IPv6 Maintenance
Internet-Draft
Intended status: Standards Track
Expires: January 14, 2021

J. Li
J. Fu
X. Li
Y. Cheng
China Mobile

July 13, 2020

IPv6 hosts detection
draft-li-6man-6hosts-detection-00

Abstract

The management of hosts and risks is important for enterprises that have large scale IP space. For IPv4, it won't take too long even to scan the entire Internet address space. For IPv6, further consideration is needed. A narrow range of IPv6 address is preferred for scanning. And in order to shorten the time for IPv6 scanning, a very specific IPv6 address list is highly needed.

This document proposes a solution to solve the problem. At first, append the information of the collection point address to the Router Advertisement packet sent by the router, and announce this address information to all nodes in the subnet. Then, each host node report its own IPv6 address information to the designated collection point by using Echo Reply message. After that, the corresponding collection point device should save these information. In this way, online IPv6 address information in the current network can be quickly collected on the collection point device.

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 [RFC2119][RFC8174].

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 14, 2021.

Table of Contents

1. Introduction

IP scanning is widely used in cybersecurity to find out online hosts and detect risks. Detection for online IPv6 hosts quickly and effectively is much more complicated than IPv4. Complications arise both from IPv6's address assignment features, e.g., stateless address

autoconfiguration (SLAAC, [RFC4862]), and from the large scale IP space. The management of IPv6 hosts is difficult. This document proposes a solution to shorten the time to scan IPv6.

2. Terminology

This document uses the terminology defined in [[RFC4443]] and [[RFC4861]].

Host – any node that is not a router.

Router – a node that forwards IP packets not explicitly addressed to itself.

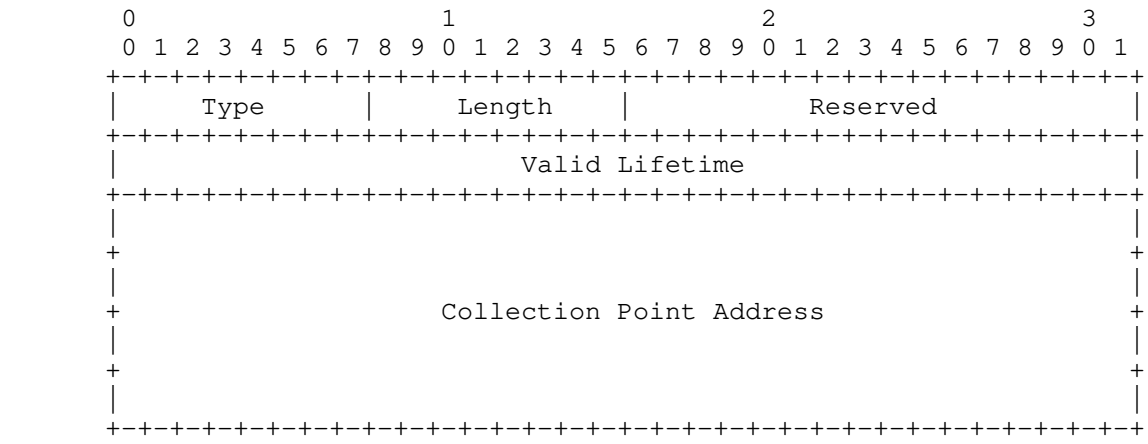
Node – a device that implements IP.

In addition, there is a new term that is defined below.

Collection Point – a device with a global IPv6 address that can store information.

3. Message Formats

3.1. Router Advertisement Option Formats



Fields:

Type 39. It is 8-bit identifier of the Collection Point option type.

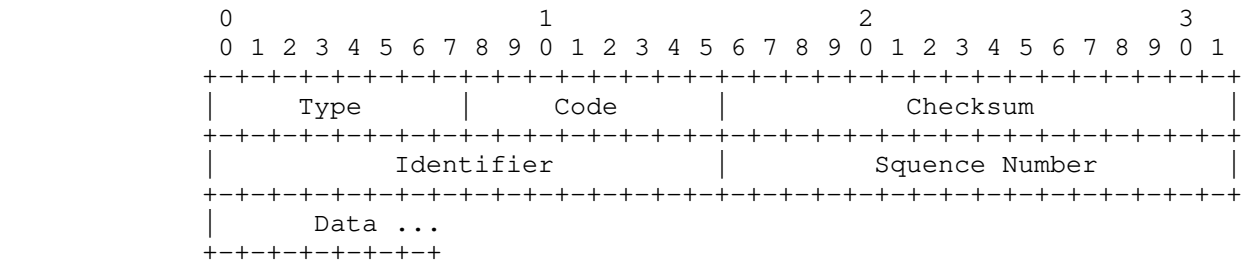
Length 3.

