Network WG
Internet-Draft
Intended status: Proposed Standard
Expires: Aug 25, 2013

James Polk
Cisco Systems

Feb 25, 2013

Dynamic Host Configuration Protocol (DHCP) IPv4 and IPv6 Option for a Location Uniform Resource Identifier (URI)

draft-ietf-geopriv-dhcp-lbyr-uri-option-19

Abstract

This document creates a Dynamic Host Configuration Protocol (DHCP) Option for transmitting a client’s geolocation Uniform Resource Identifier (URI). This Location URI can then be dereferenced in a separate transaction by the client or sent to another entity and dereferenced to learn physically where the client is located, but only while valid.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

This document creates a Dynamic Host Configuration Protocol (DHCP) Option for transmitting a client's geolocation Uniform Resource Identifier (URI) [RFC3986]. In this scenario, the DHCP client is a Geopriv Target (i.e., the entity whose geolocation is associated with the location URI). The DHCP implementation of the client can then make this location information available to other applications for their usage. This location URI points to a Location Server [RFC5808] which has the geolocation of the client (e.g., previously uploaded into a wiremap database then the client attaches to a known wall-jack, or by means of 802.11 geolocation mechanisms).

Applications within the Target can then choose to dereference this location URI and/or transmit the URI to another entity as a means of conveying where the Target is located. Both Conveying and Dereferencing a location URI is described in [RFC6442]. Session Initiation Protocol (SIP) [RFC3261] is not the only protocol that can dereference a location URI; there is also HTTP-Enabled Location Delivery (HELD) [RFC6753] and HTTP [RFC2616].

A Location Server (LS) stores the Target's location as a presence document, called a Presence Information Data Format - Location Object (PIDF-LO), defined in RFC 4119 [RFC4119]. The Location Server is the entity contacted during the act of dereferencing a Target's location. If the dereferencing entity has permission, defined in [RFC6772], the location of the target will be received. The LS will grant permission to location inquiries based on the rules established by a Rule Holder [RFC3693]. The LS has the ability to challenge any request for a target's location, thereby providing additive security properties before location revelation.

Possessing a location URI has advantages over having a PIDF-LO, especially when a target's location changes. With a location URI, when a target moves, the location URI does not change (at least within the same domain). The location URI can still be given out as the reference to the Target's current location. The opposite is true if the location is conveyed by value in a message. Once the Target moves, the previously given location is no longer valid, and if the Target wants to inform another entity about its location, it has to send the PIDF-LO to the location recipient (again).

A problem exists within existing RFCs that provide location to the UA ([RFC6225] and [RFC4776]). Those DHCP Options for geolocation values require an update of the entire location information (LI) every time a client moves. Not all clients will move frequently, but some will. Refreshing location values every time a client moves does not scale in certain networks/environments, such as IP-based cellular networks, enterprise networks or service provider networks with mobile endpoints. An 802.11 based access network is one example of this. Constantly updating Location Configuration Information (LCI) to endpoints might not scale in mobile (residential or enterprise or municipal) networks in which the client is moving through more than one network attachment point, perhaps as a person walks or drives with their client down a neighborhood street or apartment complex or a shopping center or through a municipality (that has IP connectivity as a service).

If the client was provided a location URI reference to retain and hand out when it wants or needs to convey its location (in a protocol other than DHCP), a location URI that would not change as the client's location changes (within a domain). Scaling issues would be significantly reduced to needing an update of the location URI only when a client changes administrative domains - which is much less often. This delivery of an indirect location has the added benefit of not using up valuable or limited bandwidth to the client with the constant updates. It also relieves the client from having to determine when it has moved far enough to consider asking for a refresh of its location.

