

Geopriv WG
Internet-Draft
Expires: May 18th, 2008
Intended status: Standards Track (PS)

James Polk
Cisco Systems
November 18th, 2007

Dynamic Host Configuration Protocol (DHCP) Option for a
Location-by-Reference (LbyR) Uniform Resource Identifier (URI)
[draft-polk-geopriv-dhcp-lbyr-uri-option-02](#)

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of 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 May 18th, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document creates a Dynamic Host Configuration Protocol (DHCP) Option for the Location-by-Reference (LbyR) Uniform Resource Identifier (URI) of an endpoint. For example, an endpoint can be a Session Initiation Protocol (SIP) User Agent (i.e., a phone). This LbyR URI can be included in a UA's messages to inform other nodes of that entity's geographic location, once the URI is dereferenced by a Location Recipient.

Polk

Expires May 18th 2008

[Page 1]

Table of Contents

1.	Introduction	2
1.1.	Conventions Used in this Document	4
2.	DHC Location URI Elements	4
2.1.	Elements of the Location Configuration Information	4
3.	DHC Option Operation	5
3.1.	Architectural Assumptions	6
3.2.	Harmful URIs and URLs	6
4.	Acknowledgements	6
5.	IANA Considerations	7
6.	Security Considerations	7
7.	References	7
7.1.	Normative References	7
7.2.	Informative References	8
	Authors' Addresses	8
	Intellectual Property and Copyright Statements	8

[1.](#) Introduction

This document creates a Dynamic Host Configuration Protocol (DHCP) Option for delivery of a client's Location-by-Reference (LbyR) Uniform Resource Identifier (URI). For example, a client can be a Session Initiation Protocol (SIP) User Agent (UA) [[RFC3261](#)] (i.e., a Phone). This LbyR URI can be included in one UA's messages to informing those remote devices of that UA's geographic location, once the URI is dereferenced by a Location Recipient [[ID-SIP-LOC](#)]. A Location Recipient is a device that has received location from another device. If this location is delivered by a URI, the URI has to be dereferenced by the Location Recipient to learn the remote device's geographic location. Dereferencing can be done in SIP by use of the SUBSCRIBE/NOTIFY Methods [[RFC3265](#)] to either a sip:, sips: or pres: scheme URI.

Endpoints will require their geographic location for a growing number of services. A popular use-case currently is for emergency services, in which SIP requires its location to be placed in a SIP INVITE request message towards a public safety answering point (PSAP), i.e., an emergency response center. The reason for this is twofold:

- o An emergency services SIP request must be routed/retargeted to the appropriate PSAP that is local to where the calling device is.
- o The first responders require the UA's location in order to know where to be dispatched to render aid to the caller.

There are other use-cases, such as calling the appropriate Pizza Hut

without having to look up which store is closest. A UA knowing its location can call a main/national/international Pizza Hut number or

Polk

Expires May 18th 2008

[Page 2]

address and let the UA's location tell Pizza Hut enough information to have them route/retarget the SIP request to the appropriate store within the Pizza Hut organization to deliver the pizza to the caller's location.

A problem exists within existing RFCs that provide location to the UA ([\[RFC3825\]](#) and [\[RFC4776\]](#)) that location has to be updated every time a UA moves. Not all UAs will move frequently, but some will. Refreshing location every time a UA moves does not scale in certain networks/environments, such as enterprise networks or service provider networks with mobile endpoints. An 802.11 based access network is an example of this. This also might not scale in mobile residential networks in which the UA is hopping between more than one network attachment point, perhaps as a person walks with their UA down a neighborhood street or apartment complex.

If the UA were provided a URI reference to retain and hand out when it wants to convey its location, one that would not change as the UA's location changes, scaling issues would be significantly reduced. This delivery of an indirect location has the added benefit of not using up valuable or limited bandwidth to the UA with the constant updates. It also relieves the UA from having to determine when it has moved far enough to consider asking for a refresh of its location. Once the UA has a LbyR URI, a service provider would merely update the location at the URI the UA already has. This document does not define how this update is done, as it will likely not be with DHCP.

In enterprise networks, a URI can be assigned to individual Ethernet ports because each is assigned a unique circuit-ID that's used by the RAI0 Option defined in [RFC 3046](#) [\[RFC3046\]](#); meaning whatever is attached to a particular port will get the same URI because that device is at a known location (where the cable attached to that port is terminated). This scenario applies to 802.11 Access Points (AP), in which the AP's location is what's fixed and known. The same URI can be given to all devices attached to the same AP. [RFC 4119](#) [\[RFC4119\]](#) has the <method> element, which indicates how the endpoint learned its location. In this scenario, the <method> element indicates in the PIDF-LO the UA learned its location through DHCP, thus informing the call taker the UA is within a certain radius of the AP.

Just as with residential router/gateways, which can be wired or wireless, in which all devices understanding this Option will be giving the location of the residence. The Option also benefits from the URI not needing identity information to still be useful.

