TOC

GEOPRIV	M. Thomson
Internet-Draft	J. Winterbottom
Intended status: Standards Track	Andrew
Expires: March 30, 2008	September 27, 2007

Discovering the Local Location Information Server (LIS)
draft-thomson-geopriv-lis-discovery-03.txt

Status of this Memo

Abstract

A method is described for the discovery of a Location Information Server. The method consists of attempting to use a Dynamic Host Configuration Protocol (DHCP) option, followed by a URI-enabled NAPTR (U-NAPTR). DHCP options are defined for both IPv4 and IPv6 DHCP. This document also defines a U-NAPTR Application Service for a LIS, with a specific Application Protocol for the HTTP Enabled Location Delivery (HELD) protocol.

Table of Contents

---

1. Introduction and Overview

TOC

Discovering a Location Information Server (LIS) is an important part of the location acquisition process. The LIS is an access network service that needs to be discovered before it can be used. This document describes a method that a host can use to discover a URI for a LIS. The product of a discovery process, such as the one described in this document, is the address of the service. In this document, the result is a URI, which identifies a LIS. A URI permits identification of a LIS that includes information about protocols and other supplementary information.

The discovery process requires that the host first attempt LIS discovery using Dynamic Host Configuration protocol (DHCP). If DHCP is not available, or the option is not supported by the network, the host attempts to discover the LIS using the DNS and URI-enabled Naming Authority Pointer (U-NAPTR). Finally, the host can rely on proprietary methods for determining the address of the LIS, including static configuration.

1.1. DHCP Discovery

TOC

DHCP ([RFC2131] (Droms, R., “Dynamic Host Configuration Protocol,” March 1997.), [RFC3315] (Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” July 2003.)) is a commonly used mechanism for providing bootstrap configuration information allowing a host 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 host 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 host with the address of a LIS.

1.2. U-NAPTR Discovery

TOC

Where DHCP is not available, the DNS might be able to provide a URI. For DNS methods, alternative discovery techniques SRV records (Gulbrandsen, A., Vixie, P., and L. Esibov, “A DNS RR for specifying the location of services (DNS SRV),” February 2000.) [RFC2782] or Straightforward NAPTR (S-NAPTR) (Daigle, L. and A. Newton, “Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS),” January 2005.) [RFC3958] provide an indication of a service for a domain, but these methods cannot be used; SRV and S-NAPTR only permit the return of a hostname and port, not a URI. URI-enabled NAPTR (U-NAPTR) (Daigle, L., “Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS),” April 2007.) [RFC4848], which is based on S-NAPTR, describes a method of applying the Dynamic Delegation Discovery Service (DDDS) for URI results.

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

Determining the domain name to be used is a critical part of the resolution process. The second part of this document describes how a domain name can be derived. Several methods are described that address different scenarios.

1.3. Terminology

TOC

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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

This document also uses the term "host" to refer to an end host. In RFC3693 (Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, “Geopriv Requirements,” February 2004.) [RFC3693] parlance, the host is the Device, which might also be the Target.

The terms "access network" refers to the network that a host 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] (Tschofenig, H. and H. Schulzrinne, “GEOPRIV Layer 7 Location Configuration Protocol; Problem Statement and Requirements,” July 2009.) which combines the Internet Access Provider (IAP) and Internet Service Provider (ISP). The access network provider is responsible for allocating the host an IP address and for directly or indirectly providing a LIS service.

2. LIS Discovery Using DHCP

TOC

DHCP allows the access network provider to specify the address of a LIS as part of network configuration. This document registers DHCP options for a LIS address for both IPv4 and IPv6.

2.1. DHCPv4 Option for a LIS Address

TOC

This section defines a DHCP for IPv4 (DHCPv4) option for the address of a LIS.

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |    LIS_URI    |     Length    |         URI ...               .
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                              URI                            ...
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: DHCPv4 LIS URI Option

> **LIS_URI:** The IANA assigned option number (TBD).

Length: The length of the URI in octets.

URI: The address of the LIS. This URI SHOULD NOT be more than 253 bytes in length, but MAY be extended by concatenating multiple option values, as described in [RFC3396] (Lemon, T. and S. Cheshire, “Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4),” November 2002.). The URI MUST NOT be NULL terminated.

2.2. DHCPv6 Option for a LIS Address

TOC

This section defines a DHCP for IPv6 (DHCPv6) option for the address of a LIS. The DHCPv6 option for this parameter is similarly formatted to the DHCPv4 option.

