**Source Address Dependent Routing and Source Address Selection for IPv6
Hosts**
draft-sarikaya-6man-sadr-overview-04

Abstract

   This document presents the source address dependent routing from the
   host perspective. Multihomed hosts and hosts with multiple
   interfaces are considered. Different architectures are introduced
   and with their help, why source address selection and next hop
   resolution in view of source address dependent routing is needed is
   explained. The document concludes with an informative guidelines on
   the different solution approaches.

Status of This Memo

Copyright Notice

include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Introduction

BCP 38 recommends ingress traffic routing to prohibit Denial of
Service (DoS) attacks, i.e. datagrams which have source addresses
that do not match with the network where the host is attached are
discarded [RFC2827]. Avoiding packets to be dropped because of
ingress filtering is difficult especially in multihomed networks
where the host receives more than one prefix from the connected
Internet Service Providers (ISP) and may have more than one source
addresses. Based on BCP 38, BCP 84 introduced recommendations on the
routing system for multihomed networks [RFC3704].

Recommendations on the routing system for ingress filtering such as
in BCP 84 inevitably involve source address checks. This leads us to
the source address dependent routing. Source address dependent
routing is an issue especially when the host is connected to a
multihomed network and is communicating with another host in another
multihomed network. In such a case, the communication can be broken
in both directions if ISPs apply ingress filtering and the datagrams
contain wrong source addresses
[I-D.huitema-multi6-ingress-filtering].

Hosts with simultaneously active interfaces receive multiple prefixes
and have multiple source addresses. Datagrams originating from such
hosts carry greats risks to be dropped due to ingress filtering.
Source address selection algorithm needs to be careful to try to
avoid ingress filtering on the next-hop router [RFC6724].

Many use cases have been reported for source/destination routing in
[I-D.baker-rtgwg-src-dst-routing-use-cases]. These use cases clearly
indicate that the multihomed host or Customer Premises Equipment
(CPE) router needs to be configured with correct source prefixes/
addresses so that it can route packets upstream correctly to avoid
ingress filtering applied by an upstream ISP to drop the packets.

In multihomed networks there is a need to do source address based
routing if some providers are performing the ingress filtering
defined in BCP38 [RFC2827]. This requires the routers to consider
the source addresses as well as the destination addresses in
determining the next hop to send the packet to.

Based on the use cases defined in
[I-D.baker-rtgwg-src-dst-routing-use-cases], the routers may be
informed about the source addresses to use in routing using
extensions to the routing protocols like IS-IS defined in
[ISO.10589.1992] [I-D.baker-ipv6-isis-dst-src-routing] and OSPF
defined in [RFC5340] [I-D.baker-ipv6-ospf-dst-src-routing]. In this
document we describe the use cases for source address dependent
routing from the host perspective.

There are two cases. A host may have a single interface with
multiple addresses (from different prefixes or /64s). Each address
or prefix is connected to or coming from different exit routers, and
this case can be called multi-prefix multihoming (MPMH). A host may
have simultaneously connected multiple interfaces where each
interface is connected to a different exit router and this case can
be called multi-prefix multiple interface (MPMI).

It should be noted that Network Address and Port Translation (NAPT)
[RFC3022] in IPv4 and IPv6-to-IPv6 Network Prefix Translation (NPTv6)
[RFC6296] in IPv6 implement the functions of source address selection
and next-hop resolution and as such they address multihoming (and
hosts with multiple interfaces) requirements arising from source
address dependent routing [RFC7157]. In this case, the gateway
router or CPE router does the source address and next hop selection
for all the hosts connected to the router. However, for end-to-end
connectivity, NAPT and NPTv6 should be avoided and because of this,
NAPT and NPTv6 are left out of scope in this document.

2. Terminology

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].

3. SADR Scenarios

Source address dependent routing can be facilitated at the host with
proper next hop and source address selection. For this, each router
connected to different interfaces of the host uses Router
Advertisements to distribute default route, next hop as well as
source address/prefix information to the host.