APs that triangulate can also have a individual URI downloaded to each endpoint with this Option, for the endpoint to hand out

whenever it is configured to. The <method> element would give a different indication in such a case, one that states the location is a triangulation of the UA's specific location, and not that of the

AP's.

This Option can be useful in WiMAX connected endpoints or IP cellular endpoints. The Location URI Option can be configured as a client if it is a router, such as a residential home gateway, with the ability to communicate to downstream endpoints as a server.

This document IANA registers the new DHC Option for a Location URI.

1.1 Conventions Used in this Document

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. DHC Location URI Elements

DHCP is a binary Protocol; URIs are alphanumeric (text) based. There is one byte per URI character.

[Editor's question: should UTF-8 vs. UTF-16 be accounted for?]

The Location URI Option format 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   | Option Length |           Valid-For           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     Location URI                                     |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
/                                     .....                                     \
\                                     .....                                     /
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     Location URI (cont'd)                                     +
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

2.1. Elements of the Location Configuration Information

Code XXX: The code for this DHCP option.

Option Length: The length of this option variable.

Valid-For: The time, in seconds, this URI is to be considered valid.

Location URI: The Location-by-Reference URI for the client

The <Valid-For> field indicates how long, in seconds, the client is

Polk

Expires May 18th 2008

[Page 4]

to consider this location URI valid before performing a refresh of this Option, with a new <Valid-For> answer. A refresh MAY be done merely at the normal DHCP refresh rate, or necessitated by this timer, perhaps just requesting this Option be refreshed.

3. DHC Option Operation

The [\[RFC3046\]](#) RAI0 MUST 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 LbyR URI Options, which are non-concatenated, overwrite the previous value.

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

sips:34LKJH534663J54@example.com

should be done, providing no identity information, rather than a LbyR URI such as this

sips:aliceisinatlanta@example.com

This Option is between a DHCP client and a DHCP server. It may be solicited (requested) by the client, or it may be pushed by the server without a request for it. Options not understood are ignored. The server MAY or MAY NOT have the location of a client within the server. If a server does not have a client's location, a topology of communication to a Location Information Server (LIS) [\[ID-LBYR-REQ\]](#) would be necessary.

The coordination between the logical entity of a DHCP server and the logical entity of a LIS as to which circuit-ID gets which LbyR URI is not done via DHCP, therefore it is not defined here. Any dereferencing of a client's LbyR URI would not involve DHCP either, but more likely an application layer protocol such as SIP, through a subscription to the LbyR URI on the LIS. The LIS would also handle all authentication and authorization of location requests, which is

also not performed with DHCP, therefore not defined here.

Polk

Expires May 18th 2008

[Page 5]

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 LbyR URI would likely indicate the residence's civic address to all wired or wireless clients within that residence. This is not inconsistent with what's stated above.

3.1 Architectural Assumptions

The following assumptions have been made for use of this URI Option for a client to learn it's location URI (in no particular order):

- o Any user control (what Geopriv calls a 'rulemaker') for the parameters and profile options a Location-Object will have is out of scope of this document, by assumed to take place via something such as a web interface between the user and the LIS (direct or indirect).
- o Any user attempting to gain access to the information at this URI will be challenged by the LIS, not the DHCP server for credentials and permissions.

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,

- o 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 have harmful scripts.

This concern will be highlighted more in a future version of this document.

4. Acknowledgements

Thanks to James Winterbottom for his useful comments. And to Lisa Dusseault for her concerns about the types of URIs that can cause harm.

Polk

Expires May 18th 2008

[Page 6]

5. IANA Considerations

IANA is requested to assigned a DHCP option code of XXX for the Location URI option, defined in [Section 2.0](#) of this document.

Any additional Location URI parameters to be defined for use via this DHC Option MUST be done through a Standards Track RFC.

6. Security Considerations

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

Since there is no privacy protection for DHCP messages, an eavesdropper who can monitor the link between the DHCP server and requesting client can discover this LbyR URI. Other than capturing the URI, the location of the client benefits from the protection of whatever server challenge mechanisms are available and configured for any device attempting access of the location record that the URI.

LbyR URIs need to reduce or eliminate client identity information within the URI itself, because DHCP is a cleartext delivery protocol.

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

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.

Polk

Expires May 18th 2008

[Page 7]

[RFC3265] Roach, A., "Session Initiation Protocol (SIP)-Specific Event Notification", [RFC 3265](#), June 2002.

7.2. Informative References

- [ID-SIP-LOC] J. Polk, B. Rosen, "SIP Location Conveyance", [draft-ietf-sip-location-conveyance-09.txt](#), "work in progress", Nov 2007
- [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
- [ID-LBYR-REQ] R. Marshall, "Requirements for a Location-by-Reference Mechanism", [draft-ietf-geopriv-lbyr-requirements-01.txt](#), "work in progress", Oct 07

Authors' Address

James Polk
3913 Treemont Circle
Colleyville, Texas 76034
USA

EMail: jmpolk@cisco.com

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

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.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

