Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 4, 2017

B. Skeen
Boeing Phantom Works
E. King
Boeing EO&T IT
F. Templin, Ed.
Boeing Research & Technology
October 31, 2016

Including Geolocation Information in IPv6 Packet Headers (IPv6 GEO)
draft-skeen-6man-ipv6geo-03.txt

Abstract

This document provides a specification for including geolocation information in the headers of IPv6 packets (IPv6 GEO). The information is intended to be included in packets for which the location of the source node is to be conveyed via the network to the destination node or nodes.

Table of Contents

1. Introduction

Internet Protocol, version 4 (IPv4) [RFC0791] provides limited capabilities for including additional information in the headers of packets. The maximum IPv4 header length is 60 bytes including any IP options, and options are not widely used due to incompatibilities with network middleboxes. On the other hand, Internet Protocol, version 6 (IPv6) [RFC2460] includes an extensible header format whereby additional information can be inserted between the IPv6 header and the transport layer header. These extensions can be included on a per-packet basis, and not necessarily for all packets of the same flow. This document specifies a format for including geolocation information within the headers of individual IPv6 packets (IPv6 GEO).

IPv6 GEO information is included at the discretion of source nodes for the benefit of destination nodes and/or network elements that may need to examine the headers of packets in transit. Legacy destination nodes that do not recognize the IPv6 GEO information must ignore it and process the rest of the packet as if it were not present. The IPv6 specification defines several extension header types, including the Destination Options header. Section 4.6 of [RFC2460] describes conditions under which new information should be

encoded as either a new extension header or as a new destination option:

> "Note that there are two possible ways to encode optional destination information in an IPv6 packet: either as an option in the Destination Options header, or as a separate extension header. The Fragment header and the Authentication header are examples of the latter approach. Which approach can be used depends on what action is desired of a destination node that does not understand the optional information:"

Section 3 of [RFC6564] further states that:

> "The base IPv6 standard [RFC2460] allows the use of both extension headers and destination options in order to encode optional destination information in an IPv6 packet. The use of destination options to encode this information provides more flexible handling characteristics and better backward compatibility than using extension headers. Because of this, implementations SHOULD use destination options as the preferred mechanism for encoding optional destination information, and use a new extension header only if destination options do not satisfy their needs. The request for creation of a new IPv6 extension header MUST be accompanied by a specific explanation of why destination options could not be used to convey this information."

Our first interpretation of this guidance and the supporting text that follows suggests that, since IPv6 GEO information must be ignored by legacy destination nodes, encoding as a Destination Option is indicated. Further investigation and community input may indicate that a new extension header type is instead warranted. In either case, future versions of this document will adopt the encoding approach indicated by community consensus.

2. Terminology

The following terms are defined within the scope of this document:

IPv6 Geolocation (IPv6 GEO)
: a means for identifying the location of the source of an IPv6 packet based on geographical coordinates, altitude, timestamp and/or other information conveyed from the source to the destination(s).

3. Requirements

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]. When used in lower case (e.g., must, must not, etc.), these words MUST NOT be interpreted as described in [RFC2119], but are rather interpreted as they would be in common English.

IPv6 forwarding nodes must not discard packets that include the destination options specified herein unless by explicit administrative policy. General forwarding considerations for packets that contain IPv6 options are discussed in [I-D.ietf-opsec-ipv6-eh-filtering].

4. Motivation and Applicability

Traditionally, a given source node will include a set of identifying criteria that can be used to help determine the relative location of that node on the network. Such criteria include, but are not limited to, IP address, Ethernet MAC addresses, 802.11 or Bluetooth MAC addresses, Wifi and RFID tags, or other user-defined variables that may be specific to a given implementation. However, these variables are often unreliable in determining the physical location of a source node as modern networks are typically implemented with a logical "layer 2" structure without emphasis on the node’s physical location. Furthermore, variables such as IP address and Wifi RFID tags are commonly defined by a network administrator and are subject to the implementation criteria of a given network, and therefore are susceptible to error in identifying the location of a given node since there is no common mechanism for associating these criteria to a given physical location. In addition, the proliferation of portable and handheld mobile devices makes it increasingly likely that nodes will at some point change the point of attachment to a given network and will need to be identified and likely authenticated against a set of reliable location-based criteria.

In the absence of location-based authentication criteria, a host will typically be configured to require either local parameters, i.e., username and password, or a strong "two-factor" authentication mechanism, or both. Whereas the merit and applicability of these methods is outside the scope of this document, some implementations require an additional layer of authentication control based on the physical location of a given source node. As a result, a means for identifying the location of the source node based on the geographical coordinates, altitude, timestamp and/or other information is needed.

