Network Working Group   H. Schulzrinne
Internet-Draft   Columbia U.
Intended status: Standards Track   J. Polk
Expires: March 31, 2007   Cisco
                                                       H. Tschofenig
                                                            Siemens
                                                 September 27, 2006

       A Dynamic Host Configuration Protocol (DHCP) based Location-to-Service
            Translation Protocol (LoST) Discovery Procedure
                 draft-polk-ecrit-dhc-lost-discovery-01.txt

Status of this Memo

Copyright Notice

Abstract

   The Location-to-Service Translation Protocol (LoST) 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
   desireable. Such a LoST server placement provides benefits in
   disaster situations with intermittent network connectivity 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 Protocol (LoST)
[I-D.ietf-ecrit-lost] 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 finally
needs to know its 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
[I-D.ietf-ecrit-lost] that reuses the URI-enabled NAPTR specification
(see [I-D.daigle-unaptr]).

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

Section 2 provides terminology. 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 Section 7 and Section 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
[I-D.ietf-ecrit-requirements] and [I-D.ietf-ecrit-lost].

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. The 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.

RFC 1035 [RFC1035] encoding was chosen to accommodate future
internationalized domain name mechanisms.

For DHCPv4 only: If the length of the domain name exceeds the
maximum permissible within a single option (i.e., 254 octets), then
the domain name MUST be represented in the DHCP message as specified
in [RFC3396].

4. LoST Server DHCPv4 Option

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

The DHCP option for this encoding has the following format:

```
     Code    Len   LoST Server Domain Name
     +-----+-----+-----+-----+-----+-----+-----+----
     | TBD |  n  |  s1 |  s2 |  s3 |  s4 | s5  |  ...
     +-----+-----+-----+-----+-----+-----+-----+----
```

                  Figure 1: LoST FQDN DHCPv4 Option

     Code: OPTION_LOST (TBD1)

     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.

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

Only a single domain name MUST be present in the DHCPv4 option.

5. LoST Server DHCPv6 Option

This document defines a DHCPv6 options to carry a domain name.

The DHCPv6 option has the format shown in Figure 3.

```
       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_LOST           |         option-length         |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                  LoST Server Domain Name                      |
      |                             ...                               |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
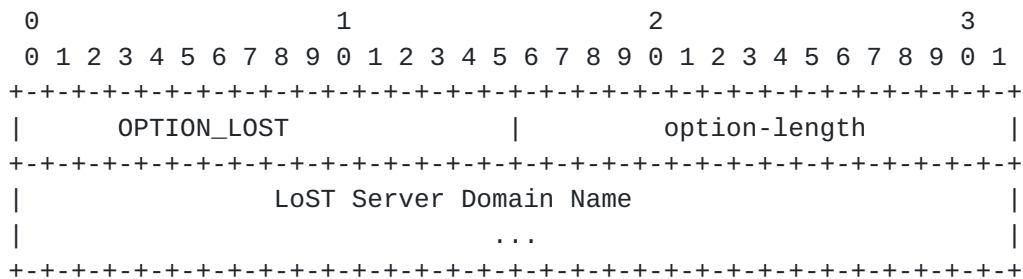
         Figure 3: DHCPv6 Option for LoST Server Domain Name List

      option-code: OPTION_LOST (TBD2)

      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.

   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.

   Only a single domain name MUST be present in the DHCPv6 option.

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:


```
      +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
      |TBD|13 | 7 |'e'|'x'|'a'|'m'|'p'|'l'|'e'| 3 |'c'|'o'|'m'| 0 |
      +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

            Figure 5: Example for a LoST FQDN DHCPv4 Option

7. IANA Considerations

7.1. IANA Consideration for DHCPv4 Option

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

      Option Name   Value   Described in

      OPTION_LOST   TBD   Section 4

7.2. IANA Consideration for DHCPv6 Option

   IANA is requested to assign the following DHCPv6 option codes for the
   Location-to-Service Translation Protocol (LoST) options:

      Option Name   Value   Described in

      OPTION_LOST   TBD   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
   [I-D.ietf-ecrit-security-threats]. The security considerations in
   [RFC2131], [RFC2132] and [RFC3315] are applicable to this document.

9. Acknowledgements

   The authors would like to thank Andrew Newton and Leslie Daigle for
   their draft review. We would like to particularly thank Andrew
   Newton for the simplifications he proposed.

10. References

10.1. Normative References

   [I-D.ietf-ecrit-lost]
              Hardie, T., "LoST: A Location-to-Service Translation
              Protocol", draft-ietf-ecrit-lost-01 (work in progress),
              September 2006.

   [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

   [I-D.daigle-unaptr]
                Daigle, L., "Domain-based Application Service Location
                Using URIs and the Dynamic Delegation Discovery Service
                (DDDS)", draft-daigle-unaptr-00 (work in progress),
                June 2006.

   [I-D.ietf-ecrit-requirements]
                Schulzrinne, H. and R. Marshall, "Requirements for
                Emergency Context Resolution with Internet Technologies",
                draft-ietf-ecrit-requirements-12 (work in progress),
                August 2006.

   [I-D.ietf-ecrit-security-threats]
                Taylor, T., "Security Threats and Requirements for
                Emergency Call Marking and Mapping",
                draft-ietf-ecrit-security-threats-03 (work in progress),
                July 2006.

   [RFC3319]   Schulzrinne, H. and B. Volz, "Dynamic Host Configuration
                Protocol (DHCPv6) Options for Session Initiation Protocol
                (SIP) Servers", RFC 3319, July 2003.

   [RFC3361]   Schulzrinne, H., "Dynamic Host Configuration Protocol
                (DHCP-for-IPv4) Option for Session Initiation Protocol
                (SIP) Servers", RFC 3361, August 2002.

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

Authors' Addresses

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

    Phone: +1 212 939 7004
    Email: hgs+ecrit@cs.columbia.edu
    URI: http://www.cs.columbia.edu

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

    Email: jmpolk@cisco.com

    Hannes Tschofenig
    Siemens
    Otto-Hahn-Ring 6
    Munich, Bavaria 81739
    Germany

    Phone: +49 89 636 40390
    Email: Hannes.Tschofenig@siemens.com
    URI: http://www.tschofenig.com

Full Copyright Statement

Intellectual Property

Acknowledgment