Network Working Group
Request for Comments: 5223
Category: Standards Track

H. Schulzrinne
Columbia University
J. Polk
Cisco
H. Tschofenig
Nokia Siemens Networks

August 2008

Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP)

Status of This Memo

Abstract

The Location-to-Service Translation (LoST) Protocol describes an XML-based protocol for mapping service identifiers and geospatial or civic location information to service contact Uniform Resource Locators (URLs). LoST servers can be located anywhere, but a placement closer to the end host, e.g., in the access network, is desirable. In disaster situations with intermittent network connectivity, such a LoST server placement provides benefits regarding the resiliency of emergency service communication.

This document describes how a LoST client can discover a LoST server using the Dynamic Host Configuration Protocol (DHCP).

Table of Contents

1. Introduction

The Location-to-Service Translation (LoST) Protocol [RFC5222] describes an XML-based protocol for mapping service identifiers and geospatial or civic location information to service contact Uniform Resource Locators (URLs).

In order to interact with a LoST server, the LoST client needs to discover the server's IP address. Several mechanisms can be used to learn this address, including manual configuration. In environments where the access network itself either deploys a LoST server or knows a third party that operates a LoST server, DHCP can provide the end host with a domain name. This domain name is then used as input to the DNS-based resolution mechanism described in LoST [RFC5222] that reuses the URI-enabled NAPTR specification (see [RFC4848]).

This document specifies a DHCPv4 and a DHCPv6 option that allows LoST clients to discover local LoST servers.

Section 2 provides terminology. Section 3 shows the encoding of the domain name. Section 4 describes the DHCPv4 option while Section 5 describes the DHCPv6 option, with the same functionality. IANA and Security Considerations complete the document in Sections 7 and 8.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [RFC2119].

Within this document, we use terminology from [RFC5012] and [RFC5222].

3. Domain Name Encoding

This section describes the encoding of the domain name used in the DHCPv4 option shown in Section 4 and also used in the DHCPv6 option shown in Section 5.

The domain name is encoded according to Section 3.1 of RFC 1035 [RFC1035] whereby each label is represented as a one-octet length field followed by that number of octets. Since every domain name ends with the null label of the root, a domain name is terminated by a length byte of zero. The high-order two bits of every length octet MUST be zero, and the remaining six bits of the length field limit the label to 63 octets or less. To simplify implementations, the total length of a domain name (i.e., label octets and label length octets) is restricted to 255 octets or less.

4. LoST Server DHCPv4 Option

The LoST server DHCPv4 option carries a DNS (RFC 1035 [RFC1035]) fully-qualified domain name (FQDN) to be used by the LoST client to locate a LoST server.

The DHCP option for this encoding has the following format:

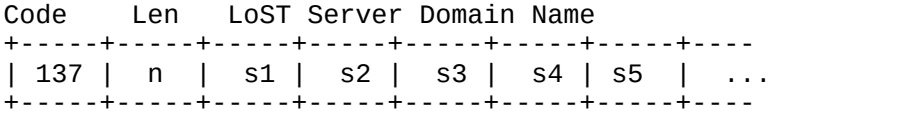


Figure 1: LoST FQDN DHCPv4 Option

The values s1, s2, s3, etc. represent the domain name labels in the domain name encoding. Note that the length field in the DHCPv4 option represents the length of the entire domain name encoding, whereas the length fields in the domain name encoding (see Section 3) is the length of a single domain name label.

Code: OPTION_V4_LOST (137)

Len: Length of the 'LoST Server Domain Name' field in octets; variable.

LoST Server Domain Name: The domain name of the LoST server for the client to use.

A DHCPv4 client MAY request a LoST server domain name in a Parameter Request List option, as described in [RFC2131].

