

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: December 15, 2014

Georgios Karagiannis
University of Twente
Alexandru Petrescu
CEA
Dimitri Papadimitriou
Alcatel-Lucent
Bastiaan Wissingh
TNO
June 15, 2014

**Problem Statement for Internet-wide Geo-networking
draft-karagiannis-geonet-problem-statement-00**

Abstract

This document describes the need of intertwining of IP networking with geographical addressing. As used today, IP routing and addressing are completely unaware of geographic parameters such as coordinates or postal addresses. Possible applications of future Internet-wide geo-networking mechanisms include, but are not limited to, dissemination of IP packets to geographical areas, or precise tracking of package positions during a shipping process, with more use-cases under discussion.

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 <http://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 15, 2014.

Copyright Notice

Copyright (c) 2014 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.

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 [RFC 2119](#) [[RFC2119](#)].

Table of Contents

1.	Introduction	2
2.	Challenges and main goal	4
3.	Internet-wide Geo-networking use cases	5
4.	Assumptions and Requirements	6
5.	Relationships between GeoNet and other IETF Working Groups . .	8
6.	Security Considerations	9
7.	IANA Considerations	9
8.	Acknowledgments	9
9.	Normative References	9
10.	Informative References	9
11.	Authors' Address	10
12.	Contributors	10

[1.](#) Introduction

Internet-based applications are currently using IP addresses to address interfaces of a node that can be for example a host, a server or a router. IP routing and addressing are completely unaware of geographic parameters such as coordinates or postal addresses.

Future applications and use cases have been identified that need to support among others the (1) dissemination IP packets to geographical areas, (2) precise tracking of package positions during a shipping process, (3) dissemination of traffic safety, traffic efficiency & management, and infotainment type of vehicular information to fixed and mobile Road Side Units (RSUs) through the Internet, (4) tracking and communicating with people or objects located in certain geographical areas, e.g., Oiler Riggers, where Oil companies want to track employees in the field, where the conditions can be dangerous and the employee's safety needs to be verified.

In order to support such future applications and use cases Internet-wide Geo-networking solutions need to be specified within the context of the new and to be started GeoNet IETF working group.

Internet-wide Geo-networking can be considered as the solution space that includes mechanisms and protocols used to disseminate packets sent by authorized source nodes located anywhere in the Internet to other nodes in areas described by geographical parameters.

An example scenario that can be used for the support of Internet-wide geo-networking is shown in Figure 1. This scenario

shows a source node, which can be located anywhere in the Internet, and is interconnected with access routers via the Internet. The packets generated by the source are disseminated through the Internet to other nodes in areas described by geographical parameters.

