

v6ops
Internet-Draft
Intended status: Informational
Expires: January 3, 2019

J. Jaeggli
Fastly
July 2, 2018

Indefensible Neighbor Discovery
draft-jaeggli-v6ops-indefensible-nd-01

Abstract

NDP resource exhaustion is a problem which cannot fundamentally be addressed through limited protocol changes or implementation tweaks; mitigations proposed in [RFC 6583](#) [[RFC6583](#)] may well prevent the outright failure of a device under duress. This draft discusses some mitigations which have or can be employed by networks looking to reduce or eliminate the exposure of the Neighbor Discovery Process.

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, 2019.

Copyright Notice

Copyright (c) 2018 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

Internet-Draft

IND

July 2018

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
1.1.	Requirements Language	3
2.	ND under stress	3
2.1.	Ways in which resources are consumed:	3
3.	Mitigations	4
3.1.	RFC 6583	4
3.2.	Link-Local	4
3.3.	RFC 6164	5
3.4.	Firewalls	5
3.5.	Subnetting	5
3.6.	Stateless Neighbor Presence Discovery	5
3.7.	Solicited Node Multicast Group Membership	6
4.	Acknowledgements	6
5.	IANA Considerations	6
6.	Security Considerations	6
7.	References	6
7.1.	Normative References	6
7.2.	Informative References	6
	Author's Address	8

[1.](#) Introduction

Neighbor discovery serves to allow the discovery of hosts and the self assignment of resources within the sparse address space of IPv6 subnets. Since the definition of Interface IDs and accompanying subnet sizes [RFC 1885](#) [[RFC1885](#)] the potential has existed for the forwarding and control plane resources of a router to be greatly exceeded by locally or remotely triggered attempts to discover connected neighbors. The problem of the number of adjacencies that can reasonably be supported and signaled is not unique to IPv6 though it is especially acute there. It also exists in IPv4 as well as other non-internet protocols. Practical scaling limits of the number of adjacencies or amount of signaling serve as incentives for operators to limit the size and number of participants in layer-2 domains.

Because of the size of typical IPv6 Interface IDs as well as the property of self-assignment, IPv6 subnets and connected devices are

particularly exposed to resource consumption; therefore proactive mitigations are required to limit the potential for resource consumption resulting in Denial of Service. In [RFC 6583](#) [[RFC6583](#)], we detailed the threat posed by neighbor discovery resource consumption to network devices as well as some mitigations which

could improve the situation. While some mitigations remove the threat entirely; [RFC 6164](#) [[RFC6164](#)] style /127 prefixes for example are not subject to ND attacks, they have the property of not being practical for subnets supporting end systems. Practical mitigations in [RFC 6583 section 7](#) [[RFC6583](#)] implementation advice serve to tamp down, but cannot entirely eliminate the threat of resource exhaustion; devices operating under duress cannot be expected to perform as well as devices which are not.

If we are to characterize the architectural challenge posed by ARP and ND. It is that traffic in the data-plane from untrusted source may impose demands on the control plane to create and then exhaust available state. In IPv4 the mitigation for this is for the most part relatively trivial and tightly coupled to subnet and forwarding hardware sizing; address conservation principles that do not apply to IPv6 subnets therefore generally but not entirely ameliorate this problem in IPv4.

[1.1](#). Requirements Language

This document does not employ and should not be interpreted through [RFC 2119](#) [[RFC2119](#)] requirements language.

[2](#). ND under stress

In characterizing the behavior of devices under stress we posit that the neighbor discovery process responsible for resolving an effectively unlimited number of unknown neighbors itself is ultimately indefensible. By Indefensible we mean that if implemented as intended by 4861 the protocol is always exposed to resource consumption constraints that require mitigation.

[2.1](#). Ways in which resources are consumed:

- o Host-routes / Negative cache entries - IPv6 subnets do not have constraints on the number of addresses which can be employed

within the limit (64 bits) imposed by the subnet mask. Networks employing stateful DHCP v6 address assignment can make some assumptions about the number of host to address mappings they are willing to support, devices performing SLAAC and deriving addresses subsequently are under no such constraints.

- o CPU / RAM - Neighbor Discovery is intended to be triggered for addresses for which no layer-2 next-hop yet exists. This allows for the classical DDOS of the ND process described in [RFC 3756](#) [[RFC3756](#)]. Since the senders of packets which might trigger ND are not subject to the same constraints as devices which have to initiate it this asymmetry is trivial to exercise.