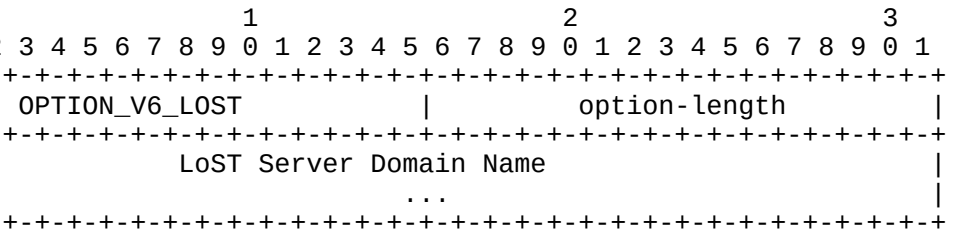
The encoding of the domain name is described in Section 3.

This option contains a single domain name and, as such, MUST contain precisely one root label.

5. LoST Server DHCPv6 Option

This section defines a DHCPv6 option to carry a domain name.

The DHCPv6 option has the format shown in Figure 2.



option-code: OPTION_V6_LOST (51)

option-length: Length of the 'LoST Server Domain Name' field in octets; variable.

LoST Server Domain Name: The domain name of the LoST server for the client to use.

Figure 2: DHCPv6 Option for LoST Server Domain Name List

A DHCPv6 client MAY request a LoST server domain name in an Options Request Option (ORO), as described in [RFC3315].

The encoding of the domain name is described in Section 3.

This option contains a single domain name and, as such, MUST contain precisely one root label.

6. Example

This section shows an example of a DHCPv4 option where the DHCP server wants to offer the "example.com" domain name to the client as input to the U-NAPTR LoST discovery procedure. This domain name would be encoded as follows:

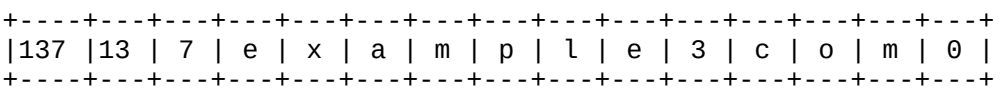


Figure 3: Example for a LoST FQDN DHCPv4 Option

7. IANA Considerations

7.1. DHCPv4 Option

The following DHCPv4 option code for the Location-to-Service Translation (LoST) Protocol server option has been assigned by IANA:

Option	Name	Value	Described in
	OPTION_V4_LOST	137	Section 4

7.2. DHCPv6 Option

IANA has assigned the following DHCPv6 option code for the Location-to-Service Translation (LoST) Protocol option:

Option	Name	Value	Described in
	OPTION_V6_LOST	51	Section 5

8. Security Considerations

If an adversary manages to modify the response from a DHCP server or insert its own response, a LoST client could be led to contact a rogue LoST server under the control of the adversary or be given an invalid address. These threats are documented in [RFC5069]. The security considerations in [RFC2131], [RFC2132], and [RFC3315] are applicable to this document.

[RFC5222] enumerates the LoST security mechanisms.

9. Acknowledgements

Andrew Newton reviewed the document and helped simplify the mechanism. Other helpful input was provided by Jari Arkko, Leslie Daigle, Vijay K. Gurbani (Gen-ART Review), David W. Hankins, Russ Housley, Tim Polk, Mark Stapp, and Christian Vogt.

10. References

10.1. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

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

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

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

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

10.2. Informative References

[RFC4848] Daigle, L., "Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS)", RFC 4848, April 2007.

[RFC5012] Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", RFC 5012, January 2008.

[RFC5069] Taylor, T., Tschofenig, H., Schulzrinne, H., and M. Shanmugam, "Security Threats and Requirements for Emergency Call Marking and Mapping", RFC 5069, January 2008.

[RFC5222] Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol", RFC 5222, August 2008.

Authors' Addresses

Henning Schulzrinne
Columbia University
Department of Computer Science
450 Computer Science Building
New York, NY 10027
US

EMail: hgs+ecrit@cs.columbia.edu
URI: http://www.cs.columbia.edu

James Polk
Cisco
2200 East President George Bush Turnpike
Richardson, TX 75082
US

EMail: jmpolk@cisco.com

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
EMail: Hannes.Tschofenig@nsn.com
URI: http://www.tschofenig.priv.at

Full Copyright Statement

Intellectual Property