Considerations of address selection policy conflicts
draft-arifumi-6man-addr-select-conflict-01.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79. This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on April 27, 2010.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.
Abstract

This document tries to speculate how policy conflicts happen, and how to address the conflicts. After making it clear what kind of address selection policy should be necessary, we proposed how to merge the possibly conflicting policies for each of the destination address selection policy and source address selection policy.

Table of Contents

1. Introduction ............................................... 3
2. Address Selection Control .................................. 3
3. Source Address Selection Conflicts and Solution .......... 4
4. Destination Address Selection Conflicts and Solution ..... 5
5. Conceptual Message Processing Model ................. 7
   5.1. Source Address Selection Policy .................... 7
   5.2. Destination Address Selection Policy ............. 9
6. Discussion .................................................. 10
7. IANA Considerations ....................................... 11
8. Security Considerations ................................... 11
9. Acknowledgements ......................................... 11
10. References ................................................ 11
    10.1. Normative References ............................. 11
    10.2. Informative References ............................ 11
Appendix A. Appendix. Revision History .................... 11
Authors’ Addresses ......................................... 12
1. Introduction

RFC 5220 [RFC5220] describes several cases that have problems caused by using multiple prefixes at hosts and sites. The address selection design team is working on this issue and summarizes their work in the considerations document [I-D.ietf-6man-addr-select-considerations]. Their solution mechanism is going to be an update mechanism of the address selection policy table at a host from the network. A new DHCPv6 option [I-D.fujisaki-dhc-addr-select-opt] is proposed for this purpose.

As mentioned in RFC 5220 [RFC5220], a host and a site can belong to multiple upstream networks. For example, a host with multiple interfaces, such as wireless and wired interfaces, can easily belong to multiple networks. A site may have connectivity to ISP and a corporate network through a VPN link.

In these cases, if two or more of the upstream networks want to control address selection behavior of his network’s customer host, those address selection policies have to be merged at the host, and they may collide there.

This document tries to speculate how policy conflicts happen, and how to address the conflicts. Moreover, this document also tries to examine a mechanism for solving conflicts in the section of conceptual processing model. This document focuses on identifying what kind of conflict related problems we have, and in what kind of manner we can solve them.

Some of the problems described in RFC 5220 are specific to and resulted from the address selection mechanism defined in RFC 3484 [RFC3484]. However, above mentioned policy collision is an intrinsic problem of address selection policy merging, and not specific to the RFC 3484 mechanism.

2. Address Selection Control

As in RFC 5220, there are various motivations for network administrator to control address selection behavior of his customers’ hosts. However, we can summarize them into two following kinds of controls.

- Source address selection behavior control:
"When accessing to PREFIX-1, use ADDRESS-1 as the source address." A lot of ISPs have this policy and they usually implement it by adopting ingress filtering to incoming packets from their customers. Another case where this policy is used is a network that makes use of multiple address blocks in the network and assigns multiple addresses/prefixes to its customers and use them for different purpose, such as the Internet access use and telephone call use.

- Destination address selection behavior control:

"When accessing to PREFIX-1 or PREFIX-2, prefer PREFIX-1 rather than PREFIX-2." This control is rather intended for optimization of the customers' traffic. This kind of control is not intended for on-off switch, but rather a preference degree. For example, this is useful when a destination site has both PREFIX-1 and PREFIX-2, and the network administrator knows connectivity to PREFIX-1 is better than PREFIX-2. The typical case of this is IPv4 and IPv6 prioritization as mentioned in RFC 5220.

On-off switch manner of control is not in scope of address selection behavior, but it should be implemented some other mechanism, such as routing table manipulation and DNS resolution. As this is intrinsically intended for optimization, it should not be used for any other purpose like security.

Here, PREFIX-* is used to denote both IPv4 and IPv6 prefixes. In the following part, policy conflict and solution for these two patterns above are examined separately.

3. Source Address Selection Conflicts and Solution

As mentioned above, source address selection policy have following meaning: "When accessing to PREFIX-1, use ADDRESS-1 as the source address." The upstream network that has this kind of policy usually assigns an address block that includes ADDRESS-1, and also provides reachability to the network that is specified by PREFIX-1.

Source address selection policy conflict can happen when different network have a policy for the same prefix. For example, in the following figure, Network-1 have a policy: "To PREFIX-1, use ADDRESS-1", and Network-2: "To PREFIX-1 and PREFIX-2, use ADDRESS-2".
In this case, the solution is straightforward. The destination address is determined before source address selection policy is used. Thus, the outgoing route, such as the next-hop node and the network interface, is determined by looking up the routing table at a host. That is, the outgoing network that carries the packet to the destination is determined without the source address selection policy.

So, the bottom line is that the source address selection policy that matches routing table’s behavior should be chosen. There is no point adopting the source address selection policy of a network where a packet does not go through.