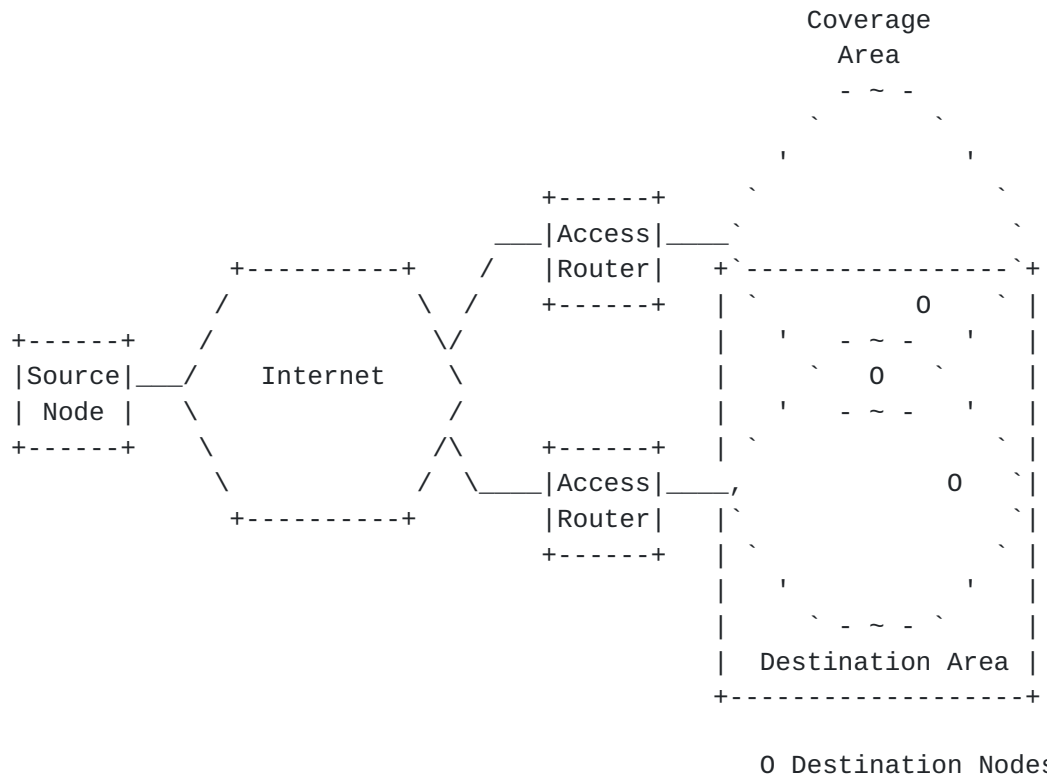


Figure 1: Internet-wide geo-networking scenario

1.2. Terminology

Internet-wide Geo Networking

the solution space that includes mechanisms and protocols used to disseminate packets sent by authorized source nodes located anywhere in the Internet to other nodes in areas described by geographical parameters.

Geographic coordinate system:

a coordinate system that enables every location on the Earth to be specified by a set of numbers or letters.

Road Side Unit (RSU)

equipment located along highways, at traffic intersections and other type of locations where timely communications with vehicles are needed. Each RSU includes DSRC (Direct Short Range Radio, e.g., IEEE 802.11p) radio, a positioning system and a router to route packets back through the infrastructure network. RSU is also known as RSE (Road Side Equipment)

Traffic safety application

application that is primarily applied to decrease the probability

of traffic accidents and the loss of life of the occupants of vehicles.

Traffic efficiency & management application:

application that is primarily applied to improve vehicle traffic flow, traffic coordination and traffic assistance and provide updated local information, maps and in general, messages of relevance bounded in space and/or time

Infotainment applications:

all other types of Internet based applications, for example media downloading

1.4. Organization of This Document

This document is organized as follows. [Section 2](#) describes several challenges and open issues associated with Internet-wide Geo-networking solutions. Furthermore, [Section 2](#) emphasizes the main goal of the GeoNet IETF working group. [Section 3](#) provides a brief description of Internet-wide Geo-networking use cases. [Section 4](#) lists the Internet-wide Geo-networking assumptions and requirements. The relationships between GeoNet and other IETF working groups are given in [Section 5](#). [Section 6](#) describes the security considerations. The IANA considerations are listed in [Section 7](#). [Section 8](#) provides the acknowledgements.

2 Challenges and main goal

2.1 Challenges and open issues

The challenges and open issues that need to be addressed by Internet-wide Geo-networking solutions are:

- o) Mechanisms and protocol solutions are needed for the accurate (i.e., precise and up to date) representation of geographic areas using (1) geo-locators such as names and (2) geographic coordinates.
- o) Mechanisms and protocol solutions are needed to ensure that geographical area information (e.g. geo-locators, names, geographic coordinates) is accurately mapped to an IP locator, i.e. an IP address. Mapping data bases can be maintained at the source nodes, intermediate or edge nodes, and at specific IP locator nodes.
- o) Mechanisms and protocol solutions are needed to ensure that the IP addresses of access routers, Road Side Units (RSUs), and so on can be accurately mapped to geographic area information (geo-locators, names, and geographic coordinates). Mapping data bases

can be maintained at the source nodes, intermediate or edge nodes,
and at specific IP locator nodes.

- o) Mechanisms and protocol solutions are needed to ensure that data packets generated by source nodes placed arbitrarily in the Internet can be disseminated over multiple hops by using, where possible, geographic coordinates of (1) the destination node(s) and/or (2) the intermediate nodes for the routing decisions, instead of using their IP addresses. Note that in order to solve the above challenge it is NOT mandated that all nodes located on the path from source to destination nodes are able to forward packets using the geo-coordinates of (1) the destination node(s) and/or (2) the intermediate nodes for the routing decisions. This is emphasized by using the words "where possible".