In enterprise networks, if a known location is assigned to each individual Ethernet port in the network, a device that attaches to the network, such as a wall-jack (directly associated with a specific Ethernet Switch port) will be associated with a known location via a unique circuit-ID that's used by the Relay Agent Information Option (RAIO) defined in RFC 3046 [RFC3046]. This assumes wall-jacks have an updated wiremap database. RFC 6225 [RFC6225] and RFC 4776 [RFC4776] would return an LCI value of location for either IPv4 or IPv6. This document specifies how a location URI is returned using DHCP. The location URI points to a PIDF-LO contained on an LS. Performing a dereferencing transaction, that Target's PIDF-LO will be returned. If local configuration has the requirement of only assigning unique location URIs to each client at the same attachment point to the network (i.e., same RJ-45 jack or same 802.11 Access Point - except when triangulation is used), then unique location URIs will be given out. They will all have the same location at the record, relieving the backend Sighter or LS from individually maintaining each location independently.

The location URI Option can be useful in IEEE 802.16e connected endpoints or IP cellular endpoints. The location URI Option can be configured on a router, such as a residential home gateway, such that the router receives this Location URI Option as a client with the ability to communicate to downstream endpoints as a server.

How an LS responds to a dereference request can vary, and a policy established by a Ruleholder [RFC3693] for a Location Target as to what type of challenge(s) is to be used, how strong a challenge is used or how precise the location information is given to a Location Recipient (LR). This document does not provide mechanisms for the LS to tell the client about policies or for the client to specify a policy for the LS. While an LS should apply an appropriate access-control policy, clients must assume that the LS will provide location in response to any request (following the possession model [RFC5808]). For further discussion of privacy, see the Security Considerations.

This document IANA-registers the new IPv4 and IPv6 DHCP Options for a location URI and Valid-For.

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].

2. Format of the DHCP LocationURI Option

2.1 Overall Format of LocationURI Option in IPv4

The LocationURI Option format for IPv4 is as follows:

```
   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 XXX    |   Length=XX   |          Valid-For        .....
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.....       Valid-For (Cont'd)    |         LocationURI...    .....
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.....                                                             |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1. IPv4 Fields for this LocationURI Option

Code XXX: The code for this DHCPv4 option (IANA assigned).

Length=XX: The length of this option, counted in bytes - not counting the Code and Length bytes. This is a variable length Option, therefore the length value will change based on the length of the URI within the Option.

Valid-For: The time, in seconds, the LocationURI is to be considered valid for dereferencing. The Valid-For is always represented as a four-byte unsigned integer.

LocationURI: Location URI - This field, in bytes, is the URI pointing at the location record where the PIDF-LO for the Location Target resides. The LocationURI is always represented in ASCII.

2.2 Overall Format of LocationURI Option in IPv6

The LocationURI Option format for IPv6 is as follows:

```
  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-code          |          option-len           |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                           Valid-For                           |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                          LocationURI...                  .....
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.....                                                            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2. IPv6 fields of this LocationURI Option

option-code: The code for this DHCPv6 option (IANA assigned).

option-len: The length of this option, counted in bytes - not counting the option-code and option-len bytes. This is a variable length Option, therefore the length value will change based on the length of the URI within the Option.

Valid-For: see Section 2.1

LocationURI: see Section 2.1

2.3 Rules for the LocationURI Option

The LocationURI Option has the following rules:

- o Implementation of the Location URI Option is REQUIRED on the DHCP server and client.

- o Clients SHOULD be expected to have to request the Location URI Option from servers. Although local policy can have servers perform an unsolicited push of a Location URI Option to a client.

Applications on a client can use the Location URI (value) until the Valid-For value reaches zero. If there is no Valid-For Option value, then the counter did not ever start (a null value), and applications on a client continue to use the Location URI value until given a new Location URI Option (with or without a Valid-For value) which overwrites any previous Location URI and Valid-For Option values.

- o A Location URI Option with a non-zero Valid-For field MUST NOT transmit the Location URI once the Valid-For field counts down to zero.

- o A received Location URI Option containing all zeros in the Valid-For field means that Location URI has no lifetime, and not "no lifetime left". All zeros in the Valid-For field equates to a null value.

- o Receipt of the Location URI Option containing all zeros in the Valid-For field MUST NOT cause any error in handling the Location URI.