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |       OPTION_LIS_URI          |           Length              |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                              URI                            ...
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: DHCPv6 LIS URI Option

OPTION_LIS_URI: The IANA assigned option number (TBD).

Length: The length of the URI in octets.

URI: The address of the LIS. The URI MUST NOT be NULL terminated.

---

3. U-NAPTR for LIS Discovery

TOC

U-NAPTR 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 7.2 (Registration of a Location Server Application Service Tag) defines an Application Service tag of LIS, which is used to identify the location service for a particular domain. The Application Protocol tag HELD, defined in Section 7.3 (Registration of a Location Server Application Protocol Tag for HELD), is used to identify a LIS that understands the HELD protocol (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, “HTTP Enabled Location Delivery (HELD),” August 2009.) [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.com. and zoneb.example.com. to outsource.example.com..

```
zonea.example.com.
;;       order pref flags
IN NAPTR 100   10   ""  "LIS:HELD" (          ; service
    ""                                        ; regex
    outsource.example.com.                    ; replacement
    )
zoneb.example.com.
;;       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.outsource.example.com/!" ; regex
    .                                         ; replacement
    )
```

Figure 3: Sample LIS:HELD Service NAPTR Records

Details for the LIS Application Service tag and the HELD Application Protocol tag are included in Section 7 (IANA Considerations).

TOC

4. Determining the Access Network Domain Name

The U-NAPTR discovery method described in Section 3 (U-NAPTR for LIS Discovery) requires that the domain name applicable to the access network is known. An unconfigured host might not have this information, therefore it must determine this value before the U-NAPTR method can be attempted.

This section describes several methods for discovering a domain name for the local access network. Each method is attempted where applicable until a domain name is derived. If a domain name is successfully derived but that domain name does not produce any U-NAPTR records, alternative methods can be attempted to determine additional domain names. Reattempting with different methods is particularly applicable when NAT is used, as is shown in Section 4.2.1 (Determining an External IP Address).

4.1. DHCP Domain Name Option

TOC

For IP version 4, Dynamic Host Configuration Protocol (DHCP) option 15 [RFC2131] (Droms, R., “Dynamic Host Configuration Protocol,” March 1997.) includes the domain name suffix for the host. If DHCP and option 15 are available, this value should be used as input the U-NAPTR procedure.

DHCP for IPv6 provides a single domain name suffix that can be used in the same manner, as a described in [I-D.ietf-dhc-dhcpv6-opt-dnsdomain] (Yan, R., “Domain Suffix Option for DHCPv6,” June 2007.).

Alternatively, a fully qualified domain name (FQDN) for the host might be provided by the server ([RFC4702] (Stapp, M., Volz, B., and Y. Rekhter, “The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option,” October 2006.) for DHCPv4, [RFC4704] (Volz, B., “The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option,” October 2006.) for DHCPv6). This domain name is used as input to the U-NAPTR resolution and is obtained from the FQDN by removing the first label. If the host has provided a fully qualified domain name using this option, it SHOULD NOT be used - the domain known to the host might not be the same as that of the access network.

Either DHCP method SHOULD be attempted first if DHCP is available. Note that this method is only attempted if the LIS address option is not available.

TOC

4.2. Reverse DNS

DNS PTR records in the in-addr.arpa. domain can be used to determine the domain name of a host, and therefore, the name of the domain for that host. The use of the in-addr.arpa. domain is described in [RFC1034] (Mockapetris, P., “Domain names - concepts and facilities,” November 1987.) and results in the domain name of the host. Likewise, IPv6 hosts use the ip6.arpa. domain. In the majority of cases, the domain part of this name (everything excluding the first label) is also the domain name for the access network. Assuming that this is true, this domain name can be used as input to the U-NAPTR process.

For example, if the for 10.1.2.3 address, if the PTR record at 3.2.1.10.in-addr.arpa. refers to host.example.com, this results in a U-NAPTR search for example.com.

The DNS hierarchy does not necessarily directly map onto a network topology (see [RFC4367] (Rosenberg, J. and IAB, “What's in a Name: False Assumptions about DNS Names,” February 2006.)); therefore, this method MUST only be used for the domain name determined by removing the first label only. This method assumes that the access network provider also provides the reverse DNS record and they control the domain that is indicated in the PTR record.

Furthermore, this method might not apply where a host is given a domain name that is different from the domain name of the access network. This might occur in some hosting configurations, such as where a number of web server hosts, with widely varying domain names, are co-located.

