Geopriv WG
Internet-Draft
Intended status: Standards Track (PS)
Expires: April 13, 2011

James Polk
Cisco Systems

Oct 13, 2010

Dynamic Host Configuration Protocol (DHCP) IPv4 and IPv6 Option for a Location Uniform Resource Identifier (URI) draft-ietf-geopriv-dhcp-lbyr-uri-option-09

Abstract

This document creates a Dynamic Host Configuration Protocol (DHCP) Option for transmitting a client's geolocation Uniform Resource Identifier (URI) of a client, which can be dereferenced in a separate transaction by the client or an entity the client sends this URI to.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on April 13, 2011.

Copyright Notice

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

document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

Table of Contents

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].

1. Introduction

This document creates a Dynamic Host Configuration Protocol (DHCP) Option for transmitting a client's geolocation Uniform Resource Identifier (URI). The DHCP implementation of the client can then make this location information available to upper layer protocols for their usage. This location URI points a Location Server [RFC5808] which has the geolocation of the client (through means not defined in this document). In this scenario, the DHCP client is a Geopriv Target (i.e., the entity whose geolocation is

associated by the location URI).

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

Having 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). It 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 it the Target wants to inform another entity about its location, it has to send the PIDF-LO to the location recipient (again).

A Location Server (LS) stores the Target's location as a presence document, called a Presence Information Date 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 [ID-GEO-POL], the location of the target will be received. The LS will grant permission to location inquires 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.

A problem exists within existing RFCs that provide location to the UA ([RFC3825] and [RFC4776]). These 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 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 were 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 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 RAIO Option defined in RFC 3046 [RFC3046]. This assumes wall-jacks have an updated wiremap

database. RFC 3825 and RFC 4776 would return an LCI value of location. This document specifies how a location URI is returned using DHCP. Behind the DHCP server, in the backend of the network, via the (logical entity of an) LS has a PIDF-LO to be dereferenced with a location URI.

If local configuration has the requirement of only assigning unique location URIs to each client, then unique location URIs will be given out, though they will all have the same location at the record, relieving the backend Sighter or LS from individually maintaining each location independently.

This Option can be useful in IEEE 802.16e connected endpoints or IP cellular endpoints. The location URI Option can be configured as a client if there is a router, such as a residential home gateway, 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 DHC Options for a location URI.

2. Format of the DHCP LuriElement Option

2.1 Overall Format of LuriElement Option in IPv4

The LuriElement Option format for IPv4 is as follows:

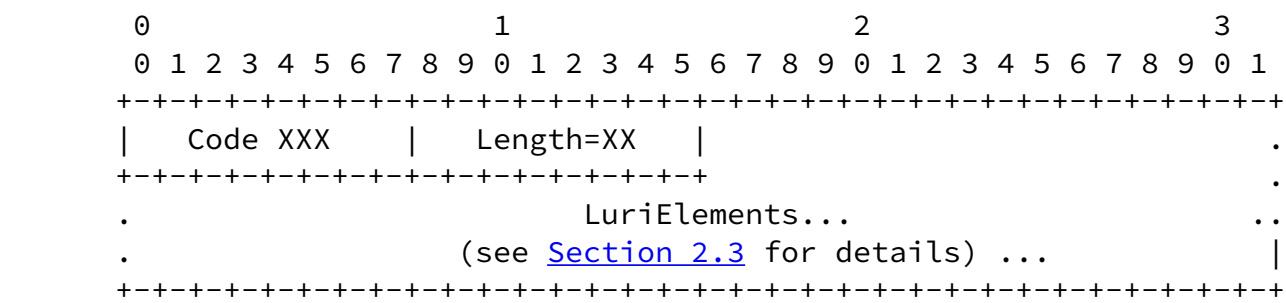

Figure 1. IPv4 Fields for this LuriElement Option

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.

