Requirements for address selection mechanisms
draft-ietf-v6ops-addr-select-req-04.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 May 9, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

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 .............................................. 3
2. Requirements of Address Selection .......................... 3
    2.1. Effectiveness ........................................ 3
    2.2. Timing ............................................... 3
    2.3. Dynamic Behavior Update ............................... 4
    2.4. Node-Specific Behavior ............................... 4
    2.5. Application-Specific Behavior ......................... 4
    2.6. Multiple Interface .................................. 4
    2.7. Central Control ..................................... 4
    2.8. Next-hop Selection ................................. 4
    2.9. Compatibility with RFC 3493 ........................ 4
3. Security Considerations ................................... 5
    3.1. List of threats introduced by new address-selection mechanism .................. 5
    3.2. List of recommendations in which security mechanism should be applied .......... 5
4. IANA Considerations ...................................... 6
5. References ............................................... 6
    5.1. Normative References ................................. 6
    5.2. Informative References .............................. 6
Appendix A. Appendix. Revision History ........................ 6
Authors’ Addresses .......................................... 7
Intellectual Property and Copyright Statements ................ 9
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 network 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]


5.2. Informative References


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

Copyright (C) The IETF Trust (2007).

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).