From the above example, the access network provider allocated 10.1.2.3 to the host; therefore, they also need to control the DNS domain example.com and the associated NAPTR records. DNS Security Extensions (DNSSEC) (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements,” March 2005.) [RFC4033] provides a cryptographic means of validating this association, through data origin authentication.

4.2.1. Determining an External IP Address

TOC

Reverse DNS relies on knowing the IP address of a host within the access domain. Initially, this SHOULD be attempted using the IP address that is assigned to a local interface on the host. However, when a NAT device is used, the IP address of the NAT device is substituted for the source IP address. If a NAT device exists between the host and the access network, the host does not have any direct way to determine the IP address that it is effectively using within the access network. The IP address of the NAT device and the corresponding domain name can be used to discover the LIS.

In order to use reverse DNS in this configuration, the hosts need to know the IP address that the NAT device uses. The following sections describe some possible methods.

These methods are particularly useful in residential broadband configurations. A large proportion of residential broadband services employ a NAT device so that several hosts can share the same Internet access. Since the network behind the NAT device are generally very small, both in numbers and geographical area, it isn't necessary for a LIS to operate within that network; the hosts are able to access a LIS in the access network outside of the NAT device.

4.2.1.1. UPnP

TOC

If a NAT device complies with the Universal Plug and Play (UPnP) specification (UPnP Forum, “Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0: WANIPConnection:1 Service Template Version 1.01 For UPnP Version 1.0,” Nov 2001.) [UPnP-IGD-WANIPConnection1], the WANIPConnection part can be used to query the device for its public IP address. The GetExternalIPAddress function provides the external address for a particular network connection.

UPnP defines a method for discovering UPnP-enabled hosts in a network; the host does not need any prior configuration to employ this method.

4.2.1.2. STUN

TOC

A host can use the Session Traversal Utilities for NAT (STUN) (Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, “Session Traversal Utilities for (NAT) (STUN),” July 2008.) [I-D.ietf-behave-rfc3489bis] to determine a public IP address. The host uses the Binding Request message and the resulting XOR-MAPPED-ADDRESS parameter that is returned in the response.

Using STUN requires cooperation from a publicly accessible STUN server. The host also requires configuration information that identifies the STUN server, or a domain name that can be used for STUN server discovery.

4.2.1.3. Other Options

TOC

The source IP address in any IP packet can be used to determine the public IP address of a host. While the STUN method uses a small part of

a more sophisticated protocol, this principle can be applied using any other protocol. Like STUN, this method requires prior knowledge of the publicly accessible server and the method that it supports.
For instance, a publicly accessible host could be configured to respond to a UDP packet on a predefined port; the data of the response could contain the source IP address that was in the request. Alternatively, a HTTP server at a particular URL could be configured to respond to a GET request with a text/plain body containing the IP address of the requester. HTTP proxies render this method unusable; in particular, transparent HTTP proxies might affect the results of this method without the knowledge of the host. Such services already exist on the public Internet.

---

5. Discovery Order

TOC

The previous sections described a set of procedures that allow a device to determine the LIS associated with the local access network. Some networks maintain a topology analogous to an onion and are comprised of layers, or segments, separating hosts from the Internet through intermediate networks. It is best therefore for a host to discover the LIS logically closest to it, and this can best be done by applying the discovery techniques in the following order:

1. DHCP LIS URI Option
2. DNS U-NAPTR Discovery, using the domain name from:
    1. DHCP Domain Name Option
    2. Reverse DNS, using the hosts IP address from:
        1. the local network interface and immediate network segment
        2. the network segment adjacent to the immediate segment, as revealed by UPnP
        3. the public Internet, as revealed by STUN; or the network segment where the STUN server resides

        (4.) any network segment, as revealed by other method
3. Static configuration

DHCP discovery MUST be attempted before DNS discovery. This allows the network access provider a direct and explicit means of configuring a LIS address. DNS discovery is used as a failsafe, providing a means to discover a LIS where the DHCP infrastructure does not support the LIS URI option.

Static host configuration MAY be used to provide a LIS address if both DHCP and DNS methods fail. Note however, that if a host has moved from its customary location, static configuration might indicate a LIS that is unable to provide a location. User interaction is NOT RECOMMENDED; the discovery process is not easily diagnosed by a user.

