Internet Engineering Task Force (IETF)
Request for Comments: 5986
Category: Standards Track
ISSN: 2070-1721

M. Thomson
J. Winterbottom
Andrew Corporation

September 2010

Discovering the Local Location Information Server (LIS)

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 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.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5986.

Copyright Notice

Table of Contents

1. Introduction and Overview 2
1.1. Discovery Procedure Overview 3
1.2. Terminology 3
2. LIS Discovery Procedure 4
2.1. Residential Gateways 6
2.2. Virtual Private Networks (VPNs) 7
3. Determining a Domain Name 7
3.1. Domain Name Encoding 7
3.2. Access Network Domain Name DHCPv4 Option 8
3.3. Access Network Domain Name DHCPv6 Option 8
3.4. Alternative Domain Names 9
4. U-NAPTR Resolution of a LIS URI 10
5. Security Considerations 11
6. IANA Considerations 13
6.1. Registration of DHCPv4 and DHCPv6 Option Codes 13
6.2. Registration of a Location Server Application Service Tag 13
6.3. Registration of a Location Server Application Protocol Tag for HELD 13
7. Acknowledgements 14
8. References 14
8.1. Normative References 14
8.2. Informative References 15

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 attached access networks used to provide Internet access. 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 [RFC2616] or HTTPS [RFC2818] URI that 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 HTTP-Enabled Location Delivery (HELD) [RFC5985]. URIs discovered in this way are not "location URIs" [RFC5808]; dereferencing one of them provides the location of the requestor 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 that allows a Device to operate in a specific network environment. The 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" have been 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 RFC 3693 [RFC3693] parlance, the Device is also the Target.

The term "access network" refers to the network to which a Device connects for Internet access. The "access network provider" is the entity that operates the access network. This is consistent with the definition in [RFC5687], 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 this process:

1. Acquire the access network domain name (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). If this option is not available, DHCPv4 option 15 [RFC2132] is used. Other domain names MAY be used, as described in Section 3.4.

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. Any HTTP 200 response containing a HELD response signifies success. This includes HELD error responses, with the exception of the "notLocatable" error.

If -- at any time -- the LIS responds to a request with the "notLocatable" error code (see Section 4.3.2 of [RFC5985]), 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. 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.

The overall discovery process is summarized in Figure 1.

```
       -----------
      (   Start   )
       -----+-----
            |<--------------------------------------+
            |                                       |
            V                                       |
      ------^-------            ------^------       |
     /              \          /      1.     \      |
    < Next interface >-------><  Get domain   >-----+
     \              / Y  ^     \             /  N
      ------v-------     |      ------v------
            | N          |            | Y
            |            |            V
            |            |      ------^------
            |            |     /      2.     \
            |            +----<    Get URI    ><----+
            |               N  \             /      |
            |                   ------v------       |
            |                         | Y           |
            |                         V             |
            |                   ------^------       |
            |                  /      3.     \      |
            |                 <   Check URI   >-----+
            |                  \             /  N
            |                   ------v------
            |                         | Y
            V                         V
       -----------                -----------
      (  Failure  )             (  Success  )
       -----------                -----------
```

Figure 1: LIS Discovery Flowchart

2.1. Residential Gateways

The options available in residential gateways will affect the success of this algorithm in residential network scenarios. A fixed wireline scenario is described in more detail in [RFC5687], Section 3.1. In this fixed wireline environment, an intervening residential gateway exists between the Device and the access network. If the residential gateway does not provide the appropriate information 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:

- acquire an access network domain name from the access network provider (possibly using DHCP) and pass the resulting value to Devices; or
- discover a LIS on its external interface, then provide Devices with the domain name that was used to successfully discover the LIS; or
- explicitly include configuration that refers to a particular LIS; or
- 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.

2.2. Virtual Private Networks (VPNs)

A Device MUST NOT attempt LIS discovery over a VPN network interface until it has attempted and failed to perform discovery on all other non-VPN interfaces. A Device MAY perform discovery over a VPN network interface if it has first attempted discovery on non-VPN interfaces, but 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. In these cases, it might be that a LIS on the remote side of a VPN is inadvertently discovered. A LIS provides a "notLocatable" error code in response to a request that it is unable to fulfill (see [RFC5985], Section 6.3). 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. Determining a Domain Name

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.

For example, the domain "example.com." is encoded in 13 octets as:

```
+---+---+---+---+---+---+---+---+---+---+---+---+---+
| 7 | e | x | a | m | p | l | e | 3 | c | o | m | 0 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

Note that the length field in either option represents the length of the entire domain name encoding, whereas the length fields in the domain name encoding is the length of a single domain name label.

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.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |   Length      |  Access Network Domain Name   .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.            Access Network Domain Name (cont.)                 .
.                              ...                              .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Access Network Domain Name DHCPv4 Option

option-code: OPTION_V4_ACCESS_DOMAIN (213).

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

option-value: The domain name associated with the access network, encoded as described in Section 3.1.

A DHCPv4 client MAY request an 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.

