Geopriv WG   James Polk
Internet-Draft   Cisco Systems
Intended status: Standards Track (PS)   March 9, 2009
Expires: September 9, 2009

Dynamic Host Configuration Protocol (DHCP) IPv4 and IPv6 Option for a Location Uniform Resource Identifier (URI)
draft-ietf-geopriv-dhcp-lbyr-uri-option-04

Legal

Abstract

This document creates a Dynamic Host Configuration Protocol (DHCP) Option for the downloading of a Uniform Resource Identifier (URI) pointing to the geolocation record of an endpoint. This URI, called a Location-by-Reference (LbyR), points to a record on a location server which tracks the geolocation of the endpoint. Once downloaded by an endpoint, this LbyR can be forwarded to another entity, to be dereferenced if this entity wants to learn the geolocation of the sender endpoint.

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 the downloading of a Uniform Resource Identifier (URI) pointing to the geolocation record of an endpoint. A client, for example, can be a Session Initiation Protocol (SIP) User Agent (UA) [RFC3261] (i.e., a Phone). This URI, called a Location-by-Reference (LbyR), points to a record on a location server [ID-LBYR-REQ] which tracks the geolocation of the endpoint (through means not defined in this document). The LbyR record stores the Geolocation of a Location Target, where the location of the Location Target changing at the record, but not in the URI used to access the record. Once downloaded by an endpoint (the target in this case), this LbyR can be forwarded to another entity, for example, using SIP as defined in [ID-SIP-LOC], to be dereferenced if this second entity wants to learn the geolocation of the Location Target.

The act of dereferencing location is explained in [ID-SIP-LOC], which demonstrates how a Location Recipient of an LbyR subscribes to a Location Server to attain the location of the Target. If the dereferencer has permission, defined in [ID-GEO-POL], the location of the target will be returned to the Location Seeker. The Location Server will grant permission to location inquires based on the rules established by a Rule Holder [RFC3693]. The Location Server has the ability to challenge any Location Seeker's request, thereby providing additive security properties to location revelation.

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 [ID-SIP-LOC] 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.

Including location in the SIP request is the most efficient means of accomplishing both requirements above.

There are other use-cases, such as calling the appropriate Pizza Hut without having to look up in a directory which store is closest. A UA knowing its location can call a main/national/international Pizza Hut number or 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]), these types of DHCP Options for geolocation requires an update of the entire location information (LI)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 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 LI to the endpoints might not scale in mobile (residential or enterprise or municipal) networks in which the UA is moving through more than one network attachment point, perhaps as a person walks or drives with their UA down a neighborhood street or apartment complex or a shopping center.

If the UA were provided a 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 reference that would not change as the UA's location changes, scaling issues would be significantly reduced to needing an update of the 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 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. Many endpoints will not have this ability, so relying on it could prove fruitless. Once the UA has a Location URI, a service provider, however it Sights the Location Target, as described in RFC 3693 [RFC3693], would merely update the actual location in the LIS record, i.e., the record the URI points towards. This document does not define how this update is done, as it will not be done with DHCP.

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 by DHCP. Behind the DHCP server, in the backend of the network, via the (logical entity of a) LIS has a PIDF-LO in each location record a Location URI points to.

If an 802.11 Access Port (AP) is at a specific known location within this enterprise network, all wireless Ethernet devices attaching to the network through this AP could be given the same location in their respective location records because the DHCP server would know each device was attaching from a known location, in this case, the same location. This is assuming no 802.11 triangulation is occurring, this would give a more precise location to be placed in the location record (URI) of each device.

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

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.

The means of challenge by any given LIS can vary, and a policy established by a rulemaker [RFC3693] for a Location Target as to what type of challenge(s) are used, how strong a challenge is used or how precise the location information is given to a requestor. All of this is outside the scope of this document (since this will not be accomplished using DHCP).

This document IANA registers the new IPv4 and IPv6 DHC Options for a Location URI.

2. Format of the DHCP LbyrElement Option

2.1 Overall Format of LbyrElement Option in IPv4

The LbyrElement 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   |  Ver  | Resv  |               .
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+               .
 .                        LbyrElements...                      ...
 .                 (see section 2.3 for details) ...           .
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1. IPv4 Fields for this LbyrElement 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 LbyR within the Option.

Ver: (4 bits) The version of this Option. This will specify version 1.

Resv: (4 bits) reserved for future use.

LbyrElement: see section 2.3 for details

2.2 Overall Format of LbyrElement Option in IPv6

The LbyrElement 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          |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |  Ver  | Resv  |                                               .
 +---------------+                                               .
 .                        LbyrElements...                        .
 .                 (see section 2.3 for details)                 .
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2. IPv6 fields of this LbyrElement 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 shape within the Option.

