Simple Service Location Protocol (SSLP) for 6LoWPAN
draft-daniel-6lowpan-sslp-02.txt

Status of This Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79. This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

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 April 29, 2010.

Copyright Notice
Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

The Simple Service Location Protocol (SSLP) provides a framework for the discovery and selection of the services working on 6LoWPAN. The protocol has a simple structure that is easy to be implemented on 6LoWPAN devices that are characterized by short range, low bit rate and low power. The protocol also offers a mechanism for interoperability with the IP networks under SLP. It enables communication between 6LoWPAN and other IP networks.

Requirements Language

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 [RFC2119].

Table of Contents

1. Introduction .................................................. 3
2. Terminology ................................................... 3
   2.1. Notation Conventions .................................. 4
3. Protocol Overview .............................................. 4
4. Required Simple Service Location Protocol (SSLP) Messages ... 6
   4.1. Service Request Message ................................ 7
   4.2. Service Reply Message .................................. 7
   4.3. Service Acknowledgment Message ....................... 9
   4.4. Directory Agent Advertisement Message ............... 9
   4.5. Service Agent Advertisement Message............... 10
5. Optional Simple Service Location Protocol (SSLP) Messages ... 10
   5.1. Service Type Request .................................. 10
   5.2. Service Type Reply .................................... 11
   5.3. Service Deregistration Message ....................... 11
6. Interoperability ............................................... 12
7. Security Considerations ....................................... 12
8. IANA Considerations .......................................... 12
9. Acknowledgements ............................................. 12
10. References ................................................... 13
    10.1. Normative References .................................. 13
    10.2. Informative References ............................... 13
1. Introduction

6LoWPAN stands for IPv6 layer over low-power wireless personal area networks (LoWPAN) which consist of devices that conform to the IEEE 802.15.4-2003 standard [ieee802.15.4]. IEEE 802.15.4 devices are used to provide services like home security, fire alarm, medical sensing/monitoring, heating control, and building automation, etc. When clients want to use services without configuration, a service discovery mechanism is needed.

In IP networks, the Service Location Protocol (SLP) is used for access to information about the existence, location, and configuration of networked services [RFC2608]. SLP is well operating in IP networks, but there are several issues to be solved [I-D.kushalnagar-lowpan-goals-assumptions] to apply it to 6LoWPAN. The limited packet size of 6LoWPANs is one of them; Given that in the worst case the maximum size available for transmitting IP packets over IEEE 802.15.4 frame is 81 octets, and that the IPv6 header is 40 octets long, (without optional headers), this leaves only 41 octets for upper-layer protocols, like UDP and TCP. UDP uses 8 octets in the header, thereby leaving 33 octets for data, like SLP, over UDP. However, the SLP message could easily be greater than this remaining octets, and it should be transmitted as multiple packets, causing traffic overheads to 6LoWPAN.

[RFC4944] introduces the adaption layer of fragmentation and reassembly for IPv6 packets, while providing a header compression scheme for reducing the size of the IPv6 header. Also, it expects that 6LoWPAN uses mesh routing for the multi-hop forwarding of IPv6 packets at sub-IP layer. This makes it difficult to use SLP directly, requiring to define a simple service discovery protocol to discover, control, and maintain services provided by devices in 6LoWPAN.

This document defines the Simple Service Location Protocol (SSLP) which provides a framework for the discovery and selection of network services in 6LoWPAN. SSLP is simple and lightweight to be transmitted efficiently in 6LoWPAN. SSLP uses the Tokenized XML strings to minimize the packet exchange. SSLP in 6LoWPAN could also interwork with SLPv2[RFC2608] in external IP networks. That is, clients can discover and control services in 6LoWPAN regardless of whether they are located inside the 6LoWPAN or not.

2. Terminology

Terminologies used in this document are defined in [RFC2608] as follows:
User Agent (UA): A process working on the user’s behalf to establish contact with some service. The UA retrieves service information from the Service Agents or Directory Agents.

Service Agent (SA): A process working on the behalf of one or more services to advertise the services.

Directory Agent (DA): A process which collects service advertisements.

Service Type: Each type of service has a unique Service Type string.

Naming Authority: The agency or group which catalogs given Service Types and Attributes. The default Naming Authority is IANA.

Scope: A set of services, typically making up a logical administrative group.

Translation Agent (TA): is newly defined in this document for interworking with SLPv2 in IP networks. TA is a process working on a device which has interfaces to both IP networks and 6LoWPAN. It translates SLPv2 messages into SSLP messages, and vice versa.

2.1. Notation Conventions

Syntax: Syntax for string based protocols follow the conventions defined for ABNF [RFC2234].

