IPv6 Diagnostic Header

draft-elkins-6man-ipv6-diagnostic-header-00.txt

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), 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/ietf/1id-abstracts.txt

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

This Internet-Draft will expire on January 4, 2012.

Copyright Notice

Copyright (c) 2011 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.

Abstract

The IPv4 main header contained a 16-bit IPID for fragmentation and reassembly. This field was commonly used by network diagnosticians for tracking packets on multi-tier networks. In IPv6, the IPID has been moved to the Fragment header. A new Diagnostic header for IPv6 which can be sent with every packet as a part of the Destination Options header with a 64-bit IPID is defined in this document.
1. Introduction

In IPv4, the 16 bit Identification field is located at an offset of 4 bytes into the IPv4 header and is described in RFC791 [RFC791]. In IPv6, it is a 32 bit field contained in the Fragment header defined by section 4.5 of RFC2460 [RFC2460]. Unfortunately, unless fragmentation is being done by the source node, the packet will not contain this Fragment header, and therefore will have no Identification field.

The intended purpose of the IPv4 Identification (ID) field is to enable fragmentation and reassembly, and as currently specified is required to be unique within the maximum segment lifetime (MSL) on all datagrams. The MSL is often 2 minutes.

In practice, the IPID field is used for more than fragmentation. Some TCP stacks have the same IPID counter for all connections; some have an IPID counter on a per connection basis. Each time a TCP stack sends out a packet, the IPID is incremented by one (or sometimes 2).

During network diagnostics, packet traces may be taken at multiple places along the path or at the source and destination. Then, packets can be matched by looking at the IPID. Obviously, the time at each device will differ according to the clock on that device; so another metric is required. This method of taking multiple traces along the path is frequently used on large multi-tier networks to see where the packet loss or packet corruption is happening.

Having said that, a known problem with the uniqueness of the IPv4 ID is that since the field is only 16 bits, then for high speed devices, wrapping will occur. As discussed in RFC4963 [RFC4963] and draft-ietf-intarea-ipv4-id-update-02.txt [Draft-ipv4-id], if the uniqueness requirement were strictly enforced, all connections would be limited to a maximum speed of 6.4 Mbps. Clearly, this uniqueness requirement is widely ignored.
In IPv6, the IPID field, which is in the Fragment header, has been increased to 32 bits. This may need to be reconsidered as data rates increase but if the IPID is used for fragmentation and reassembly alone, the requirement for uniqueness within the MSL period is generally not an issue today. RFC4963 [RFC4963] discusses the issue of reassembly errors at high data rates for IPv4 with a 16-bit counter.

However, for its de-facto diagnostic mode usage, an IPID needs to be available whether or not fragmentation occurs, and needs to be unique in the context of the entire session, and across all the connections controlled by the TCP stack. The problem of 32 bit counters is known and has been resolved in areas such as SNMP counters by creating 64-bit counters as described in RFC2233 [RFC2233].

This document will address a way to make the IPv6 IPID field available and unique for its valuable diagnostic usage. A Destination Options header is proposed which may be sent by TCP stacks in diagnostic mode. The implementation MAY provide the option of either turning on the Diagnostic Header for all connections or turn it on just for specific connections. The more sophisticated usage of this header would be to send it for a single connection only.

2. Conventions used in this document

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 [RFC2119].

3. Applicability

The base IPv6 standard, RFC2460, [RFC2460] allows the use of extension headers including destination options in order to encode optional destination information in an IPv6 packet. Extended diagnostic information such as this MUST be sent by implementations upon request. The proposed Diagnostic Options header is an implementation of the destination options header.
4. IPv6 Diagnostics Header Format

4.1 Destination Options Header

The Destination Options header is used to carry optional information that need be examined only by a packet’s destination node(s). The Destination Options header is identified by a Next Header value of 60 in the immediately preceding header, and has the following format:

```
+-------------------------------+-------------------+
|  Next Header     |  Hdr Ext Len     |
+-------------------------------+-------------------+
```

Next Header          8-bit selector. Identifies the type of header immediately following the Destination Options header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].

Hdr Ext Len          8-bit unsigned integer. Length of the Destination Options header in 8-octet units, not including the first 8 octets.