- o When the Valid-For timer reaches zero, the client MUST purge any location URI received via DHCP from its memory.

The choice of the Valid-For value is a policy decision for the operator of the DHCP server. Like location URIs themselves, it can be statically configured on the DHCP server or provisioned dynamically (via an out-of-band exchange with a Location Information Server) as requests for location URIs are received.

- o Clients receiving a Location URI Option start the Valid-For timer upon receipt of the DHCP message containing the Option.

- o Clients MUST NOT trigger an automatic DHCP refresh on expiry of the Valid-For timer; rather, they MUST follow normal DHCP mechanics.

If the Valid-For timer is set to expire before the lease refresh, the client will not have the ability to hand out its location until the lease refresh, inadvertently allowing a gap of coverage. If the Valid-For timer is set to expire after the lease refresh, some wayward application on the client can divulge that location URI after it is no longer valid, meaning the location could be stale or just plain wrong.

- o Servers SHOULD set the Valid-For timer to that of the lease refresh, or bad things can happen.

3. DHCP Option Operation

The [RFC3046] RAIO can be utilized to provide the appropriate indication to the DHCP Server where this DISCOVER or REQUEST message came from, in order to supply the correct response.

Caution SHOULD always be used involving the creation of large Options, meaning that this Option may need to be in its own INFORM, OPTION or ACK message. DHCP messages are limited in size, and long URIs will require the use of multiple messages and concatenation [RFC3396]. It is, therefore, best to limit the total length of a URI, including any parameters, to 220 bytes.

Location URIs MUST NOT reveal identity information of the user of the device, since DHCP is a cleartext delivery protocol. For example, creating a location URI such as

    sips:34LKJH534663J54@example.com

is better than a location URI such as

    sips:aliceisat123mainstatlantageorgiaus@example.com

The username portion of the first example URI provides no direct identity information (in which 34LKJH534663J54 is considered to be a random number in this example).

In the <presence> element of a PIDF-LO document, there is an 'entity' attribute that identifies what entity *this* presence document (including the associated location) refers to. It is up to the PIDF-LO generator, either Location Server or an application in the endpoint, to insert the identity in the 'entity' attribute. This can be seen in [RFC4119]. The considerations for populating the entity attribute value in a PIDF-LO document are independent from the considerations for avoiding exposing identification information in the username part of a location URI.

This Option is used only for communications between a DHCP client and a DHCP server. It can be solicited (requested) by the client, or it can be pushed by the server without a request for it. DHCP Options not understood MUST be ignored [RFC2131]. A DHCP server supporting this Option might or might not have the location of a client. If a server does not have a client's location, but needs to provide this Location URI Option to a client (for whatever reason), an LS is contacted. This server-to-LS transaction is not DHCP, therefore it is out of scope of this document. Note that this server-to-LS transaction could delay the DHCP messaging to the client. If the server fails to have location before it transmits its message to the client, location will not be part of that DHCP message. Any timers involved here are a matter of local configuration.

The dereference of a target’s location URI would not involve DHCP, but an application layer protocol, such as SIP or HTTP, therefore dereferencing is out of scope of this document.

In the case of residential gateways being DHCP servers, they usually perform as DHCP clients in a hierarchical fashion up into a service provider’s network DHCP server(s), or learn what information to provide via DHCP to residential clients through a protocol, such as PPP. In these cases, the location URI would likely indicate the residence’s civic address to all wired or wireless clients within that residence.

4. Architectural Assumptions

The following assumptions are made once the client has obtained a location URI, and not about DHCP operation specifics (in no particular order):

- Any user control (what [RFC3693] calls a ’Ruleholder’) for access to the dereferencing step is assumed to be out of scope of this document. An example authorization policy is in [RFC6772].

- The authorization security model vs. possession security model discussion can be found in [RFC5606], describing what is expected in each model of operation. It should be assumed that a location URI attained using DHCP will operate under a possession model by default. An authorization model can be instituted as a matter of local policy. An authorization model means possessing the location URI does not give that entity the right to view the PIDF-LO of the target whose location is indicated in a presence document. The dereference transaction will be challenged by the Location Server only in an authorization model. The nature of this challenge is out of scope of this document.