Numerous use cases can be identified for location-based authentication control that would require the source node to provide its current location to one or more destination node(s). The source node to be geolocated can be defined as any IPv6 GEO node capable of encoding the geolocation data within the IPv6 Destination Options header; for example, an airplane, an automobile, a remote corporate user, a ground soldier, or an unmanned aerial vehicle, to name a few. The destination node can be any IPv6 node that can interpret the IPv6 GEO encoded data contained in the Destination Options header; for example, an authentication server responsible for deriving the geolocation criteria received from the source node and authenticating it against a location-based access policy.

Potential use cases for IPv6 GEO include:

- A remote corporate user that requires an encrypted tunnel connection to a corporate VPN server must provide authentic location information. In addition to a two-factor authentication request, an IPv6 source node using IPv6 GEO would also encode its geolocation data into the authentication request to be sent to the corporate VPN server. The corporate VPN server would authenticate the specified location of the source node to the corporate policy that includes the list of approved locations for the source node on the corporate authentication server in order to accept the connection request.

- An expeditionary team may want to relay geolocation data to a mission control center in order to provide emergency response coordinates, humanitarian support vectors, new terrain characteristics, or as a means to coordinate the search of a large geographic region. Further, a method to authenticate the control messages sent from the expedition team leader to the control center may require that the geolocation authenticity of the messages be verified

- A first responder may require a rapidly deployable means of providing geolocation data to emergency teams engaged in rescuing lost or injured personnel or in coordinating the location of support personnel conducting a search over wide geographic areas. The ability to provide location awareness could provide the critical communication needed to reduce the time to contact in life-threatening emergency situations.

- Civil aviation Air Traffic Management (ATM) systems require a means for tracking the location of aircraft in their various phases of flight (both on the ground and in the sky). As ATM becomes increasingly dependent on data communications, the ability to associate an aircraft’s location with its communications

messaging can augment and in some instances replace mechanisms such as Automatic Dependent Surveillance - Broadcast (ADS-B).

- Unmanned Air Systems (UAS) are envisioned in a wide variety of use cases. IPv6 GEO information sharing for both ground control and UAS-to-UAS communications will naturally result in more effective fleet coordination and tracking.

- Automobiles and vehicles of all types are increasingly connected to the Internet. Comfort-enhancing entertainment applications, road safety applications using bidirectional data flows, and connected automated driving are but a few new features expected in automobiles to hit the roads from now to year 2020. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) use-cases where IP is well-suited as a networking technology, supporting also applications that involve exchanges of safety-related messages between vehicles and infrastructure if necessary.

- Space exploration vehicles must be tracked by control stations and other vehicles throughout all mission phases. Especially for deep space applications, an extraterrestrial location coordinate system may be needed.

- Convergence of dynamic routing protocols in a wide variety of mobile networks can benefit greatly from knowledge of the geographical locations of prospective neighbors. This information is best conveyed in the headers of IPv6 packets used for routing protocol control message exchanges.

- The networks that make up the greater "Internet," including all various forms of Intranets (Enterprises, small businesses, Service Providers, etc.) all need to manage those assets that constitute their administrative domain. Sometimes these networks are millions of dollars and all of the time are critical to business value. Being able to locate and place where these devices are located may mean actual dollar value to the businesses bottom line because of various tax and depreciation details that are variable, depending on which taxing authority these devices are located (City, State (Province), Country or any other various taxing authority in which the business provides value with those assets. Having a clear location, at any time has distinct advantages to the business as to where exactly those devices are, at any one time.

In these cases, the actual implementation of a geolocation authentication layer in a multi-layered security scheme is considered outside the scope of this document. This document seeks to specify a method for including the geolocation data in the IPv6 Destination

Options header in order for it to be utilized in the manner specified by a set of given implementation criteria.

In the final analysis, if a subject node that willingly submits itself for surveillance sends only a single IPv6 packet or fragment before falling silent, then any tracking node(s) should be able to determine where the packet came from.

5. IPv6 GEO Specification

5.1. IPv6 GEO Destination Option Format

The IPv6 GEO "Type 0" Destination Option is formatted as shown in Figure 1:

