

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 23, 2007

H. Tschofenig
Siemens
August 22, 2006

A Dynamic Host Configuration Protocol (DHCP) based Location-to-Service
Translation Protocol (LoST) Discovery Procedure
draft-tschofenig-dhc-lost-discovery-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of 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/lid-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 February 23, 2007.

Copyright Notice

Copyright (C) The Internet Society (2006).

Internet-Draft

DHCP-based LoST Discovery

August 2006

Abstract

The Location-to-Service Translation Protocol (LoST) describes an XML-based protocol for mapping service identifiers and geospatial or civic location information to service contact Uniform Resource Locators (URIs). LoST servers can be located anywhere but a placement closer to the end host, i.e., in the access network, is desirable. Such a LoST server placement provides benefits in disaster situations with intermittent network connectivity regarding the resiliency of emergency service communication.

This document describes such a LoST discovery procedure based on DHCP.

Table of Contents

1.	Introduction	3
2.	Terminology	6
3.	Location-to-Service Translation Protocol (LoST) DHCPv4 Option	7
4.	Location-to-Service Translation Protocol (LoST) DHCPv6 Option	8
5.	IANA Considerations	9
6.	Security Considerations	10
7.	Acknowledgements	11
8.	References	12
8.1.	Normative References	12
8.2.	Informative References	12
	Author's Address	14
	Intellectual Property and Copyright Statements	15

1. Introduction

The Location-to-Service Translation Protocol (LoST) describes an XML-based protocol for mapping service identifiers and geospatial or civic location information to service contact Uniform Resource Locators (URIs). The typical procedure for running LoST at an end host can be described via the following example. Note that the details of the LoST protocol mechanisms are not relevant for this protocol. The example aims to motivate the scenario behind this document. More information about LoST can be found at [\[I-D.ietf-ecrit-lost\]](#).

After performing link layer attachment an end host performs stateful address autoconfiguration using DHCP. Then, DHCP provides the end host with civic location (as described in [\[I-D.ietf-geopriv-dhcp-civil\]](#)) or with geospatial location information (as described in [\[RFC3825\]](#)). The following example below shows civic location information returned to the end host via DHCP. Note that other protocols may be used to provide the end host with location information. Furthermore, manual configuration or GPS might be used.

The following example shown in Figure 1 indicates a location in the US, state=New York, city=New York, group of streets=Broadway, additional location information=Suite 75, and zip code=10027-0401.

+-----+-----+		
CAtype	CAvalue	
+-----+-----+		
0	US	
1	New York	
3	New York	
6	Broadway	
22	Suite 75	
24	10027-0401	

+-----+-----+

Figure 1: DHCP Civic Information Example

Additionally, DHCP may provide information about the LoST server that can be contacted. This document describes such an extension to allow the DHCP server to also provide the IP address of the LoST server.

The end host can trigger the LoST protocol at any time: at attachment time, at call time or some time in between. When the end host initiates a LoST request, it includes its civic location and the desired service URN in the message. Examples of service URNs can be

found in [[I-D.ietf-ecrit-service-urn](#)]. The request in Figure 2 shows the location information received with DHCP (as shown in Figure 1) together with a request for an emergency service, namely 'urn:service:sos.police'.

```
<?xml version="1.0"?>
<findLoSTByCivic
  validate="false"
  xmlns="urn:ietf:params:xml:ns:lost1"
  xmlns:p2="urn:ietf:params:xml:ns:pidf:geopriv10:civilLoc"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <civicLocation>
    <p2:country>US</p2:country>
    <p2:A1>New York</p2:A1>
    <p2:A3>New York</p2:A3>
    <p2:A6>Broadway</p2:A6>
    <p2:LOC>Suite 75</p2:LOC>
    <p2:PC>10027-0401</p2:PC>
  </civicLocation>
  <service>urn:service:sos.police</service>
</findLoSTByCivic>
```

Figure 2: Mapping Request

In our example we assume that the LoST server has the requested information available and returns a successful response. The response indicates, as a human readable display string that the 'New York City Police Department' is responsible for the given

geographical area. The indicated URI allows the user to start communication using SIP or XMPP. The 'validated' element indicates which parts of the civic address were matched successfully against a database and represent a known address. Other parts of the address, in this example, the suite number, were ignored and not validated. The returned service boundary indicates that all of New York City would result in the same response. The service-number element indicates that the service can be reached via the dial string 9-1-1.

```
<?xml version="1.0" encoding="UTF-8"?>
<responseCivic
  timeToLive="10000"
  xmlns="urn:ietf:params:xml:ns:lost1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:p2="urn:ietf:params:xml:ns:pidf:geopriv10:civilLoc">
  <displayName>New York City Police Department</displayName>
  <region>
    <civicLocation>
      <p2:country>US</p2:country>
      <p2:A1>New York</p2:A1>
      <p2:A3>New York</p2:A3>
    </civicLocation>
  </region>
  <uri>sip:nypd@example.com</uri>
  <uri>xmpp:nypd@example.com</uri>
  <service-number>911</service-number>
</responseCivic>
```

