Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: May 18, 2012

O. Troan, Ed.
Cisco
D. Miles
Alcatel-Lucent
S. Matsushima
Softbank Telecom
T. Okimoto
NTT West
D. Wing
Cisco

November 15, 2011

IPv6 Multihoming without Network Address Translation
draft-ietf-v6ops-ipv6-multihoming-without-ipv6nat-03

Abstract

Network Address and Port Translation (NAPT) works well for conserving global addresses and addressing multihoming requirements, because an IPv4 NAPT router implements three functions: source address selection, next-hop resolution and optionally DNS resolution. For IPv6 hosts one approach could be the use of NPTv6. However, NAT should be avoided, if at all possible, to permit transparent end-to-end connectivity. In this document, we analyze the use cases of multihoming. We also describe functional requirements and possible solutions for multihoming without the use of NAT in IPv6 for hosts and small IPv6 networks that would otherwise be unable to meet minimum IPv6 allocation criteria. We conclude that DHCPv6 based solutions are suitable to solve the multihoming issues, which described in this document. Nevertheless, we mention that the possible needs for NPTv6 in the transition phase to the fully deployment of the proposed solutions.

Status of this Memo

This Internet-Draft will expire on May 18, 2012.

Copyright Notice

Table of Contents

1. Introduction

IPv6 provides enough globally unique addresses to permit every conceivable host on the Internet to be uniquely addressed without the requirement for Network Address Port Translation (NAPT [RFC3022]), offering a renaissance in end-to-end transparent connectivity.

Unfortunately, this may not be possible in every case, due to the possible necessity of NAT even in IPv6, because of multihoming. Though there are some mechanisms to implement multihoming, such as BGP multihoming [RFC4116] in network level, and SCTP based multihoming [RFC4960] in transport layer for application level, there is no mechanism in IPv6 that serves as a replacement for NAT based multihoming in IPv4. In IPv4, for a host or a small network, NAT based multihoming is easily deployable and an already deployed technique. Some of the same reasons for IPv4 NATs may be applicable to IPv6.

Whenever a host or small network (which does not meet minimum IPv6 allocation criteria) is connected to multiple upstream networks, an IPv6 address is assigned by each respective service provider resulting in hosts with multiple global scope IPv6 addresses with different prefixes. As each service provider is allocated a different address space from its Internet Registry, it in-turn assigns a different address space to the end-user network or host. For example, a remote access user's host or router may use a VPN to simultaneously connect to a remote network and retain a default route to the Internet for other purposes.

In IPv4 a common solution to the multihoming problem is to employ NAPT on a border router and use private address space for individual host addressing. The use of NAPT allows hosts to have exactly one IP address visible on the public network and the combination of NAPT with provider-specific outside addresses (one for each uplink) and destination-based routing insulates a host from the impacts of multiple upstream networks. The border router may also implement a DNS cache or DNS policy to resolve address queries from hosts.

It is our goal to avoid the IPv6 equivalent of NAT. So, the goals for IPv6 multihoming defined in [RFC3582] do not match the goals of this document. Also regardless of what the NPTv6 specification is, we are trying to avoid any form of network address translation technique that may not be visible for either of the end hosts. To reach this goal, mechanisms are needed for end-user hosts to have multiple address assignments and resolve issues such as which address to use for sourcing traffic to which destination:

- If multiple routers exist on a single link the host must select the appropriate next-hop for each connected network. Each router is in turn connected to a different service provider network, which provides independent address assignment. Routing protocols that would normally be employed for router-to-router network advertisement seem inappropriate for use by individual hosts.

- Source address selection also becomes difficult whenever a host has more than one address within the same address scope. Current address selection criteria may result in hosts using an arbitrary or random address when sourcing upstream traffic. Unfortunately, for the host, the appropriate source address is a function of the upstream network for which the packet is bound for. If an upstream service provider uses IP anti-spoofing or ingress filtering, it is conceivable that the packets that have an inappropriate source address for the upstream network would never reach their destination.

- In a multihomed environment, different DNS scopes or partitions may exist in each independent upstream network. A DNS query sent to an arbitrary upstream DNS recursive name servier may result in incorrect or poisoned responses.

In short, while IPv6 facilitates hosts having more than one address in the same address scope, the application of this causes significant issues for a host from routing, source address selection and DNS resolution perspectives. A possible consequence of assigning a host multiple identically-scoped addresses is severely impaired IP connectivity.

