

Internet Draft

<[draft-halpern-6man-nd-pre-resolve-addr-00.txt](#)>

Category: Informational

Expires in 6 months

I. Chen

J. Halpern

Ericsson

January 10, 2014

Triggering ND Address Resolution on Receiving DAD-NS

<[draft-halpern-6man-nd-pre-resolve-addr-00.txt](#)>

Status of this Memo

Distribution of this memo is unlimited.

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [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/lid-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 date.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This draft proposes a new optional event to trigger address

Internet Draft

nd-pre-resolve-addr

January 10, 2014

resolution using IPv6 Neighbor Discovery. This helps optimize router performance, and can help mitigate certain potential ND-related denial-of-service attacks. Upon receiving a DAD-NS message, the neighbor solicitation message used to detect duplicate addresses, if the target address encoded in the DAD-NS is not a duplicate address, the receiving device responds by triggering address resolution for the target address in the DAD-NS, in preparation for expectant future communication with the sending device.

Internet Draft

nd-pre-resolve-addr

January 10, 2014

Table of Contents

| | |
|--|-------------------|
| 1. Introduction | 3 |
| 2. Proposed Trigger for Address Resolution | 4 |
| 3. Which Devices to Upgrade and the Consequences | 6 |
| 4. Security Considerations | 6 |
| 5. IANA Considerations | 6 |
| 6. References | 6 |

[1. Introduction](#)

Due to the large address space for IPv6 [[RFC2460](#)] and a large /64 default subnet size, Neighbor Discovery (ND) for IPv6 [[RFC4861](#)] could suffer from off-link flooding Denial-of-Service (DoS) attacks [[RFC6583](#)]. In such an attack, a remote malicious device could flood a router with packets destined to billions of unassigned IPv6 addresses. Although these packets are destined to unused IPv6 addresses, cache misses could occur nonetheless. Without special handling of cache misses, the router would trigger address resolution for billions of unused IPv6 addresses. The sheer volume of IPv6 addresses could overwhelm the router's normal ND protocol processing and ultimately prevent the router from forwarding packets destined to legitimate IPv6 addresses.

[RFC6583] proposes implementation and operational practices to reduce the impact of an off-link flooding DoS attack without modifying the ND protocol. The Internet Draft [[ndmit](#)] goes further and poses the question whether cache misses, an important trigger for address resolution in the ND protocol, are necessary. If cache misses can be ignored, then an off-link flooding DoS attack that uses cache misses to compromise a router can be neutralized. To eliminate the need for cache misses, a router should retain the neighbor cache entries of all legitimate neighbors on the physical link.

This draft proposes that a router further triggers address resolution based on an event other than a cache miss. In addition to waiting

for a cache miss to trigger address resolution, a router should initiate address resolution for the target address in a DAD-NS, provided that the target address is not a duplicate address of the receiving device or a resolved neighbor.

Consequently, to optimize IPv6 router performance and to avoid neighbor cache overrun by remote exploration, an IPv6 device:

- 1) SHOULD NOT remove a populated cache entry to make room for a pending entry based on a received packet trigger.
- 2) SHOULD NOT remove a DAD triggered pending entry to make room

for a remote received packet triggered entry.

- 3) SHOULD remove remote trigger pending entries if needed to make room for DAD triggered pending entries.

For an even stronger solution to prevent neighbor cache overrun by remote exploration, a router can implement [[ndmit](#)] in conjunction with the mechanism in this draft.

[2.](#) Proposed Trigger for Address Resolution

In IPv6, when a device initializes an interface, a special Neighbor Solicitation (NS) message is sent to perform Duplicate Address Detection (DAD) [[RFC4862](#)] to determine whether a particular address is already assigned to a different interface on the same multi-access link. This special message, referred to as DAD-NS in the rest of this draft, is an NS message with an unspecified source address. The target address of this DAD-NS is the IPv6 unicast address that is intended for new interface.

In addition to the detection of duplicate addresses, a DAD-NS can also be treated as an announcement for a new address, the target address in the DAD-NS, which will be used in the near future, after the DAD algorithm has been completed. Consequently, after allowing time for the DAD algorithm to be completed, rather than waiting for a cache miss, the router that received the DAD-NS can perform address resolution for the target address in the DAD-NS.

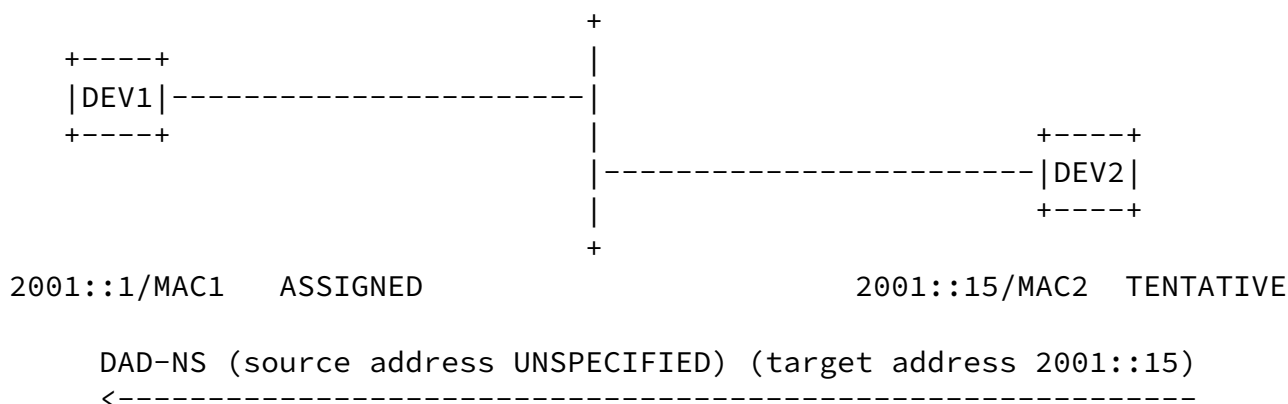
The proposed steps are similar to how address resolution is initiated

