

GEOPRIV  
Internet-Draft  
Intended status: Standards Track  
Expires: November 8, 2009

M. Thomson  
J. Winterbottom  
Andrew  
May 7, 2009

Discovering the Local Location Information Server (LIS)  
draft-ietf-geopriv-lis-discovery-11

## 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/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 November 8, 2009.

## Copyright Notice

Copyright (c) 2009 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 in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

## Abstract

Discovery of the correct Location Information Server (LIS) in the local access network is necessary for devices that wish to acquire location information from the network. A method is described for the

Internet-Draft

LIS Discovery

May 2009

discovery of a LIS in the access network serving a device. Dynamic Host Configuration Protocol (DHCP) options for IP versions 4 and 6 are defined that specify a domain name. This domain name is then used as input to a URI-enabled NAPTR (U-NAPTR) resolution process.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction and Overview</a>	<a href="#">3</a>
<a href="#">1.1.</a>	<a href="#">Discovery Procedure Overview</a>	<a href="#">3</a>
<a href="#">1.2.</a>	<a href="#">Terminology</a>	<a href="#">4</a>
<a href="#">2.</a>	<a href="#">LIS Discovery Procedure</a>	<a href="#">4</a>
<a href="#">2.1.</a>	<a href="#">Residential Gateways</a>	<a href="#">5</a>
<a href="#">2.2.</a>	<a href="#">Virtual Private Networks (VPNs)</a>	<a href="#">6</a>
<a href="#">3.</a>	<a href="#">Access Network Domain Name DHCP Option</a>	<a href="#">7</a>
<a href="#">3.1.</a>	<a href="#">Domain Name Encoding</a>	<a href="#">7</a>
<a href="#">3.2.</a>	<a href="#">Access Network Domain Name DHCPv4 Option</a>	<a href="#">7</a>
<a href="#">3.3.</a>	<a href="#">Access Network Domain Name DHCPv6 Option</a>	<a href="#">8</a>
<a href="#">4.</a>	<a href="#">U-NAPTR Resolution of a LIS URI</a>	<a href="#">9</a>
<a href="#">4.1.</a>	<a href="#">Determining a Domain Name</a>	<a href="#">10</a>
<a href="#">5.</a>	<a href="#">Security Considerations</a>	<a href="#">10</a>
<a href="#">6.</a>	<a href="#">IANA Considerations</a>	<a href="#">11</a>
<a href="#">6.1.</a>	<a href="#">Registration of DHCPv4 and DHCPv6 Option Codes</a>	<a href="#">11</a>
<a href="#">6.2.</a>	<a href="#">Registration of a Location Server Application Service Tag</a>	<a href="#">12</a>
<a href="#">6.3.</a>	<a href="#">Registration of a Location Server Application Protocol Tag for HELD</a>	<a href="#">12</a>
<a href="#">7.</a>	<a href="#">Acknowledgements</a>	<a href="#">13</a>
<a href="#">8.</a>	<a href="#">References</a>	<a href="#">13</a>
<a href="#">8.1.</a>	<a href="#">Normative References</a>	<a href="#">13</a>
<a href="#">8.2.</a>	<a href="#">Informative References</a>	<a href="#">14</a>

## 1. Introduction and Overview

The location of a device is a useful and sometimes necessary part of many services. A Location Information Server (LIS) is responsible for providing that location information to devices with an access network. The LIS uses knowledge of the access network and its physical topology to generate and serve location information to devices.

Each access network requires specific knowledge about topology. Therefore, it is important to discover the LIS that has the specific knowledge necessary to locate a device. That is, the LIS that serves the current access network. Automatic discovery is important where there is any chance of movement outside a single access network. Reliance on static configuration can lead to unexpected errors if a device moves between access networks.

This document describes a process that a device can use to discover a LIS. This process uses a DHCP option and the DNS. The product of this discovery process is an http: or https: URI, which identifies a LIS.

The URI result from the discovery process is suitable for location configuration only; that is, the device MUST dereference the URI using the process described in HELD [[I-D.ietf-geopriv-http-location-delivery](#)]. URIs discovered in this way are not "location URIs" [[I-D.ietf-geopriv-lbyr-requirements](#)]; dereferencing one of them provides the location of the requester only. Devices MUST NOT embed these URIs in fields in other protocols designed to carry the location of the device.