In other words, if the routing table is fixed before the source address selection policy is fixed, then the source address selection policy should be implemented while avoiding contradiction with the routing table. If not, the routing table should be coordinated to match the source address selection policy.

In a case where a site is connected to the multiple ISPs, like the figure above, and receives policies from the ISPs and re-distribute policies to the downstream hosts, the hosts cannot know which ISP are chosen for transit to PREFIX-1. So, in this case, the entity who knows which way is chosen have to address the policy conflict.

4. Destination Address Selection Conflicts and Solution

As mentioned in section 2, destination address selection policy have following meaning: "When accessing to a destination site that has PREFIX-1 and PREFIX-2, prefer PREFIX-1 rather than PREFIX-2." The upstream network that has this kind of policy should provides reachability to both networks that are specified by PREFIX-1 and PREFIX-2.
Destination address selection policy conflict can happen when a network has a policy that has inverse effect of another network’s policy. That is, in the figure below, Network-1 prefers PREFIX-1 rather than PREFIX-2, and Network-2 prefers PREFIX-2 rather than PREFIX-1.

```
bad   bad
PREFIX-1 ---- ---- PREFIX-2
 |      X      |
good |     / \     | good
+-------+-------+ +-------+-------+
| Network-1 | | Network-2 |
+-------+-------+ +-------+-------+
 \     /   \     /
 ADDRESS-1 \   / ADDRESS-2
+---------+     
 | Host/Site |
+-----------+
```

In routing mechanism, a router advertises a route A to a certain destination, another advertises a route B to the same destination, and the receiver decides which route to take by looking at the cost of the routes and other information.

In destination address selection policy, a network advertises prefix A and the precedence degree. The destination address selection policy conflict happens when multiple entities provide policies for the same or the overlapping destination prefix with different costs. This is the same situation as the routing mechanism in that there can be multiple "routes" for the same destination.

Here, we can choose the better, that is, higher precedence "route" for the destination prefix, but there is no point if the route is not actually used by the routing mechanism. Even if we choose a policy for prefix A provided from Network-1, a packet destined for the prefix A does not always go through Network-1. This is what the routing mechanism of the host or the site router decides.

So, we propose to adopt the policy that is provided from the network the routing mechanism selected and thus a packet goes through, because the routing mechanism is already there and performs routing decisions by making use of the routing protocols metrics and also implementation dependent information.

For example, Network-1 router advertises the following policy to the customers:
to PREFIX-1, precedence 20
to PREFIX-2, precedence 10

Network-2 advertises:
  to PREFIX-1, precedence 30
  to PREFIX-2, precedence 40

And when the routing table is:
  PREFIX-1 via Network-1
  PREFIX-2 via Network-2

Then, the receiving host should have the following merged destination address selection policy:
  to PREFIX-1, precedence 20 via Network-1
  to PREFIX-2, precedence 40 via Network-2

5. Conceptual Message Processing Model

The merging process described here does not demand any modification to the address selection mechanism defined in RFC 3484. However, the policy receiver has to keep multiple sets of the received policy as they are somewhere other than the policy table defined in RFC 3484. Also, the default policy table defined in RFC 3484 has to be kept.

The merging process retrieves all the above stored sets of policy, processes them, and put the merged policy into the policy table. This process should be performed every time the received policy changes.

The default priority should be defined which to prioritize the default policy table or the received policy, or possibly the manually configured policy on the host. The priority should also be configurable.

5.1. Source Address Selection Policy
When these two ISPs, Network-1 and Network-2, provide the source address selection policy below,

Network-1 "if dst ::/0, then src 2001:db8:1::/64"
Network-2 "if dst ::/0 or fd00:2::/48, then src 2001:db8:2::/64"

and when the Host’s routing table looks like below,

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Nexthop</th>
</tr>
</thead>
<tbody>
<tr>
<td>::/0</td>
<td>Network-1</td>
</tr>
<tr>
<td>fd00:2::/48</td>
<td>Network-2</td>
</tr>
</tbody>
</table>

as mentioned in the previous section, the policy that came from the selected entity in the routing table should be selected in the policy table also. In this case, the routing table selected Network-1 for the nexthop for the prefix ::/0, so the Network-1’s policy should be selected in the policy table.

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Precedence</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>::/0</td>
<td>?</td>
<td>1</td>
</tr>
<tr>
<td>2001:db8:1::/64</td>
<td>?</td>
<td>1</td>
</tr>
<tr>
<td>fd00:2::/48</td>
<td>?</td>
<td>5</td>
</tr>
<tr>
<td>2001:db8:2::/64</td>
<td>?</td>
<td>5</td>
</tr>
</tbody>
</table>

If we consider about the merging with the default policy table, which is pasted below from the RFC 3484,

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Precedence</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>::/128</td>
<td>50</td>
<td>0</td>
</tr>
<tr>
<td>::/0</td>
<td>40</td>
<td>1</td>
</tr>
<tr>
<td>2002::/16</td>
<td>30</td>
<td>2</td>
</tr>
<tr>
<td>::/96</td>
<td>20</td>
<td>3</td>
</tr>
</tbody>
</table>
We can have the following merged table.