- o Multicast - Multicast replication of Neighbor solicitations may be expensive for certain link-layers or hosts particularly wireless networks. In cases where multicast is transmitted at lower rates than the prevailing unicast rate, performance of other traffic may be directly impacted by the presence of this traffic even at relatively low levels ([draft-perkins-intarea-multicast-ieee802-03](#) [[draft-perkins-intarea-multicast-ieee802-03](#)])).

[3.](#) Mitigations

Recognition of the short-comings of IPv6 neighbor discovery are sufficiently common that link-layers supporting resource constrained infrastructure typically have to address them directly, 6LowPAN for example has [RFC 6775](#) [[RFC6775](#)] utilizing an address registration scheme to limit the need for discovery.

There are various forms of mitigation which can be applied in order to avoid having neighbor discovery become the ineluctable bottleneck in defending a subnet. Many of these approaches are more specially changes to harden networks or transfer the burden of state rather than alterations of the neighbor discovery process itself.

[3.1.](#) [RFC 6583](#)

[RFC 6583](#) [[RFC6583](#)] suggests some practical mitigations, which can reduce the extent to which ND fails but not eliminate it.

[3.2.](#) Link-Local

[RFC 7404](#) [[RFC7404](#)](Using Only Link-Local Addressing inside an IPv6 Network) style approaches, link-local-only numbered interfaces make it impossible to target the subnet address from off-link, at the cost of limiting the ability to ping interfaces, return useful interface IPs in traceroute and so on.

Link-local-only addressing may be extended to Hosts by assigning unicast addressees on loopback interfaces rather than on subnet connected interfaces. In conjunction with routing (typically BGP but alternatives are possible), it is possible to construct networks in which no external targeting of neighbor discovery on connected subnets is possible. The existence of a prefix of arbitrary length is signaled in a routing protocol. Probes addressed to unused addresses may be discarded by an aggregate route.

[3.3.](#) [RFC 6164](#)

[RFC 6164](#) [[RFC6164](#)] uses /127s allows for the use of /127s for inter-router links. This effectively precludes ND exhaustion attempts for point to point links.

[3.4.](#) Firewalls

Stateful inspection firewalls may limit the expense of performing neighbor discovering for unknown addresses by discarding packets for unestablished connections. While this may be a transfer of expense from one account (ND) to another (firewall) it never-the-less precludes targeting subnets for NDP exhaustion.

[3.5.](#) Subnetting

Sizing subnets effectively to support the number of hosts present does limit the scope for ND exhaustion attacks. [RFC 7608](#) [[RFC7608](#)] does instruct that devices be able to forward to arbitrary length subnets. Arbitrary length subnets e.g. a /120 or /121 are presently considered incompatible with SLAAC and conflict with some goals for privacy address [RFC 4941](#) [[RFC4941](#)]. In the draft [draft-bourbaki-](#)

[6man-classless-ipv6-03](#) [[draft-bourbaki-6man-classless-ipv6-03](#)] is a proposal to eliminate the expectation of fixed length subnetting.

Alternative to resizing the subnet, stateful DHCPv6 address assignment can be used to limit the range of IPs within a /64 subnet which are consumed which may be used to ACL to target sub-prefixes of the entire subnet.

Use of very long prefixes has the potential to expose subnets to the considerations in [RFC 7707](#) [[RFC7707](#)] where for example neighboring devices on a subnet might be trivial to discover via scanning as for example are router interfaces numbered as ":::1" out of convience . The extent to which discoverability is an issue may vary by usage and also methodoly, so for example sparsely allocated pseudo-randomly assigned /128s may be no more discoverable then IPv6 self assigned privacy addresses, but machines clumped together in a /121 may be trivially identified when one of them is located. other methods of discovering detailed in [RFC 7707](#) [[RFC7707](#)] e.g. forward or reverse dns mappings may trivialy reveal the presence of additional hosts within a prefix.

[3.6.](#) Stateless Neighbor Presence Discovery

"Mitigating IPv6 Neighbor Discovery DoS Attack Using Stateless Neighbor Presence Discovery"

[[draft-smith-6man-mitigate-nd-cache-dos-slnd](#)] was a proposal by Mark

Jaeggli

Expires January 3, 2019

[Page 5]

Internet-Draft

IND

July 2018

Smith, to aleviate the pressure on the neghbor discovery process when under duress.

[3.7.](#) Solicited Node Multicast Group Membership

"Further Mitigating Router ND Cache Exhaustion DoS Attacks Using Solicited-Node Group Membership"

[[draft-smith-v6ops-mitigate-rtr-dos-mld-slctd-node](#)] was a proposal by Mark Smith, to use the solicited node multicast group to limit the need to multicast ND to all ports when performing ND.