Figure 3: Mapping Response

The received URIs then serve, for example, as input to SIP as

described in [[I-D.rosen-ecrit-framework](#)] whereby the SIP message might carry location information as shown in [[I-D.ietf-sip-location-conveyance](#)].

This document describes only a LoST discovery procedure based on information returned by the DHCP server. Other documents listed in the example above provide further building blocks in order to obtain location information via DHCP (see [[I-D.ietf-geopriv-dhcp-civil](#)] and [[RFC3825](#)]), to map location and a service identifier to a service URI (using LoST [[I-D.ietf-ecrit-lost](#)]), and a mechanism to convey the received information in SIP using [[I-D.ietf-sip-location-conveyance](#)].

[2.](#) Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

Within this document we use terminology from [[I-D.ietf-ecrit-requirements](#)].

[3.](#) Location-to-Service Translation Protocol (LoST) DHCPv4 Option

This section defines a LoST option that carries a list of 32-bit (binary) IPv4 addresses indicating one or more Location-to-Service Translation Protocol (LoST) servers available to the end host.

The DHCPv4 option for the LoST server has the format shown in Figure 4.

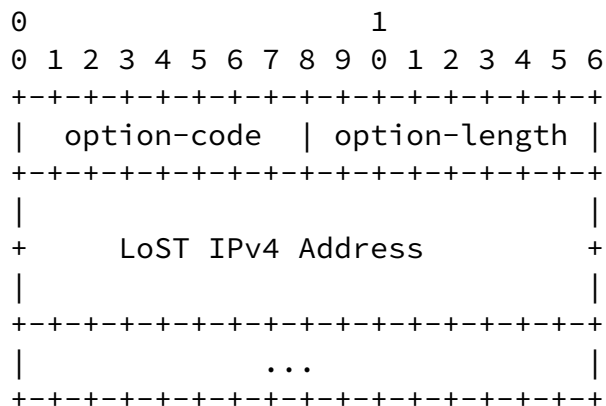


Figure 4: Location-to-Service Translation Protocol (LoST) DHCPv4 Option

option-code: OPTION_LOST (TBD)

option-length: Length of the 'options' field in octets;
MUST be a multiple of four (4)

LOST IPv4 Address: IPv4 address of a LoST server for the client to use.
The LoST servers are listed in the order of preference
for use by the client.

A DHCPv4 client requests the LOST DHCPv4 Option in a Parameter Request List as described in [[RFC2131](#)] and [[RFC2132](#)].

The DHCPv4 client MUST try the records in the order listed in the LOST DHCPv4 option.

This section defines a DHCPv6 option that carries a list of 128-bit (binary) IPv6 addresses indicating one or more Location-to-Service Translation Protocol (LoST) servers available to the end host.

The DHCPv6 option for Location-to-Service Translation Protocol (LoST) server has the format shown in Figure 6.