The use case shown in Figure 1 is multi-prefix multi interface use
case where rtr1 and rtr2 represent customer premises equipment/
routers (CPE) and there are exit routers in both network 1 and
network 2. The issue in this case is ingress filtering. If the
packets from the host communicating with a remote destination are
routed to the wrong exit router, i.e. carry wrong source address,
they will get dropped.

```
   +------+     +------+          _____
   |      |     |      |         /          \
   |      |-----| rtr1 |=====/    network   \
   |      |     |      |     \       1       /
   |      |     +------+      _____/
   |      |
   | host |
   |      |
   |      |     +------+          _____
   |      |     |      |         /          \
   |      |=====| rtr2 |=====/    network   \
   |      |     |      |     \       2       /
   +------+     +------+      _____/
```
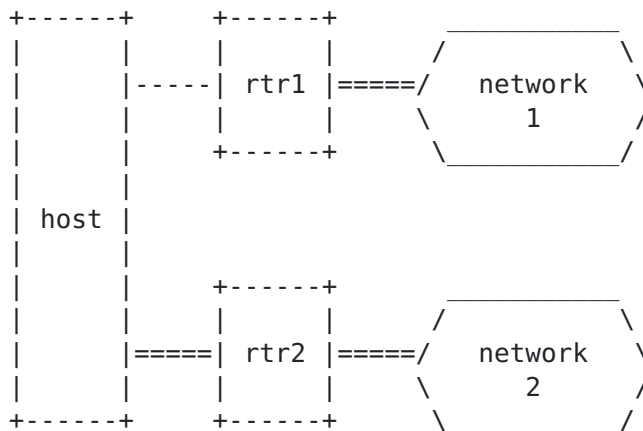
Figure 1: Multihomed Host with Two CPE Routers

Our next use case is shown in Figure 2. This use case is a multi-
prefix multihoming use case. rtr is CPE router which is connected to
two ISPs each advertising their own prefixes. In this case, the host
may have a single interface but it receives multiple prefixes from
the connected ISPs. Assuming that ISPs apply ingress filtering
policy the packets for any external communication from the host
should follow source address dependent routing in order to avoid
getting dropped.

```
     +------+                   |
     |      |                   |
     |      |                   |=====|(ISP1)|=====
     |      |    +------+       |
     |      |    |      |       |
     |      |====|  rtr |=====|
     | host |    |      |       |
     |      |    +------+       |
     |      |                   |
     |      |                   |
     |      |                   |=====|(ISP2)|=====
     |      |                   |
     +------+                   |
```

                 Figure 2: Multihomed Host with Multiple CPE Routers

   A variation of this use case is specialized egress routing. Upstream
   networks offer different services with specific requirements, e.g.
   video service. The hosts using this service need to use the
   service's source and destination addresses. No other service will
   accept this source address, i.e. those packets will be dropped
   [I-D.baker-rtgwg-src-dst-routing-use-cases].

```
    _____               +------+
   /           \  +------+     |      |
  /   network   \ |      |     |      |
  \     1       /--| rtr1 |----|      |
   _____/   |      |     |      |       +------+           _____
                   +------+     | host |       |      |          /           \
                                |      |       |      |         /   network   \
                                |      |=====| rtr3 |=====/   network   \
    _____                 |      |       |      |         \     3       /
   /           \  +------+       |      |       +------+          _____/
  /   network   \ |      |       |      |
  \     2       /--| rtr2 |----|      |
   _____/   |      |     |      |
                   +------+     |      |
                                +------+
```

