IPv6 Operations Working Group
Internet-Draft
Intended status: Informational
Expires: May 9, 2008

A. Matsumoto
T. Fujisaki
NTT
R. Hiromi
K. Kanayama
Intec Netcore

November 6, 2007

# Requirements for address selection mechanisms
# draft-ietf-v6ops-addr-select-req-04.txt

## Status of this Memo

## Copyright Notice

## Abstract

In a multi-prefix environment, nodes could have multiple addresses on one network interface. RFC 3484 defines a source and destination address-selection algorithm, which is commonly deployed in current popular OSs. However, nodes could encounter some difficulties in network communication when they use default address selection rules defined in RFC 3484. Some mechanisms for solving address-selection problems are proposed including the RFC 3484 policy table distribution and ICMP error-based mechanisms. This document describes requirements for these address-selection mechanisms.

Table of Contents

## 1. Introduction

One physical network can have multiple logical networks. In that case, an end-host has multiple IP addresses. (e.g., in the IPv4-IPv6 dual-stack environment, in a site that uses both ULA [RFC4193] and global scope addresses or in a site connected to multiple upstream IPv6 networks) For such a host, RFC 3484 [RFC3484] defines default address-selection rules for the source and destination addresses.

Today, the RFC 3484 mechanism is widely implemented in major OSs. However, we and others have found that in many sites the default address-selection rules are not appropriate for the network structure. PS [I-D.ietf-v6ops-addr-select-ps] lists problematic cases that resulted from incorrect address selection.

Though RFC 3484 made the address-selection behavior of a host configurable, typical users cannot make use of that because of the complexity of the mechanism and lack of knowledge about their network topologies. Therefore, an address-selection autoconfiguration mechanism is necessary, especially for unmanaged hosts of typical users.

This document contains requirements for address-selection mechanisms that enable hosts to perform appropriate address selection automatically.

## 2. Requirements of Address Selection

Address-selection mechanisms have to fulfill the following seven requirements.

### 2.1. Effectiveness

The mechanism can modify RFC 3484 default address-selection behavior at nodes. As documented in PS [I-D.ietf-v6ops-addr-select-ps], the default rules defined in RFC 3484 do not work properly in some environments. Therefore, the mechanism has to be able to modify address-selection behavior of a host.

### 2.2. Timing

Nodes can obtain address selection information when necessary. If nodes need to have address-selection information before performing address selection, then the mechanism has to provide a function for nodes to obtain necessary information beforehand. The mechanism should not degrade usability. The mechanism should not enforce long address-selection processing time upon users.

## 2.3. Dynamic Behavior Update

Address-selection behavior of nodes can be dynamically updated. When the network structure changes and address-selection behavior has to be changed accordingly, a network administrator can modify the address-selection behavior of nodes.

## 2.4. Node-Specific Behavior

The mechanism can support node-specific address-selection 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 address-selection behavior may be different.

## 2.5. Application-Specific Behavior

The mechanism can support application-specific address-selection behavior or combined use with an application-specific address-selection mechanism such as address-selection APIs.

## 2.6. Multiple Interface

The mechanism can support those nodes equipped with multiple interfaces. The mechanism has to assume that nodes have multiple interfaces and makes address selection of those nodes work appropriately.

## 2.7. Central Control

The address selection behavior of nodes can be centrally controlled. A site administrator or a service provider could determine or could have effect on address-selection behavior at their users' hosts.

## 2.8. Next-hop Selection

The mechanism can control next-hop-selection behavior at hosts or cooperate with other routing mechanisms, such as routing protocols and RFC 4191 [RFC4191]. If the address-selection mechanism is used with a routing mechanism, the two mechanisms have to be able to work synchronously.

## 2.9. Compatibility with RFC 3493

The mechanism can allow an application that uses the basic socket interface defined in RFC 3493 [RFC3493] to work correctly. That is, with the basic socket interface the application can select an

appropriate source and destination addresses and can communicate with the destination host. This requirement does not necessarily mean that OS protocol stack and socket libraries should not be changed.

## 3. Security Considerations

### 3.1. List of threats introduced by new address-selection mechanism

There are some security incidents when combining these requirements described in Section 2 into a protocol. In particular, here are six possible threats.

1. Hijacking or tapping from malicious nodes connecting from beyond unapproved network boundaries.
2. Malicious changing of policy data by nonapproved nodes.
3. Denial of Service Attack due to higher traffic volume, and blocked communication, for example, at both node and network caused by sending unsafe and tampered data from unbidden controller.
4. Attempt to stop service on node/computer resources caused by unnecessary communication between the controller and nodes.
5. Intrusion into security boundary caused by malicious use of multiprefix environment.
6. Leakage of network policy information from central controller.

### 3.2. List of recommendations in which security mechanism should be applied

All the methods listed below should be well-considered for protecting against security threats. There is no necessity to comply with all items at same time, if one or more spec(s) could apply to other security requirements. Secure network operation will also be considered, and describing network operation for network security will be better. Referring to and using existing technologies is also preferable.

1. Consideration of the necessity to use digitally signed or cryptographic messages.
2. Consideration of the necessity to maintain confidentiality of source of policy data.
3. Consideration of the necessity of authentication and validation of both entity and message integrity.
4. Consideration of the necessity of having a mechanism for the avoidance of data conflicts if the policy data comes from multiple controllers.

5. Consideration of the necessity of an appropriate filtering method at domain boundaries.
6. Consideration of the necessity of data independency at every node or every interface for avoidance of mixing multiple policy data.
7. Consideration of the necessity of having a mechanism for controlling policy and all related network information on the server if the server stores policy and all related neetowrk information on the outside of its network domain.
8. Consideration of the necessity to log and collect related system data.

## 4. IANA Considerations

This document has no actions for IANA.

## 5. References

### 5.1. Normative References

[I-D.ietf-v6ops-addr-select-ps]
Matsumoto, A., "Problem Statement of Default Address Selection in Multi-prefix Environment: Operational Issues of RFC3484 Default Rules", draft-ietf-v6ops-addr-select-ps-02 (work in progress), October 2007.

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

[RFC3493] Gilligan, R., Thomson, S., Bound, J., McCann, J., and W. Stevens, "Basic Socket Interface Extensions for IPv6", RFC 3493, February 2003.

### 5.2. Informative References

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

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

## Appendix A. Appendix. Revision History

04:

A new requirement item "Compatibility with RFC 3493" was added, which reflected a comment from Remi Denis-Courmont at the v6ops mailing list.

03:

Security Consideration section was rewritten according to comments from SECDIR.

02:

The description and evaluation of solution approaches were separated into a new document called draft-arifumi-v6ops-addr-select-sol-00.

01:

Other than policy table distribution approach, the solution section included several solutions discussed at 67th IETF meeting.

## 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@nttv6.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

Ken-ichi Kanayama
Intec Netcore, Inc.
Shinsuna 1-3-3
Koto-ku, Tokyo 136-0075
Japan

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

## Full Copyright Statement

## Intellectual Property

## Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).