### 1.1. Discovery Procedure Overview

DHCP ([[RFC2131](#)], [[RFC3315](#)]) is a commonly used mechanism for providing bootstrap configuration information allowing a device to operate in a specific network environment. The bulk of DHCP

information is largely static; consisting of configuration information that does not change over the period that the device is attached to the network. Physical location information might change over this time, however the address of the LIS does not. Thus, DHCP is suitable for configuring a device with the address of a LIS.

This document defines a DHCP option that produces a domain name that identifies the local access network in [Section 3](#).

[Section 4](#) describes a method that uses URI-enabled NAPTR (U-NAPTR) [[RFC4848](#)], a Dynamic Delegation Discovery Service (DDDS) profile that produces a URI for the LIS. The input to this process is provided by

the DHCP option.

For the LIS discovery DDDS application, an Application Service tag "LIS" and an Application Protocol tag "HELD" are created and registered with the IANA. Based on the domain name, this U-NAPTR application uses the two tags to determine a URI for a LIS that supports the HELD protocol.

## [1.2](#). Terminology

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](#)].

This document also uses the term "device" to refer to an end host, or client consistent with its use in HELD. In HELD and [RFC3693](#) [[RFC3693](#)] parlance, the Device is also the Target.

The terms "access network" refers to the network that a device connects to for Internet access. The "access network provider" is the entity that operates the access network. This is consistent with the definition in [[I-D.ietf-geopriv-l7-lcp-ps](#)] which combines the Internet Access Provider (IAP) and Internet Service Provider (ISP). The access network provider is responsible for allocating the device a public IP address and for directly or indirectly providing a LIS service.

## [2](#). LIS Discovery Procedure

A device that has multiple network interfaces could potentially be served by a different access network on each interface, each with a different LIS. The device SHOULD attempt to discover the LIS applicable to each network interface, stopping when a LIS is successfully discovered on any interface.

The LIS discovery procedure follows the following process:

1. Acquire the access network domain name DHCP option ([Section 3](#)).

This process might be repeated for each of the network interfaces on the device. Domain names acquired from other sources might also be added.

2. Apply U-NAPTR resolution ([Section 4](#)) to discover a LIS URI.

The U-NAPTR process is applied using each of the domain names as input.

3. Verify that the LIS is able to provide location information.

The first URI that results in a successful response from the LIS is used.

A device MUST support discovery using the access network domain name DHCP option ([Section 3](#)) as input to U-NAPTR resolution ([Section 4](#)). Other domain names MAY be used, as described in [Section 4.1](#).

A device that discovers a LIS URI MUST attempt to verify that the LIS is able to provide location information. For the HELD protocol, the device verifies the URI by making a location request to the LIS. If - at any time - the LIS responds to a request with the "notLocatable" error code (see Section 4.3.2 of [\[I-D.ietf-geopriv-http-location-delivery\]](#)), the device MUST continue or restart the discovery process. A device SHOULD NOT make further requests to a LIS that provides a "notLocatable" error until its network attachment changes, or it discovers the LIS on an alternative network interface.

Static configuration of a domain name or a LIS URI MAY be used if all other discovery methods fail. Note that if a device has moved from

its customary location, static configuration might indicate a LIS that is unable to provide accurate location information.

The product of the LIS discovery process for HELD is an "https:" or "http:" URI. Nothing distinguishes this URI from other URIs with the same scheme, aside from the fact that it is the product of this process. Only URIs produced by the discovery process can be used for location configuration using HELD.

## [2.1.](#) Residential Gateways

The process described in this document is known to not work in a very common deployment scenario. A fixed wireline scenario is described in more detail in Section 3.1 of [[I-D.ietf-geopriv-l7-lcp-ps](#)]. In this fixed wireline environment an intervening residential gateway exists between the device and the access network. If the residential gateway does not provide this option to the devices it serves, those devices are unable to discover a LIS.

