Network Working Group
Internet Draft
Expiration: Dec 19th, 2006
File: draft-polk-dhc-ecrit-uri-psap-esrp-00.txt

James Polk
Cisco Systems
June 19th, 2006

A Dynamic Host Configuration Protocol Option for Requesting and Receiving a Uniform Resource Identifier of a Public Safety Answering Point or Emergency Services Routing Proxy

Status of this Memo

Copyright Notice

Abstract

This document defines a new Dynamic Host Configuration Protocol (DHC) Option for client requesting and/or receiving a Public Safety Answering Point (PSAP) or Emergency Services Routing Proxy (ESRP) URI to be used by higher layer protocols during emergency calling. In some network models, an ESRP URI and a PSAP URI will be equivalent from the client's point of view, therefore this document purposely vague differentiating between the two, as the difference does not matter to DHCP.

Table of Contents

1. Introduction

In IP communications, destination addressing can be to an IP address directly, or to a Uniform Resource Identifier (URI), where the service at the URI is resolved to a destination IP address by the source system or along the path. In Voice over IP communications, the destination IP address is infrequently used by the calling device; rather, a URI is used. The burden is on call servers along the path to resolve this URI to IP address to determine where to ultimately route the packet(s) to.

Understanding the decomposed nature of voice communications, quite pronounced with peer-to-peer protocols potentially having servers 100s and 1000s of miles away from the calling device, call signaling at a higher layer may lack the local knowledge to appropriately provide the client with what is necessary to make a local emergency call. In emergency communications, the act of calling for help is a highly localized event, requiring knowledge of where the caller is. The destination of that emergency call will also be local in nature.

This document defines a new Dynamic Host Configuration Protocol (DHC) Option [RFC2131] to allow an emergency services URI be requested by a client of a server, and transmitted unrequested from a server to a client. The URI is a SIP(S)-URI of a Public Safety Answering Point (PSAP) for that access network, at that user agent's location, which may be unknown or undiscoverable to a SIP server for this client. Most access networks are not served by a single PSAP. Increased granularity within the same access network

may provide a different PSAP URI to different clients depending on where each is in the local access network if there is more than one PSAPs necessary within the underlying infrastructure.

In a Voice over IP system, an emergency URI is an essential part of configuration information necessary for usage by an client for the particular purpose of contacting what is at that local URI.

Using SIP [RFC3261] as the application layer call message flow example protocol, emergency calling wants the following message flow to occur when Alice is in trouble:

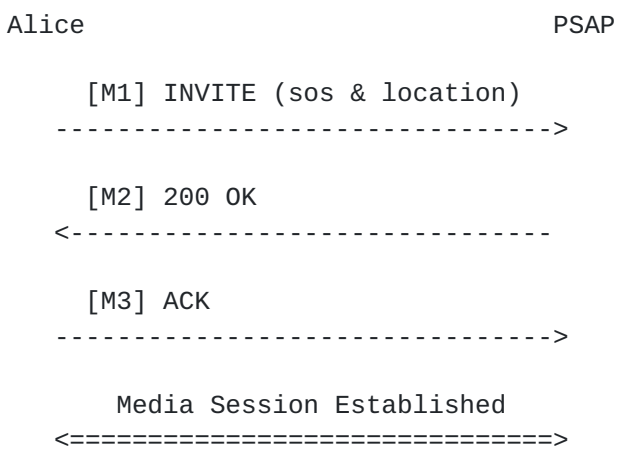

Figure 1. Basic Emergency Message Flow

SIP uses an INVITE message as its initial call set-up message. All relevant addressing and other information can be in this one message, including the destination URI (address) for Alice's appropriate PSAP, given where she is. Where Alice's voice device, called a user agent (UA) by SIP, learned the destination URI is what this document solves for some network topologies.

In Figure 1., Message-1 contains Alice's location, defined in [ID-SIP-LOC], perhaps learned from the UA requesting DHC Option 123 [RFC3825] at boot time (shown in Figure 2). This location information, which is vital to an emergency call because it informs the PSAP where to send first responders, is encoded inside the INVITE's message body in the form of an XML document PIDF-LO [RFC4119]. The destination URI can be learned via the UA performing a LoST [ID-LoST] mapping request itself, or in certain circumstances, the UA could request a DHCP server do the mapping query. This is similar to how a DHCP server relays the necessary information of a circuit-ID to a backend server to provide the client its location.

This mechanism is an alternative to each client having the LoST protocol code within it, doing a LoST query during boot-time.