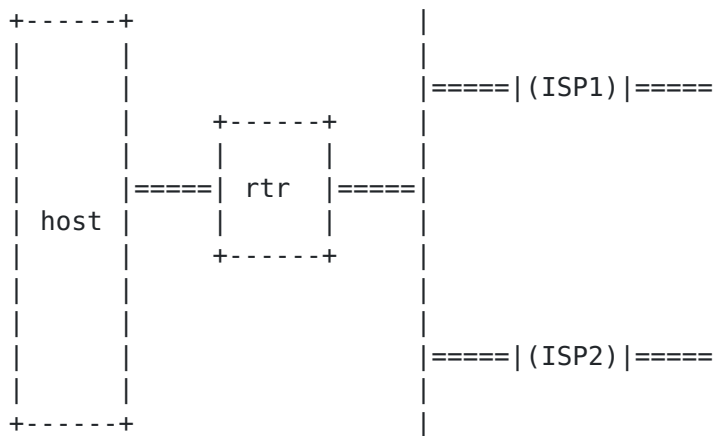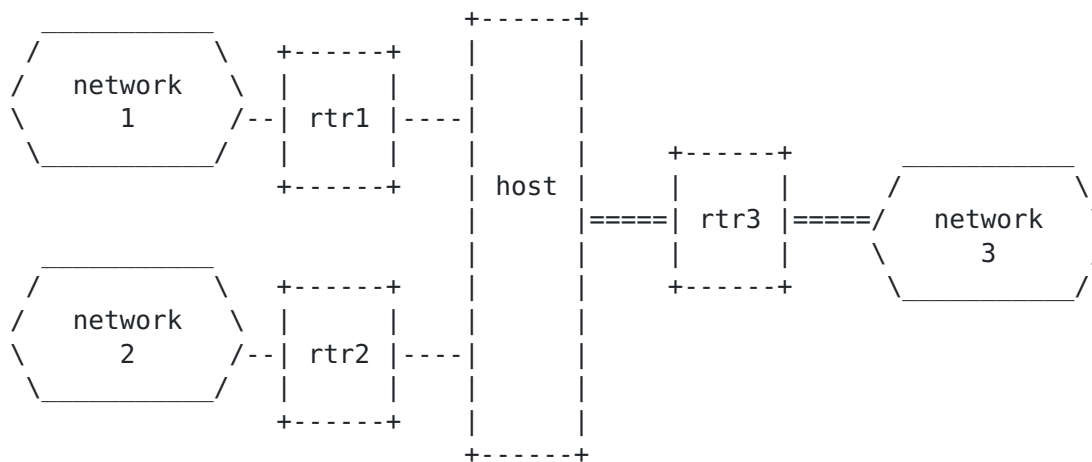   Figure 3: Multihomed Host with Three CPE Routers

   Next use case is shown in Figure 3. It is a variation of multi-
   prefix multi interface use case above. rtr1, rtr2 and rtr3 are CPE
   Routers. The networks apply ingress routing. Source address
   dependent routing should be used to avoid any external communications
   be dropped.

In the homenet scenario given in Figure 4, representing a simple home
network, there is a host connected to two CPEs which are connected to
ISP1 and ISP2, respectively. Each ISP provides a different prefix.
Also each router provides a different prefix to the host. The issue
in this scenario is also ingress filtering used by each ISP.

```
   +------+
   |      |    +------+
   |      |    |      |
   |      |==+==| rtr1 |=====|(ISP1)|=====
   |      |  |  |      |     |
   |      |  |  +------+
   | host |  |
   |      |  |
   |      |  |  +------+
   |      |  |  |      |
   |      |  +==| rtr2 |=====|(ISP2)|=====
   |      |     |      |     |
   +------+     +------+
```
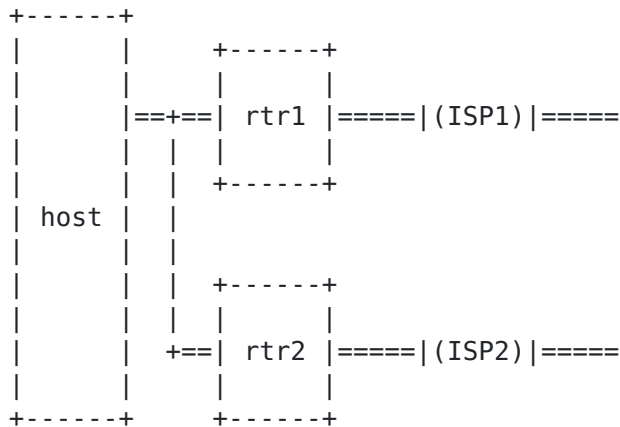
           Figure 4: Simple Home Network with Two CPE Routers