Support of this specification by residential gateways ensures that the devices they serve are able to acquire location information. In many cases the residential gateway configures the devices it serves using DHCP. A residential gateway is able to use DHCP to assist devices in gaining access to their location information. This can be accomplished by providing an access network domain name DHCP option suitable for LIS discovery, or by acting as a LIS directly. To

actively assist devices, a residential gateway can either:

- o acquire an access network domain name from the access network provider (possibly using DHCP) and pass the resulting value to devices; or
- o discover a LIS on its external interface, then provide devices with the domain name that was used to successfully discover the LIS; or
- o explicitly include configuration that refers to a particular LIS; or
- o act as a LIS and directly provide location information to the devices it serves, including providing a means to discover this

service.

As with devices, configuration of a specific domain name or location information is only accurate as long as the residential gateway does not move. If a residential gateway that relies on configuration rather than automatic discovery is moved, the devices it serves could be provided with inaccurate information. Devices could be led to discover a LIS that is unable to provide accurate location information, or - if location is configured on the residential gateway - the residential gateway could provide incorrect location information.

[I-D.ietf-dhc-container-opt] might be used by an access network provider to convey configuration information to a residential gateway for use by the devices it serves. Support and use of this option is RECOMMENDED for both residential gateways and devices. Option values found within the container MUST be used after values that are directly in the DHCP response.

## [2.2.](#) Virtual Private Networks (VPNs)

LIS discovery over a VPN network interface SHOULD NOT be performed. A LIS discovered in this way is unlikely to have the information necessary to determine an accurate location.

Not all interfaces connected to a VPN can be detected by devices or the software running on them. A LIS MUST NOT provide location information in response to requests that it can identify as originating from a device on the remote end of a VPN tunnel, unless it is able to accurately determine location. The "notLocatable" HELD error code can be used to indicate to a device that discovery has revealed an unsuitable LIS. This ensures that even if a device discovers a LIS over the VPN, it does not rely on a LIS that is

unable to provide accurate location information.

## [3.](#) Access Network Domain Name DHCP Option

DHCP provides a direct means for the access network provider to configure a device. The access network domain name option identifies a domain name that is suitable for service discovery within the access network. This domain name is used as input to the U-NAPTR

resolution process for LIS discovery.

The domain name provided in this option is one owned by the access network operator. This domain name is intended for use in discovering services within the access network.

This document registers a DHCP option for the access network domain name for both IPv4 and IPv6.

### [3.1.](#) Domain Name Encoding

This section describes the encoding of the domain name used in the DHCPv4 option defined in [Section 3.2](#) and also used in the DHCPv6 option defined in [Section 3.3](#).

The domain name is encoded according to [Section 3.1 of \[RFC1035\]](#). Each label is represented as a one-octet length field followed by that number of octets. Since every domain name ends with the null label of the root, a domain name is terminated by a length byte of zero. The high-order two bits of every length octet MUST be zero, and the remaining six bits of the length field limit the label to 63 octets or less. To simplify implementations, the total length of a domain name (i.e., label octets and label length octets) is restricted to 255 octets or less.

### [3.2.](#) Access Network Domain Name DHCPv4 Option

This section defines a DHCP for IPv4 (DHCPv4) option for the domain name associated with the access network.

Code	Len	Access Network Domain Name					
-----	-----	-----	-----	-----	-----	-----	-----
TBD	n	s1	s2	s3	s4	s5	...
-----	-----	-----	-----	-----	-----	-----	-----

Figure 1: Access Network Domain Name DHCPv4 Option

The values s1, s2, s3, etc. represent the domain name labels in the domain name encoding. Note that the length field in the DHCPv4 option represents the length of the entire domain name encoding,

whereas the length fields in the domain name encoding (see [Section 3](#))



is the length of a single domain name label.

Code: OPTION\_V4\_ACCESS\_DOMAIN (TBD). [[IANA/RFC-Editor Note: Please replace TBD with the assigned DHCPv4 option code, both here and in Figure 1.]]

Length: The length of the entire access network domain name option in octets.

Access Network Domain Name: The domain name associated with the access network, encoded as described in [Section 3.1](#).

A DHCPv4 client MAY request a access network domain name option in a Parameter Request List option, as described in [[RFC2131](#)].

This option contains a single domain name and, as such, MUST contain precisely one root label.

