Workgroup: v6ops Working Group
Internet-Draft: draft-linkova-v6ops-ipmaclim
Published: 7 November 2022
Intended Status: Best Current Practice
Expires: 11 May 2023
Authors: J. Linkova, Ed.
Google

Minimizing Damage of Limiting Number of IPv6 Addresses per Host

Abstract

This document provides recommendations to network infrastructure vendors on how to deal with multiple IPv6 addresses per host.

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 11 May 2023.

Copyright Notice

Table of Contents

1. Introduction

One of the fundamental differences between IPv4 and IPv6 is that an IPv6 host can, and almost always does have multiple IPv6 addresses. RFC7934 discusses this aspect and explicitly states that IPv6 deployments SHOULD NOT limit number of IPv6 addresses a host can have. RFC7934 is mostly focuses on various methods of address assignment and how those methods should provide multiple addresses per host. However network devices, especially wireless ones performing Neighbor Discovery proxy, often have hardcoded limits on how many IPv6 addresses are allowed per a single MAC. When that limit is exceeded, traffic to/from the affected IPv6 addresses is blocked. Such failure mode is rather hard to diagnoze (as IPv6 addresses on a device may obtain and lose connectivity randomly) and leads to poor user experience. This document provides recommendations to network infrastructure device vendors on how to deal with multiple IPv6 addresses per device.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Impact of Limiting Number of IPv6 Addresses per Host

The most common scenario of network-imposed limitations is Neighbor Discovery (ND) proxy. Many enterprise-scale wireless solutions implement ND proxy to reduce amount of broadcast and multicast downstream (AP to clients) traffic. To perform ND proxy a device usually maintains a table, containing IPv6 and MAC addresses of connected clients. At least some implementations have hardcoded

limits on how many IPv6 addresses per a single MAC such a table can contain. When the limit is exceeded the behaviour is implementation-dependent. Some vendors just fail to install N+1 address to the table. Other delete the oldest entry for this MAC and replace it with the new address. In any case the affected addresses lose network connectivity. The problem is exacerbated by the following:

- For the given set of device IPv6 addresses the affected subset may vary over time (depending on what addresses have been used to send traffic recently), which drastically complicates the troubleshooting.

- The host and applications do not receive any explicit signals, the traffic is just blackholed.

- Previously working address might become affected if another IPv6 address is assigned to the host. In that case existing traffic flows can be interrupted and even on a dual-stack network Happy Eyeballs would not be able to mitigate the issue, as the failure occurs too late for IPv4 fallback.

As internal implementation details might require a vendor to limit the number of IPv6 addresses per host, it's crucial to provide some recommendations on how to minimize the negative impact of imposing such a limit, especially as virtualiztion on endpoints and IPv6-only WiFi networks are gaining momentum.

3. Recommendations on Handling Multiple IPv6 Addresses per Host

If a network equipment manufacturer deems it necessary to impose any limit to a number of IPv6 addresses per host (or MAC address):

- The limit SHOULD be configurable.

- The default value MUST be at least 20.

- If the limit is exceeded, the device SHOULD log an error message containing the affected IPv6 address and device identificator (MAC address).

- If the limit is exceeded, the device SHOULD attempt to minimize the disruptions to existing flows, for example use Least-Recently-Used (LRU) algorithm to remove the oldest entry from the list of addresses.

4. IANA Considerations

This memo includes no request to IANA.

5. Security Considerations

TBA - I guess there is a risk of a host to create a lot of addresses and exhaust device memory.

6. References

6.1. 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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC7934] Colitti, L., Cerf, V., Cheshire, S., and D. Schinazi, "Host Address Availability Recommendations", BCP 204, RFC 7934, DOI 10.17487/RFC7934, July 2016, <https://www.rfc-editor.org/info/rfc7934>.

6.2. Informative References

Acknowledgements

TBA

Contributors

Thanks to Lorenzo Colitti for the discussions, the input and all contribution.

Author's Address

Jen Linkova (editor)
Google
1 Darling Island Rd
Pyrmont NSW 2009
Australia

Email: furry13@gmail.com, furry@google.com