Strings: All strings are encoded using the UTF-8 [RFC3629] transformation of the Unicode character set and are NOT null terminated when transmitted. Strings are preceded by a two byte length field.

string-list: A comma delimited list of strings with the following syntax: string-list = string / string ’,’ string-list

In format diagrams, any field ending with a \ indicates a variable length field, given by a prior length field in the protocol.

3. Protocol Overview

The Simple Service Location Protocol (SSLP) supports the same framework as SLP in which client applications are modeled as ‘User Agents’ (UAs), and services are advertised by ‘Service Agents’ (SAs). The ‘Directory Agent’ (DA) functions as a cache of the information about services registered by SAs and informs UAs of the existence of services. Besides, SSLP introduces ‘Translation Agents’ which
perform the translation of messages (which are defined in Section 4) for the interoperability with SLPv2.

The role of UA, SA, and DA in SSLP is not quite different from the ones in SLP. The UA issues a ‘Service Request’ (SREQ) on behalf of the client application, specifying the characteristics of the service which the client requires. The UA will receive a ‘Service Reply’ (SREP) specifying the location of all services in the 6LoWPAN which satisfy the request.

SSLP allows both the two-party and three-party service discovery mechanisms. In the two-party discovery, the UA directly issues SREQ to SAs. This mechanism is useful for a small-sized 6LoWPAN because it doesn’t require the configuration of DAs. In this case, the UA broadcasts (or multicasts if possible) a SREQ to the entire 6LoWPAN to which it belongs using the link layer broadcasting scheme.

In the three-party discovery, one or more DAs are employed in order to reduce the broadcasting overheads of service requests especially for a large 6LoWPAN. SAs send a ‘Service Registration’ (SREG) containing all the services they advertise to DAs and receive ‘Service Acknowledgement’ (SACK) in reply. DA caches mapping of Service to XML Token. SACK includes the corresponding Token that DA has assign to the SREG service. These advertisements must be refreshed with the DA or they expire. UAs unicast SREQ to DAs instead of SAs if any DAs are known. UAs and SAs MAY discover DAs in two ways. One, they broadcast a (SREQ) message for the DA service when they start up. Two, the DA sends unsilicited DA advertisement message periodically, which is listened by UAs and SAs. In both the cases the UAs and SAs receive DA Advertisement (DADV) message. DADV message contains the XML token corresponding to SREQ service message.

Services are grouped together using ‘scopes’. These are strings which identify services by location, administrative grouping, proximity in a network topology or some other category.

```
+--------+-SSLP message- > +-----------+-SLPv2 message- > +--------+
|UA,SA,DA|                 |Translation|                  |UA,SA,DA|
+--------+ < -SSLP message-+-----------+ > -SLPv2 message-+--------+
```

Figure 1: The operation of Translation Agent (TA)

The ‘Translation Agent’ (TA) must work on a machine which reaches both a IP network and a 6LoWPAN. If a TA receives either a SLP message from a IP network or a SSLP message from a 6LoWPAN, it maps the SSLP messages to SLP messages and vice versa. TA gets Service Request Messages from DA of SSLP and forwards to corresponding SLP messages. This operation is essentially needed for SSLP to be
interoperable with SLP and vice versa. With the TA, a UA can
discover and control services in 6LoWPAN regardless of whether they
are located inside the 6LoWPAN or not. Further work on TA TBD.

4. Required Simple Service Location Protocol (SSLP) Messages

The minimum required implementation of SSLP consists of a UA, SA or
both. The use of DA in itself is optional but in case a DA is
deployed it MUST support all the SSLP messages.

SAs and UAs MUST support SREQ, SREP, and DADV. SAs MUST also support
SREG, SACK, and SADV. For UAs and SAs, to support the other messages
is OPTIONAL.

All SSLP messages begin with the following header:

```
+---------------+---------------+---------------+
|   Ver   |  Msg-ID  |O|F|  rsv  |        Sequence number        |
+---------------+---------------+---------------+
```

Figure 2: SSLP general header format

Ver field describes the version of SSLP being used.

Msg-ID is the number representing a message type as shown below:

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Abbreviation</th>
<th>Msg-ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Request</td>
<td>SREQ</td>
<td>1</td>
</tr>
<tr>
<td>Service Reply</td>
<td>SREP</td>
<td>2</td>
</tr>
<tr>
<td>Service Registration</td>
<td>SREG</td>
<td>3</td>
</tr>
<tr>
<td>Service Acknowledge</td>
<td>SACK</td>
<td>4</td>
</tr>
<tr>
<td>DA Advertisement</td>
<td>DADV</td>
<td>5</td>
</tr>
<tr>
<td>SA Advertisement</td>
<td>SADV</td>
<td>6</td>
</tr>
<tr>
<td>Service Type Request</td>
<td>STREQ</td>
<td>7</td>
</tr>
<tr>
<td>Service Type Reply</td>
<td>STREP</td>
<td>8</td>
</tr>
<tr>
<td>Service Deregistration</td>
<td>SDER</td>
<td>9</td>
</tr>
</tbody>
</table>

Two more message types and there detail needs TBD

O and F bit are compatible with the flag field in SLPv2 and defined
in [RFC2608]. OVERFLOW is set when a message’s length exceeds what
fits into a datagram. FRESH is set on every new SREG.