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Precedence</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>::1/128</td>
<td>50</td>
<td>0</td>
</tr>
<tr>
<td>::/0</td>
<td>40</td>
<td>1</td>
</tr>
<tr>
<td>* 2001:db8:1::/64</td>
<td>40</td>
<td>1</td>
</tr>
<tr>
<td>* fd00:2::/48</td>
<td>40</td>
<td>5</td>
</tr>
<tr>
<td>* 2001:db8:2::/64</td>
<td>40</td>
<td>5</td>
</tr>
<tr>
<td>2002::/16</td>
<td>30</td>
<td>2</td>
</tr>
<tr>
<td>::/96</td>
<td>20</td>
<td>3</td>
</tr>
<tr>
<td>::ffff:0:0/96</td>
<td>10</td>
<td>4</td>
</tr>
</tbody>
</table>

Here, the merging process was used that chooses the most harmless Precedence value. That means, the Precedence value that does not spoil or change the other policy table entries’ effects.

The process is to find a prefix that includes or overlaps with the inserting entry in the default policy table, and to use the Precedence value of the prefix. In this example, the prefix 2001:db8:1::/64 longestly matches with the existing prefix ::/0, so the Precedence value 40 was used for the merged entries.

### 5.2. Destination Address Selection Policy

When these two ISPs, Network-1 and Network-2, provide the source address selection policy below,

Network-1 "::/0 Precedence 20, ::ffff:0:0/96 Precedence 10"
Network-2 "::/0 Precedence 30, ::ffff:0:0/96 Precedence 40"
and the routing table of the Host is like below.

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Nexthop</th>
</tr>
</thead>
<tbody>
<tr>
<td>::/0</td>
<td>Network-1</td>
</tr>
<tr>
<td>::ffff:0:0/96</td>
<td>Network-2</td>
</tr>
</tbody>
</table>

Here, the merging process selects the Precedence value of the policy that is selected in the routing table. That is, the routing table above selects Network-1 for the prefix ::/0, so the Precedence value for the prefix ::/0 should be the value of the Network-1’s policy. The result of this merging process is below.

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Precedence</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>::/0</td>
<td>20</td>
<td>?</td>
</tr>
<tr>
<td>::ffff:0:0/96</td>
<td>40</td>
<td>?</td>
</tr>
</tbody>
</table>

If we consider about the merging with the default policy table, the merged policy table is going to be

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Precedence</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>::/128</td>
<td>50</td>
<td>0</td>
</tr>
<tr>
<td>* ::/0</td>
<td>20</td>
<td>1</td>
</tr>
<tr>
<td>2002::/16</td>
<td>30</td>
<td>2</td>
</tr>
<tr>
<td>::/96</td>
<td>20</td>
<td>3</td>
</tr>
<tr>
<td>* ::ffff:0:0/96</td>
<td>40</td>
<td>4</td>
</tr>
</tbody>
</table>

by adopting almost the same process as the source address policy merging. That is, the merging process was used that chooses the most harmless Label value. The Label value should be used that does not spoil or change the other policy table entries’ effects. It seems to be harmless to use the same Label value as the existing entry that longestly matches the inserting entry’s prefix.

6. Discussion

In this document, we examined and classified address selection policies. For each class, we proposed how to solve the merging conflicting policies.

As documented here, the merging process has close relationship with the routing table. It should be noted that the address selection policy distribution has to be considered and used along with the routing mechanism.
7. IANA Considerations

This document has no actions for IANA.

8. Security Considerations

TBD

9. Acknowledgements

Dave Thaler and Aleksi Suhonen has given invaluable advice and feedback on this document.

10. References

10.1. Normative References


10.2. Informative References


Appendix A. Appendix. Revision History

01:
The section 4 was made clearer.
The section 5 "Conceptual processing model" was added.
The section "Conclusions" was renamed to "Discussion".

Authors' Addresses

Arifumi Matsumoto
NTT PF Lab
Midori-Cho 3-9-11
Musashino-shi, Tokyo 180-8585
Japan

Phone: +81 422 59 3334
Email: arifumi@nttv6.net

Tomohiro Fujisaki
NTT PF Lab
Midori-Cho 3-9-11
Musashino-shi, Tokyo 180-8585
Japan

Phone: +81 422 59 7351
Email: fujisaki@syce.net

Ruri Hiromi
Intec Netcore, Inc.
Shinsuna 1-3-3
Koto-ku, Tokyo 136-0075
Japan

Phone: +81 3 5665 5069
Email: hiromi@inetcore.com