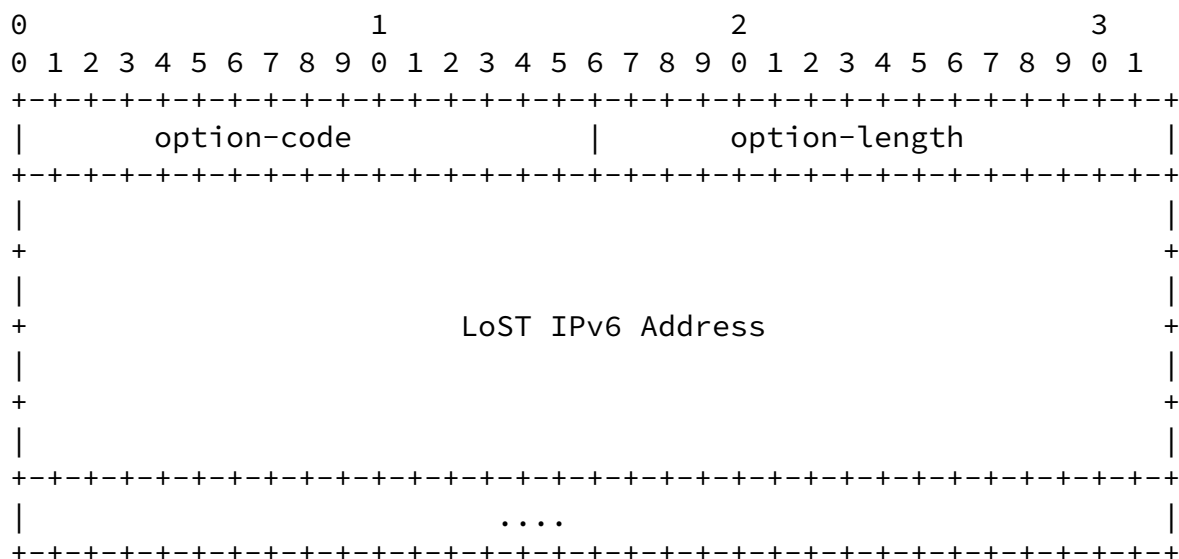


Figure 6: Location-to-Service Translation Protocol (LoST) DHCPv6 Option

option-code: OPTION_LOST (TBD)

option-length: Length of the 'options' field in octets;
MUST be a multiple of sixteen (16)

LOST IPv6 Address: IPv6 address of a LoST server for the client to use.
The LoST servers are listed in the order of preference
for use by the client.

A DHCPv6 client requests the LOST DHCPv6 option in an Options Request Option (ORO) as described in the DHCPv6 specification [[RFC3315](#)].

The DHCPv6 client MUST try the records in the order listed in the LOST DHCPv6 option.

[5.](#) IANA Considerations

The following DHCPv4 option code for the Location-to-Service Translation Protocol (LoST) server option must be assigned by IANA:

Option	Name	Value	Described in

OPTION_LOST		TBD	Section 5

The following DHCPv6 option codes for the Location-to-Service Translation Protocol (LoST) options must be assigned by IANA:

Option	Name	Value	Described in

OPTION_LOST		TBD	Section 6

6. Security Considerations

If an adversary manages to modify the response from a DHCP server or insert its own response, a LoST client could be led to contact a rogue LoST server. As a consequence the address of a non-existent LoST server could be returned to the end host. Alternatively, the adversary returns an IP address of a LoST server under the control of the adversary. These threats are documented in [\[I-D.ietf-ecrit-security-threats\]](#). The security considerations in [\[RFC2131\]](#), [\[RFC2132\]](#) and [\[RFC3315\]](#) are applicable to this document.

7. Acknowledgements

The author of this document used [draft-ietf-dhc-paa-option](#) as a template. Hence, acknowledgements go to the draft authors of [draft-ietf-dhc-paa-option](#).

The author would like to thank Christian Dickmann and Mayutan Arumaithurai for their draft review.

[8.](#) References

[8.1.](#) Normative References

- [I-D.ietf-ecrit-lost]
Hardie, T., "LoST: A Location-to-Service Translation Protocol", [draft-ietf-ecrit-lost-00](#) (work in progress), June 2006.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), [BCP 14](#), March 1997.
- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.
- [RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", [RFC 2132](#), March 1997.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), July 2003.

[8.2.](#) Informative References

[I-D.ietf-ecrit-requirements]

Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", [draft-ietf-ecrit-requirements-11](#) (work in progress), August 2006.

[I-D.ietf-ecrit-security-threats]

Taylor, T., "Security Threats and Requirements for Emergency Call Marking and Mapping", [draft-ietf-ecrit-security-threats-03](#) (work in progress), July 2006.

[I-D.ietf-ecrit-service-urn]

Schulzrinne, H., "A Uniform Resource Name (URN) for Services", [draft-ietf-ecrit-service-urn-04](#) (work in progress), August 2006.

[I-D.ietf-geopriv-dhcp-civil]

Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", [draft-ietf-geopriv-dhcp-civil-09](#) (work in progress), January 2006.

Tschofenig

Expires February 23, 2007

[Page 12]

Internet-Draft

DHCP-based LoST Discovery

August 2006

[I-D.ietf-sip-location-conveyance]

Polk, J. and B. Rosen, "Session Initiation Protocol Location Conveyance", [draft-ietf-sip-location-conveyance-03](#) (work in progress), June 2006.

[I-D.rosen-ecrit-framework]

Rosen, B., "Framework for Emergency Calling in Internet Multimedia", [draft-rosen-ecrit-framework-00](#) (work in progress), June 2006.

[RFC3825]

Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", [RFC 3825](#), July 2004.

Author's Address

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Phone: +49 89 636 40390
Email: Hannes.Tschofenig@siemens.com
URI: <http://www.tschofenig.com>

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).