IPv6 Operations Working Group
Internet-Draft
Intended status: Informational
Expires: September 7, 2008

A. Matsumoto
T. Fujisaki
NTT
R. Hiromi
K. Kanayama
Intec Netcore
March 6, 2008

Requirements for address selection mechanisms
draft-ietf-v6ops-addr-select-req-05.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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 September 7, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

There are some problematic cases when using default address selection mechanism which RFC 3484 defines. This document describes additional requirements co-working with RFC3484 to solve the problems.

Table of Contents

1. Introduction

Today, the RFC 3484 [RFC3484] mechanism is widely implemented in major OSs. However, in many sites, the default address-selection rules are not appropriate, and cause a communication failure. 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.

2.10. Security

The mechanism works without any security problems. Possible security threats are described in Security Considerations section.

3. Security Considerations

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

There will be some security incidents when combining these requirements described in Section 2 into a protocol. In particular, there are 3 types of threats, "Leakage","Hijacking", and "Denial of Services".

1. Tapping from malicious nodes to collect the network policy information and leak them to unauthorized parties.
2. Hijacking of nodes made possible by malicious injection of illegitimate policy information: RFC3484 defines both of source and destination selection algorithm. An attacker able to inject malicious policy information could redirect packets sent by a victim node to an intentionally chosen server that would scan the

victim node activities to find out exploit code. Once exploit code is found the attacker can take control of the victim node.

3. Denial of Service Attack on the ability of nodes to communicate in the absence of the address selection policy: An attacker could launch a flooding attack on the controller to prevent it to deliver the address selection policy information to nodes, thus preventing these nodes to appropriately communicate in the absence of that information.

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

The source address selection protocol should be afforded security services listed below. It is preferable that these security services are afforded via use of existing protocols(e.g. IPsec).

1. Integrity of the network policy information itself and the messages exchanging in the protocol. This is countermeasure against "Leakage", "Hijacking", and "Denial of Services".
2. Authentication and authorization of parties involved in the protocol. This is countermeasure against "Leakage" and "Hijacking".

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., Fujisaki, T., Hiromi, R., and K. Kanayama, "Problem Statement of Default Address Selection in Multi-prefix Environment: Operational Issues of RFC3484 Default Rules", draft-ietf-v6ops-addr-select-ps-04 (work in progress), February 2008.

[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.

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

5.2. Informative References

Appendix A. Appendix. Revision History

05:
A new requirement item "Security" was added. Security Considerations section was rewritten according to comments from SECDIR.
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 Considerations 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

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

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