when a device receives a regular NS message, one that has a specified source address. The difference in the mechanism proposed by this draft is that the address resolution is not triggered immediately after receiving the DAD-NS. Instead, address resolution is triggered with a time delay to accommodate the DAD algorithm.

For example in Figure 1, when DEV2 initializes an interface that is expected to use the IP address 2001::15, a DAD-NS with an unspecified source address and a target address of 2001::15 is multicast on the physical link. Following the DAD algorithm in [\[RFC4862\]](#), when DEV1 on the physical link receives such a DAD-NS, the DEV1 device does not respond to the DAD-NS if the target address 2001::15 is not used by one of its interfaces. Assuming that DEV1 implements the proposed DAD-NS response in this draft, then after allowing for the DAD algorithm to be completed, DEV1 can trigger address resolution for 2001::15, the target address announced in the previous DAD-NS, without waiting for a cache miss to occur.

Furthermore, when DEV2 receives the NS to query for target address

2001::15, [\[RFC4861\] Section 7.2.3](#) specifies that DEV2 respond with an NS query of its own for the source address of the NS that DEV2 just received. Thus, at the end of the DAD-NS, NS, and Neighbor Advertisement (NA) message exchanges that are triggered by the initialization of DEV2's interface, DEV1 and DEV2 have each others' neighbor entries. The two devices can immediately begin communication shortly after DEV2 sends the DAD-NS and very likely before any cache miss occurs.



Neighbor entry

2001::15 INCOMPLETE

2001::15/MAC2 ASSIGNED

NS (source address 2001::1) (target address 2001::15)
----->

Neighbor entry
2001::1 INCOMPLETE

NA (source address 2001:15) (target address 2001::15) (MAC2)
<-----

Neighbor entry
2001::15/MAC2 REACH

NS (source address 2001::15) (target address 2001::1)
<-----

NA (source address 2001::1) (target address 2001::1) (MAC1)
----->

Neighbor entry
2001::1/MAC1 REACH

Figure 1. An example of DAD-NS triggering address resolution.

[3.](#) Which Devices to Upgrade and the Consequences

This proposed mechanism does not require changes to [\[RFC4861\]](#). Further, devices that implement this proposal can interoperate with devices that do not implement this proposal. Ericsson's Smart Services Router implemented this change in early 2013, is deployed in operational IPv6 networks, and has not encountered any problems.

The proposed mechanism probably is more useful for routers than for hosts, although nothing prevents a host from implementing this proposal and hosts might benefit from implementing this proposal.

If all devices, both routers and hosts, on a physical link implement the proposed change, then when a device restarts, the restarting device can easily recover all the pre-restart neighbor cache entries.

Using Figure 1 as an example, assume that DEV2 restarts and re-initializes its interface, and once again wishes to assign its interface the address 2001::15. Because DEV1 implements this draft and responds to the DAD-NS by querying for 2001::15, both DEV1 and DEV2 end up with the same neighbor cache entries from before DEV2 restarted.

[4.](#) Security Considerations

The proposed trigger for address resolution might suffer from certain attacks if the attacker is on the same physical link as the new IPv6 device and sends bogus DAD-NS messages. However, no mechanism can protect a device when the attacker is on the same physical link as the device, other than ensuring that only authorized devices have access to a physical link (e.g., by using link-layer security mechanisms, such as IEEE 802.1AE link encryption [[802.1AE](#)]).

[5.](#) IANA Considerations

No actions are required from IANA as result of the publication of this document.

[6.](#) References

[6.1.](#) Normative References

- [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), December 1998.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.

I. Chen & J. Halpern Expires in 6 months [Page 6]

Internet Draft nd-pre-resolve-addr January 10, 2014

- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", [RFC 4862](#), September 2007.

[6.2.](#) Informative References

- [RFC6583] Gashinsky, I., Jaeggli, J., and W. Kumari, "Operational Neighbor Discovery Problems", [RFC 6583](#), March 2012.

- [ndmit] Halpern, J, Work in progress, "[draft-halpern-6man-nddos-mitigation-00](#)", October 2011.
- [802.1AE] IEEE Standards Association, "IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security", IEEE Standard 802.1AE, IEEE, Piscataway, NJ, USA, August 18, 2006.

Authors' Addresses

I. Chen
Ericsson
Email: ing-wher.chen@ericsson.com

J. Halpern
Ericsson
EMail: joel.halpern@ericsson.com