If a host connects to a network behind an IPv4 NAPT, the host has one private address in the local network. There is no confusion. The NAT becomes the gateway of the host and forwards the packet to an appropriate network when it is multihomed. It also operates a DNS cache server, which receives all DNS inquires, and gives a correct answer to the host.

In this document, we analyze the use cases of multihoming. We also describe functional requirements and possible solutions for multihoming without the use of prefix translation in IPv6 for hosts and small IPv6 networks that would otherwise be unable to meet minimum IPv6 allocation criteria. We conclude that DHCPv6 based solutions are suitable to solve the multihoming issues, which described in this document. Nevertheless, we mention that the possible needs for NPTv6 in the transition phase to the fully deployment of the proposed solutions.

2. Terminology

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

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

Multihomed with multi-prefix (MHMP) A host implementation which supports the mechanisms described in this document. Namely source address selection policy, next-hop selection and DNS selection policy.

3. IPv6 multihomed network scenarios

In this section, we classify three scenarios of the multihoming environment.

3.1. Classification of network scenarios for multihomed host

Scenario 1:

In this scenario, two or more routers are present on a single link shared with the host(s). Each router is in turn connected to a different service provider network, which provides independent address assignment and DNS recursive name servers. A host in this environment would be offered multiple prefixes and DNS recursive name servers advertised from the two different routers.

```
                                +------+       ___________
                                |      |      /           \
                            +---| rtr1 |=====/   network   \
                            |   |      |     \      1      /
               +------+     |   +------+      \___________/
               |      |     |
               | hosts|-----+
               |      |     |
               +------+     |   +------+       ___________
                            |   |      |      /           \
                            +---| rtr2 |=====/   network   \
                                |      |     \      2      /
                                +------+      \___________/
```

Figure 1: single uplink, multiple next-hop, multiple prefix
(Scenario 1)

Figure 1 illustrates the host connecting to rtr1 and rtr2 via a shared link. Networks 1 and 2 are reachable via rtr1 and rtr2 respectively. When the host sends packets to network 1, the next-hop to network 1 is rtr1. Similarly, rtr2 is the next-hop to network 2.

- e.g., multiple broadband service providers (Internet, VoIP, IPTV, etc.)

Scenario 2:

In this scenario, a single gateway router connects the host to two or more upstream service provider networks. This gateway router would receive prefix delegations and a different set of DNS recursive name servers from each independent service provider network. The gateway in turn advertises the provider prefixes to the host, and for DNS, may either act as a lightweight DNS cache server or may advertise the complete set of service provider DNS recursive name servers to the hosts.

```
                                     +------+       ___________
                       +-----+       |      |      /           \
                       |     |=======| rtr1 |=====/   network   \
                       |     |port1  |      |     \      1      /
          +------+     |     |       +------+      \___________/
          |      |     |     |
          | hosts|-----| GW  |
          |      |     | rtr |
          +------+     |     |       +------+       ___________
                       |     |port2  |      |      /           \
                       |     |-------| rtr2 |=====/   network   \
                       +-----+       |      |     \      2      /
                                     +------+      \___________/
```

Figure 2: single uplink, single next-hop, multiple prefix (Scenario 2)

Figure 2 illustrates the host connected to GW rtr. GW rtr connects to networks 1 and 2 via port1 and 2 respectively. As the figure shows a logical topology of the scenario, the port1 could be a pseudo interface for tunneling, which connects to the network 1 through the network 2, and vice versa. When the host sends packets to either network 1 or 2, the next-hop is GW rtr. When the packets are sent to network 1 (network 2), GW rtr forwards the packets to port1 (port2).

- e.g, Internet + VPN/Application Service Provider (ASP)

Scenario 3:

In this scenario, a host has more than one active interface that connects to different routers and service provider networks. Each router provides the host with a different address prefix and set of DNS recursive name servers, resulting in a host with a unique address per link/interface.

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

Figure 3: Multiple uplink, multiple next-hop, multiple prefix (Scenario 3)

Figure 3 illustrates the host connecting to rtr1 and rtr2 via a direct connection or a virtual link. When the host sends packets network 1, the next-hop to network 1 is rtr1. Similarly, rtr2 is the next-hop to network 2.