The host has to select the source address from the prefixes of ISP1
or ISP2 when communicating with other hosts in ISP1 or ISP2. The
next issue is to select the correct next hop router, rtr1 or rtr2
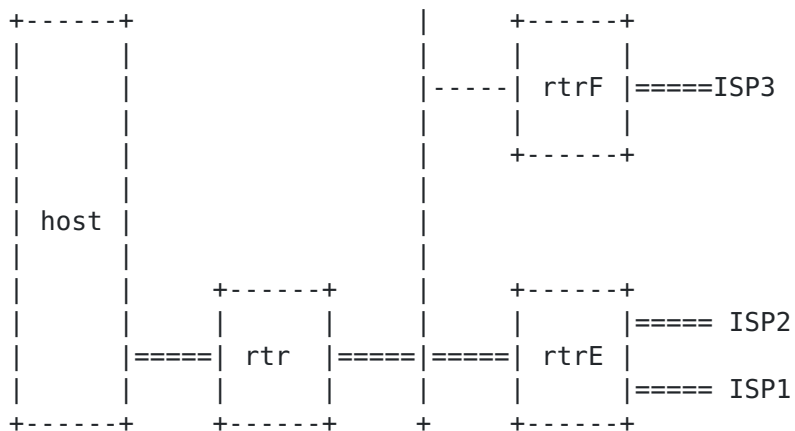that can reach the right ISP, ISP1 or ISP2.

```
   +------+                   |    +------+
   |      |                   |    |      |
   |      |                   |----| rtrF |=====ISP3
   |      |                   |    |      |
   |      |                   |    +------+
   |      |                   |
   | host |                   |
   |      |                   |
   |      |    +------+       |    +------+
   |      |    |      |       |    |      |===== ISP2
   |      |=====| rtr  |=====|=====| rtrE |
   |      |    |      |       |    |      |===== ISP1
   +------+    +------+    +    +------+
```

              Figure 5: Shim6 Host with Two Routers

The last use case in Figure 5 is also a variation of multi-prefix
multihoming use case above. In this case rtrE is connected to two
ISPs. All ISPs are assumed to apply ingress routing. The host
receives prefixes from each ISP and starts communicating with

external hosts, e.g. H1, H2, etc. H1 and H2 may be accessible both
from ISP1 and ISP3.

The host receives multiple provider-allocated IPv6 address prefixes,
e.g. P1, P2 and P3 for ISP1, ISP2 and ISP3 and supports shim6
protocol [RFC5533]. rtr is a CPE router and the default router for
the host. rtr receives OSPF routes and has a default route for rtrE
and rtrF.

4. Analysis of Source Address Dependent Routing

In this section we present an analysis of the scenarios of Section 3
and then discuss the relevance of SADR to the provisioning domains.

4.1. Scenarios Analysis

As in [RFC7157] we assume that the routers in Section 3 use Router
Advertisements to distribute default route, next hop and source
address prefixes supported in each next hop to the hosts or the
gateway/CPE router relays this information to the hosts.

Referring to the scenario in Figure 1, source address dependent
routing can present a solution to the problem of the host wishes to
reach a destination in network 2 and the host may choose rtr1 as the
default router. The solution should start with the correct
configuration of the host. The host should be configured with the
next hop addresses and the prefixes supported in these next hops.
This way the host having received many prefixes will have the correct
knowledge in selecting the right source address and next hop when
sending packets to remote destinations.

Note that similar considerations apply to the scenario in Figure 3.

In the configuration of the scenario in Figure 2 also it is useful to
configure the host with the next hop addresses and the prefixes and
source address prefixes they support. This will enable the host to
select the right prefix when sending packets to the right next hop
and avoid any ingress filtering.

Source address dependent routing in the use case of specialized
egress routing may work as follows. The specialized service router
advertizes one or more specific prefixes with appropriate source
prefixes, e.g. to the CPE Router, rtr in Figure 2. The CPE router in
turn advertizes the specific service's prefixes and source prefixes
to the host. This will allow proper configuration at the host so
that the host can use the service by sending the packets with the
correct source and destination addresses.

Let us analyze the use case in Figure 4. If a source address
dependent routing protocol is used, the two routers (rtr1 and rtr2)
are both able to route traffic correctly, no matter which next-hop
router and source address the host selects. In case the host chooses
the wrong next hop router, e.g. for ISP2 rtr1 is selected, rtr1 will
forward the traffic to rtr2 to be sent to ISP2 and no ingress
filtering will happen.

Note that home networks are expected to comply with requirements for
source address dependent routing and the routers will be configured
accordingly, no matter which routing protocol, e.g. OSPF is used
[I-D.ietf-homenet-hncp].