### [3.3](#). Access Network Domain Name DHCPv6 Option

This section defines a DHCP for IPv6 (DHCPv6) option for the domain name associated with the access network. The DHCPv6 option for this parameter is similarly formatted to the DHCPv4 option.

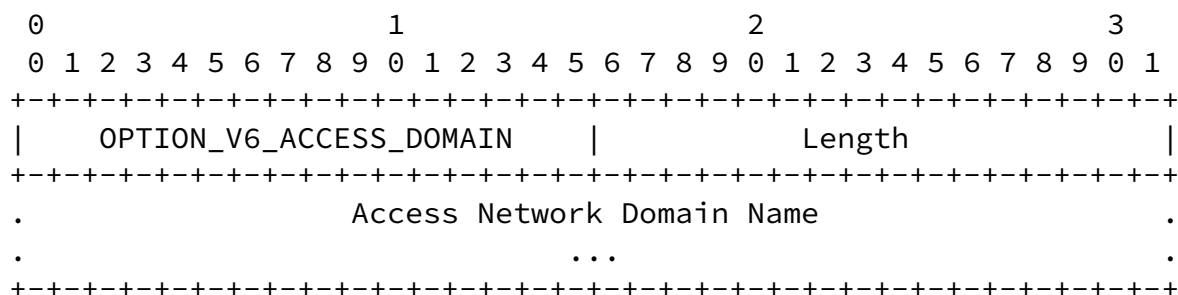


Figure 2: DHCPv6 Access Network Domain Name Option

option-code: OPTION\_V6\_ACCESS\_DOMAIN (TBD). [[IANA/RFC-Editor Note: Please replace TBD with the assigned DHCPv6 option code.]]

option-length: The length of the entire access network domain name option in octets.

option-value: The access network domain name, encoded as described in [Section 3.1](#).

A DHCPv6 client MAY request a access network domain name option in a Options Request Option (ORO), as described in [[RFC3315](#)].

This option contains a single domain name and, as such, MUST contain precisely one root label.

#### 4. U-NAPTR Resolution of a LIS URI

U-NAPTR [[RFC4848](#)] resolution for a LIS takes a domain name as input and produces a URI that identifies the LIS. This process also requires an Application Service tag and an Application Protocol tag, which differentiate LIS-related NAPTR records from other records for that domain.

[Section 6.2](#) defines an Application Service tag of "LIS", which is used to identify the location service for a given domain. The Application Protocol tag "HELD", defined in [Section 6.3](#), is used to identify a LIS that understands the HELD protocol [[I-D.ietf-geopriv-http-location-delivery](#)].

The NAPTR records in the following example demonstrate the use of the Application Service and Protocol tags. Iterative NAPTR resolution is used to delegate responsibility for the LIS service from "zonea.example.net." and "zoneb.example.net." to "outsource.example.com.".

```
zonea.example.net.
;;      order pref flags
IN NAPTR 100  10  ""  "LIS:HELD" (          ; service
    ""                                     ; regex
    outsource.example.com.                ; replacement
)
zoneb.example.net.
;;      order pref flags
IN NAPTR 100  10  ""  "LIS:HELD" (          ; service
    ""                                     ; regex
    outsource.example.com.                ; replacement
)
outsource.example.com.
;;      order pref flags
IN NAPTR 100  10  "u"  "LIS:HELD" (          ; service
    "!.*.!https://lis.example.org:4802/?c=ex!" ; regex
    .                                       ; replacement
)
```

Figure 3: Sample LIS:HELD Service NAPTR Records

Details for the "LIS" Application Service tag and the "HELD"

An "https:" LIS URI that is a product of U-NAPTR MUST be authenticated using the domain name method described in [Section 3.1 of RFC 2818](#) [[RFC2818](#)]. The domain name that is used in this authentication is the one extracted from the URI, not the input to the U-NAPTR resolution process.

#### [4.1](#). Determining a Domain Name

The U-NAPTR resolution method described requires a domain name as input. The access network domain name DHCP option ([Section 3](#)) describes one source of this domain name.

If a device knows one or more alternative domain names that might be used for discovery, it MAY repeat the U-NAPTR process using those domain names as input. For instance, static configuration of a device might be used to provide a device with a domain name.