Options              Variable-length field, of length such that the complete Destination Options header is an integer multiple of 8 octets long. Contains one or more TLV-encoded options.

Figure 1: Destination Options Extension header layout

The desired action for a destination node who does not recognize this option is to ignore the header and continue processing the packet normally.

According to RFC2460 [RFC2460], if the Destination Options header Option Type has the value 00 in its highest-order two bits, the receiving device should skip over this option and continue processing the header.
4.2. IPv6 Diagnostic Header Option

The IPv6 Diagnostic Header option is carried by the Destination Option extension header (Next Header value = 60). It is used in a packet sent by a node to facilitate diagnostics by informing the recipient and passive viewers of the packet such as packet capture facilities of the packet’s IP Identifier.

The IPv6 Diagnostic Header option is encoded in type-length-value (TLV) format as follows:

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

Option Type

`nnn = 0xXX  [To be assigned by IANA] [RFC2780]`

Option Length

8-bit unsigned integer. Length of the option, in octets, excluding the Option Type and Option Length fields. This field MUST be set to 64.

Elkins                     Expires January 4, 2012           [Page 05]
IP Identifier

The IP Identifier of the packet for 64 bits.

The alignment requirement for the IP Identifier option is 8n+6.

The two highest-order bits of the Option Type field are encoded to indicate specific processing of the option; for the IP Identifier option, these two bits MUST be set to 00. This indicates the following processing requirements:

- 00 - skip over this option and continue processing the header.
- The data within the option cannot change en route to the packet’s final destination.

The IPv6 Diagnostic Header option MUST be placed as follows:

- After the routing header, if that header is present
- Before the Fragment Header, if that header is present
- Before the AH Header or ESP Header, if either one of those headers are present.

For each IPv6 packet header, the IPv6 Diagnostic Header MUST NOT appear more than once. However, an encapsulated packet MAY contain a separate IP Identifier option associated with each encapsulating IP header.

The inclusion of a IPv6 Diagnostic Header in a packet affects the receiving node’s processing of only this single packet. No state is created or modified in the receiving node as a result of receiving a IPv6 diagnostic Header in a packet.

4.3. Implementation Considerations

In implementation, a TCP stack may send this additional header for all connections or, in a more sophisticated usage, a single connection only.

We suggest that initiation of this header be done in a ‘Debug on’, ‘Debug off’ mode. That is, a diagnostician may decide that this header is required for a certain timeframe or for a certain set of packets after a network problem is encountered. The diagnostician may then issue a command to the TCP stack indicating that addition of the IP Identifier header should now begin. This is the ‘Debug on’ state. After a certain amount of time, then 'Debug off' should be issued as a command. Alternatively, the TCP stack may have a fixed time (for example, 5 minutes) after which debug mode will automatically be turned off.
5. Backward Compatibility

The scheme proposed in this document is backward compatible with all the currently defined IPv6 extension headers. According to RFC2460 [RFC2460], if the destination node does not recognize this option, it should skip over this option and continue processing the header.

6. Security Considerations

There are no security considerations.

7. IANA Considerations

A Destination Options value of XXX is pending IANA action. [RFC2780]

10. References

10.1. Normative References


See also: http://www.iana.org/assignments/ipv6-parameters

10.2. Informative References


11. Acknowledgments

The authors would like to thank Fred Baker, Bill Jouris, Jose Isidro and James Ashton for their reviews and suggestions that made this document better.

This document was prepared using 2-Word-v2.0.template.dot.

Authors’ Addresses

Nalini Elkins
Inside Products, Inc.
36A Upper Circle
Carmel Valley, CA
United States

Phone: +1 831 659 8360
Email: nalini.elkins@insidethestack.com

Lawrence Kratzke
IBM
8121 Glenbrittle Way
Raleigh, NC 27615
United States

Phone: +1 800-876-8801
Email: kratzke@us.ibm.com

Michael Ackermann
Blue Cross Blue Shield of Michigan
P.O. Box 2888
Detroit, Michigan 48231
United States

Phone: +1 310 460 4080
Email: mackermann@bcbsmi.com