This would work but with issues. The host traffic to ISP2 will have
to go over two links instead of one, i.e. the link bandwidth will be
halved. Another possibility is rtr1 can send an ICMPv6 Redirect
message to the host to direct the traffic to rtr2. Host would
redirect ISP2 traffic to rtr2.

The problem with redirects is that ICMPv6 Redirect message can only
convey two addresses, i.e. in this case the router address, or rtr2
address and the destination address, or the destination host in ISP2.
That means the source address will not be communicated. As a result,
the host would send packets to the same destination using both source
addresses which causes rtr2 to send a redirect message to rtr1,
resulting in ping-pong redirects sent by rtr1 and rtr2.

The best solution to these issues is to configure the host with both
the next hop and the source address prefixes that the next hop
supports. In homenets, each interface of the host can be configured
by its next hop, so that all that is needed is to add the information
on source address prefixes. This results in the hosts to select the
right router no matter what.

Finally, the use case in Figure 5 shows that even though all the
routers may have source address dependent routing support, the
packets still may get dropped.

The host in Figure 5 starts external communication with H1 and sends
the first packet with source address P3::iid. Since rtr has a
default route to rtrE it will use this default route in sending the
host's packet out towards rtrE. rtrE will route this packet to ISP1
and the packet will be dropped due to the ingress filtering.

A solution to this issue could be that rtrE having multiple routes to
H1 could use the path through rtrF and could direct the packet to the
other route, i.e. rtrF which would reach H1 in ISP3 without being

subject to ingress routing
[I-D.baker-6man-multiprefix-default-route].

4.2. Provisioning Domains and SADR

Consistent set of network configuration information is called
provisioning domain (PvD). In case of multi-prefix multihoming
(MPMH), more than one provisioning domain is present on a single
link. In case of multi-prefix multiple interface (MPMI)
environments, elements of the same domain may be present on multiple
links. PvD aware nodes support association of configuration
information into PvDs and use these PvDs to serve requests for
network connections, e.g. chosing the right source address for the
packets. PvDs can be constructed from one of more DHCP or Router
Advertisement (RA) options carrying such information as PvD identity
and PvD container [I-D.ietf-mif-mpvd-ndp-support],
[I-D.ietf-mif-mpvd-dhcp-support]. PvDs constructed based on such
information are called explicit PvDs [I-D.ietf-mif-mpvd-arch].

Apart from PvD identity, PvD content may be encapsulated in separate
RA or DHCP options called PvD Container Option. Examples of such
content are defined in [I-D.sarikaya-6man-next-hop-ra] and
[I-D.sarikaya-dhc-6man-dhcpv6-sadr]. They constitute the content or
parts of the content of an explicit PvD.

Explicit PvDs may be received from different interfaces. Single PvD
may be accessible over one interface or simulatenously accessible
over multiple interfaces. Explicit PvDs may be scoped to a
configuration related to a particular interface, however in general
this may not apply. What matters is PvD ID provided that PvD ID is
authenticated by the node even in cases where the node has a single
connected interface. Single PvD information may be received over
multiple interfaces as long as PvD ID is the same. This applies to
the router advertisements (RAs) in which case a multi-homed host
(that is, with multiple interfaces) should trust a message from a
router on one interface to install a route to a different router on
another interface.

5. Guidelines on Standardization Work

We presented many topologies in which a host with multiple interfaces
or a multihomed host is connected to various networks or ISPs which
in turn may apply ingress routing. Our scenario analysis showed that
in order to avoid packets getting dropped due to ingress routing,
source address dependent routing is needed. Also, source address
dependent routing should be supported by routers throughout a site
that has multiple exits.

In this section, we provide informative guidelines on different
existing and future solutions vis a vis the scenarios presented in
Section 3. We start with source address selection rule 5.5 and the
scenarios it solves and continue with solutions that state exactly
what information hosts need in terms of new router advertisement
options for correct source address selection in those scenarios.

5.1. Source Address Selection Rule 5.5

One possible solution is the default source address selection Rule
5.5 in [RFC6724] which recommends to select source addresses
advertized by the next hop. Considering the above scenarios, we can
state that this rule can solve the problem in Figure 1, Figure 2 and
Figure 3.

In using Rule 5.5 the following guidelines should be kept in mind.
Source address selection rules can be distributed by DHCP server
using DHCP Option OPTION_ADDRSEL_TABLE defined in [RFC7078].