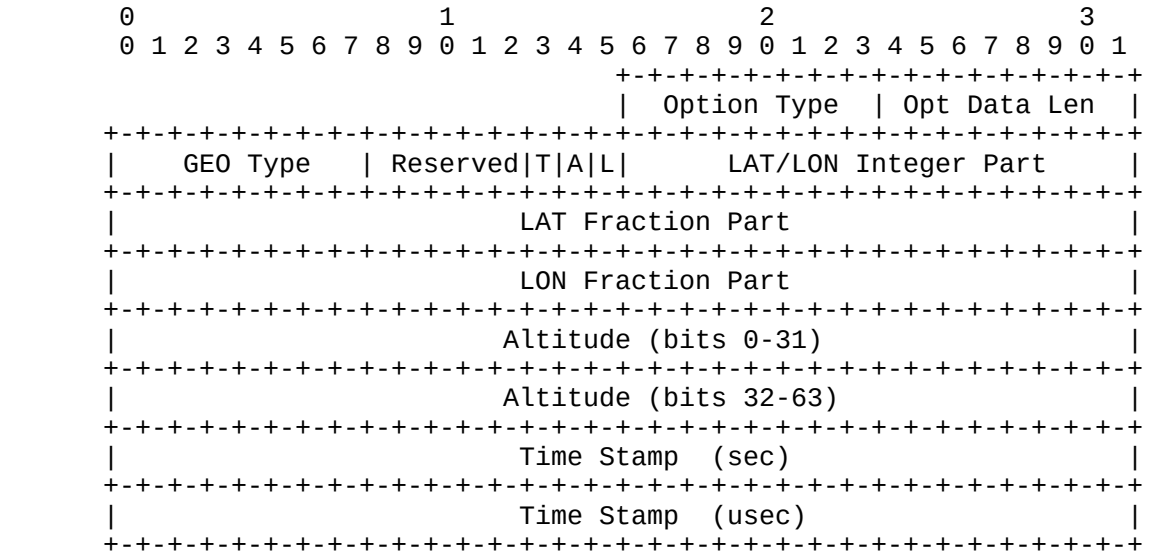

Figure 1: IPv6 GEO Type 0 Destination Option Format

The fields of the option are defined as follows:

Option Type (8)
: the IPv6 Option Type code for IPv6 GEO; to be assigned by IANA. The high order three bits of the Option Type encode the value '000' to indicate that the option is to be skipped over if not recognized, and that the data must not change en route (see: Section 4.2 of [RFC2460]).

Opt Data Len (8)
: the length of the data portion of the IPv6 GEO Option.

GEO Type (8)
the IPv6 GEO encoding type; set to 0 for the encapsulation format specified in this section.

Flags (8)
an 8-bit flags field. Contains a 5-bit Reserved field that is set to 0 on transmission and ignored on reception. The following three bits (T, A, L) are set to 1 if the corresponding GEO information fields are included and set to 0 otherwise.

LAT/LON Integer Part (16)
a 16 bit field that encodes the integer part of the Latitude and Longitude coordinates (see below). Included when 'L' is 1 and omitted when 'L' is 0.

LAT Fraction Part (32)
a 32 bit field that encodes the fractional part of the Latitude coordinate (see below). Included when 'L' is 1 and omitted when 'L' is 0.

LON Fractional Part (32)
a 32 bit field that encodes the fractional part of the Longitude coordinate (see below). Included when 'L' is 1 and omitted when 'L' is 0.

Altitude (64)
two 32-bit fields that together encode the altitude (in centimeters). Included when 'A' is 1 and omitted when 'A' is 0.

Time Stamp (sec) (32)
a 32 bit field that encodes the time that the IPv6 GEO data was generated in seconds since the epoch (00:00:00 UTC on 1 January 1970). Included when 'T' is 1 and omitted when 'T' is 0.

Time Stamp (usec) (32)
a 32 bit field that encodes the microseconds at the time that the IPv6 GEO data was generated. Included when 'T' is 1 and omitted when 'T' is 0.

In the language of Section 4.2 of [RFC2460], the option has alignment requirement '4n+2' when the 'L' flag is set and '4n' when the 'L' flag is clear. Future specifications may include new IPv6 GEO types to encode alternate formats.

5.2. IPv6 GEO Option Encoding Algorithm

The Latitude (LAT) and Longitude (LON) coordinate values are treated as floating point numbers with 10^-10 precision. LAT values range from 0 degrees at the equator to +90 degress northward and -90 degrees southward. LON values range from 0 degrees at the IERS Reference Meridian [WGS-84] to +180 degrees eastward and -180 degrees westward. The LAT/LON coordinates are then encoded as follows:

```
LAT/LON Integer Part = int(LAT+90)*360 + int(LON+180)

LAT Fraction Part = fra(LAT)*1,000,000,000

LON Fraction Part = fra(LON)*1,000,000,000
```

where "int()" returns the integer part of the floating point number and "fra()" returns the fractional part of the floating point number. This encoding scheme is similar to one proposed in "Efficient WGS84 (aka GPS) coordinates compression" [WGS-ENCODE].

5.3. IPv6 Node Requirements

IPv6 source hosts MAY insert the IPv6 GEO destination option in any IPv6 packets they send to IPv6 destinations (unicast, multicast or anycast). Any IPv6 packet is eligible, including a minimal packet that includes only an (extended) IPv6 header with the value "No Next Header" in the final "Next Header" field.

If the host inserts the IPv6 GEO destination option, it MUST construct the option using the format specified in Section 5.1 and using the encoding algorithm specified in Section 5.2. The host MUST further ensure that the geolocation information encoded in the option is current and accurate.