LuriElement: see Section 2.3 for details

2.2 Overall Format of LuriElement Option in IPv6

The LuriElement Option format for IPv6 is as follows:

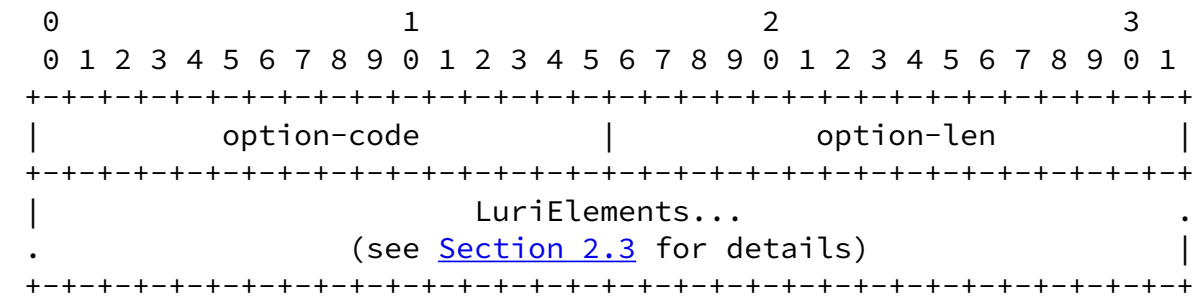

Figure 2. IPv6 fields of this LuriElement Option

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

option-len: 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.

LuriElement: see below (Section 2.3 for details).

2.3 LuriElement Format for both IPv4 and IPv6

The LuriElement, in both DHCPv4 and DHCPv6, have the following format:

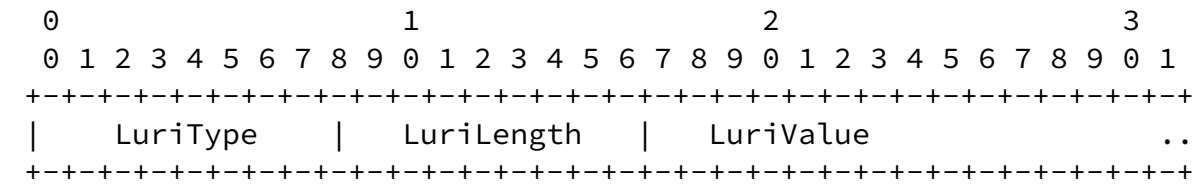

Figure 3. LuriElement Format for both IPv4 and IPv6

LuriType: A one-byte identifier of the data location value.

LuriLength: The length, in bytes, of the LuriValue, not including the LuriLength field itself, up to a maximum of 255

bytes.

LuriValue: The LuriElement value, as described in detail below.

The LuriValue is always in UTP-8.

The LuriTypes this document defines (and IANA registers) for a point are:

LuriType=1 Location URI - This is the URI pointing at the location record where the PIDF-LO resides which indicates the location of the Location Target.

LuriType=2 Valid-For - The time, in seconds, this URI is to be considered Valid for dereferencing. The timer associated with this LuriType starts upon receipt of this Option by the client.

The LuriType=2 (Valid-For) indicates how long, in seconds, the client is to consider this LuriType=1 (location URI) valid before performing a refresh of this Option, with a refreshed LuriType=2 (Valid-For) value. A Location URI refresh SHOULD be done the normal DHCP refresh rate, or necessitated by this timer, perhaps with the client only requesting this Option be refreshed.

If the LuriType=2 (Valid-For) timer is received (solicited or unsolicited), it is RECOMMENDED that the client refresh the Location URI when the (Valid-For) counter value has reaches the halfway point. For example, if 16000 was the initial value of the LuriType=2 (Valid-For) value, when 8000 seconds have passed, the Option SHOULD be refreshed.

The LuriType=2 (Valid-For) is not mandated for use by this document. However, its presence MUST NOT cause any error in handling the location URI (i.e., if not understood, it MUST be ignored).

This Option format is highly extensible. Additional LuriType types created MUST be done so through IANA registration with a standards track RFC.

3. DHC 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.

It is RECOMMENDED to avoid building URIs, with any parameters, larger than what a single DHCP response can be. However, if a

message is larger than 255 bytes, concatenation is allowed, per RFC 3396 [RFC3396].

Per [RFC2131], subsequent LuriElement Options, which are non-concatenated, overwrite the previous value.

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

sips:34LKJH534663J54@example.com

are to be done, providing no identity information, rather than a location URI such as this

sips:aliceisat123mainstalanta@example.com

In the <presence> element of a PIDF-LO document, there is an 'entity' attribute that identities what entity *this* 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 entity= discussion is orthogonal to the identification information contained within the 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 are ignored. 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.

The deference 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.

3.1 Architectural Assumptions

The following assumptions have been made for use of this LuriElement Option for a client to learn its location URI (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 [ID-GEO-POL].