Reserved This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Valid Lifetime 32-bit unsigned integer. The length of time in seconds (relative to the time the packet is sent) that the address is valid for the purpose of on-link determination. A value of all one bits (0xffffffff) represents infinity.

Collection Point Address
A 128-bit IPv6 address of the Collection Point.

3.2. Echo Reply Message Format



IPv6 Fields:

Destination Address	A 128-bit IPv6 address of the Collection Point.

ICMPv6 Fields:

Type	129
Code	0
Identifier	0xffff
Sequence Number	1
Data	Special tag content is set. The default value is COLLECTION ONLY

4. Online Address Collection

4.1. Router Specification

4.1.1. Router Configuration Variables

AdvCollectionPoint

A global IPv6 address to be placed in Collection Point Information options in Router Advertisement messages sent from the interface.

Default: all Collection Point that the router advertises via routing protocols as being on-link for the interface from which the advertisement is sent.

The link-local address SHOULD NOT be included in the list of advertised address.

Each Collection Point has an associated:

AdvValidLifetime

The value to be placed in the Valid Lifetime in the Collection Point Information option, in seconds. The designated value of all 1's (0xffffffff) represents infinity.

Implementations MAY allow AdvValidLifetime to be specified in two ways:

- a time that decrements in real time, that is, one that will result in a Lifetime of zero at the specified time in the future, or

- a fixed time that stays the same in consecutive advertisements.

Default: 2592000 seconds (30 days), fixed(i.e., stays the same in consecutive advertisements).

4.1.2. Router Advertisement Message Content

The details of the technical part of Router Advertisement of the router are the same as the relevant provisions in RFC 4861. When there is a Collection Point Address in the router, the router should carry the content information of Collection Point Address in the option of the Router Advertisement Message, with the message format given in Section 3.1.

4.2. Host Specification

4.2.1. Processing Received Router Advertisements and Sending Echo Reply

When a host receives the Router Advertisement sent by the router, and finds that there is the information of Collection Point Address in the Router Advertisement, the host delays a random time, and then an Echo Reply should be sent to Collection Point.

The specific information of the Echo Reply packet is as follows. The destination address is the Collection Point Address, and the source address is the global unicast address of the host.

The Data in the Echo Reply packet contains special tag content, which is COLLECTION ONLY defined in Section 3.2.

The frequency of the Echo Reply packet sent by the host is the same as the frequency of receiving valid Router Advertisement packets which contains the information of Collection Point Address

When the host interface is used as a router in any other network, the device needs to transfer the information of Collection Point Address received by the host to its AdvCollectionPoint parameter as a router node

4.3. Collection Point Specification

When the Collection Point receives an Echo Reply packet while it doesn't actively send any Echo Request packet, it should extract the source address of this Echo Reply packet, which should be a global unicast address. And save the source address by attaching the current system timestamp.

5. Security Considerations

Because RAs are required in all IPv6 configuration scenarios, on IPv6-only networks, RAs must already be secured -- e.g., by deploying an RA-Guard [[RFC6105]]. Providing all configuration in RAs reduces the attack surface to be targeted by malicious attackers trying to provide hosts with invalid configuration, as compared to distributing the configuration through multiple different mechanisms that need to be secured independently.

Connectivity to destinations reachable over IPv6 would not be impacted just by providing a host with an incorrect Collection Point address; however, if attackers are capable of sending rogue RAs, they can perform denial-of-service or man-in-the-middle attacks, as described in [[RFC6104]].

6. IANA Considerations

IANA has assigned a new IPv6 Neighbor Discovery Option type for the Collection Point option defined in this document in the "IPv6 Neighbor Discovery Option Formats" registry [IANA].

Description	Type
Collection Point option	39

Table 1: New IANA Registry Assignment

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>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-editor.org/info/rfc4443>.

[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>.

[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>.

7.2. Informative References

[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>.

[RFC6104] Chown, T. and S. Venaas, "Rogue IPv6 Router Advertisement Problem Statement", RFC 6104, DOI 10.17487/RFC6104, February 2011, <https://www.rfc-editor.org/info/rfc6104>.

[RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105, DOI 10.17487/RFC6105, February 2011, <https://www.rfc-editor.org/info/rfc6105>.

Authors' Addresses

Jiang Li
China Mobile
Beijing 100053
China

Email: lijiang@chinamobile.com

Jun Fu
China Mobile
Beijing 100053
China

Email: fujun@chinamobile.com

Xiaoxiao Li
China Mobile
Beijing 100053
China

Email: lixiaoxiao@chinamobile.com

Yexia Cheng
China Mobile
Beijing 100053
China

Email: chengyexia@chinamobile.com