Authors: A. Ogawa   K. Nishizuka
         Professional writer   NTT Communications
         Y. Atarashi   A. Kanai
         Alaxala Networks Co.   NTT Communications

Host behavior to short prefix length

Abstract

The Prefix Information Option in the IPv6 Neighbor Discovery Router
Advertisement message defines an 8-bit prefix length field. Prefix
List entries are created using the prefix length in the Prefix
Information Option. The Conceptual Model of a Host described in RFC
4861[RFC4861] does not clarify behavior of a host, when a short
prefix length is received. This document updates RFC 4861(if
approved), and clarifies that hosts SHOULD NOT accept prefix length
shorter than /64.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

RFC 4861 describes a conceptual model of a host for Neighbor Discovery. Conceptual data structures in the conceptual model includes the Prefix List.

The Prefix List is,

"A list of the prefixes that define a set of addresses that are on-link. Prefix List entries are created from information received in Router Advertisements."

The Prefix Information Option (PIO) in the IPv6 Neighbor Discovery Router Advertisement defines an 8-bit prefix length field. When a host is configured to accept RAs, it will add prefixes included in the PIO, into the Prefix List. When prefixes are added into the Prefix List of a host, the prefix added will be assumed on-link.

The PIO in the Router Advertisement has an 8-bit prefix length field. The value ranges from 0 to 128[RFC4861]. IPv6 Address Architecture[RFC4291] requires the length of interface ID to be 64 bits long. RFC 4291 states,

"For all unicast addresses, except those that start with the binary value 000, Interface IDs are required to be 64 bits long"

Therefore, on-link prefixes with bits shorter than 64 bits violate RFC 4291.

The SLAAC specification[RFC4862] refers RFC 4291 about the interface identifier length. And current host implementations do not accept prefix length other than 64, in the SLAAC process.

2. Problem Statement

When an RA with short prefix length field with autonomous address-configuration flag value 1 is received, some host implementations (Windows, macOS, Linux) will not add an IPv6 address to the network interface. Even though a new IPv6 address is not added, the host assumes the prefix as on-link. When autonomous address-configuration flag value is 0, the host will not run the SLAAC process, but assume that the prefix is on-link.

Current implementations accept up to /4 as prefix length. Because current IANA allocation of GUA is limited to 2000::/3, it would be very easy to mislead the whole IPv6 Internet as on-link. Which can lead to a DoS attack, MITM attack, etc.

3. Limiting Prefix Length

RFC 3756[RFC3756] Section 4.2.5. describes mitigation for DoS attacks using rogue RAs.

"As an example, one possible approach to limiting the damage of this attack is to require advertised on-link prefixes be /64s (otherwise it's easy to advertise something short like 0/0 and this attack is very easy)."

RFC 4291[RFC4291] limits the interface identifier length to 64 bits. When IID is 64 bits, the subnet prefix length will be 64 bits. Therefore, the prefix length other than 64 bits is rogue, and the host should not accept the prefix information.

4. Update to RFC 4861

If approved, this draft adds the following sentence and updates Section 6. of RFC 4861.

A host SHOULD NOT accept a prefix length shorter than 64.

5. Security Considerations

The purpose of this document is to mitigate adverse effects caused by a rogue RA. Limitation of the prefix length as described in Section 4.

6. Acknowledgements

Many thanks to Tatsuya Hayashi, Yuji Suga and Katsushi Kobayashi for many comments.

7. Normative References

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

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing
           Architecture", RFC 4291, DOI 10.17487/RFC4291, February
           2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman,
           "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861,
           DOI 10.17487/RFC4861, September 2007, <https://www.rfc-
           editor.org/info/rfc4861>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless
           Address Autoconfiguration", RFC 4862, DOI 10.17487/
           RFC4862, September 2007, <https://www.rfc-editor.org/
           info/rfc4862>.

Authors' Addresses

Akimichi Ogawa
Professional writer

Email: akimichi@sfc.wide.ad.jp

Kaname Nishizuka
NTT Communications

Email: kaname@nttv6.jp

Yoshifumi Atarashi
Alaxala Networks Co.

Email: atarashi@alaxala.net

Akira Kanai
NTT Communications

Email: a.kanai@ntt.com