- The authorization vs. possession security model can be found in [RFC5808], describing what is expected in each model of operation. It should be assumed that a location URI attained using DHCP will operate under an authorization model. This 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, in many environments, challenged by the Location Server. The nature of this challenge is out of scope of this document.

- This document does not prevent some environments from operating in a possession model, for example - tightly controlled enterprise networks, but this operation SHOULD NOT be assumed to exist as a matter of local policy. The costs associated with authorization vs. possession models are discussed in Section 3.3.2 of [RFC5606].

3.2 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 sent to a general-browser to connect to a web page, because they could have harmful scripts.

o This Option SHOULD NOT contain "data:" URLs, because they could contain harmful scripts.

Instead of listing all the types of URIs and URLs that can be misused or potentially have harmful affects, Section 3.3 IANA registers acceptable location URI schemes (or types).

3.3 Valid Location URI Schemes or Types

This section specifies which URI types are acceptable as a location URI scheme (or type) for this DHCP Option:

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 MIME type 'application/pidf+xml'. Alternatively, HTTP and HTTPS URIs MAY refer to information with MIME type 'application/held+xml', in order to support HELD dereferencing [ID-HELD-DEREF]. Clients can indicate which MIME types they support using the "Accept" header field in SIP [RFC3261] or HTTP [RFC2616].

These location URI types are IANA registered in Section 4.2 of this document.

4. IANA Considerations

4.1 The IPv4 Option number for this Option

This document IANA registers this IPv4 Option number XXX (to be assigned by IANA once this document becomes an RFC).

4.2 The IPv6 Option-Code for this Option

This document IANA registers this IPv6 Option-Code XXX (to be assigned by IANA once this document becomes an RFC).

4.3 IANA Considerations for Acceptable Location URI Types

IANA is requested to create a new registry for acceptable location URI types.

The following 3 URI types are registered by this document:

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

Any additional location URI types to be defined for use via this DHC Option need to be created and IANA registered with peer review and an RFC.

4.4 IANA Considerations for LuriTypes

IANA is requested to create a new registry for acceptable location types defined in Section 3.2 of this document, arranged similar to

this:

LuriType	Name	Reference
1	Location URI	RFC XXXX*
2	Valid-For	RFC XXXX*

* RFC XXXX is to be replaced with this document's RFC-Editor RFC number.

Additions to this registry require a standards track RFC.

5. Security Considerations

Where critical decisions might be based on the value of this location URI option, DHCP authentication in [RFC3118] SHOULD be used to protect the integrity of the DHCP options.

A real concern with RFC 3118 it is that not widely deployed because it 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. It does not provide security at the network layer. Instead, it relies on lower-layer security mechanisms. In today's infrastructures, DHCP will be primarily used over a wired, switched Ethernet network, requiring physical access to within a wire to gain access. Further, within an 802.11 wireless network, the 802.11 specs offer layer 2 security mechanisms to prevent a location URI from being learned by an unauthorized entity.

Once a client has a 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"). With the LuriTypes defined in this document, the DHCP option for delivering location URIs can only tell the user how long the URI will be valid. 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).

Penetrating an LS is supposed to be hard, and hopefully vendors that

implement an LS accomplish this goal.

As to the concerns about the location URI itself, as stated in the document here (in 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.

When implementing a DHC server that will serve clients across an uncontrolled network, one should consider the potential security risks therein.

6. 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. To Richard Barnes for his guidance with respect to the model used by this document and fine tuning the security considerations section.

7. References

7.1. Normative References

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

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

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

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

[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

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

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

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

7.2. Informative References

[ID-SIP-LOC] J. Polk, B. Rosen, J. Peterson, "SIP Location Conveyance", "work in progress", July 2010

[ID-HELD-DEREF] J. Winterbottom, H. Tschofenig, H. Schulzrinne, M. Thomson, M. Dawson, "A Location Dereferencing Protocol Using HELD", "work in progress", January 2010

[RFC3825] J. Polk, J. Schnizlein, M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", RFC 3825, July 2004

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

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

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

[ID-GEO-POL] H. Schulzrinne, H. Tschofenig, J. Morris, J. Cuellar, J. Polk, "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", "work in progress", July 2010

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

[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

[ID-POLICY-URI] R. Barnes, M. Thomson, J. Winterbottom, "Location Configuration Extensions for Policy Management", "work in progress", May 2010

Authors' Address

James Polk
3913 Treemont Circle
Colleyville, Texas 76034
USA

Email: jmpolk@cisco.com