This document does not limit the means of a client from gaining knowledge of a SIP-URI to DHCP, but provides DHCP as a means for a

client to gain knowledge of a SIP-URI through local configuration, considered essential for use by applications within that client.

Awareness of how stale a URI may become is something local administrators should consider when implementing this Option. For this particular Option, DHCP servers are assumed to periodically query an authoritative source providing non-stale or an updated URI. How this is accomplished is out of scope for this document.

Section 2 provides an example message flow of what this document achieves. Section 3 states that a PSAP URI and an ESRP URI are to be considered equivalent. Section 4 shows the DHC Relay Option Format. Section 4.1 discusses the rules of usage of this Option. Section 5 is the IANA Considerations section of this DHCP Option.

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 [RFC 2119].

1.2 Terms, Acronyms and Definitions

The following terms and acronyms are used within this document:

Emergency Services Routing Proxy - a special instance of a SIP Proxy that understands emergency routing to a PSAP based on the location of the caller

ESRP - Emergency Services Routing Proxy

Location-to-Service Translation Protocol - A mapping function protocol that takes a given location and determines the PSAP URI for a user who calls from that location.

LoST - Location-to-Service Translation Protocol

PSAP - Public Safety Answering Point

Public Safety Answering Point - the emergency response call center talking the local emergency calls from people in distress. This facility can be logical, and can transfer (reroute) any request sent to it to another facility deemed more appropriate to receive the request.

2. Solution Message Flow Example

Figure 2. dissects Figure 1. to provide where Alice's client learns the essential configuration information to place an emergency call. Omitted is SIP registration step, which may or may not be necessary,

depending on location policy.

In Message-3, Alice's client requests both Location and her PSAP URI. The server receives this request and generates Message-4, this is a LoST query to a Mapping server. Message-5 is the LoST response. Message-6 Provides Alice's client with her current PSAP URI.

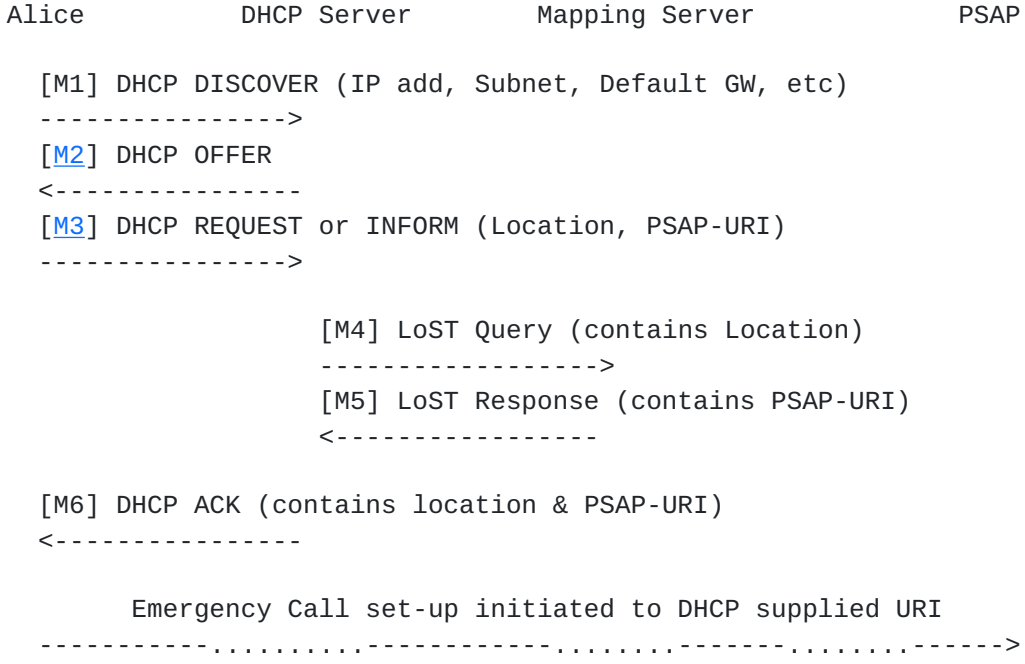

Figure 2. Location-to-URI Mapping Requested by DHCP Server

It is conceivable that this PSAP URI is not the primary URI used to contact a PSAP should Alice call for help, but used as a back-up or fallback SIP-URI used if an active mapping look-up fails. This is to be decided elsewhere.

It is also possible that the server will not perform the LoST query each time a client requests this information, depending on the intervals since the last request for a PSAP-URI.