- This document does not prevent some environments from operating in an authorization model, for example - in less tightly controlled networks. The costs associated with authorization vs. possession models are discussed in Section 3.3.2 of [RFC5606].

4.1 Harmful URIs and URLs

There are, in fact, some types of URIs that are not good to receive, due to security concerns. For example, any URLs that can have scripts, such as "data:" URLs, and some "HTTP:" URLs that go to web pages that have scripts. Therefore,

- URIs received via this Option SHOULD NOT be automatically sent to a general-browser to connect to a web page, because they could have harmful scripts, unless o the browser has been set up to defend against harmful scripts,

or

o the browser does not run scripts automatically.

- o This Option MUST NOT contain "data:" URLs [RFC2397], because they could contain harmful scripts.

4.2 Valid Location URI Schemes or Types

URIs carried by this DHCP Option MUST have one of the following URI schemes:

1. sip:
2. sips:
3. pres:
4. http:
5. https:

URIs using the "pres" scheme are dereferenced using the presence event package for SIP [RFC3856], so they will reference a PIDF-LO document when location is available. Responses to requests for URIs with other schemes ("sip", "sips", "http", and "https") MUST have media type 'application/pidf+xml'[RFC4119]. Alternatively, HTTP and HTTPS URIs MAY refer to information with media type 'application/held+xml', in order to support HELD dereferencing [RFC6753]. Clients can indicate which media types they support using the "Accept" header field in SIP [RFC3261] or HTTP [RFC2616].

See RFC 3922 [RFC3922] for using the "pres:" URI with XMPP.

It is RECOMMENDED that implementers follow Section 4.6 of RFC 6442 [RFC6442] as guidance regarding which Location URI schemes to provide in DHCP. That document discusses what a receiving entity does when receiving a URI scheme that is not understood. Awareness to the two URI types there is important for conveying location, if SIP is used to convey a Location URI provided by DHCP.

5. IANA Considerations

5.1 The IPv4 Option number for the Location URI Option

This document IANA registers the DHCP Location URI Option Number in the BOOTP Vendor Extensions and DHCP Options subregistry of the Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) Parameters registry located.

Tag	Name	Data Length	Meaning	Reference
XXX	LocationURI	N	GeoLocation URI	[this document]

The authors have no preference at this time on what number IANA chooses.

5.2 The IPv6 Option-Code for the Location URI Option

This document IANA registers the DHCPv6 Option Code in the DHCP Option Codes subregistry of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) registry.

Value	Description	Reference
XX	OPTION_GEOLOCATION_URI	[this document]

The authors have no preference at this time on what number IANA chooses.

5.3 Valid Location URI Schemes

This document creates a new IANA registry (Valid Location URI Schemes) of acceptable location URI schemes (or types) for this DHCP Location URI Option of the Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) Parameters registry.

Initial values are given below; new assignments are to be made following the "IETF Review" policies [RFC5226].

"Valid Location URI Schemes"

Location URI Scheme	Reference
sip:	[this document]
sips:	[this document]
pres:	[this document]
http:	[this document]
https:	[this document]

6. Security Considerations

Where critical decisions might be based on the value of this location URI option, DHCP authentication as defined in "Authentication for DHCP Messages" [RFC3118] and "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)" [RFC3315] SHOULD be used to protect the integrity of the DHCP options.

A real concern with RFC 3118 or RFC 3315 is that neither is widely deployed because each requires pre-shared keys to successfully work (i.e., in the client and in the server). Most implementations do not accommodate this.

DHCP, initially, is a broadcast request (a client looking for a server), and a unicast response (answer from a server) type of protocol. There is no privacy protection for DHCP messages, an eavesdropper who can monitor the link between the DHCP server and requesting client can discover the Location URI.

