Abstract

Neighbor Discovery (RFC4861) used by IPv6 nodes to determine the link-layer addresses of neighboring nodes as well as to discover and maintain reachability information. This document discusses how the neighbor discovery state machine on a first-hop router is causing user-visible connectivity issues when a new (not being seen on the network before) IPv6 address is being used.

Status of This Memo

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). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on January 3, 2020.

Copyright Notice

Copyright (c) 2019 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 (https://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. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of
The section 7.2.5 of [RFC4861] states: "When a valid Neighbor Advertisement is received (either solicited or unsolicited), the Neighbor Cache is searched for the target’s entry. If no entry exists, the advertisement SHOULD be silently discarded. There is no need to create an entry if none exists, since the recipient has apparently not initiated any communication with the target."
This approach is perfectly suitable for host2host communications which are in most cases bi-directional and it could be expected that if a host A has an ND cache entry for the host B IPv6 address, the host B also has the corresponding ND entry for the host A address in its cache. However when a host communicates to off-link destinations via its first-hop router that logic does not apply. Here is the most typical scenario when the problem may arise:

1. When a host joins the network it receives an RA packet from the first-hop router (either a periodic unsolicited RA or a response to an RS sent by the host). The RA contains information the host needs to perform SLAAC and to configure its network stack. Among other things the host populates its ND cache with the router link-local address and potentially link-layer address (if included in the RA Source Link-Layer Address option).

2. The host starts opening connections to off-link destinations. Very common use case is a mobile device sending probes to detect the Internet connectivity and/or the captive portals presence on the network. To speed up that process many implementations are using the Optimistic Duplicate Address Detection ([RFC4429]) which allows them to send probes from their GUA before the DAD process is completed. Important point here is that at that moment the device ND cache contains all information required to send those probes (such as the default gateway LLA and the link-layer address). The router ND cache, however, might contain an entry for the device link-local address (if the device has been performing the ND process for the router LLA) but there are no entries for the device GUA.

3. Response packets for the probes (or any other traffic sent by the host) are received by the first-hop router. As the router does not have any ND cache entry for the host GUA, the router starts the neighbor discover process by creating an INCOMPLETE cache entry and then sending an NS to the Solicited Node Multicast Address. Apparently most of the router implementations buffer only one data packet while performing the ND process for its destination. Therefore all packets for the host GUA, except for the very first one, are dropped until the address resolution process is completed.

4. As many implementations send multiple probes in parallel it’s very likely that all probes except the first one would be considered failed. If the host implements an exponential backoff for probing it leads to user-noticeable delay in detecting network connectivity/reporting the network as usable.
The above-mentioned scenario illustrates the problem happening when the device connects to the network for the first time/after a long timeout. However the same sequence of events happen when the host starts using the new (previously unseen by the router) GUA (e.g. a new privacy address [RFC4941]).

While in dual-stack networks this problem might hidden by Happy Eyeballs ([RFC8305]) it manifests itself quite clearly in IPv6-only networks, especially wireless ones, leading to poor user experience and contributing to negative perception of IPv6-only solutions as unstable and non-deployable.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

1.2. Terminology

ND: Neighbor Discovery, [RFC4861].

SLAAC: IPv6 Stateless Address Autoconfiguration, [RFC4862].

NS: Neighbor Solicitation, [RFC4861].

NA: Neighbor Advertisement, [RFC4861].

RS: Router Solicitation, [RFC4861].

RA: Router Advertisement, [RFC4861].

SLLA: Source link-layer Address, an option in the ND packets containing the link-layer address of the sender of the packet ([RFC4861]).

TLLA: Target link-layer Address, an option in the ND packets containing the link-layer address of the target ([RFC4861]).

GUA: Global Unicast Address ([RFC4291]).

DAD: Duplicate Address Detection, [RFC4862].

Optimistic DAD: a modification of DAD, [RFC4429].
2. Potential Solutions

The problem could be addressed from different angles. Possible approaches are:

- Just do nothing.
- The host explicitly advertizes its GUAs using Neighbor Discovery mechanisms.
- The host initiates bidirectional communication to the router using the host GUA.
- Making the probing logic on hosts more robust.
- Increasing the buffer size on routers.

The following sections discuss those approaches in more details.

2.1. Do Nothing

One of the possible approaches might be to declare that everything is working as intended.

2.1.1. Pros

- No work required.

2.1.2. Cons

- Unhappy users.
- Many support tickets.

2.2. Hosts Explicitly Advertizing Their GUAs Using Existing ND Mechanisms

The Neighbor Discovery is designed to allow IPv6 nodes to discover neighboring nodes reachability and learn IPv6 to link-layer addresses mapping. Therefore ND seems to be the most appropriate tool to inform the first-hop routers about addresses the host is going to use. The following sections discusses potential approaches in more details.
2.2.1. Host Sending Unsolicited NA

Section 4.4 of [RFC4861] says:

"A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly."

Propagating information about new GUA as quickly as possible is exactly what is required to solve the problem outlined in this document. Therefore the host might send an unsolicited NA to advertise its GUA as soon as the said address enters Optimistic or Preferred state. The NA should include the target link-layer address option. To ensure that all first-hop routers receive the advertisement it could be sent to all-routers multicast address (ff02::2).

As it’s been mentioned, [RFC4861] explicitly states that receiving a NA should not create a new NC entry. However the justification for that requirement ("There is no need to create an entry if none exists, since the recipient has apparently not initiated any communication with the target.") clearly does not apply for the case discussed. As per [RFC2119] "there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.". Therefore routers creating a new NC entry upon receiving an unsolicited NA would still be compliant with [RFC4861].