3. PSAP vs. ESRP URI - Why They Can Be the Same

From Alice's point of view, reaching an ESRP can be the equivalent of reaching a PSAP. An ESRP is a SIP intermediary that understands the concept of location and emergency calling. This could well be at the border of an Emergency Services Network, in which a group of PSAPs are within. The effort was to get the message to the ESRP, knowing it will be able to "take it from here", meaning take it away from the burdens on the public network(s) that may or may not have the functionality to perform all the necessary look-ups and such to complete the call to the PSAP directly. Further, there has been talk of an Emergency Services Network acting as a buffer between the

PSAPs and the public networks. With this in mind, if local routing decisions and local policy has an ESRP as Alice's destination, a URI

called one is the same as a URI called the other.

4. DHC Relay Option Format

The format for this Option is as follows:

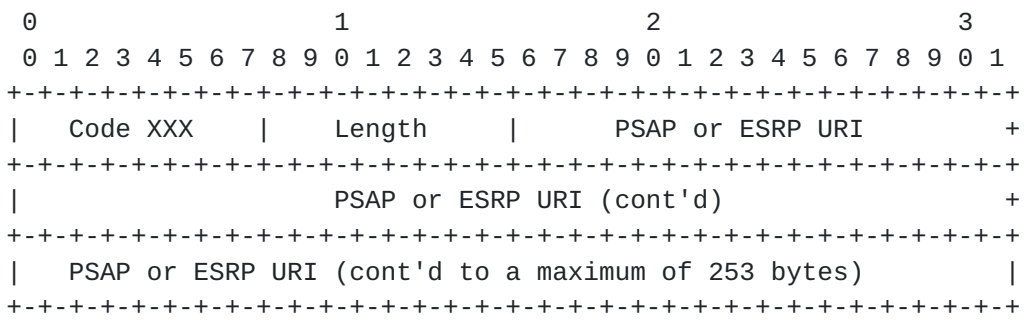

Figure 1. The URI Option Format

Code = The IANA Assigned Option number

Length = one octet providing a variable length value of the number of bytes in the Option, including this length field

URI = This is a variable length field containing the URI being transmitted, to a maximum of 253 bytes in length

4.1 Rules of Usage

The following are the rules of usage of this DHCP Option:

- An ESRP URI is equivalent to a PSAP URI from the client's point of view. This terminology has not been worked out in some circles.

- the schema used for a PSAP/ESRP URI is the SIP(S)-URI schema [RFC3261]

- a URI MUST NOT have a Length field of more than 253 (bytes), complying with [RFC2131]

- Clients making a request for one this URI, using a [REQUEST] message, will send this message to the Server with URI length field set to zero

- Implementations of this Option SHOULD plan to have the contents of an initial PSAP-URI in an ACK refreshed periodically, either through unsolicited server-to-client transmissions or client requests. Local policy SHOULD determine how and the rate.

5. IANA Considerations

IANA has assigned a DHCP option code of [XXX] for the PSAP-URI option defined in this document.

6. Security Considerations

Where critical decisions might be based on the value of this 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 client and destination DHCP server to capture any URIs in transit.

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

There is a risk of the information in this ACK message becoming old, relative to the comfort of the PSAP community. Although many wish the Internet to be truly dynamic in its updates to topology changes (for whatever reason), this does not always happen as planned.

7. Acknowledgements

To Andy Newton and Ralph Droms for guidance and assistance in the shaping of this effort. To Josh Littlefield, Ted Lemon, Andre Kostur for their constructive comments. Everyone can thank Stig Venaas for his relentless pounding on me to break my original effort up into individual URIs per option (but that means you have more docs to read too).

8. References

8.1 Normative References

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

[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.

[ID-SIP-LOC] J. Polk, B. Rosen, "SIP Location Conveyance", draft-ietf-sip-location-conveyance-03.txt, "work in progress", June 2006

[RFC3825] J. Polk, J. Schnizlein, M. Linsner, "Dynamic Host

Configuration Protocol Option for Coordinate-based Location Configuration Information", RFC 3825, July 2004

[ID-LoST] T. Hardie, H. Schulzrinne, A. Newton, H. Tschofenig, "LoST: A Location-to-Service Translation Protocol", draft-hardie-ecrit-lost-00.txt, "work in progress", February 2006

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

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

8.2 Informative References

[RFC4119] J. Peterson, "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2006

Author's Address

James M. Polk
3913 Treemont Circle
Colleyville, Texas 76034
USA

Phone: +1-817-271-3552
Fax: none
Email: jmpolk@cisco.com

Intellectual Property Statement

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.

Disclaimer of Validity

Copyright Statement

Acknowledgment

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