```
     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_V6_ACCESS_DOMAIN    |           Length              |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    .                  Access Network Domain Name                   .
    .                              ...                              .
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3: DHCPv6 Access Network Domain Name Option

option-code: OPTION_V6_ACCESS_DOMAIN (57).

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

option-value: The domain name associated with the access network, encoded as described in Section 3.1.

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

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

3.4. Alternative Domain Names

The U-NAPTR resolution method described requires a domain name as input. The access network domain name DHCP options (Sections 3.2 and 3.3) are 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.

DHCPv4 option 15 [RFC2132] provides an indication of the domain name that a host uses when resolving hostnames in DNS. This option is used when the DHCPv4 access domain name is not available.

DHCPv4 option 15 might not be suitable for some network deployments. For instance, a global enterprise could operate multiple sites, with Devices at all sites using the same value for option 15. In this type of deployment, it might be desirable to discover a LIS local to a site. The access domain name option can be given a different value at each site to enable discovery of a LIS at that site.

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.

Other domain names might be provided by a DHCP server (for example, [RFC4702] for DHCPv4, [RFC4704] for DHCPv6). However, these domain names could be provided without considering their use for LIS discovery; therefore, it is not likely that these other domain names contain useful values.

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 [RFC5985].

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 4: Sample LIS:HELD Service NAPTR Records

Details for the "LIS" Application Service tag and the "HELD" Application Protocol tag are included in Section 6.

U-NAPTR resolution might produce multiple results from each iteration of the algorithm. Order and preference values in the NAPTR record determine which value is chosen. A Device MAY attempt to use alternative choices if the first choice is not successful. However, if a request to the resulting URI produces a HELD "notLocatable" response, or equivalent, the Device SHOULD NOT attempt to use any alternative choices from the same domain name.

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 one that was input to the U-NAPTR resolution process.

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. impersonating the LIS

The domain name that used to authenticate the LIS is the domain name input to the U-NAPTR process, not the output of that process [RFC3958], [RFC4848]. As a result, the results of DNS queries do not need integrity protection.

An HTTPS URI is authenticated using the method described in Section 3.1 of [RFC2818]. HTTP client implementations frequently do not provide a means to authenticate based on a domain name other than the one indicated in the request URI, namely the U-NAPTR output. To avoid having to authenticate the LIS with a domain name that is different from the one used to identify it, a client MAY choose to reject URIs that contain a domain name that is different to the U-NAPTR input. To support endpoints that enforce the above restriction on URIs, network administrators SHOULD ensure that the domain name in the DHCP option is the same as the one contained in the resulting URI.

Authentication of a LIS relies on the integrity of the domain name acquired from DHCP. An attacker that is able to falsify a domain name circumvents the protections provided. 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 commonly used to reduce the possibility of such an attack within an access network. DHCP authentication [RFC3118] might also provide a degree of protection against modification or spoofing.

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 213 for the DHCPv4 option for an access network domain name option, as described in Section 3.2 of this document.

The IANA has assigned an option code of 57 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 LIS, as mandated by [RFC3958].

Application Service Tag: LIS

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

Defining publication: RFC 5986

Related publications: HELD [RFC5985]

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 protocol [RFC5985], as mandated by [RFC3958].

Application Protocol Tag: HELD

Intended Usage: Identifies the HELD protocol.

Applicable Service Tag(s): LIS

Terminal NAPTR Record Type(s): U

Defining Publication: RFC 5986

Related Publications: HELD [RFC5985]

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; and 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.

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

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[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.

[RFC5985] Barnes, M., Ed., "HTTP-Enabled Location Delivery (HELD)", RFC 5985, September 2010.

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.

[RFC5687] Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol: Problem Statement and Requirements", RFC 5687, March 2010.

[RFC5808] Marshall, R., "Requirements for a Location-by-Reference Mechanism", RFC 5808, May 2010.

Authors' Addresses

Martin Thomson
Andrew Corporation
Andrew Building (39)
Wollongong University Campus
Northfields Avenue
Wollongong, NSW 2522
AU

Phone: +61 2 4221 2915
EMail: martin.thomson@andrew.com

James Winterbottom
Andrew Corporation
Andrew Building (39)
Wollongong University Campus
Northfields Avenue
Wollongong, NSW 2522
AU

Phone: +61 2 4221 2938
EMail: james.winterbottom@andrew.com