The sequence number is set to a unique value for each unique SREQ
message. If the request message is retransmitted, the same sequence
number is used. Replies set the sequence number to the same value as
the sequence number in the SREQ message. This field is compatible
with XID field in SLPv2.

4.1. Service Request Message

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Simple Service Location header (Msg-ID = SREQ = 1)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AM</td>
<td>Source Address (16/64/128 bit)</td>
</tr>
<tr>
<td></td>
<td>length of &lt;service-type&gt;</td>
<td>&lt;service-type&gt; String</td>
</tr>
<tr>
<td></td>
<td>length of &lt;scope-list&gt;</td>
<td>&lt;scope-list&gt; String</td>
</tr>
<tr>
<td></td>
<td>+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3: SSLP service request message header format

Addressing Mode (AM) field has three different values as follows:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>16 bit short address is used as Source Address field</td>
</tr>
<tr>
<td>10</td>
<td>64 bit extended address is used as Source Address field</td>
</tr>
<tr>
<td>11</td>
<td>128 bit IPv6 address is used as Source Address field</td>
</tr>
</tbody>
</table>

If < scope-list > field is omitted, length of < scope-list > field MUST
be set to zero and all services matching < service-type > are
discovered independent of < scope-list >.

The < service-type > field consists of service type strings. Service
Types SHOULD be defined by a "Service Template" [RFC2609], which
provides expected attributes, values and protocol behavior.

In the presence of one or more DAs, UAs unicast SREQ messages to
them. DAs MUST issue SREP messages in response to SREQ messages
whether they know the service location UAs inquire or not.

4.2. Service Reply Message

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Simple Service Location header (Msg-ID = SREP = 2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Error Code</td>
<td>Service Location Entry count</td>
</tr>
<tr>
<td></td>
<td>&lt; Service Location Entry 1 &gt; ... &lt; Service Location Entry N &gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+</td>
<td></td>
</tr>
</tbody>
</table>

Figure 4: SSLP service reply message header format
A nonzero value in Error Code field indicates an error. In case of a nonzero value of Error Code, the rest of the message MAY be ignored. Moreover, errors are only returned against unicast requests.

Error Code field has different values as follows:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PARSING_ERROR: The message does not obey the SSLP syntax.</td>
</tr>
<tr>
<td>2</td>
<td>SCOPE_ERROR: The scope field in SSLP message did not match to the scope supported by DA or SA.</td>
</tr>
<tr>
<td>3</td>
<td>INTERNAL_ERROR: The DA or SA is not working properly</td>
</tr>
<tr>
<td>4</td>
<td>MSG_NOT_SUPPORTED: The DA or SA gets an optional message not being supported</td>
</tr>
<tr>
<td>5</td>
<td>ILLEGAL_REGISTRATION: The SREG has problems</td>
</tr>
<tr>
<td>6</td>
<td>DA_BUSY: UA or SA should retry</td>
</tr>
</tbody>
</table>

SREP message contains zero or more service location entries. If no matching service locations are present in SAs or DAs, the SREP message with zero service location entries is returned in response to a unicast SREQ message. However, a SREP message with zero service location entries MUST NOT be sent in response to a broadcast SREQ message.

The service location entry is defined as follows:

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Lifetime            |LT |     Service Location      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

A service location entry may not be cached longer than the Lifetime seconds mentioned in the Lifetime field of Service location entry.

Location Type (LT) field has three different values as follows:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>16 bit short address is used as Service Location field</td>
</tr>
<tr>
<td>10</td>
<td>64 bit extended address is used as Service Location field</td>
</tr>
<tr>
<td>11</td>
<td>URL Location field is used as Service Location field</td>
</tr>
</tbody>
</table>

If LT field has the value of 11, Service Location field is replaced by the URL Location field defined as follows.
4.3. Service Acknowledgment Message

A SACK message is received in response to the SREG messages. The values of Error Code are same as defined in section 4.2.

4.4. Directory Agent Advertisement Message

A DADV message is sent in two cases. First, when a DA receives a SREQ message with service type of "service: directory-agent". Second, to send an unsolicited advertising message by the DA.

The Error Code is set to zero when the DA broadcasts an unsolicited advertisement message. If the DADV is unicast (in response to SREQ message with "service:directory agent") the DA returns the same errors a SREP would.

The <scope-list> includes the scope provided by the DA. The <scope-list> of DA MUST not be NULL.

