6man
Internet-Draft
Intended status: Standards Track
Expires: December 10, 2018

R. Bonica
Juniper Networks
J. Leddy
Comcast

June 8, 2018

The IPv6 Unrecognized Option
draft-bonica-6man-unrecognized-opt-01

Abstract

This document describes a method by which a source node can determine whether the underlying network can a) convey a packet that contains IPv6 destination options from itself to a destination node, and b) convey an ICMPv6 Parameter Problem message in the reverse direction.

In order to support this method, this document defines a new IPv6 option, called the Unrecognized option. The Unrecognized option is not recognized by any destination node and always elicits an ICMPv6 Parameter Problem message.

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 December 10, 2018.

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

Table of Contents

1. Introduction 2
2. Requirements Language 3
3. The Unrecognized Option 4
4. Application 4
5. Non-Implementation 5
6. Security Considerations 5
7. IANA Considerations 6
8. Acknowledgements 6
9. References 6
9.1. Normative References 6
9.2. Informative References 6
Authors' Addresses 7

1. Introduction

In IPv6 [RFC8200], optional internet-layer information is encoded in extension headers that are placed between the IPv6 header and the upper-layer header. Two of the extension headers specified in [RFC8200], the Hop-by-Hop Options header and the Destination Options header, carry a variable number of "options". Each option contains the following fields:

- o Option Type - 8-bit identifier of the type of option.

- o Opt Data Len - 8-bit unsigned integer. Length of the Option Data field of this option, in octets.

- o Option Data - Variable-length field. Option-Type-specific data.

The Option Type identifiers are encoded so that their highest-order 2 bits specify the action that must be taken if the processing IPv6 node does not recognize the option. Actions follow:

- o 00 - Skip over this option and continue processing the header.

- o 01 - Discard the packet.

- o 10 - Discard the packet and, regardless of whether or not the packet's Destination Address was a multicast address, send an

ICMPv6 [RFC4443] Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

- o 11 - Discard the packet and, only if the packet's Destination Address was not a multicast address, send an ICMPv6 Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

Several upper-layer protocols [RFC6275] [I-D.leddy-6man-truncate] emit packets that contain IPv6 destination options. These protocols rely the underlying network to forward packets that contain IPv6 destination options.

A subset of those protocols emit IPv6 destination options with high-order bits equal to "10" and "11". These IPv6 destination options elicit ICMP Parameter Problem messages from destination nodes that do not recognize them. The above-mentioned protocols perform better when the network can convey ICMPv6 Parameter Problem messages from the destination node to the source node.

Operational experience [RFC7872] reveals that a significant number of networks drop packets that contain IPv6 destination options. Likewise, many networks drop ICMP Parameter Problem messages.

This document describes a method by which a source node can determine whether the underlying network can:

- o Convey a packet that contains IPv6 destination options from itself to a destination node.

- o Convey an ICMPv6 Parameter Problem message in the reverse direction.

In order to support this method, this document defines a new IPv6 option, called the Unrecognized option. The Unrecognized option is not recognized by any destination node and always elicits an ICMPv6 Parameter Problem message.

2. 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.

3. The Unrecognized Option

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Option Type  |  Opt Data Len |    Option Data
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Figure 1

Figure 1 depicts the Unrecognized Option.

Option fields are as follows:

- o Option Type - Unrecognized Option. Value TBD by IANA. See Notes below.

- o Opt Data Len - Length of Option Data, measured in bytes.

- o Option Data - MUST be set to zero on transmission. MUST be ignored on receipt.

The Unrecognized option MUST NOT be implemented on any node. It must be unrecognized on all nodes so that it elicits an ICMP Parameter Problem message.

NOTE 1: The highest-order two bits of the Option Type (i.e., the "act" bits) are 10. These bits specify the action taken by a destination node that does not recognize Unrecognized option. The required action is to discard the packet and, regardless of whether or not the packet's Destination Address was a multicast address, send an ICMPv6 Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

NOTE 2: The third highest-order bit of the Option Type (i.e., the "chg" bit) is 0. This indicates that Option Data cannot be modified along the path between the packet's source and its destination.

4. Application

Upper-layer protocols execute the following procedure:

- o Set a short timer (e.g., two or three seconds).

- o Send a probe packet.

- o Wait for either a) timer expiration or b) an ICMPv6 Parameter Problem message that matches the probe packet.

The probe packet contains an IPv6 Destination Options header and the IPv6 Destination Options header contains an Unrecognized option. The Unrecognized Option MAY contain option data of any length. In order to influence how the packet is routed to its destination, the probe packet MAY contain upper-layer headers. However, because the packet contains the Unrecognized option, it is always discarded and is never delivered to an upper-layer protocol.

An ICMPv6 Parameter Problem message matches a probe packet if the initial bytes of the probe packet appear in the ICMP Parameter Problem message.

If the timer expires, one or both of the following is true:

- o The underlying network cannot convey a packet that contains IPv6 destination options from itself to a destination node.

- o The underlying network cannot convey an ICMPv6 Parameter Problem message in the reverse direction

If a matching ICMPv6 Parameter Problem arrives, both of the following are true:

- o The underlying network can convey a packet that contains IPv6 destination options from itself to a destination node.

- o The underlying network can convey an ICMPv6 Parameter Problem message in the reverse direction

5. Non-Implementation

A stated above, the Unrecognized option MUST NOT be implemented on any node. It must be unrecognized on all nodes so that it elicits an ICMP Parameter Problem message.

The sole purpose of this document is to reserve a IPv6 Option Type, so that the procedures described in Section 4, can be executed without using an unassigned Option Type.

6. Security Considerations

Because this document introduces no new functionality, it introduces no new security vulnerabilities.

7. IANA Considerations

IANA is requested to allocate a codepoint from the Destination Options and Hop-by-hop Options registry (https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml#ipv6-parameters-2). This option is called "Unrecognized". The "act" bits are 10 and the "chg" bit is 0.

8. Acknowledgements

Thanks to Ross Callon for his careful review of this document.

9. References

9.1. 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>.

[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>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

9.2. Informative References

[I-D.leddy-6man-truncate] Leddy, J. and R. Bonica, "Destination Originates Internet Control Message Protocol (ICMP) Packet Too Big (PTB) Messages", draft-leddy-6man-truncate-01 (work in progress), May 2018.

[RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <https://www.rfc-editor.org/info/rfc6275>.

[RFC7872] Gont, F., Linkova, J., Chown, T., and W. Liu, "Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World", RFC 7872, DOI 10.17487/RFC7872, June 2016, <https://www.rfc-editor.org/info/rfc7872>.

Authors' Addresses

Ron Bonica
Juniper Networks
2251 Corporate Park Drive
Herndon, Virginia 20171
USA

Email: rbonica@juniper.net

John Leddy
Comcast
1717 John F Kennedy Blvd.
Philadelphia, PA 19103
USA

Email: john_leddy@comcast.com