LIS discovery through DNS requires the host to determine the domain name of the local access network. Where DHCP is available, the DHCP domain name option (Section 4.1 (DHCP Domain Name Option)) can be used to provide this information. If the domain name cannot be determined from DHCP, or the resulting domain name fails to yield a valid LIS address then reverse DNS is used.

The discovery procedure assumes that the correct LIS is in a network segment that is closer to the host. Each network segment between the host and LIS decreases the chance that the LIS is able to correctly determine a location for the host.

Discovery methods follow an order of precedence. The exception is for alternative methods of determining the hosts IP address in each network segment; precedence is given to addresses in the network segments closer to the host. Therefore, the host MUST attempt to use the IP address assigned to its local network interface before attempting to determine its IP address. Precedence is given to methods, like UPnP that provide an IP address in adjacent network segments. Methods for determining addresses on the public Internet are given lower precedence.

To claim compliance with this document, a host MUST support both DHCP discovery and U-NAPTR discovery. Further, the host MUST support retrieval of domain name from DHCP and reverse DNS, using a local interface address, UPnP and STUN. Additional methods for determining the IP address of the host in different network segments are optional.

5.1. Virtual Private Networks (VPNs)

TOC

Where a host has multiple network interfaces the host MAY independently discover the LIS corresponding to the access networks reached by each network interface. Resolving which LIS to contact for location information is a host application issue.

LIS discovery over a VPN network interface SHOULD NOT be performed since such a LIS does not have the physical presence generally necessary to determine location. However, since not all VPN interfaces can be detected by hosts, a LIS SHOULD NOT respond to requests originating from a VPN pool. This ensures that even if a host discovers a LIS over the VPN, it does not rely on a LIS that is unable to provide accurate location information. The exception to this is where the LIS and host are able to determine a location without access network support.

TBD: Is there an advantage in providing a HELD error code that indicates that the host has reached the LIS over a VPN?

---

6. Security Considerations

TOC

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 host does not necessarily have a prior relationship with a LIS. Several methods are described here that can limit the probablity of, or provide some protection against, such an attack.

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

If DHCP is used, the integrity of DHCP options is limited by the security of the channel over which they are provided. Physical security and separation of DHCP messages from other packets are commonplace methods that can reduce the possibility of attack within an access network; alternatively, DHCP authentication (Droms, R. and W. Arbaugh, “Authentication for DHCP Messages,” June 2001.) [RFC3118] can provide a degree of protection against modification.

An attacker could attempt to compromise the U-NAPTR resolution. A description of the security considerations for U-NAPTR applications is included in [RFC4848] (Daigle, L., “Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS),” April 2007.).

In addition to considerations related to U-NAPTR, it is important to recognize that the output of this is entirely dependent on its input. An attacker who can control the domain name can also control the final URI. Because a number of methods are provided for determining the domain name, a host implementation needs to consider attacks against each of the methods that are used.

Reverse DNS is subject to the maintenance of the in-addr.arpa. or ip6.arpa. domain and the integrity of the results that it provides. DNSSEC (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements,” March 2005.) [RFC4033] provides some measures that can improve the reliability of DNS results. In particular, DNSSEC SHOULD be applied to ensure that the reverse DNS record and the resulting domain are provided by the same entity before this method is used. Without this assurance, the host cannot be certain that the access network provider has provided the NAPTR record for the domain name that is provided.

Hosts behind NAT devices are also subject to attacks when retrieving their public IP address. [I-D.ietf-behave-rfc3489bis] (Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, “Session Traversal Utilities for (NAT) (STUN),” July 2008.) describes some means of mitigating this attack for STUN.

7. IANA Considerations

TOC

7.1. Registration of DHCPv4 and DHCPv6 Option Codes

TOC

The IANA is requested to assign an option code for the DHCPv4 option for a LIS address, as described in Section 2.1 (DHCPv4 Option for a LIS Address) of this document.
The IANA is requested to assign an option code for the DHCPv6 option for a LIS address, as described in Section 2.2 (DHCPv6 Option for a LIS Address) of this document.

7.2. Registration of a Location Server Application Service Tag

TOC

This section registers a new S-NAPTR/U-NAPTR Application Service tag for a LIS, as mandated by [RFC3958] (Daigle, L. and A. Newton, “Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS),” January 2005.).