2.2 Goal

Mechanisms and IETF protocols are needed for authorized source nodes anywhere in the Internet to disseminate packets to other nodes in areas described by geographical parameters, all while respecting privacy concerns of sender and receiver. Parameters such as geographical coordinates and other geo-locators such as civic addresses should be used.

3. Internet-wide Geo-networking use cases

This section provides a brief description of the Internet-wide Geo-networking use cases. The detailed description of each of these use cases is provided in separate Internet drafts.

3.1 Dissemination of IP packets to geographical areas

A source node, which may be located anywhere, sends packets to an access router through the Internet. Those access routers are selected based on geographical location information, and traffic is routed to them using the IP address of the router and conventional IP routing. Each of the destination access routers then copies and broadcasts the received packets to listeners within its (1) radio coverage for wireless access routers or (2) IP subnet for wired access routers.

3.2 Precise tracking of package positions during a shipping process

A good delivered by a shipping organization has a provider independent IP address. This good is tracked in that its geographical position is known to end-users continuously throughout the entire delivery process. The IP address of the good is associated to the geographical coordinates of the router to which it connects. Using IP addresses enables very finely grained and precise tracking. An important issue that needs to be taken into consideration in this use case is the protection of privacy, i.e., provide confidentiality to personal data and protect leaking information through protocol

behavior, such as relation between identifier and location.

3.3 Dissemination of ITS (Intelligent Transportation System) information to fixed and mobile RSUs via Internet

Karagiannis, et al. Expires December 15, 2014

[Page 5]

In this use case traffic safety, traffic efficiency & management, and infotainment type of vehicular information is disseminated to fixed and mobile Road Side Units (RSUs) through the Internet. Most RSUs are placed at a fixed geographical location that will most likely not be

changed until the device either reaches its end of life or is no longer needed at that location. A so called 'Mobile RSU' on the other hand is portable and not "torn down" while moving, meaning that among other settings its geographical position adjusts according to the location where it is positioned. Such a 'Mobile RSU' is very flexible for use in multiple situations. Examples of such situations include the case that a permanently installed unit fails and needs a temporarily backup unit or during road construction. In the latter case, a road worker could take a Mobile RSU, position it somewhere at the road works site, and start sending warning messages to approaching vehicles. The next day the mobile RSU can be positioned elsewhere. The protection of privacy is an important issue for this use case and needs to be taken into consideration.

3.4 Tracking and communicating with people or objects located in certain geographical areas

Companies, like Oil companies want to track employees in the field, where the conditions can be dangerous and the employee's safety needs to be verified. Such a dangerous situation can be the explosion (or the high risk of explosion) of an Oil rigger. In such a situation the Oil company needs to be able to disseminate recovery instructions to all employees that are within a certain radius of the explosion (e.g., 1 mile).

4. Assumptions and Requirements

This section includes the assumptions and the requirements that need to be fulfilled by Internet-wide Geo-networking solutions.

4.1 Assumptions

The assumptions associated with the Internet-wide geo-networking solutions are:

- o) The destination nodes can be static or moving entities, such as hosts, vehicles, goods sensors and actuators, that are spread in a certain target/destination geographic area.
- o) existing IETF mechanisms and protocols like the ones specified and standardized by the IETF WGs: LISP [[LISP](#)], GEOPRIV [[GEOPRIV](#)], ECRIT [[ECRIT](#)] will be taken into consideration during the design phase.

- o) The document "ISO 19107: Geographic information - Spatial Schema" [[ISO19107](#)] will be considered for the representation of spatial characteristics of geographic features (including geometries), and a set of spatial operations consistent with these schemas. This document treats of vector geometry and topology of up to three dimensions. Geometries range from point, multipoint, to polygon, to Bezier curves and to Clothoids.
- o) Documents from IEEE P1609.2 [[IEEE1609.2](#)] may be considered for security and privacy support on IEEE 802.11p [[IEEE802.11p](#)] links.