Ver: See above (Section 2.1). This will specify version 1.

Resv: See above (Section 2.1).

LbyrElement: see below (Section 2.3 for details).

2.3 LbyrElement Format for both IPv4 and IPv6

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

```
  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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |    LbyrType     |   LbyrLength    |   LbyrValue                ...
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3. LbyrElement Format for both IPv4 and IPv6

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

LbyrLength: The length, in bytes, of the LbyrValue, not including the LbyrLength field itself, up to a maximum of 255 bytes.

LbyrValue: The LbyrElement value, as described in detail below. The LbyrValue is always in UTP-8.

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

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

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

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

It is RECOMMENDED when the counter associated with this LbyrType=2 (Valid-For) value has passed, the client perform a refresh of this Option. For example, if 16000 was the initial value of the LbyrType=2 (Valid-For) value, when 8000 seconds have passed, the Option SHOULD be refreshed.

The LbyrType=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 LbyrType types created MUST be done so through IANA registration with peer review and an RFC.

3. DHC Option Operation

The [RFC3046] RAIO 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. That said, this Option SHOULD NOT be in a DISCOVER message, because there is zero knowledge by the client of which Server will answer.

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 LbyrElement 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

SHOULD be done, providing no identity information, rather than a Location URI such as this

    sips:aliceisinatlanta@example.com

This Option is for only 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 might or might not have the location of a client, therefore direct knowledge of a Location URI within the server. If a server does not have a client's location, a communication path (or request) to a LIS would be necessary.

The LIS function, which is logical, is what creates the LbyR. The coordination between the logical entity of a DHCP server and the logical entity of a LIS as to which circuit-ID gets which Location URI is not done via DHCP, therefore it is not defined here. Further, any location revelation rules and policies a user has regarding the treatment of their actual location, and who can access (what precision of) their location will be done with other than DHCP, and likely will be done before anything other than default authentication and authorization permissions are used when a Location Seeker, as defined in RFC 3693, requests a for a Target's location.

Differentiating clients is done via client identifiers. Therefore, in many implementations, each client can be assigned unique LbyRs, though this is not mandatory.

Any dereferencing of a client's Location URI would not involve DHCP either, but more likely by an application layer protocol such as SIP, through a subscription to the Location 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.

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. This is not inconsistent with what's stated above.

3.1 Architectural Assumptions

The following assumptions have been made for use of this LbyrElement Option for a client to learn its 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, but assumed to take place via an external 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 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

Therefore, this document specifies which URI types are acceptable as a Location URI scheme (or type):

1. sip:
2. sips:

3. pres:

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 The Version number for this Option

This document IANA registers the version number 1 of this Option.

4.4 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:

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.

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 keys on both ends of a communication to work (i.e., in the client and in the server). Most implementations do not accommodate this.

DHCP is a broadcast initially (a client looking for a server), unicast response (answer from a server) type of protocol. It is not secure in a practical sense. In today's infrastructures, it 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 have layer 2 security mechanisms in place to help prevent a Location URI from being learned by an unauthorized entity.

That said, having the Location URI does not mean this unauthorized entity has the location of a client. The Location URI still needs to be dereferenced to learn the location of the client. This dereferencing function, which is not done using DHCP, is done by requesting the location record at a Location Information Server, or LIS, which is a defined entity built to challenge each request it receives based on a joint policy of what is called a rulemaker. The rulemaker, as defined in RFC 3693, configures the authentication and authorization policies for the location revelation of a Target. This includes giving out more or less precise location information in an answer, therefore it can answer a bad-hat, but not allow it from learning exactly where a user is. The rulemaker, which is a combination of the default rules set up by the location provider and those decided on by the user of the Target device. Likely, the rules the user wants will not be allowed to go past some limits established by the location provider, i.e., the administrator of the LIS, for various capability or security reasons.

Penetrating a LIS is supposed to be hard, and hopefully vendors that implement a LIS 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 string itself. The Location URI also must be hard to guess that it belongs to a specific user. There is some debate as to whether this Location URI need be a random alphanumeric string or just unique. If the latter, there is some debate as to the how we define unique. Is that through space as time, as RFC 3261 defines a SIP Call-ID needs to be (meaning: never a duplicate, ever, by any device, ever)? Or is it unique to within a specific domain for as long as it is actively assigned to a client (plus some interval).

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.

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.

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

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

7.2. Informative References

[ID-SIP-LOC] J. Polk, B. Rosen, "SIP Location Conveyance", "work in progress", Mar 2009

[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", "work in progress", Feb 2009

[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", Feb 2009

Authors' Address

James Polk
3913 Treemont Circle
Colleyville, Texas 76034
USA

Email: jmpolk@cisco.com