Alternative domain names MUST NOT be used unless the access network domain name option is unsuccessful or where external information indicates that a particular domain name is to be used. For instance, domain names for the device might be provided by a DHCP server ([\[RFC4702\]](#) for DHCPv4, [\[RFC4704\]](#) for DHCPv6); DHCPv4 option 15 [\[RFC2131\]](#) could also be used as a source of a domain name suffix for the device. However, these domain names could be provided without considering their use for LIS discovery; therefore, many DHCP servers do not provide a sensible value for these options.

### [5](#). Security Considerations

The address of a LIS is usually well-known within an access network; therefore, interception of messages does not introduce any specific concerns.

The primary attack against the methods described in this document is one that would lead to impersonation of a LIS. The LIS is responsible for providing location information and this information is critical to a number of network services; furthermore, a device does not necessarily have a prior relationship with a LIS. Several methods are described here that can limit the probability of, or

provide some protection against, such an attack. These methods MUST be applied unless similar protections are in place, or in cases - such as an emergency - where location information of dubious origin is arguably better than none at all.

An attacker could attempt to compromise LIS discovery at any of three stages:

1. providing a falsified domain name to be used as input to U-NAPTR
2. altering the DNS records used in U-NAPTR resolution
3. impersonation of the LIS

U-NAPTR is entirely dependent on its inputs. In falsifying a domain name, an attacker avoids any later protections, bypassing them entirely. To ensure that the access network domain name DHCP option can be relied upon, preventing DHCP messages from being modified or spoofed by attackers is necessary. Physical or link layer security are commonplace methods that can reduce the possibility of such an attack within an access network; alternatively, DHCP authentication [[RFC3118](#)] can provide a degree of protection against modification or spoofing.

The domain name that is used to authenticated the LIS is the domain name in the URI that is the result of the U-NAPTR resolution. Therefore, if an attacker were able to modify or spoof any of the DNS records used in the DDDS resolution, this URI could be replaced by an invalid URI. The application of DNS security (DNSSEC) [[RFC4033](#)] provides a means to limit attacks that rely on modification of the DNS records used in U-NAPTR resolution. Security considerations specific to U-NAPTR are described in more detail in [[RFC4848](#)].

An "https:" URI is authenticated using the method described in [Section 3.1 of \[RFC2818\]](#). The domain name used for this authentication is the domain name in the URI resulting from U-NAPTR resolution, not the input domain name as in [[RFC3958](#)]. Using the domain name in the URI is more compatible with existing HTTP client software, which authenticate servers based on the domain name in the URI.

A LIS that is identified by an "http:" URI cannot be authenticated. Use of unsecured HTTP also does not meet requirements in HELD for confidentiality and integrity. If an "http:" URI is the product of LIS discovery, this leaves devices vulnerable to several attacks. Lower layer protections, such as layer 2 traffic separation might be used to provide some guarantees.

## [6.](#) IANA Considerations

### [6.1.](#) Registration of DHCPv4 and DHCPv6 Option Codes

The IANA has assigned an option code of (TBD) for the DHCPv4 option for an access network domain name option, as described in [Section 3.2](#) of this document.

Thomson & Winterbottom Expires November 8, 2009

[Page 11]

---

Internet-Draft

LIS Discovery

May 2009

The IANA has assigned an option code of (TBD) for the DHCPv6 option for an access network domain name option, as described in [Section 3.3](#) of this document.

### [6.2.](#) Registration of a Location Server Application Service Tag

This section registers a new S-NAPTR/U-NAPTR Application Service tag for a LIS, as mandated by [[RFC3958](#)].

Application Service Tag: LIS

Intended usage: Identifies a service that provides a device with its location information.

Defining publication: RFCXXXX

Related publications: HELD [[I-D.ietf-geopriv-http-location-delivery](#)]

Contact information: The authors of this document

Author/Change controller: The IESG

### [6.3.](#) Registration of a Location Server Application Protocol Tag for HELD

This section registers a new S-NAPTR/U-NAPTR Application Protocol tag for the HELD [[I-D.ietf-geopriv-http-location-delivery](#)] protocol, as mandated by [[RFC3958](#)].

Application Service Tag: HELD

Intended Usage: Identifies the HELD protocol.

