

Network Working Group
Internet-Draft
Expires: October 3, 2005

S. Roy
Sun Microsystems, Inc.
A. Durand
Comcast Corporation
J. Paugh
April 2005

IPv6 Neighbor Discovery On-Link Assumption Considered Harmful
draft-ietf-v6ops-onlinkassumption-03.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 October 3, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This document describes the historical and background information behind the removal of the "on-link assumption" from the conceptual host sending algorithm defined in Neighbor Discovery for IP Version 6 (IPv6). According to the algorithm as originally described, when a host's default router list is empty, the host assumes that all destinations are on-link. This is particularly problematic with

IPv6-capable nodes that do not have off-link IPv6 connectivity (e.g., no default router). This document describes how making this assumption causes problems, and describes how these problems outweigh the benefits of this part of the conceptual sending algorithm.

Table of Contents

1.	Introduction	3
2.	Background on the On-link Assumption	3
3.	Problems	3
3.1	First Rule of Destination Address Selection	3
3.2	Delays Associated with Address Resolution	4
3.3	Multi-interface Ambiguity	5
3.4	Security Related Issues	5
4.	Changes to RFC2461	6
5.	Security Considerations	6
6.	References	6
6.1	Normative References	6
6.2	Informative References	7
	Authors' Addresses	7
A.	Acknowledgments	7
B.	Changes from draft-ietf-v6ops-onlinkassumption-02	7
C.	Changes from draft-ietf-v6ops-onlinkassumption-01	8
D.	Changes from draft-ietf-v6ops-onlinkassumption-00	8
	Intellectual Property and Copyright Statements	9

1. Introduction

Neighbor Discovery for IPv6 [[I-D.ietf-ipv6-2461bis](#)] defines a conceptual sending algorithm for hosts. The version of the algorithm described in [[RFC2461](#)] states that if a host's default router list is empty, then the host assumes that all destinations are on-link. This memo documents the removal of this assumption in the updated Neighbor Discovery specification [[I-D.ietf-ipv6-2461bis](#)], and describes the reasons why this assumption was removed.

This assumption is problematic with IPv6-capable nodes that do not have off-link IPv6 connectivity. This is typical when systems that have IPv6 enabled on their network interfaces (either on by default or administratively configured that way) are attached to networks that have no IPv6 services such as off-link routing. Such systems will resolve DNS names to AAAA and A records, and may attempt to connect to unreachable IPv6 off-link nodes.

The on-link assumption creates problems for destination address selection as defined in [[RFC3484](#)], and adds connection delays associated with unnecessary address resolution and neighbor unreachability detection. The behavior associated with the assumption is undefined on multi-interface nodes, and has some subtle security implications. All of these issues are discussed in this document.

2. Background on the On-link Assumption

This part of Neighbor Discovery's [[RFC2461](#)] conceptual sending algorithm was created to facilitate communication on a single link between systems manually configured with different global prefixes. For example, consider the case where two systems on separate links are manually configured with global addresses, and are then plugged in back-to-back. They can still communicate with each other via their global addresses because they'll correctly assume that each is on-link.

Without the on-link assumption, the above scenario wouldn't work, and the systems would need to be configured to share a common prefix such as the link-local prefix.

3. Problems

The on-link assumption causes the following problems.

3.1 First Rule of Destination Address Selection

Default Address Selection for IPv6 [[RFC3484](#)] defines a destination

address selection algorithm that takes an unordered list of destination addresses as input, and produces a sorted list of destination addresses as output. The algorithm consists of destination address sorting rules, the first of which is "Avoid unusable destinations". The idea behind this rule is to place unreachable destinations at the end of the sorted list so that applications will be least likely to try to communicate with those addresses first.

The on-link assumption could potentially cause false positives when attempting unreachability determination for this rule. On a network where there is no IPv6 router (all off-link IPv6 destinations are unreachable), the on-link assumption states that destinations are assumed to be on-link. An implementation could interpret that as, if the default router list is empty, then all destinations are reachable on-link. This may cause the rule to prefer an unreachable IPv6 destination over a reachable IPv4 destination.

3.2 Delays Associated with Address Resolution

Users expect that applications quickly connect to a given destination regardless of the number of IP addresses assigned to that destination. If a destination name resolves to multiple addresses and the application attempts to communicate to each address until one succeeds, this process shouldn't take an unreasonable amount of time. It is therefore important that the system quickly determine if IPv6 destinations are unreachable so that the application can try other destinations when those IPv6 destinations are unreachable.

For an IPv6 enabled host deployed on a network that has no IPv6 routers, the result of the on-link assumption is that link-layer address resolution must be performed on all IPv6 addresses to which the host sends packets. The Application will not receive acknowledgment of the unreachability of destinations that are not on-link until at least address resolution has failed, which is no less than three seconds ($\text{MAX_MULTICAST_SOLICIT} * \text{RETRANS_TIMER}$). This is greatly amplified by transport protocol delays. For example, [\[RFC1122\]](#) requires that TCP retransmit for at least 3 minutes before aborting the connection attempt.

When the application has a large list of off-link unreachable IPv6 addresses followed by at least one reachable IPv4 address, the delay associated with Neighbor Unreachability Detection (NUD) of each IPv6 addresses before successful communication with the IPv4 address is unacceptable.

3.3 Multi-interface Ambiguity

There is no defined way to implement this aspect of the sending algorithm on a node that is attached to multiple links. From an implementor's point of view, there are three ways to handle sending an IPv6 packet to a destination in the face of the on-link assumption on a multi-interface node:

1. Attempt to resolve the destination on a single link.
2. Attempt to resolve the destination on every link.
3. Drop the packet.