4.2 Requirements

The specified Internet-wide geo-networking mechanisms and protocol solutions:

- o) SHOULD ideally support IPv4 and IPv6
- o) MUST at a minimum support IPv6
- o) MUST be able to use and insert geographic area information for selection of receivers
- o) MUST be able to disseminate the information from senders to the destination nodes located in the destination geographic area in a point to multipoint manner.
- o) SHOULD be able to scale, leveraging stable and deterministic under-layers when available, and maintain its performance and precision to acceptable levels even if it is applied in contexts of:
 - (1) global coverage with small destination geographic areas,
 - (2) large traffic volumes or large flows,
 - (3) large number of simultaneously active sources.
- o) MUST be able to provide accurate representation of geographic areas using: (1) standardized geo-locators where available and/or (2) geographic physical coordinates.
- o) MUST be able to ensure that geographical area information (geo-locators, names and geographic physical coordinates) is accurately mapped to an IP address, even if the relation between geographical area information and IP address is not a one-to-one relationship.
- o) MUST be able to ensure that an IP address can be accurately

mapped to a geographic area information (geo-locators, names and geographic physical coordinates), even if the relation between locator and geographical information is not a one-to-one relationship.

- o) MUST be able to ensure that the used mapping data bases of IP locators to a geographic area information are up to date.
- o) MUST support security and privacy: Given the sensitivity of location data and the possibility of the technology being used in emergency and/or road traffic management scenarios a particular attention must be paid to security and privacy. A thorough threat analysis should be conducted, and mitigations specified; this applies to any protocol documents in this context, for any communication modes. Security objectives particularly include integrity, privacy and non-repudiation and SHOULD protect the network and transport layer protocol headers. In addition any potential Internet-wide geo-networking solution MUST also protect privacy, i.e. provide confidentiality to personal data and protect leaking information through protocol behavior, such as the relation between identifier and location.
- o) SHOULD support timely and guaranteed delivery of information.

5. Relationships between GeoNet and other IETF Working Groups

Any new use-cases that the GeoNet WG comes up with that require protocol changes for any overlay technology, such as LISP, can be done in the appropriate protocol working groups, such as the LISP WG.

The following relationships between GeoNet and other IETF WGs have been identified:

- o) The GEOPRIV WG [[GEOPRIV](#)] concentrates on protocols that allow applications to represent location/geography objects and to allow users to express policies on how these representations are exposed and used. Moreover, the GEOPRIV WG analyses the authorization, integrity, and privacy requirements that must be met when these representations of location/geography are created, stored, and used. GeoNet mainly focuses on how IP routing and addressing uses such location/geography representations.
- o) The LISP WG [[LISP](#)] mainly focuses on network-layer-based protocol solutions that enable the separation of routing locators (where you are attached to the network) and identifiers (who you are) in one number space. GeoNet mainly focuses on how IP routing and addressing uses geography parameters, like geographical coordinates to disseminate packets sent by a sender located anywhere in the Internet to nodes that are located in the area specified by these geography parameters.

- o) The ECRIT WG [[ECRIT](#)] mainly focuses on how location data and call routing information are used to enable communication between a user and a relevant emergency response center.

In particular, the ECRIT WG has specified protocols to map emergency services identifiers and geodetic or civic location information to service contact URIs. GeoNet mainly focuses on how IP routing and addressing uses geodetic or civic location information to disseminate packets sent by a sender located anywhere in the Internet to nodes that are located in the area specified by this geodetic or civic location information.

6. Security Considerations

Due to the sensitivity of location data and the possibility of the technology being used in emergency and/or road traffic management scenarios a particular attention must be paid to security and privacy. Security objectives particularly include integrity, privacy and non-repudiation and SHOULD protect the network and transport layer protocol headers. In addition any potential Internet-wide Geo-networking solution MUST also protect privacy, i.e. provide confidentiality to personal data and protect leaking information through protocol behavior, such as the relation between identifier and location.

7. IANA Considerations

No IANA considerations are considered in this document.