> **Application Service Tag:** LIS
>
> **Intended usage:** Identifies a service that provides a host with its location information.
>
> **Defining publication:** RFCXXXX
>
> **Related publications:** HELD (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, “HTTP Enabled Location Delivery (HELD),” August 2009.) [I-D.ietf-geopriv-http-location-delivery]
>
> **Contact information:** The authors of this document
>
> **Author/Change controller:** The IESG

7.3. Registration of a Location Server Application Protocol Tag for HELD

TOC

This section registers a new S-NAPTR/U-NAPTR Application Protocol tag for the HELD (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)," August 2009.) [I-D.ietf-geopriv-http-location-delivery] protocol, as mandated by [RFC3958] (Daigle, L. and A. Newton, "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)," January 2005.).

> **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 (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)," August 2009.) [I-D.ietf-geopriv-http-location-delivery]
>
> **Contact Information:** The authors of this document
>
> **Author/Change Controller:** The IESG

---

8. Acknowledgements

TOC

The authors would like to thank Leslie Daigle for her work on U-NAPTR; Peter Koch for his feedback on the DNS aspects of this document; Andy Newton for constructive suggestions with regards to document direction; Hannes Tschofenig for input and reviews.

---

9. References

TOC

9.1. Normative References

TOC

[RFC1034]	Mockapetris, P., “Domain names - concepts and facilities,” STD 13, RFC 1034, November 1987 (TXT).
[RFC2131]	Droms, R., “Dynamic Host Configuration Protocol,” RFC 2131, March 1997 (TXT, HTML, XML).
[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 (TXT).
[RFC3396]	Lemon, T. and S. Cheshire, “Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4),” RFC 3396, November 2002 (TXT).
[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 (TXT).
[RFC4704]	Volz, B., “The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option,” RFC 4704, October 2006 (TXT).
[RFC4848]	Daigle, L., “Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS),” RFC 4848, April 2007 (TXT).
[I-D.ietf-behave-rfc3489bis]	Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, “Session Traversal Utilities for (NAT) (STUN),” draft-ietf-behave-rfc3489bis-18 (work in progress), July 2008 (TXT).
[I-D.ietf-dhc-dhcpv6-opt-dnsdomain]	Yan, R., “Domain Suffix Option for DHCPv6,” draft-ietf-dhc-dhcpv6-opt-dnsdomain-04 (work in progress), June 2007 (TXT).
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).

9.2. Informative References

TOC

[RFC2782]	Gulbrandsen, A., Vixie, P., and L. Esibov, “A DNS RR for specifying the location of services (DNS SRV),” RFC 2782, February 2000 (TXT).
[RFC3118]	Droms, R. and W. Arbaugh, “Authentication for DHCP Messages,” RFC 3118, June 2001 (TXT).
[RFC3693]	

	Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, “Geopriv Requirements,” RFC 3693, February 2004 (TXT).
[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 (TXT).
[RFC4033]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements,” RFC 4033, March 2005 (TXT).
[RFC4367]	Rosenberg, J. and IAB, “What's in a Name: False Assumptions about DNS Names,” RFC 4367, February 2006 (TXT).
[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-10 (work in progress), July 2009 (TXT).
[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-16 (work in progress), August 2009 (TXT).
[UPnP-IGD-WANIPConnection1]	UPnP Forum, “Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0: WANIPConnection:1 Service Template Version 1.01 For UPnP Version 1.0,” DCP 05-001, Nov 2001.

Appendix A. Residential Broadband LIS Discovery Example

TOC

This example shows how LIS discovery using U-NAPTR and DNS might be performed in a residential broadband scenario. The assumed network topology for this network is shown in Figure 4 (Example Network Topology).

```
                               __________             __________
   +----------------+         (          )           (          )
   |      NAT       |        (   ACCESS   )         (            )
   | (Home Router)  |-------(    NETWORK   )-------(   INTERNET   )
   |   192.0.2.75   |        ( my.isp.net )         (            )
   +----------------+         (          )           (          )
           |                   ----------             ----------
           |                                               :
           |                                               :
   +----------------+                            +-----------------+
   |     DEVICE     |                            |  VOICE SERVICE  |
   |                |                            |  PROVIDER (VSP) |
   |  192.168.0.55  |                            |   STUN SERVER   |
   +----------------+                            +-----------------+
```

Figure 4: Example Network Topology

In this example, the host sits behind a home router that includes a NAT function. The host is assigned an address from the private 192.168.x.x address range, in this case 192.168.0.55. The outbound IP address provided to the home router is public and and belongs to the my.isp.net domain; in this example the home router is assigned 192.0.2.75, which is also given the domain name 192-0-2-75.my.isp.net.