Once a client has a Location URI, it needs information on how the location server will control access to dereference requests. A client might treat a tightly access-controlled URI differently from one that can be dereferenced by anyone on the Internet (i.e., one following the "possession model"). Since the client does not know what policy will be applied during this validity interval, clients MUST handle location URIs as if they could be dereferenced by anybody until they expire. For example, such open location URIs should only be transmitted in encrypted channels. Nonetheless, location servers SHOULD apply appropriate access control policies, for example by limiting the number of queries that any given client can make, or limiting access to users within an enterprise.

Extensions to this option, such as [ID-POLICY-URI] can provide mechanisms for accessing and provisioning policy. Giving users access to policy information will allow them to make more informed decisions about how to use their location URIs. Allowing users to provide policy information to the LS will enable them to tailor access control policies to their needs (within the bounds of policy that the LS will accept).

As to the concerns about the location URI itself, as stated in the document (see Section 3), it MUST NOT have any user identifying information in the URI user-part/string itself. The location URI also needs to be hard to guess that it belongs to a specific user.

In some cases a DHCP server may be implemented across an uncontrolled network. In those cases, it would be appropriate for a network administrator to perform a threat analysis (see RFC 3552) and take precautions as needed.

Link-layer confidentiality and integrity protection may also be employed to reduce the risk of location disclosure and tampering.

7. Acknowledgements

Thanks to James Winterbottom, Marc Linsner, Roger Marshall and Robert Sparks for their useful comments. And to Lisa Dusseault for her concerns about the types of URIs that can cause harm. To

Richard Barnes for inspiring a more robust Security Considerations section, and for offering the text to incorporate HTTP URIs. To Hannes Tschofenig and Ted Hardie for riding me to comply with their concerns, including a good scrubbing of the nearly final doc.

8. References

8.1. Normative References

[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.

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

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

[RFC3315] R. Droms, Ed., J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003

[RFC3261] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, May 2002.

[RFC3396] T. Lemon, S. Cheshire, "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)", RFC 3396, November 2002

[RFC3856] J. Rosenberg, "A Presence Event Package for the Session Initiation Protocol (SIP)", RFC 3856, August 2004

[RFC3922] P. Saint-Andre, " Mapping the Extensible Messaging and Presence Protocol (XMPP) to Common Presence and Instant Messaging (CPIM)", RFC 3922, October 2004

[RFC3986] T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", RFC 3986, January 2005

[RFC4119] J. Peterson, "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005

[RFC5226] T. Narten, H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, May 2008

[RFC6442] Polk, J., Rosen, B., and J. Peterson, "Location Conveyance for the Session Initiation Protocol", RFC 6442, December 2011.

[RFC6753] J. Winterbottom, H. Tschofenig, H. Schulzrinne, M. Thomson, M. Dawson, "A Location Dereferencing Protocol Using HELD", October 2012

8.2. Informative References

[RFC2397] L. Masinter, "The "data" URL scheme", RFC 2397, August 1998

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

[RFC3693] J. Cuellar, J. Morris, D. Mulligan, J. Peterson. J. Polk, "Geopriv Requirements", RFC 3693, February 2004

[RFC6225] Polk, J., Linsner, M., Thomson, M., and B. Aboba, "Dynamic Host Configuration Protocol Options for Coordinate-Based Location Configuration Information", RFC 6225, July 2011.

[RFC4776] H. Schulzrinne, "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information ", RFC 4776, November 2006

[RFC5606] J. Peterson, T. Hardie, J. Morris, "Implications of ’retransmission-allowed’ for SIP Location Conveyance", August 2009

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

[RFC6772] H. Schulzrinne, H. Tschofenig, J. Morris, J. Cuellar, J. Polk, "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", January 2013

[ID-POLICY-URI] R. Barnes, M. Thomson, J. Winterbottom, "Location Configuration Extensions for Policy Management", "work in progress", November 2011

Authors’ Address

James Polk
3913 Treemont Circle
Colleyville, Texas 76034
USA

Email: jmpolk@cisco.com