Abstract

This document describes how the experimental IPv6 Hop-by-Hop and Destinations Option types can concurrently support different experimental options. This is accomplished by employing a format in the Option Data for experimental option types. The format contains an experiment identifier that indicates an experimental option contained in the trailing Option Data. This approach is robust to experiments that are not registered and to those that do not use this sharing mechanism. It is recommended for all new Destination and Hop-by-Hop options that use experimental codepoints.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

Copyright (c) 2019 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 (http://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 ...................................................... 3
2 Requirements Language ......................................... 4
3 Hop-by-Hop and Destination Experimental Option Format .......... 4
   3.1 Selecting an ExID ........................................... 5
   3.2 Impact on Option Processing ................................ 6
   3.3 Interaction with the Authentication Header ................. 6
4 Reducing the Impact of False Positives .......................... 7
5 Migration to Assigned Options ................................... 7
6 Rationale .......................................................... 7
7 Security Considerations .......................................... 7
8 IANA Considerations ............................................... 7
9 References ........................................................ 9
   9.1 Normative References ..................................... 9
   9.2 Informative References .................................... 9
Author’s Address .................................................. 9
1 Introduction

IPv6 Hop-by-Hop and Destination Options extension headers contain lists of TLV (Type-Length-Value) options as the means to extend the IPv6 protocol and to enable new protocol capabilities [RFC8200]. This document describes how the experimental IPv6 Hop-by-Hop and Destinations Option experimental types can concurrently support different experimental options.

The space for identifying Hop-by-Hop and Destination options is small. An Option Type is eight bits, however the three high order bits are defined by [RFC8200] to hold a directive on what processing is to be done if the option is not recognized ("act" bits), as well as an indication of whether the Option Data is modifiable in flight ("chg" bit). Effectively, for a given combination of these three control bits there are only thirty-two possible types.

[RFC4727] defines experimental option types for Hop-by-Hop and Destination options. A single base option type is assigned with all possible values of the "act" and "chg" fields, resulting in eight distinct option type codes (types 0x1e, 0x3e, 0x5e, 0x7e, 0x9e, 0xbe, 0xde, and 0xfe). These values are intended for testing purposes or for use when an assigned codepoint is either not warranted or not available, e.g., based on the maturity status of the defined capability (i.e., Experimental or Informational, rather than Standards Track).

Here, the term "experimental IPv6 Hop-by-Hop and Destination options" refers to options that use the Hop-by-Hop or Destination experimental option codepoints [RFC4727]. Such experiments can be described in an RFC of any status (e.g., Experimental, Informational, etc.) and are intended to be used in controlled environments and are allowed in public deployments (when not enabled as default [RFC3692]). Nothing prohibits the deployment of multiple experiments in the same environment -- controlled or public. Furthermore, some protocols are specified in Experimental or Informational RFCs, which either include parameters or design choices not yet understood or which might not be widely deployed [RFC2026].

There is currently no mechanism to support shared use of the Hop-by-Hop and Destination experimental option codepoints. Different implementations use the same experimental option type for different purposes which results in collisions in which a single codepoint can be received at different times with different meanings intended by the sender.

The approach proposed in this document does not require additional Hop-by-Hop and Destination option codepoints and is robust to those
who choose either not to support it or not to register their experiments. The solution defines a field in the Option Data of experimental Hop-by-Hop and Destination options. This field is populated with an "experiment identifier" (ExID) defined as part of a specific option experiment. The ExID helps reduce the probability of a collision of independent experimental uses of the same option codepoint, both for those who follow this document (using registered ExIDs) and those who do not (squatters who either ignore this extension or do not register their ExIDs).

The solution proposed in this document is recommended for all new protocols that use Hop-by-Hop or Destination experimental option codepoints.

The techniques described in this document are adapted from [RFC6994] which describes the mechanism to concurrently support different experimental TCP options.

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] when, and only when, they appear in all capitals, as shown here.

3 Hop-by-Hop and Destination Experimental Option Format

Hop-by-Hop and Destination options share a common format [RFC8200], in which the first byte is the codepoint (Option Type) and the second byte is the length of the option data in bytes (Opt Data Len):

```
+-----------------------------+-
| Option Type | Opt Data Len | Option Data
+-----------------------------+-
```

This document extends the option format for experimental Hop-by-Hop and Destination option codepoints with an experiment identifier (ExID), which is four bytes in length. The ExID is used to differentiate experiments and is the first field after the Option Type and Opt Data Len, as follows:
3.1 Selecting an ExID

ExIDs are selected at design time, when the protocol designer first implements or specifies the experimental option. An ExID is thirty-two bits. The value is stored in the header in network-standard (big-endian) byte order. ExIDs combine properties of IANA registered codepoints with "magic numbers".

Use of the ExID helps reduce the probability of a false positive collision with those who either do not register their experiment or who do not implement this mechanism.

ExIDs are registered with IANA using "first come, first served" (FCFS) priority. ExIDs MUST be unique. It is RECOMMENDED to use random numbers with sufficient entropy and to avoid any values that might commonly be present in unrelated data (e.g. 0x1, 0xffffffff would be poor choices). The ExID value of 0x0 is reserved and MAY be used internally in an implementation to represent the absence of an ExID value.

The use of randomly assigned 32-bit identifiers in a sparsely populated space takes on the characteristics of a "magic number". A magic number is a randomized codepoint whose primary value is its unlikely collision with values selected by others [RFC6994].