In this example, several methods are not possible due to the configuration of the devices and network. The DHCP server on the home router does not support the LIS URI option, and a domain name is not configured on the router. In addition to this, the UPnP service on home router is disabled. Therefore, the host attempts these methods and is unsuccessful.

The example first covers the unsuccessful attempts to discover the LIS, followed by a successful application of DNS discovery based on an address provided by a STUN server. In this situation, the STUN server is provided by a Voice Service Provider (VSP) that the owner of the host purchases a voice service from. The address of the STUN server is configured on the host. The VSP is a separate entity on the public Internet with no relation to the access network provider.

The sequence diagram below shows each of the failed attempts to discover the LIS, followed by the successful discovery using the STUN server, reverse DNS and the DNS discovery method.

```
+-------+         +--------+    +-----+     +-----+    +--------+
| HOST  |         |  HOME  |    | DNS |     | LIS |    |  STUN  |
|       |         | ROUTER |    |     |     |     |    | SERVER |
+---+---+         +----+---+    +--+--+     +--+--+    +---+----+
    |                  |            |           |           |
  1 +--- DHCPINFORM -->|            |           |           |
    |                  |            |           |           |
  2 |<---- DHCPACK ----+            |           |           |
    |                  |            |           |           |
  3 +------- DNS: PTR ------------->|           |           |
    |   55.0.168.192.in-addr.arpa.  |           |           |
    |                  |            |           |           |
  4 |<------ DNS: no domain --------+           |           |
    |                  |            |           |           |
  5 +----- UPnP: ----->|            |           |           |
    |   ssdp:discover  |            |           |           |
    |                  |            |           |           |
  6 |  (no response)   |            |           |           |
    |                  |            |           |           |
  7 +---------------- STUN: Binding Request --------------->|
    |                  |            |           |           |
  8 |<------- STUN: XOR-MAPPED-ADDRESS = (192.0.2.75) ------+
    |                  |            |           |           |
  9 +------- DNS: PTR ------------->|           |           |
    |    75.2.0.192.in-addr.arpa.   |           |           |
    |                  |            |           |           |
 10 |<--- 192-0-2-205.my.isp.net ---+           |           |
    |                  |            |           |           |
 11 +--- DNS: NAPTR my.isp.net ---->|           |           |
    |                  |            |           |           |
 12 |<--- https://lis.my.isp.net/ --+           |           |
    |                  |            |           |           |
 13 +-------- HELD: locationRequest ----------->|           |
    |                  |            |           |           |
    .                  .            .           .           .
```

Figure 5: LIS Discovery Sequence

1. The host makes a DHCP request for the LIS URI option. To reduce the overall time required in case the LIS URI is unknown, the host also requests the domain name option.

2. The DHCP server (in the home router) responds but does not have either datum. Therefore, the host is unable to use the DHCP method, or use the domain name to perform U-NAPTR discovery.

3. The host then attempts reverse DNS based on its IP address (192.168.0.55). The host makes a DNS PTR request for 55.0.168.192.in-addr.arpa.
4. The DNS server has no knowledge of the private network segment and so indicates that there is no such domain.
5. The host then must determine its address in a different network segment. It first attempts to discover this using UPnP. The host broadcasts a UPnP discovery message, attempting to locate a UPnP capable device that supports the WANIPConnection profile.
6. There are no UPnP devices on the network and the UPnP discovery message is unanswered.
7. The host contacts a STUN server, which is configured on the host. It sends a Binding Request to the STUN server.
8. The STUN server responds to the Binding Request, including the XOR-MAPPED-ADDRESS parameter. The host decodes this parameter, which reveals the IP address of the home router: 192.0.2.75.
9. The host requests the domain name assigned to 192.0.2.75. It makes a DNS PTR request to 75.2.0.192.in-addr.arpa.
10. The DNS server indicates that 192.0.2.75 is assigned the name 192-0-2-75.my.isp.net.
11. The host removes the host part of the domain name and makes a DNS NAPTR request for the domain my.isp.net.
12. The DNS server provides all NAPTR records for the my.isp.net. domain. The host finds the record with a service tag of LIS:HELD and retrieves the URI from the regexp field. The URI of the LIS is found to be https://lis.my.isp.net/.
13. The host sends a HELD locationRequest to the LIS.

Authors' Addresses

TOC

	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/

Full Copyright Statement

TOC

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.