IPv6 destinations that do not recognize the IPv6 GEO destination option MUST ignore it and continue to process the IPv6 destination options extension header as though the IPv6 GEO option were not present.

6. IANA Considerations

IANA is requested to allocate an IPv6 Option number for the IPv6 GEO Option in the "Destination Options and Hop-by-Hop Options" registry.

7. Security Considerations

Packets with IPv6 GEO options that are sent in the clear without encryption risk exposure of sensitive information to unauthorized eavesdroppers. When location privacy is desired, Internet security protocols (e.g., IPsec [RFC4301], etc.) and/or link layer security SHOULD be used to ensure confidentiality.

A spoofing attack is exposed when a source includes forged IPv6 GEO information that is incorrect for its current location and/or time. Destinations SHOULD therefore authenticate the source of IPv6 packets before accepting any IPv6 GEO information they may include.

User agents MUST NOT send geolocation information to unauthorized correspondents (e.g., Web sites, etc.) without the express permission of the user.

8. Related Work in the IETF

The IETF GEOPRIV working group is chartered to "continue to develop and refine representations of location in Internet protocols, and to analyze the authorization, integrity, and privacy requirements that must be met when these representations of location are created, stored, and used". However, the group is located within the Real-time Applications and Infrastructure area, and as such it is not clear whether the Internet layer approach proposed in this document would fit within the area focus. The GEOPRIV working group has published a BCP on "An Architecture for Location and Location Privacy in Internet Applications" [RFC6280].

A BoF on "Internet-wide Geo-Networking (geonet)" was held at IETF88 in November 2013. A Problem Statement related to the BoF states that: "Internet-based applications use IP addresses to address a node that can be a host, a server or a router. Scenarios and use cases exist where nodes are being addressed using their geographical location instead of their IP address" [I-D.karagiannis-problem-statement-geonetworking]. This BoF was held within the Internet area and concerns geolocation at the Internet layer.

As a result of the geonet BoF, a new working group known as ’Intelligent Transportation Systems (its) is undergoing chartering activities. It is expected that IPv6GEO will be closely related to the its charter.

9. Implementation Status

A prototype implementation has been developed and tested, but not yet available for public release. The prototype implementation uses the Option Type value reserved for experimentation [RFC3692].

10. Contributers

The authors greatly appreciate the efforts of Jin Fang, who jointly developed the IPv6 GEO message format and was the primary author of the prototype implementation. We wish Jin the best of success in his future endeavors.

11. Acknowledgments

The following individuals are acknowledged for helpful comments and suggestions: Jeff Ahrenholz, Kerry Hu.

12. References

12.1. Normative References

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <http://www.rfc-editor.org/info/rfc791>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[RFC3692] Narten, T., "Assigning Experimental and Testing Numbers Considered Useful", BCP 82, RFC 3692, DOI 10.17487/RFC3692, January 2004, <http://www.rfc-editor.org/info/rfc3692>.

[RFC6564] Krishnan, S., Woodyatt, J., Kline, E., Hoagland, J., and M. Bhatia, "A Uniform Format for IPv6 Extension Headers", RFC 6564, DOI 10.17487/RFC6564, April 2012, <http://www.rfc-editor.org/info/rfc6564>.

12.2. Informative References

[I-D.ietf-opsec-ipv6-eh-filtering]
Gont, F., LIU, S., and R. Bonica, "Recommendations on Filtering of IPv6 Packets Containing IPv6 Extension Headers", draft-ietf-opsec-ipv6-eh-filtering-01 (work in progress), July 2016.

[I-D.karagiannis-problem-statement-geonetworking]
Karagiannis, G., Heijenk, G., Festag, A., Petrescu, A., and A. Chaiken, "Internet-wide Geo-networking Problem Statement", draft-karagiannis-problem-statement-geonetworking-01 (work in progress), November 2013.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <http://www.rfc-editor.org/info/rfc4301>.

[RFC6280] Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications", BCP 160, RFC 6280, DOI 10.17487/RFC6280, July 2011, <http://www.rfc-editor.org/info/rfc6280>.

[WGS-84] Wikipedia, W., "World Geodetic System (http://en.wikipedia.org/wiki/World_Geodetic_System)", November 2013.

[WGS-ENCODE]
Dupuis, L., "Efficient WGS84 (aka GPS) Coordinates Compression (http://www.dupuis.me/node/35)", August 2013.

Authors' Addresses

Brian Skeen
Boeing Phantom Works
P.O. Box 3707
Seattle, WA 98124
USA

Email: brian.l.skeen@boeing.com

Edwin King
Boeing EO&T IT
P.O. Box 3707
Seattle, WA 98124
USA

Email: edwin.e.king@boeing.com

Fred L. Templin (editor)
Boeing Research & Technology
P.O. Box 3707
Seattle, WA 98124
USA

Email: fltemplin@acm.org