In case of DHCP based host configuration, DHCP server can configure
only the interface of the host to which it is directly connected. In
order for Rule 5.5 to apply on other interfaces the option should be
sent on those interfaces as well using [RFC7078].

The default source address selection Rule 5.5 solves that problem
when an application sends a packet with an unspecified source
address. In the presence of two default routes, one route will be
chosen, and Rule 5.5 will make sure the right source address is used.

When the application selects a source address, i.e. the source
address is chosen before next-hop selection, even though the source
address is a way for the application to select the exit point, in
this case that purpose will not be served. In the presence of
multiple default routes, one will be picked, ignoring the source
address which was selected by the application because it is known
that IPv6 implementations are not required to remember which next-
hops advertised which prefixes. Therefore, the next-hop router may
not be the correct one, and the packets may be filtered.

This implies that the hosts should register which next-hop router
announced each prefix.

5.2. Router Advertisement Option

There is a need to configure the host not only with the next hops and
their prefixes but also with the source prefixes they support. Such
a configuration may avoid the host getting ingress/egress policy
error messages such as ICMP source address failure message.

If host configuration is done using router advertisement messages
then there is a need to define new router advertisement options for
source address dependent routing. These options include Route Prefix
with Source Address/Prefix Option. Other options such as Next Hop
Address with Route Prefix option and Next Hop Address with Source
Address and Route Prefix option will be considered in Section 5.3.

As we observed in Section 4.1, the scenario in Figure 4 can be solved
by defining a new router advertisement option, i.e. Route Prefix
with Source Address/Prefix Option as defined in Section 13 in
[I-D.sarikaya-6man-next-hop-ra].

If host configuration is done using DHCP then there is a need to
define new DHCP options for Route Prefix with Source Address/Prefix.
As mentioned above, DHCP server configuration is interface specific.
New DHCP options for source address dependent routing such as route
prefix and source prefix need to be configured for each interface
separately.

The scenario in Figure 4 can be solved by defining a new DHCP option,
i.e. Route Prefix with Source Address/Prefix Option, if DHCP
configuration is a must.

5.3. Router Advertisement Option Set

Motivated by the observation that source address selection rule 5.5
requires many conditions to be correctly applied, an alternative
solution can be presented. This solution calls for configuring hosts
with Next Hop Addresses and the Route Prefix, Source Address/Prefixes
that they support.

The scenarios in Figure 1, Figure 2, Figure 3 and Figure 4 can be
solved by defining new router advertisement options as in
[I-D.sarikaya-6man-next-hop-ra].

The guideline for this solution is that routers in the whole site
should be configured to provide the correct configuration information
to the hosts.

If host configuration is done using DHCP then there is a need to
define new DHCP options for Next Hop Address, Route Prefix with
Source Address/Prefix. Since DHCP server configuration is interface
specific, new DHCP options for source address dependent routing such
as next hop address, route prefix and source prefix need to be
configured for each interface separately.

The scenarios in Figure 1, Figure 2, Figure 3 and Figure 4 can be solved by defining new DHCP options as in [I-D.sarikaya-dhc-6man-dhcpv6-sadr].

5.4. Other Solutions

So far we have singled out the scenario in Figure 5. All the above solutions do not work in this case. This brings us the issue of IP path probing [I-D.naderi-ipv6-probing].

For a given destination, the host selects a source address and a next hop and sends its packet. When the selected path fails, in case of IP probing, the host can probe all available paths until finding one that works.

The guideline in probing is Source Address Dependent Routing (SADR) should be used, i.e. it is a necessary tool. Basically, SADR saves time in eliminating wrong paths, i.e. sending the packets to the wrong exit router. If SADR is not taken into account correctly the host will end up wasting resources trying to explore paths that are certain to fail.

6. Security Considerations

This document describes some use cases and thus brings no new security risks to the Internet.

7. IANA Considerations

None.

8. Acknowledgements

In writing this document, the author benefited from face to face discussions he had with Brian Carpenter and Ole Troan. Pierre Pfister proposed the scenario in Figure 4 as well as some text for Rule 5.5.

9. References

9.1. Normative References

[I-D.ietf-homenet-hncp]
          Stenberg, M., Barth, S., and P. Pfister, "Home Networking
          Control Protocol", draft-ietf-homenet-hncp-03 (work in
          progress), January 2015.