[4.](#) Acknowledgements

This Document is entirely depedent on previous work done in the IETF community and other authors. Mark Smith offered valuable

contributions and References to the initial Draft. Brian Carpenter reviewed the initial draft and provided additional references.

5. IANA Considerations

This memo includes no request to IANA.

6. Security Considerations

All drafts are required to have a security considerations section. This document is essentially a collection of related security considerations, it is hoped that by exploring these issues some insight into the rationale and methodology for mitigating the exposure posed by ND may be gained. Some methods considered here are currently and may remain non-standard.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.

7.2. Informative References

[[draft-bourbaki-6man-classless-ipv6-03](#)]
Nicholas Bourbaki, "Classes IPv6", 2018, <<https://tools.ietf.org/html/draft-bourbaki-6man-classless-ipv6-03>>.

[[draft-perkins-intarea-multicast-ieee802-03](#)]
Perkins, C., "Multicast Considerations over IEEE 802 Wireless Media", 2018, <<https://tools.ietf.org/html/draft-perkins-intarea-multicast-ieee802-03>>.

[[draft-smith-6man-mitigate-nd-cache-dos-slnd](#)]
Smith, M., "Mitigating IPv6 Neighbor Discovery DoS Attack Using Stateless Neighbor Presence Discovery", 2013,

<https://datatracker.ietf.org/doc/draft-smith-6man-mitigate-nd-cache-dos-slnd/>>.

[[draft-smith-v6ops-mitigate-rtr-dos-mld-slctd-node](https://datatracker.ietf.org/doc/draft-smith-v6ops-mitigate-rtr-dos-mld-slctd-node)]

Smith, M., "Mitigating IPv6 Neighbor Discovery DoS Attack Using Stateless Neighbor Presence Discovery", 2016, <https://datatracker.ietf.org/doc/draft-smith-v6ops-mitigate-rtr-dos-mld-slctd-node/>>.

[RFC1885] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)", [RFC 1885](https://www.rfc-editor.org/info/rfc1885), DOI 10.17487/RFC1885, December 1995, <https://www.rfc-editor.org/info/rfc1885>>.

[RFC3756] Nikander, P., Ed., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", [RFC 3756](https://www.rfc-editor.org/info/rfc3756), DOI 10.17487/RFC3756, May 2004, <https://www.rfc-editor.org/info/rfc3756>>.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", [RFC 4941](https://www.rfc-editor.org/info/rfc4941), DOI 10.17487/RFC4941, September 2007, <https://www.rfc-editor.org/info/rfc4941>>.

[RFC6164] Kohno, M., Nitzan, B., Bush, R., Matsuzaki, Y., Colitti, L., and T. Narten, "Using 127-Bit IPv6 Prefixes on Inter-Router Links", [RFC 6164](https://www.rfc-editor.org/info/rfc6164), DOI 10.17487/RFC6164, April 2011, <https://www.rfc-editor.org/info/rfc6164>>.

[RFC6583] Gashinsky, I., Jaeggli, J., and W. Kumari, "Operational Neighbor Discovery Problems", [RFC 6583](https://www.rfc-editor.org/info/rfc6583), DOI 10.17487/RFC6583, March 2012, <https://www.rfc-editor.org/info/rfc6583>>.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", [RFC 6775](https://www.rfc-editor.org/info/rfc6775), DOI 10.17487/RFC6775, November 2012, <https://www.rfc-editor.org/info/rfc6775>>.

[RFC7404] Behringer, M. and E. Vyncke, "Using Only Link-Local

Addressing inside an IPv6 Network", [RFC 7404](#),
DOI 10.17487/RFC7404, November 2014,
<<https://www.rfc-editor.org/info/rfc7404>>.

[RFC7608] Boucadair, M., Petrescu, A., and F. Baker, "IPv6 Prefix
Length Recommendation for Forwarding", [BCP 198](#), [RFC 7608](#),
DOI 10.17487/RFC7608, July 2015,
<<https://www.rfc-editor.org/info/rfc7608>>.

[RFC7707] Gont, F. and T. Chown, "Network Reconnaissance in IPv6
Networks", [RFC 7707](#), DOI 10.17487/RFC7707, March 2016,
<<https://www.rfc-editor.org/info/rfc7707>>.

Author's Address

Joel Jaeggli
Fastly
Mountain View, CA 94043
US

Phone: +5415134095
Email: joelja@bogus.com