- e.g., Mobile Wifi + 3G, ISP A + ISP B

3.2. Multihomed network environment

In an IPv6 multihomed network, a host is assigned two or more IPv6 addresses and DNS recursive name servers from independent service provider networks. When this multihomed host attempts to connect with other hosts, it may incorrectly resolve the next-hop router, use an inappropriate source address, or use a DNS response from an incorrect service provider that may result in impaired IP connectivity.

Multihomed networks in IPv4 have been implemented through the use of a gateway router with NAPT function (scenario 2 with NAPT) in many cases. An analysis of the current IPv4 NAPT and DNS functions within the gateway router should provide a baseline set of requirements for IPv6 multihomed environments. A destination prefix/route is often used on the gateway router to separate traffic between the networks.

```
                                     +------+       ___________
                                     |      |      /           \
                                 +---| rtr1 |=====/   network   \
                                 |   |      |     \      1      /
          +------+     +-----+   |   +------+      \___________/
          | IPv4 |     |     |   |
          | hosts|-----| GW  |---+
          |      |     | rtr |   |
          +------+     +-----+   |   +------+       ___________
                      (NAPT&DNS) |   |      |      /           \
          (private               +---| rtr2 |=====/   network   \
              address                |      |     \      2      /
                 space)              +------+      \___________/
```

Figure 4: IPv4 Multihomed environment with Gateway Router performing NAPT

3.3. Problem Statement

A multihomed IPv6 host has one or more assigned IPv6 addresses and DNS recursive name servers from each upstream service provider, resulting in the host having multiple valid IPv6 addresses and DNS recursive name servers. The host must be able to resolve the appropriate next-hop, the correct source address and DNS recursive name server to use based on the destination prefix. To prevent IP spoofing, operators will often implement ingress filtering to discard traffic with an inappropriate source address, making it essential for the host to correctly resolve these three items before sourcing the first packet.

IPv6 has mechanisms for the provision of multiple routers on a single link and multiple address assignments to a single host. However, when these mechanisms are applied to the three scenarios in Section 3.1 a number of connectivity issues are identified:

Scenario 1:

The host has been assigned an address from each router and recognizes both rtr1 and rtr2 as valid default routers (in the default routers list).

- The source address selection policy on the host does not deterministically resolve a source address. Ingress filtering or filter policies will discard traffic with source addresses that the operator did not assign.

- The host will select one of the two routers as the active default router. No traffic is sent to the other router.

Scenario 2:

The host has been assigned two different addresses from the single gateway router. The gateway router is the only default router on the link.

- The source address selection policy on the host does not deterministically resolve a source address. Ingress filtering or filter policies will discard traffic with source addresses that the operator did not assign.

- The gateway router does not have an autonomous mechanism for determining which traffic should be sent to which network. If the gateway router is implementing host functions (i.e., processing Router Advertisement) then two valid default routers may be recognized.

Scenario 3:

A host has two separate interfaces and on each interface a different address is assigned. Each link has its own router.

- The host does not have enough information for determining which traffic should be sent to which upstream routers. The host will select one of the two routers as the active default router, and no traffic is sent to the other router. The default address selection rules select the address assigned to the outgoing interface as the source address. So, if a host has an appropriate routing table, an appropriate source address will be selected.

All scenarios:

- In network deployments utilizing local namespaces, the host may choose to communicate with a "wrong" DNS recursive server unable to serve a local namespace.

4. Requirements

This section describes requirements that any solution multi-address and multi-uplink architectures need to meet.

4.1. End-to-End transparency

One of the major design goals for IPv6 is to restore the end-to-end transparency of the Internet. If NAT mechanism is applied to IP communication between hosts, it is required to apply complex NAT traversal mechanism to establish bi-directional IP communication.

Essentially, extra NAT traversal meachanism does not need to be implemented on application, on an environment with end-to-end transparency. Therefore, The IPv6 multihoming solution should guarantee end-to-end transparency by avoiding NPTv6.

4.2. Policy distribution

The solution SHOULD have a function to provide a policy on sites/ nodes. In particular, a network service provider has to control his or her user nodes such as CPE devices. All nodes are not necessarily controlled evenly with policy providing. It is required to identify a nodes and provide indepenent policy by each node.