[ISO.10589.1992]
          International Organization for Standardization,
          "Intermediate system to intermediate system intra-domain-
          routing routine information exchange protocol for use in
          conjunction with the protocol for providing the
          connectionless-mode Network Service (ISO 8473), ISO
          Standard 10589", ISO ISO.10589.1992, 1992.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
          Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629,
          June 1999.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering:
          Defeating Denial of Service Attacks which employ IP Source
          Address Spoofing", BCP 38, RFC 2827, May 2000.

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

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed
          Networks", BCP 84, RFC 3704, March 2004.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure
          Neighbor Discovery (SEND)", RFC 3971, March 2005.

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

[RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick,
          "Internet Group Management Protocol (IGMP) / Multicast
          Listener Discovery (MLD)-Based Multicast Forwarding
          ("IGMP/MLD Proxying")", RFC 4605, August 2006.

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

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless
          Address Autoconfiguration", RFC 4862, September 2007.

[RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF
          for IPv6", RFC 5340, July 2008.

[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.

   [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.

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

   [RFC7157] Troan, O., Miles, D., Matsushima, S., Okimoto, T., and D.
              Wing, "IPv6 Multihoming without Network Address
              Translation", RFC 7157, March 2014.

9.2. Informative References

   [I-D.baker-6man-multiprefix-default-route]
              Baker, F., "Multiprefix IPv6 Routing for Ingress Filters",
              draft-baker-6man-multiprefix-default-route-00 (work in
              progress), November 2007.

   [I-D.baker-ipv6-isis-dst-src-routing]
              Baker, F. and D. Lamparter, "IPv6 Source/Destination
              Routing using IS-IS", draft-baker-ipv6-isis-dst-src-
              routing-02 (work in progress), October 2014.

   [I-D.baker-ipv6-ospf-dst-src-routing]
              Baker, F., "IPv6 Source/Destination Routing using OSPFv3",
              draft-baker-ipv6-ospf-dst-src-routing-03 (work in
              progress), August 2013.

   [I-D.baker-rtgwg-src-dst-routing-use-cases]
              Baker, F., "Requirements and Use Cases for Source/
              Destination Routing", draft-baker-rtgwg-src-dst-routing-
              use-cases-01 (work in progress), October 2014.

   [I-D.huitema-multi6-ingress-filtering]
              Huitema, C., "Ingress filtering compatibility for IPv6
              multihomed sites", draft-huitema-multi6-ingress-
              filtering-00 (work in progress), October 2004.

   [I-D.ietf-mif-mpvd-arch]
              Anipko, D., "Multiple Provisioning Domain Architecture",
              draft-ietf-mif-mpvd-arch-08 (work in progress), January
              2015.

   [I-D.ietf-mif-mpvd-dhcp-support]
              Krishnan, S., Korhonen, J., and S. Bhandari, "Support for
              multiple provisioning domains in DHCPv6", draft-ietf-mif-
              mpvd-dhcp-support-00 (work in progress), August 2014.

   [I-D.ietf-mif-mpvd-ndp-support]
              Korhonen, J., Krishnan, S., and S. Gundavelli, "Support
              for multiple provisioning domains in IPv6 Neighbor
              Discovery Protocol", draft-ietf-mif-mpvd-ndp-support-00
              (work in progress), August 2014.

   [I-D.naderi-ipv6-probing]
              Naderi, H. and B. Carpenter, "Experience with IPv6 path
              probing", draft-naderi-ipv6-probing-00 (work in progress),
              October 2014.

   [I-D.sarikaya-6man-next-hop-ra]
              Sarikaya, B., "IPv6 RA Options for Next Hop Routes",
              draft-sarikaya-6man-next-hop-ra-04 (work in progress),
              December 2014.

   [I-D.sarikaya-dhc-6man-dhcpv6-sadr]
              Sarikaya, B., "DHCPv6 Route Options for Source Address
              Dependent Routing", draft-sarikaya-dhc-6man-dhcpv6-sadr-00
              (work in progress), December 2014.

Author's Address

   Behcet Sarikaya
   Huawei USA
   5340 Legacy Dr. Building 175
   Plano, TX 75024

   Email: sarikaya@ieee.org