8. Acknowledgments

We would like to thank the members of the IETF ITS and GeoNet community for their comments and discussions. In particular, we would like than the following contributors: Melinda Shore, Dino Farinacci, Geert Heijenk, Andreas Festag, Alison Chaiken, Duan Shihui, Rex Buddenberg, Carl Reed, Brian Rosen, Yong-Geun Hong, Robert Moskowitz, Ray Bellis.

9. Normative References

10. Informative References

[ISO19107] International standard ISO 19107, "Geographic information - Spatial Schema", International Standards Organization (ISO), 01-05-2003

[IEEE1609.2] IEEE 1609.2, "Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages", IEEE, (date Original version) July 6 2006; Revised on October 17, 2013

[IEEE802.11p] IEEE Std 802.11p(TM)-2010, "IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks -Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and

Physical Layer (PHY) Specifications, Amendment 6: Wireless Access in Vehicular Environments", IEEE, 2010, document freely available at URL <http://standards.ieee.org/getieee802/download/802.11p-2010.pdf>

[ECRIT] official website of IETF WG ECRIT (Emergency Context Resolution with Internet Technologies),
<http://datatracker.ietf.org/wg/ecrit/>

[GEOPRIV] official website of IETF WG GEOPRIV (Geographic Location/Privacy), <http://datatracker.ietf.org/wg/geopriv/>

[LISP] official website of IETF WG LISP (Locator/ID Separation Protocol), <http://datatracker.ietf.org/wg/lisp/>

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

11. Authors' Address

Georgios Karagiannis
University of Twente
P.O. Box 217
7500 AE Enschede,
The Netherlands
EMail: g.karagiannis@utwente.nl

Alexandru Petrescu
CEA
Communicating Systems Laboratory, Point Courier 173
Palaiseau, F-91120
France
Phone: +33(0)169089223
Email: alexandru.petrescu@cea.fr

Dimitri Papadimitriou
Alcatel-Lucent
Copernicuslaan, 50
2018 Antwerpen, Belgium
Phone: +32 3 240 8491
EMail: dimitri.papadimitriou@alcatel-lucent.com

Bastiaan Wissingh
TNO
Brassersplein 2
Delft 2612CT
the Netherlands
EMail: bastiaan.wissingh@tno.nl

12. Contributors

Melinda Shore
No Mountain Software
PO Box 16271
Two Rivers, AK 99716

US

Phone: +1 907 322 9522

EMail: melinda.shore@nomountain.net

Dino Farinacci
lispers.net
San Jose, California
USA
Phone: 408-718-2001
Email: farinacci@gmail.com

Geert Heijen
University of Twente
P.O. Box 217
7500 AE Enschede,
The Netherlands
EMail: geert.heijenkg@utwente.nl

Andreas Festag
Technical University Dresden & NEC Laboratories Europe
Germany
Email: andreas.festag@ifn.et.tu-dresden.de?;

Alison Chaiken
Mentor Embedded Software Division
46871 Bayside Parkway
Fremont, CA 94538
USA Email: alison@she-devel.com

Duan Shihui
RITT
EMail: duanshihui@ritt.cn

Rex Buddenberg
EMail: buddenbergr@gmail.com

Carl Reed
Open Geospatial Consortium (OGC)
Email: creed@opengeospatial.org

Brian Rosen
Neustar
470 Conrad Dr
Mars, PA 16046
USA
EMail: br@brianrosen.net

Yong-Geun Hong
ETRI
218 Gajeong-ro Yuseung-Gu
Daejeon 305-700
Korea
Phone: +82 42 860 6557

Email: yghong@etri.re.kr

Karagiannis, et al. Expires December 15, 2014

[Page 11]

Robert Moskowitz
Verizon
1000 Bent Creek Blvd, Suite 200
Mechanicsburg, PA
USA
EMail: robert.moskowitz@verizon.com

Robert Moskowitz
Verizon
1000 Bent Creek Blvd, Suite 200
Mechanicsburg, PA
USA
EMail: robert.moskowitz@verizon.com

Ray Bellis
Nominet UK
Edmund Halley Road
Oxford OX4 4DQ
United Kingdom
Phone: +44 1865 332211
Email: ray.bellis@nominet.org.uk