The providing mechanisms should have:

- a function to distribute policies to nodes dynamically to update their behavior. When the network environment changes and the nodes' behavior has to be changed, a network administrator can modify the behavior of the nodes.

- a function to control every node centrally. A site administrator or a service provider could determine or could have an effect on the behavior at their users' hosts.

- a function to control node-specific behavior. Even when multiple nodes are on the same subnet, the mechanism should be able to provide a method for the network administrator to make nodes behave differently. For example, each node may have a different set of assigned prefixes. In such a case, the appropriate behavior may be different.

4.3. Scalability

The solution will have to be able to manage a large number of sites/ nodes. In services for residential users, provider edge devices have to manage thousands of sites. In such environments, sending packets periodically to each site may affect edge system performance.

5. Problem statement and analysis

The problems described in Section 3 can be classified into these three types:

- Wrong source address selection

- Wrong next-hop selection

- Wrong DNS server selection

This section reviews the problem statements presented above and the proposed functional requirements to resolve the issues.

5.1. Source address selection

A multihomed IPv6 host will typically have different addresses assigned from each service provider either on the same link (scenarios 1 & 2) or different links (scenario 3). When the host wishes to send a packet to any given destination, the current source address selection rules [RFC3484] may not deterministically resolve the correct source address when the host addressing was via Router Advertisement (RA) or DHCPv6. [I-D.ietf-6man-addr-select-considerations] describes the use of the policy table [RFC3484] to resolve this problem, but there is no mechanism defined to disseminate the policy table information to a host. A proposal is in [I-D.ietf-6man-addr-select-opt] to provide a DHCPv6 mechanism for host policy table management.

Again, by employing DHCPv6, the server could restrict address assignment (of additional prefixes) only to hosts that support policy table management.

Scenario 1: "Host" needs to support the solution for this problem.

Scenario 2: "Host" needs to support the solution for this problem.

Scenario 3: If "Host" support the next-hop selection solution, there is no need to support the address selection functionality on the host.

It is noted that the service providers (i.e., ISP and enterprise/VPN) must also support [I-D.ietf-6man-addr-select-opt].

5.2. Next-hop selection

A multihomed IPv6 host or gateway may have multiple uplinks to different service providers. Here each router would use Router Advertisements [RFC4861] for distributing default route/next-hop information to the host or gateway router.

In this case, the host or gateway router may select any valid default router from the default routers list, resulting in traffic being sent to the wrong router and discarded by the upstream service provider. Using the above scenarios as an example, whenever the host wishes to reach a destination in network 2 and there is no connectivity between networks 1 and 2 (as is the case for a walled-garden or closed

service), the host or gateway router does not know whether to forward traffic to rtr1 or rtr2 to reach a destination in network 2. The host or gateway router may choose rtr1 as the default router, and traffic fails to reach the destination server. The host or gateway router requires route information for each upstream service provider, but the use of a routing protocol between the gateway and the two routers causes both configuration and scaling issues. For IPv4 hosts, the gateway router is often pre-configured with static route information or uses of Classless Static Route Options [RFC3442] for DHCPv4. Extensions to Router Advertisements through Default Router Preference and More-Specific Routes [RFC4191] provides for link-specific preferences but does not address per-host configuration in a multi-access topology because of its reliance on Router Advertisements. A DHCPv6 option, such as that in [I-D.ietf-mif-dhcpv6-route-option], is preferred for host-specific configuration. By employing a DHCPv6 solution, a DHCPv6 server could restrict address assignment (of additional prefixes) only to hosts that support more advanced next-hop and address selection requirements.

Scenario 1: "Host" needs to support the solution for this problem.

Scenario 2: "GW rtr" needs to support the solution for this problem.

Scenario 3: "Host" needs to support the solution for this problem.

It is noted that the service providers (i.e., ISP and enterprise/VPN) must also support [I-D.ietf-mif-dhcpv6-route-option].

5.3. DNS recursive name server selection

A multihomed IPv6 host or gateway router may be provided multiple DNS recursive name servers through DHCPv6 [RFC3646] or RA [RFC6106]. When the host or gateway router sends a DNS query, it would normally choose one of the available DNS recursive name servers for the query.