If the destination is indeed on-link, the first option might not succeed since the wrong link could be picked. The second option might succeed in reaching a destination (assuming that one is reachable) but is more complex to implement, and isn't guaranteed to pick the correct destination. For example, there is still ambiguity about which link to use if more than one node answers the solicitations on multiple links. Dropping the packet is equivalent to not making the on-link assumption at all. In other words, if there is no route to the destination, don't attempt to send the packet.

3.4 Security Related Issues

The on-link assumption discussed here introduces a security vulnerability to the Neighbor Discovery protocol described in [section 4.2.2](#) of IPv6 Neighbor Discovery Trust Models and Threats [[RFC3756](#)] titled "Default router is 'killed'". There is a threat that a host's router can be maliciously killed in order to cause the host to start sending all packets on-link. The attacker can then spoof off-link nodes by sending packets on the same link as the host. The vulnerability is discussed in detail in [[RFC3756](#)].

Another security related side-effect of the on-link assumption has to do with virtual private networks (VPN's). It has been observed that some commercially available VPN software solutions that don't support IPv6 send IPv6 packets to the local media in the clear (their security policy doesn't simply drop IPv6 packets). Consider a scenario where a system has a single Ethernet interface with VPN software that encrypts and encapsulates certain packets. The system attempts to send a packet to an IPv6 destination that it obtained by doing a DNS lookup, and the packet ends up going in the clear to the local media. A malicious third party could then spoof the destination on-link.

4. Changes to [RFC2461](#)

The following changes have been made to the Neighbor Discovery specification between [[RFC2461](#)] and [[I-D.ietf-ipv6-2461bis](#)]:

The last sentence of the second paragraph of [section 5.2](#) ("Conceptual Sending Algorithm") was removed. This sentence was, "If the Default Router List is empty, the sender assumes that the destination is on-link."

Bullet item 3) in [section 6.3.6](#) ("Default Router Selection") was removed. The item read, "If the Default Router List is empty, assume that all destinations are on-link as specified in [Section 5.2](#)."

APPENDIX A was modified to remove on-link assumption related text in bullet item 1) under the discussion on what happens when a multihomed host fails to receive Router Advertisements.

The result of these changes is that destinations are considered unreachable when there is no routing information for that destination (through a default router or otherwise). Instead of attempting link-layer address resolution when sending to such a destination, a node should send an ICMPv6 Destination Unreachable message (code 0 - no route to destination) message up the stack.

5. Security Considerations

The removal of the on-link assumption from Neighbor Discovery removes some security related vulnerabilities of the protocol as described in [Section 3.4](#).

6. References

[6.1](#) Normative References

- [I-D.ietf-ipv6-2461bis]
Narten, T., "Neighbor Discovery for IP version 6 (IPv6)",
[draft-ietf-ipv6-2461bis-02](#) (work in progress),
February 2005.
- [RFC1122] Braden, R., "Requirements for Internet Hosts -
Communication Layers", STD 3, [RFC 1122](#), October 1989.
- [RFC2461] Narten, T., Nordmark, E., and W. Simpson, "Neighbor
Discovery for IP Version 6 (IPv6)", [RFC 2461](#),
December 1998.

- [RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", [RFC 3484](#), February 2003.
- [RFC3756] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", [RFC 3756](#), May 2004.

[6.2](#) Informative References

- [RFC2462] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", [RFC 2462](#), December 1998.

Authors' Addresses

Sebastien Roy
Sun Microsystems, Inc.
1 Network Drive
UBUR02-212
Burlington, MA 01801

Email: sebastien.roy@sun.com

Alain Durand
Comcast Corporation
1500 Market St.
Philadelphia, PA 09102

Email: alain_durand@cable.comcast.com

James Paugh

Email: jpaugh@speakeasy.net

[Appendix A](#). Acknowledgments

The authors gratefully acknowledge the contributions of Jim Bound, Tony Hain, Mika Liljeberg, Erik Nordmark, Pekka Savola, and Ronald van der Pol.

[Appendix B](#). Changes from [draft-ietf-v6ops-onlinkassumption-02](#)

- o Changed abstract to reflect the historical nature of this document.

- o Changed the introduction to stress that this is historical information documenting the removal of the on-link assumption from the ND spec.
- o Added text to the introduction stating that the assumption is a problem for nodes with IPv6 on by default.
- o Added mention to [RFC1122](#) in [section 3.2](#).
- o Changed use of the term multi-homed nodes to "nodes that are attached to multiple links".
- o Changed [section 4](#) from "Proposed Changes" to "Changes" and adjusted included text to reflect that the changes have been made.

[Appendix C.](#) Changes from [draft-ietf-v6ops-onlinkassumption-01](#)

- o Added text in the Introduction stating that rfc2461bis has removed the on-link assumption, and that this memo gives the historical reference and background for its removal.
- o Stated in [Section 2](#) that users may not have sufficient privileges or knowledge to manually configure addresses or routers in order to work-around the lack of an on-link assumption.
- o Removed implementation details of the on-link assumption from [Section 3.1](#).
- o Miscellaneous editorial changes.

[Appendix D.](#) Changes from [draft-ietf-v6ops-onlinkassumption-00](#)

- o Clarified in the abstract and introduction that the problem is with systems that are IPv6 enabled but have no off-link connectivity.
- o In [Section 3.3](#), clarified that soliciting on all links could have ambiguous results.
- o The old Security Considerations section was moved to [Section 3.4](#), and the new Security Considerations section refers to that new section.
- o Miscellaneous editorial changes.

Intellectual Property Statement

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.

Disclaimer of Validity

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 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.

Copyright Statement

Copyright (C) The Internet Society (2005). 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.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