DAs MUST send unsolicited periodically. SAs MUST listen for DADVs.
UAs MAY do this. In case UAs do not listen to the DADVs, they must
discover the DAs by sending SREQ message with service type of
"service: directory-agent".

4.5. Service Agent Advertisement Message

A SADV message is sent when a SA receives a SREQ message with service
type of "service: service-agent" or when SAs send unsolicited
advertisements in the absence of DAs. SAs MUST not generate
Service Agent Advertisement (SADV) messages if they have been
configured to use specific DA(s).

The Service Location Entry Count is set to 1 while responding to a
SREQ with service type of "service: directory-agent". The Service
Location Entry is filled as "service:directory-agent://<adr of SA>".

In case of unsolicited DADV, all the services provided by the SA are
listed in the Service Location Entry preceded by the Service Location
Entry count.

5. Optional Simple Service Location Protocol (SSLP) Messages

5.1. Service Type Request

The service type request (STREQ) allows a UA to find all the service
types available on the network.

| 1 2 3 |
| --- --- --- |
| 0 1 2 3 4 5 6 7 8 9 0 |
| 0 1 2 3 4 5 6 7 8 9 0 1 |
| +--------------------------------------------------------------------+
| Simple Service Location header (Msg-ID = STREQ = 7) |
| +----------------------------------------------------------+
| AM| Source Address (16/64/128 bit) |
| +--------------------------------------------------------------------+
| length of <scope-list> | <scope-list> String |
| +--------------------------------------------------------------------+

Figure 10: SSLP service type message header format
In the presence of one or more DAs, UAs unicast STREQ messages to them. DAs MUST issue Service Type Reply (STREP) messages in response to STREQ messages.

In the absence of DAs, STREQ messages are broadcast over 6LoWPAN and SAs respond with STREP messages.

5.2. Service Type Reply

```
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 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Simple Service Location header (Msg-ID = STREP = 8)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Error Code         |    Service Location Entry     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     length of <stype-list>    |      <stype-list> String      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
Figure 11: SSLP service type reply header format
```

The Service Location Entry is included in STREQ to reduce the communication overhead when there is no DA. Without Service Location Entry the UA has to make two broadcasts. First, it shall broadcast STREQ to find all the service types in the network. Second, UA shall broadcast SREQ to discover the SAs which can provide a specific service type. However, in the presence of Service Location Entry a unicast SREQ can be made after knowing all the service types.

The service type list < stype-list > is a < string-list > field which contains the list of available service types with an SA or a DA.

5.3. Service Deregistration Message

The DA deletes a service registration when the Lifetime for the service expires. In case an SA terminates the service provisioning before its Lifetime is expired, it SHOULD deregister with the DA. SA MUST derigister the services with the same scope list which was used for service registration.
SDER messages are sent to DAs when SAs do not provide their services any more. These messages help eliminating any stale entries in the DAs.

6. Interoperability

SSLP interoperates with SLPv2 via Translation Agent (TA). A TA MUST be capable of the translation between SLPv2 and SSLP. In other words, TA translates SLPv2 messages into SSLP messages, and vice versa. SSLP Service Request will be tranformed to SLP Service Request message. TA receives Service Reply from SLP and then transforms that message to SSLP Service Reply Message.

7. Security Considerations

The security considerations of the [RFC3111] are applicable to this document. Especially, Translation Agent (TA) MUST be secured for processing SSLP/SLP messages translation and specific considerations will be carefully studied in the next versions.

8. IANA Considerations

TBD.

9. Acknowledgements

Thanks to Shafique Ahmad Chaudhry, Byung-hee Roh, Sun-ho Kim, Mi-jung Lee, and Minho Lee for their useful discussions and supports for writing this document.

10. References
10.1. Normative References


10.2. Informative References


Authors' Addresses

Kim, Ki Hyung (editor)
Ajou University
San 5 Wonchun-dong, Yeongtong-gu
Suwon-si, Gyeonggi-do  443-749
KOREA
Phone: +82 31 219 2433
EMail: kkim86@ajou.ac.kr

Waleed Akram Baig
Ajou University
San 5 Wonchun-dong, Yeongtong-gu
Suwon-si, Gyeonggi-do  443-749
KOREA
Phone: +82 31 219 1894
EMail: waleedbaig@ajou.ac.kr

Seung Wha Yoo
Ajou University
San 5 Wonchun-dong, Yeongtong-gu
Suwon-si, Gyeonggi-do  443-749
KOREA
Phone: +82 31 219 1603
EMail: swyoo@ajou.ac.kr

Soohong Daniel Park
SAMSUNG Electronics
Mobile Platform Laboratory, SAMSUNG Electronics 416 Maetan-3dong, Yeongtong-gu
Suwon-si, Gyeonggi-do  442-742
KOREA
Phone: +82 31 200 4508
EMail: soohong.park@samsung.com