It should be noted that some routing platforms have implemented such behaviour already. Administrators could enable creating neighbor discovery cache entries based on unsolicited NA packets sent from the previously unknown neighbors on that interface.

2.2.1.1. Pros

- Already implemented on some platforms.
- In accordance with [RFC4861].

2.2.1.2. Cons

- Allows a malicious host to execute an ND cache exhaustion attack. It’s recommended that this functionality is configurable and recommendations from [RFC6583] are taken into account.
- Requires hosts to send unsolicited NA (changes to the hosts).
Some wireless devices are known to fiddle with ND packets and perform various non-obvious forms of ND proxy actions. In some cases unsolicited NAs might not even reach the routers.

2.2.2. Host Sending NS to the Router Address from Its GUA

The host could force creating a STALE entry for its GUA in the router ND cache by sending the following Neighbor Solicitation message:

- The NS source address is the host GUA.
- The Source Link-Layer Address option contains the host link-layer address.
- The target address is the host default gateway address (the default router address the host received in the RA).

The main disadvantage of this approach is that it would not work if the GUA the host needs to advertise is still in the Optimistic state. The section 2.2 of [RFC4429] explicitly prohibits sending Neighbor Solicitations from an Optimistic Address.

2.2.2.1. Pros

- Router implementations which follow recommendations made in [RFC6583] might prioritize responding to NS packets to own addresses.

2.2.2.2. Cons

- Does not work for Optimistic addresses (see section 2.2 of [RFC4429]).
- If first-hop redundancy is deployed in the network, the NS would reach the active router only, so all backup routers (or all active routers ex. one) would not get their neighbor cache updated.
- Some wireless devices are known to fiddle with ND packets and perform various non-obvious forms of ND proxy actions. In some cases unsolicited NAs might not even reach the routers.

2.2.3. Host Sending Router Solicitation from its GUA

The host could send a router solicitation message to ‘all routers’ multicast address, using its GUA as a source and including its link-layer address in Source Link-Layer Address option. As per the Section 6.2.6 of [RFC4861] the router would create a STALE entry for the host GUA.
2.2.3.1. Pros

- Unlike NS packets, RS packets would reach all routers on link, allowing all routers to update their neighbor caches and preventing packet loss in case of asymmetric routing.

2.2.3.2. Cons

- Would not work for the host optimistic addresses (see section 2.2 of [RFC4429] which prohibits using an Optimistic Address as the source address of a Router Solicitation with a SLLAO.

- Responding to RS with RA is not instant but delayed by a random interval. Additional delay would compromise the idea of populating the routers ND cache before the return traffic to the host GUA arrives.

- Some wireless devices are known to fiddle with ND packets and perform various non-obvious forms of ND proxy actions. In some cases unsolicited NAs might not even reach the routers.

2.3. Initiating Hosts2Routers Communication

Every time the host configures a new GUA (when the address enters the Optimistic state or, if the optimistic DAD is not used, as soon as it changes the state from tentative to preferred) the host can a ping or traceroute packet to the default gateway LLA. As the RTT to the default gateway is lower than RTT to any off-link destinations it’s quite likely that the router would start the neighbor discovery process for the host GUA before the first packet of the returning traffic arrives. There are pretty good chances that the process would be completed before the actual data traffic reaches the router.

2.3.1. Pros

- As data packets are involved, there is no potential impact caused by smart wireless infrastructure performing ND proxy.

- Full compliance with existing standards.

2.3.2. Cons

- Data packets to the router LLA could be blocked by security policy or control plane protection mechanism.

- Maximum overhead for routers control plane (in addition to processing ND packets, the data packet needs to be processed as well).
If the first hop redundancy is implemented in the network the host ping/traceroute packet would reach the active router only. All backup routers would not receive it and therefore would not start populating the cache. So in the case of asymmetric traffic flow (packets leave the network via one router while the return flow is going via another) the backup router(s) still would not have the cache entry. (A hacky way to overcome this limitation would be sending ping/tracroute packet to ‘all routers’ ff02::2 multicast address).

2.4. Tweaking Probing Algorithms

While tweaking the probing logic on devices might make the problem less visible it would be still desirable to avoid packet loss everytime the new GUA is used by a host. It would be quite tricky to adjust every probing algorithm to find the right balance between prompt detection of network connectivity and false positives in IPv6-only mode.

2.5. Routers Buffering More Packets

Another way to mitigate the issue, at least partially, would be increasing the number of packets the router could buffer while performing the neighbor discovery process for the INCOMPLETE cache entry. However it would be against recommendations made in the section 7.2.2 of [RFC4861] and [RFC6583].

2.5.1. Pros

- Does not require changes on hosts.

2.5.2. Cons

- This approach makes the routers even more vulnerable to attack vectors described in [RFC6583]. In particular, it would amplify the impact of any scanning attack.

- Against the recommendations from the section 7 of [RFC6583].

- Requires router vendors support.

3. Recommendations

- Hosts SHOULD send at least one unsolicited NA packet to all-routers multicast address (ff02::2) as soon as one of the following events happens:
* (if Optimistic DAD is used): a new Optimistic GUA is assigned to the host interface.

* (if Optimistic DAD is not used): a GUA changes the state from tentative to preferred.

- Routers SHOULD have a configuration knob to enable creating ND cache entry upon receiving unsolicited NAs on a specific interface.

4. IANA Considerations

This memo asks the IANA for no new parameters.

5. Security Considerations

6. Acknowledgements

Thanks to the following people (in alphabetical order) for their review and feedback: Lorenzo Colitti, Erik Kline.

7. References

7.1. Normative References


7.2. Informative References


Author's Address

Jen Linkova
Google
1 Darling Island Rd
Pyrmont, NSW 2009
AU

Email: furry@google.com