenario host May chose a next hop which does not have reachability to reach particular destination. There could be scenario, internet destination reachable via multiple service provider sites.

To reach internet destination, selection of next hop does not matter for data packet transfer. But to reach DNS to resolve domain name, selection of next hop is vital. If next hop being chosen wrongly, packet will reach to wrong DNS and will be discarded. Similarly for data packet when destination must be routed through a particular local site, next hop selection play a pivotal role on successful packet delivery.

3.3 Private and Public RDNSS co-existence.

In an implementation End host have to contact local site deployed DNS to resolve organization internal destination, also end host have to contact service provider DNS to resolve internet destination. Such implementation referred as private and public RDNSS co-existence. Typical issue with this implementation , end host does not has clue which DNS to reach for which destination URL ,wrong destination choice will lead to unsuccessful attempts on address resolve process . Even if selection of DNS problem being bell out,further packet forwarding should be with same source address and next hop.Otherwise packet will not get fate to reach final destination. Such way,presence of private and public RDNSS co-existence provoke more complex issue regards to source address and next hop selection.

4. Router Advertisement message on details

4.1 Router Advertising message.

```
   0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |     Code      |          Checksum             |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | Cur Hop Limit |M|O|  Reserved |       Router Lifetime         |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                         Reachable Time                        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                          Retrans Timer                        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |   Options...
    +-+-+-+-+-+-+-+-+-+-+-+-
```

4.2 Recursive DNS Server option.

```
     0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |     Type      |     Length    |           Reserved            |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                           Lifetime                            |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                                                               |
     :            Addresses of IPv6 Recursive DNS Servers            :
     |                                                               |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

4.3 DNS Search list option.

```
      0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |     Type      |     Length    |           Reserved            |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                           Lifetime                            |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                                                               |
     :                Domain Names of DNS Search List                :
     |                                                               |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

4.4 Router information option.

```
      0                   1                   2                   3
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |     Type      |    Length     | Prefix Length |Resvd|Prf|Resvd|
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                        Route Lifetime                         |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                   Prefix (Variable Length)                    |
      .                                                               .
      .                                                               .
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

5. Solution