In the IPv6 gateway router scenario, the Broadband Forum [TR124] required that the query be sent to all DNS recursive name servers, and the gateway waits for the first reply. In IPv6, given our use of specific destination-based policy for both routing and source address selection, it is desirable to extend a policy-based concept to DNS recursive name server selection. Doing so can minimize DNS recursive name server load and avoid issues where DNS recursive name servers in different networks have connectivity issues, or the DNS recursive name server are not publicly accessible. In the worst case, a DNS query for a name from a local namespace may not be resolved correctly if sent towards a DNS server not aware of said local namespace, resulting in a lack of connectivity.

It is not issue of Domain Name System model itself, but an IPv6 multihomed host or gateway router should have the ability to select appropriate DNS recursive name servers for each service based on the domain space for the destination, and each service should provide rules specific to that network. [I-D.ietf-mif-dns-server-selection] proposes a solution for distributing DNS server selection policy using a DHCPv6 option.

Scenario 1: "Host" needs to support the solution for this problem.

Scenario 2: "GW rtr" needs to support the solution for this problem.

Scenario 3: "Host" needs to support the solution for this problem.

It is noted that the service providers (i.e., ISP and enterprise/VPN) must also support [I-D.ietf-mif-dns-server-selection].

6. Implementation approach

As mentioned in Section 5, in the multi-prefix environment, we have three problems in source address selection, next-hop selection, and DNS recursive name server selection. In this section, possible solution mechanisms for each problem are introduced and evaluated against the requirements in Section 4.

6.1. Source address selection

Possible solutions and their evaluation are summarized in [I-D.ietf-6man-addr-select-considerations]. When those solutions are examined against the requirements in Section 4, the proactive approaches, such as the policy table distribution mechanism and the routing hints mechanism, are more appropriate in that they can propagate the network administrator's policy directly. The policy distribution mechanism has an advantage with regard to the host's protocol stack impact and the static nature of the assumed target network environment.

6.2. Next-hop selection

As for the source address selection problem, both a policy-based approach and a non policy-based approach are possible with regard to the next-hop selection problem. Because of the same requirements, the policy propagation-based solution mechanism, whatever the policy, should be more appropriate.

Routing information is a typical example of policy related to next-hop selection. If we assume source address-based routing at hosts or

intermediate routers, the pairs of source prefixes and next-hops can be another example of next-hop selection policy.

The routing information-based approach has a clear advantage in implementation and is already commonly used.

The existing proposed or standardized routing information distribution mechanisms are routing protocols, such as RIPng and OSPFv3, the RA extension option defined in [RFC4191], the DHCPv6 route information option proposed in [I-D.ietf-mif-dhcpv6-route-option], and the [TR069] standardized at BBF.

The RA-based mechanism has difficulty in per-host routing information distribution. The dynamic routing protocols such as RIPng are not usually used between the residential users and ISP networks because of their scalability implications. The DHCPv6 mechanism does not have these difficulties and has the advantage of its relaying functionality. It is commonly used and is thus easy to deploy.

[TR069], mentioned above, is a possible solution mechanism for routing information distribution to customer-premises equipment (CPE). It assumes, however, IP reachability to the Auto Configuration Server (ACS) is established. Therefore, if the CPE requires routing information to reach the ACS, [TR069] cannot be used to distribute this information.

6.3. DNS recursive name server selection

As in the above two problems, a policy-based approach and non policy-based approach are possible. In a non policy-based approach, a host or a home gateway router is assumed to send DNS queries to several DNS recursive name servers at once or to select one of the available servers.

In the non policy-based approach, by making a query to a DNS recursive name server in a different service provider to that which hosts the service, a user could be directed to unexpected IP address or receive an invalid response, and thus cannot connect to the service provider's private and legitimate service. For example, some DNS recursive name servers reply with different answers depending on the source address of the DNS query, which is sometimes called split-horizon. When the host mistakenly makes a query to a different provider's DNS recursive name server to resolve a FQDN of another provider's private service, and the DNS recursive name server adopts the split-horizon configuration, the queried server returns an IP address of the non-private side of the service. Another problem with this approach is that it causes unnecessary DNS traffic to the DNS

recursive name servers that are visible to the users.

The alternative of a policy-based approach is documented in [I-D.ietf-mif-dns-server-selection], where several pairs of DNS recursive name server addresses and DNS domain suffixes are defined as part of a policy and conveyed to hosts in a new DHCP option. In an environment where there is a home gateway router, that router can act as a DNS recursive name server, interpret this option and distribute DNS queries to the appropriate DNS servers according to the policy.