A thirty-bit ExID maintains four byte alignment of the trailing Option Data. A common alignment requirement of Hop-by-Hop and Destination Options is 4n + 2, so maintaining four byte alignment reduces the potential for implementation errors, especially in using the same word-alignment padding, if the same implementation is later
modified to use a conventional codepoint.

3.2 Impact on Option Processing

The ExID number is part of the Hop-by-Hop or Destination Option Data. The presence of the ExID increases the effective Option Data Length field by the size of the ExID. The presence of an ExID is transparent to implementations that do not implement the experimental option types or the mechanism described here.

During receive processing, ExIDs in experimental options are matched against the ExIDs for each implemented protocol. If an ExID is not recognized, then the whole option is assumed to be unrecognized per the definition in [RFC8200]. The high order 2 bits of the Option Type specify the action in this case. If the action bits indicate that an ICMP error is warranted then an ICMP Parameter Problem, Code 2, is sent pointing to the first byte of the unrecognized ExID.

Although an ExID is in Option Data, it is considered to always be immutable in flight even if the change bit is set in the Option Type. Intermediate nodes MUST NOT modify an experimental identifier, or equivalently, intermediate nodes MUST NOT modify the first four bytes of Option Data in an option with an experimental Hop-by-Hop or Destination option type.

3.3 Interaction with the Authentication Header

When an Authentication header is present, the ExID in any experimental Hop-by-Hop or Destination option is included in the computation for authenticating a packet, regardless of whether the change bit is set. Specifically, the requirements of [RFC8200] are updated so that if the Hop-by-Hop or Destination option type is 0x3e, 0x7e, 0xbe, or 0xfe, and an authentication header is present in a packet, then the bytes in the Option Data field after the first four bytes MUST be treated as zero-valued octets when computing or verifying the packet’s authenticating value (note that the first four bytes of Option Data are not treated as zero-valued octets).

In a controlled environment, not on the public Internet for instance, this requirement MAY be relaxed at the discretion of the administrator in order to maintain backwards compatibility. In a controlled environment, for Hop-by-Hop and Destination option types 0x3e, 0x7e, 0xbe, or 0xfe, the first four bytes of the Option Data MAY be treated as zero-valued octets when computing or verifying the packet’s authenticating value. This SHOULD be controlled by configuration where the RECOMMENDED default is to always include the first four bytes in authentication calculations. Configuration can be system wide or selective based on matching the ExID (e.g. if a
receiver receives an experimental option with a known ExID it might include the ExID in calculations, otherwise it could zero the first four bytes for calculation). Note that the sender and receiver MUST agree on whether the ExID bytes are included or not included in calculations for authentication. Mechanisms to achieve such agreement are out of scope of this document.

4 Reducing the Impact of False Positives

False positives occur where the registered ExID of an experiment matches the value of an option that does not use ExIDs. Such collisions can cause an option to be interpreted by the incorrect processing routine. Experiments that are not robust to ExID false positives SHOULD implement other detection measures, such as checksums or minimal digital signatures over the experimental options they support.

5 Migration to Assigned Options

Some experiments may transition away from being experimental and become eligible for an assigned Hop-by-Hop or Destination option codepoint. This document does not recommend a specific migration plan to transition from use of the experimental Hop-by-Hop or Destination options/ExIDs to use of an assigned codepoint.

Once an assigned codepoint is allocated, use of an ExID represents unnecessary overhead. Therefore, once a Hop-by-Hop or Destination option codepoint is assigned to a protocol, that protocol SHOULD NOT continue to send the corresponding experimental option. An implementation MAY continue receiving the experimental option and MAY allow a fallback to sending the experimental option during some transition period to maintain backwards compatibility.

6 Rationale

The rationale for 32-bit ExIDs as a combination of an assigned value and a magic number is provided in section 6 of [RFC6994].

7 Security Considerations

The interaction between the mechanisms described in this document and the Authentication Header is described in section 3.3. Otherwise, the mechanism neither weakens nor enhances the existing security of Hop-by-Hop and Destination options.

8 IANA Considerations

IANA is requested to create an "IPv6 Hop-by-Hop and Destination
Option Experiment Identifiers (IPv6 Opt ExIDs) registry. The registry records 32-bit ExIDs, as well as a reference (description, document pointer, assignee name, and e-mail contact) for each entry. ExIDs are registered for use with any of the experimental Hop-by-Hop and Destination option codepoints (i.e. option types 0x1e, 0x3e, 0x5e, 0x7e, 0x9e, 0xbe, 0xde, and 0xfe).

Entries are assigned on a First Come, First Served (FCFS) basis [RFC5226]. The registry operates FCFS on the entire ExID (in network-standard order).

IANA will advise applicants of duplicate entries to select an alternate value, as per typical FCFS processing.

IANA will record known duplicate uses to assist the community in both debugging assigned uses as well as correcting unauthorized duplicate uses.

IANA should impose no requirements on making a registration other than indicating the desired codepoint and providing a point of contact. A short description or acronym for the use is desired but should not be required.

Initial assignments are:

```
+----------------+----------------+---------------+
|      ExI D     | Description    | Reference     |
|----------------+----------------+---------------+
| 0              | Invalid ExID, Implementation | This document |
|                | internal use    |               |
| 1..x0fffffff   | Unassigned      |               |
+----------------+----------------+---------------+
```
9 References

9.1 Normative References


9.2 Informative References


Author’s Address

Tom Herbert
Quantonium
Santa Clara, CA
USA

Email: tom@quantonium.net