Applicable Service Tag(s): LIS

Terminal NAPTR Record Type(s): U

Defining Publication: RFCXXXX

Related Publications: HELD [[I-D.ietf-geopriv-http-location-delivery](#)]

Contact Information: The authors of this document

Author/Change Controller: The IESG

## [7.](#) Acknowledgements

This document uses a mechanism that is largely identical to that in [[RFC5222](#)] and [[RFC5223](#)]. The authors would like to thank Leslie Daigle for her work on U-NAPTR; Peter Koch for feedback on how not to use DNS for discovery; Andy Newton for constructive suggestions with regards to document direction; Richard Barnes, Joe Salowey, Barbara Stark, and Hannes Tschofenig for input and reviews; Dean Willis for constructive feedback.

## [8.](#) References

### [8.1.](#) Normative References

[RFC1035]

Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), November 1987.

- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.
- [RFC2818] Rescorla, E., "HTTP Over TLS", [RFC 2818](#), May 2000.
- [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.
- [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", [RFC 4033](#), March 2005.
- [RFC4702] Stapp, M., Volz, B., and Y. Rekhter, "The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option", [RFC 4702](#), October 2006.

- [RFC4704] Volz, B., "The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option", [RFC 4704](#), October 2006.
- [RFC4848] Daigle, L., "Domain-Based Application Service Location Using URIs and

the Dynamic Delegation  
Discovery Service (DDDS)",  
[RFC 4848](#), April 2007.

[I-D.ietf-geopriv-http-location-delivery] Barnes, M., Winterbottom,  
J., Thomson, M., and B.  
Stark, "HTTP Enabled  
Location Delivery (HELD)",  
[draft-ietf-geopriv-http-  
location-delivery-13](#) (work  
in progress),  
February 2009.

[I-D.ietf-dhc-container-opt] Droms, R., "Container  
Option for Server  
Configuration", [draft-  
ietf-dhc-container-opt-05](#)  
(work in progress),  
March 2009.

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

## [8.2.](#) Informative References

[RFC3118] Droms, R. and W. Arbaugh,  
"Authentication for DHCP  
Messages", [RFC 3118](#),  
June 2001.

[RFC3693] Cuellar, J., Morris, J.,  
Mulligan, D., Peterson,  
J., and J. Polk, "Geopriv  
Requirements", [RFC 3693](#),

February 2004.

[RFC3958] Daigle, L. and A. Newton,  
"Domain-Based Application



- Service Location Using SRV  
RRs and the Dynamic  
Delegation Discovery  
Service (DDDS)", [RFC 3958](#),  
January 2005.
- [RFC5222] Hardie, T., Newton, A.,  
Schulzrinne, H., and H.  
Tschofenig, "LoST: A  
Location-to-Service  
Translation Protocol",  
[RFC 5222](#), August 2008.
- [RFC5223] Schulzrinne, H., Polk, J.,  
and H. Tschofenig,  
"Discovering Location-to-  
Service Translation (LoST)  
Servers Using the Dynamic  
Host Configuration  
Protocol (DHCP)",  
[RFC 5223](#), August 2008.
- [I-D.ietf-geopriv-l7-lcp-ps] Tschofenig, H. and H.  
Schulzrinne, "GEOPRIV  
Layer 7 Location  
Configuration Protocol;  
Problem Statement and  
Requirements", [draft-ietf-geopriv-l7-lcp-ps-09](#) (work  
in progress),  
February 2009.
- [I-D.ietf-geopriv-lbyr-requirements] Marshall, R.,  
"Requirements for a  
Location-by-Reference  
Mechanism", [draft-ietf-geopriv-lbyr-requirements-07](#) (work in progress),  
February 2009.

Authors' Addresses

Martin Thomson  
Andrew  
PO Box U40  
Wollongong University Campus, NSW 2500  
AU

Phone: +61 2 4221 2915  
EMail: martin.thomson@andrew.com  
URI: <http://www.andrew.com/>

James Winterbottom  
Andrew  
PO Box U40  
Wollongong University Campus, NSW 2500  
AU

Phone: +61 2 4221 2938  
EMail: james.winterbottom@andrew.com  
URI: <http://www.andrew.com/>