6.4. Other algorithms available in RFCs

The authors of this document are aware of a variety of other algorithms and architectures, such as shim6 [RFC5533] and HIP [RFC5206], that may be useful in this environment. At this writing, there is not enough operational experience on which to base a recommendation. Should such operational experience become available, this document may be updated in the future.

7. Considerations for MHMP deployment

This section describes considerations to mitigate possible problem in a network which implements MHMP described in Section 6.

7.1. Non-MHMP host consideration

In a typical IPv4 multihomed network deployment, IPv4 NAPT is practically used and it can eventually avoid assigning multiple addresses to the hosts and solve the next-hop selection problem. In a similar fashion, NPTv6 can be used as a last resort for IPv6 multihomed network deployments where one needs to assign a single IPv6 address to a non-MHMP host.

```
                                                       __________
                                                      /          \
                                                 +---/  Internet  \
                             gateway router      |   \            /
           +------+     +---------------------+  |    \__________/
           |      |     |   |       |  WAN1  +--+
           | host |-----|LAN| Router |--------|
           |      |     |   |       |NAT|WAN2+--+
           +------+     +---------------------+  |     __________
                                                 |    /          \
                                                 +---/    ASP     \
                                                     \            /
                                                      \__________/
```

Figure 5: Legacy Host

The gateway router also has to support the two features, next-hop selection and DNS server selection, shown in Section 6.

The implementation and issues of NPTv6 are out of the scope of this document. They may be covered by another document under discussion [RFC6296].

7.2. Co-existence consideration

To allow the co-existence of non-MHMP hosts and MHMP hosts (i.e. hosts supporting multi-prefix with the enhancements for the source address selection), GW-rtr may need to treat those hosts separately.

An idea to achieve this is that GW-rtr identifies the hosts, and then assigns a single prefix to non-MHMP hosts and assigns multiple prefixes to MHMP hosts. In this case, GW-rtr can perform IPv6 NAT only for the traffic from non-MHMP hosts if its source address is not appropriate.

Another idea is that GW-rtr assigns multiple prefixes to the both hosts, and it performs IPv6 NAT for the traffic from non-MHMP hosts if its source address is not appropriate.

In scenario 1 and 3, the non-MHMP hosts can be placed behind the NAT box. In this case, the non-MHMP host can access the service through the NAT box.

The implementation of identifying non-MHMP hosts and NAT policy is outside the scope of this document.

7.3. Policy collision consideration

When multiple policy distributors exist, a policy receiver may not follow one or each of the received policy. In particular, when a policy conflicts with another policy, a policy receiver cannot implement each of the policy. To solve or mitigate this issue, it is required that prioritization rule to align these policies along preference on a trusted interface. Another solution is to preclude the functionality of multiple policy acceptance at the receiver side. In this case, a policy distributor should cooperate with other policy distributors, and a single representative provider should distribute a merged policy.

This document does not presume specific recommendations for resolving policy collision. It is expected to the implementation to decide how to resolve the conflicts. If they are not resolved consistently by different implementations, that could affect interoperability and security trust boundaries. Future work will be expected to address the need for consistent policy resolution to avoid interoperability and security trust boundary issues.

8. Security Considerations

This document requires that the solutions for MHMP should have policy providing functions. New security threats can be introduced depending on what kind and what form of the policy. The threats can be categorized in two parts: the policy receiver side and the policy distributor side.

A policy receiver may receive an evil policy from a policy distributor. A policy distributor should expect some hosts in its network do not follow the distributed policy. The security threats related to IPv6 multihoming are described in [RFC4218]. Those threats that are specific to MHMP solutions are enumerated below.

Threats related to the policy distributor side:

> Service provider should expect the existence of hosts that will not obey the received policy. A possible solutions is to ingress-filter those packets that do not match the distributed policy and drop them. About the route selection, packet forwarding or redirection can be another possible solution. About the source address selection, IPv6 NAT can be another possible solution.

Administrators of different networks might need to control policies (and nodes' behaviors) independently of other administrators. It means that the need to have access controls for such cross-administrative policy access. Administrators must control only nodes that are part of their own networks, or some administrators must control only nodes that are part of their own networks, while others are authorized to control nodes across administrative boundaries. To be success to cross-administrative policy-control, per-user authorization might be required with existing AAA and network management standards.