```
                                  100::/
                             +------+       ___________
                   fe80::11 |      |      /           \ DNS 101::1
                        +---| rtr1 |=====/   network   \
                        |   |      |     \    1 ISP A  /
               +------+     |   +------+      \___________/
               |      |     |
               |host  |-----+
               |      |     |        200::/
               +------+     |   +------+       ___________
                        |   |      |      /           \
                        +---| rtr2 |=====/   network   \ DNS 202::1
                  fe80::12  |      |     \  2 ISP B    /
                            +------+      \___________/
```

Fig 3: Ipv6 Multi homing Part figure.

5.1 Next Hop selection

Network designer or Administrator should provision router to aware of DNS address and service provider prefix which end host will use as DNS address to resolve destination URL and provided prefix to build up its interface address respectively. Administrator should provision correct mapping of this information, so that when end host select service provider prefix corresponding address as source address and pair DNS address , packet forward successfully. Also, particular router is the prefer router to reach destination for both DNS traffic and data traffic using corresponding service provider dependent source address.This should be ensure for error free traveling to destination with correct mapping of source address and next hop. Further Router will send router advertisement with router information list carrying DNS server prefix with prf value as high. By receiving such router advertisement, host select advertising router link-local address as next hop or default gate way router to reach prefix mention on router information list. Hence, to reach particular DNS host will chose advertising router as next hop. Further all traffic destined for same destination should use same Next hop as its being used to reach DNS while discovering domain to address mapping. In some case host may know destination ipv6 address and do not go through DNS resolve process. In that circumstances, if destination belongs to particular service provider dependent prefix or prefix being advertise through Router advertisement on its router information list setting, advertising router Link-local address being used as next hop address. In other all case Next hop being selected current rule of random selection.

Example :

In above [Fig 3], consider ISP A DNS server address 101::1 and ISP B DNS server address 202::1. When rtr1 send RA message along with all info it's propagate to host,Recursive DNS option, DNS search list option; it's also should add Router information option , for prefix 101::1/128. By receiving such RA, host will set highest default router as rtr1 link-local address for 101:: 1/128 prefix. Similarly, rtr2's link-local will be considered as highest default router for prefix 202:: 1/128.Now there is no difficulty to select correct next hop. If host want to resolve via ISP A, it will choose rtr1 and when via ISP B it will choose rtr2.

5.2 Source Address Selection

Similar to Next hop rule , Network designer or Administrator should provision router to aware of service provider prefix and DNS address which end host will adopt to build up its interface address and to use as DNS to resolve destination URL respectively. Router should hold correct mapping of this information, so that if end host wanted to reach any destination including mapping DNS using provision prefix corresponding source address, particular router should be the next hop. This should be ensure. Router send router advertisement with router information list carrying DNS server prefix with prf value as high. By receiving such router advertisement, hos ensure while advertising router being chosen as Next hop address, advertise prefix corresponding address also being chosen as source address. Even for the traffic which not going through DNS resolve, also should chose source address based on Next hop its select. That ensure right choice of source address in all implementations and use cases.

Example :

In above figure [Fig3] rtr1 send RA with prefix 100::/64 to configure ISP dependent address. Rtr1 Link-local address is fe80::11 Similarly rtr2 send RA with prefix 200::/64 to configure ISP dependent address. Rtr2 Link-local address is fe80::12 Let consider 400::/64 is the destination traffic need to be destine. As this is being off-link prefix, traffic is being send base on default router and next hop will be selected as either rtr1 or rtr2 link-local address. Proposed enhancement will select source as 100::xxxx address when rtr1 is being selected as next hop or will select 200::xxx address when rtr2 is being selected as next hop.

5.3 Private and Public RDNS co-existence

When a local site have private DNS , router should advertise local DNS prefix mapping to DNS search list containing entire private domain name. Also, when site local have local destination without subject to DNS resolve, those local destination also should be advertise on router advertisement in router information list setting prf bit high. In other word, administrator should ensure all destination prefixes are being advertise on router information list for which particular router must be consider as Next hop. As RFC 4919 already laid guideline,how host should behave and which default router would be selected based on router information list prefix and prf bit value further not being described here. Using same guideline and with care full declaration of router information list would help to nail down all issues related to Next Hop and Source address selection on Private and Public RDNS co-existence network.

5.4 DNS search-list extenssion

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Length    | RDNS  |     Reserved             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Lifetime                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
:                Domain Names of DNS Search List                :
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

RDNS Flag - This Flag indicate - Map domain suffix received on this RA to RDNS option received in same RA.

6. Security Considerations

Major part of end host police enforcement depends on Router advertisement and router information list its carry. Its necessary router advertisement should be from a trusted router. In a LAN to verify router advertisement from trusted source there are already well define solution which carve out Rouge RA problem, secure neighbor discovery etc. Also, creation of router list depends on router aware ness of information which could be potential thread of misinform. Careful approach of configuration only by authorized network user or Authorized dynamic update process should be in place to adhere those information for further use.

7. IANA Considerations

This document has no action for IANA

8. Reference

8.1 Normative Reference

[RFC 7157] O. Troan,D. Miles ,S. Matsushima , T. Okimoto , D. Wing , "IPv6 Multihoming without Network Address Translation" , RFC 7157 , March 2014

[RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, November 2005.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC6296] Wasserman, M. and F. Baker, "IPv6-to-IPv6 Network Prefix Translation", RFC 6296, June 2011.

[RFC6724] Thaler, D., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, September 2012.

[RFC6731] Savolainen, T., Kato, J., and T. Lemon, "Improved Recursive DNS Server Selection for Multi-Interfaced Nodes", RFC 6731, December 2012.

[RFC7078] Matsumoto, A., Fujisaki, T., and T. Chown, "Distributing Address Selection Policy Using DHCPv6", RFC 7078, January 2014.

8.2 Informative References

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001.

[RFC3442] Lemon, T., Cheshire, S., and B. Volz, "The Classless

Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4", RFC 3442, December 2002.

[RFC3582] Abley, J., Black, B., and V. Gill, "Goals for IPv6 Site-Multihoming Architectures", RFC 3582, August 2003.

[RFC3646] Droms, R., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.

[RFC4116] Abley, J., Lindqvist, K., Davies, E., Black, B., and V. Gill, "IPv4 Multihoming Practices and Limitations", RFC 4116, July 2005.

[RFC4218] Nordmark, E. and T. Li, "Threats Relating to IPv6 Multihoming Solutions", RFC 4218, October 2005.

[RFC5206] Nikander, P., Henderson, T., Vogt, C., and J. Arkko, "End-Host Mobility and Multihoming with the Host Identity Protocol", RFC 5206, April 2008.

[RFC5220] Matsumoto, A., Fujisaki, T., Hiromi, R., and K. Kanayama, "Problem Statement for Default Address Selection in Multi-Prefix Environments: Operational Issues of RFC 3484 Default Rules", RFC 5220, July 2008.

[RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, April 2010.

[RFC5533] Nordmark, E. and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", RFC 5533, June 2009.

[RFC6106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 6106, November 2010.

9. Author's Address

Sumanta Das Gajendra Mahapatra
Dell international services India private limited
Chennai , INDIA
Email : Sumanta.dgmp@gmail.com