Threats related to the policy receiver side:

For policy receiver side, who should be trusted to accept policies is a fundamental issue. How is the trust established, and how can the network element be assured that it can established that trust before the network is fully configured. If a policy receiver trusts untrusted network, it will cause that distributing unwanted and unauthorized policy that described below.

A policy receiver are exposed to the threats of unauthorized policy, which can lead to session hijack, falsification, DoS, wiretapping and phishing. Unauthorized policy here means a policy distributed from an entity that does not have rights to do so. Usually, only a site administrator and a network service provider have rights to distribute these policies just as well as IP address assignment and DNS server address notification. Regarding source address selection, unauthorized policy can expose an IP address that will not usually be exposed to an external server, which can be a privacy problem. To solve or mitigate this problem of unauthorized policy, one approach is limiting on use of these policy distribution mechanisms, as described in the section 4.4 of [I-D.ietf-mif-dns-server-selection]. For example, a policy should be preferred or accepted when the policy is verified its integrity and delivered across a secure, trusted channel such as 3G connection in cellular services. The proposed solutions are based on DHCP, so the limitation of local site communication, which is often used in WiFi access services, should be another solution or mitigation for this problem. About DNS server selection issue, DNSSEC can be another solution. About source address selection, the ingress filter at the network service provider router can be a solution.

Another threat is the leakage of the policy and privacy issues resulting from that. Especially when each client is distributed its own policy from the network service provider, the policy can give a hint of which service the client subscribes. Encryption of communication channel, separation of communication channel per host can be solutions for this problem.

9. IANA Considerations

This document has no IANA actions.

10. Contributors

The following people contributed to this document: Akiko Hattori, Arifumi Matsumoto, Frank Brockners, Fred Baker, Tomohiro Fujisaki, Jun-ya Kato, Shigeru Akiyama, Seiichi Morikawa, Mark Townsley, Wojciech Dec, Yasuo Kashimura, Yuji Yamazaki. This document has greatly benefited from inputs by Randy Bush, Brian Carpenter, and Teemu Savolainen.

11. References

11.1. Normative References

[I-D.ietf-6man-addr-select-considerations]
Chown, T. and A. Matsumoto, "Considerations for IPv6 Address Selection Policy Changes", draft-ietf-6man-addr-select-considerations-04 (work in progress), October 2011.

[I-D.ietf-6man-addr-select-opt]
Matsumoto, A., Fujisaki, T., Kato, J., and T. Chown, "Distributing Address Selection Policy using DHCPv6", draft-ietf-6man-addr-select-opt-01 (work in progress), June 2011.

[I-D.ietf-mif-dhcpv6-route-option]
Dec, W., Mrugalski, T., Sun, T., and B. Sarikaya, "DHCPv6 Route Options", draft-ietf-mif-dhcpv6-route-option-03 (work in progress), September 2011.

[I-D.ietf-mif-dns-server-selection]
Savolainen, T., Kato, J., and T. Lemon, "Improved DNS Server Selection for Multi-Interfaced Nodes",

draft-ietf-mif-dns-server-selection-07 (work in progress), October 2011.

[RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[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.

11.2. 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.

[RFC4960] Stewart, R., "Stream Control Transmission Protocol", RFC 4960, September 2007.

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

[TR069] The BroadBand Forum, "TR-069, CPE WAN Management Protocol v1.1, Version: Issue 1 Amendment 2", December 2007.

[TR124] The BroadBand Forum, "TR-124i2, Functional Requirements for Broadband Residential Gateway Devices (work in progress)", May 2010.

Authors' Addresses

Ole Troan (editor)
Cisco
Bergen
Norway

Email: ot@cisco.com

David Miles
Alcatel-Lucent
Melbourne
Australia

Email: david.miles@alcatel-lucent.com

Satoru Matsushima
Softbank Telecom
Tokyo
Japan

Email: satoru.matsushima@g.softbank.co.jp

Tadahisa Okimoto
NTT West
Osaka
Japan

Email: t.okimoto@west.ntt.co.jp

Dan Wing
Cisco
170 West Tasman Drive
San Jose
USA

Email: dwing@cisco.com