Network Working Group
Request for Comments: 3111
Category: Standards Track

E. Guttman
Sun Microsystems

May 2001

Service Location Protocol Modifications for IPv6

Status of this Memo

Copyright Notice

Abstract

This document defines the Service Location Protocol Version 2's (SLPv2) use over IPv6 networks. Since this protocol relies on UDP and TCP, the changes to support its use over IPv6 are minor.

This document does not describe how to use SLPv1 over IPv6 networks. There is at the time of this publication no implementation or deployment of SLPv1 over IPv6. It is RECOMMENDED that SLPv2 be used in general, and specifically on networks which support IPv6.

Table of Contents

1. Introduction

The Service Location Protocol (SLP) provides a scalable framework for the discovery and selection of network services. Using this protocol, computers using IP based networks no longer need so much static configuration of network services for network based applications. This is especially important as computers become more portable, and users less tolerant of or less able to fulfill the demands of network administration.

The following are changes required to have the Service Location Protocol work over IPv6. These changes include:

- Eliminating support for broadcast SLP requests
- Address Specification for IPv6 Addresses in URLs
- Use of IPv6 multicast addresses and IPv6 address scopes
- Restricted Propagation of Service Advertisements

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 [4].

2. Eliminating support for broadcast SLP requests

Service Location over IPv4 allows broadcasts to send Service Location request messages. IPv6 makes use of link-local multicast in place of broadcast. Broadcast-only configuration for SLP is not supported under IPv6. If a User Agent wishes to make a request to discover Directory Agents or make a request of multiple Service Agents, the User Agent must multicast the request to the appropriate multicast address.

This change modifies the requirements described in Section 6.1 (Use of Ports, UDP and Multicast) of the Service Location Protocol [2].

3. Address Specification for IPv6 Addresses in URLs

Whenever possible the DNS [5] name of the service should be used rather than the numerical representation described in this section.

Service Location allows the use of the protocol without the benefit of DNS. This is relevant when a group of systems is connected to build a network without any previous configuration of servers to support this network. When Service Location is used in this manner, numerical addresses must be used to identify the location of services.

The format of a "service:" URL is defined in [6]. This URL is an "absolute URI" as defined by [7].

A numerical IPv6 address, such as may be used in a "service:" URL, is specified as in [8]. The textual representation defined for literal IPv6 addresses in [9]:

```
ipv6-addr  =  "[" num-addr "]"
num-addr   =  ; Text represented IPv6 address syntax is as
              ; specified in RFC 2373 [8], Section 2.2,
```

Examples:

This is a site-local scoped address, as could be used in a SLP DAAdvert message.

```
service:directory-agent://[FEC0::323:A3F9:25ff:fe91:109D]
```

This is a link-local scoped address, as could be used by a SA to advertise its service on a IPv6 network with no routers or DNS service.

```
service:printer:ipp://[FE80::a15A:93ff:fe5D:B098]:8080/path
```

4. SLP multicast and unicast behavior over IPv6

Section 4.1 describes how different multicast addresses are used for transmitting and receiving SLPv2 messages over IPv6. Section 4.2 defines rules for the use of these addresses and covers scoped address issues in general.

4.1 SLPv2 Multicast Group-IDs for IPv6

SLPv2 for IPv4 specifies only one multicast address, relative to an Administratively Scoped Address range [11]. The reason only one address was used is that there are only 256 relative assignments available for this purpose. IPv6, on the other hand, has scoped addresses and enough space for a range of assignments.

SLPv2 for IPv6 uses the following multicast group-id assignments:

```
FF0X:0:0:0:0:0:0:116     SVRLOC
FF0X:0:0:0:0:0:0:123     SVRLOC-DA
FF0X:0:0:0:0:0:1:1000    Service Location
 -FF0X:0:0:0:0:0:1:13FF
```

These group-ids are combined with the scope prefix of the scope to which the multicast message is to be sent.

The SVRLOC group-id is used for the following messages: Service Type Request and Attribute Request messages.

The SVRLOC-DA group-id is used for multicast Service Requests for the "service:directory-agent" service type. Also, DAs send unsolicited DA Advert messages to the SVRLOC-DA multicast group-id.

All other multicast Service Request messages are sent to the appropriate Service Location multicast group-id. SAs join the groups which correspond to the Service Types of the services they advertise. The group-id is determined using the algorithm provided in SLPv1 [3]. The Service Type string used in the SrvRqst is hashed to a value from 0-1023. This determines the offset into the FF0X::1:1000-13FF range.

The hash algorithm is defined as follows:

An unsigned 32 bit value V is initialized to 0. Each byte of the Service Type UTF-8 [12] encoded string value is considered consecutively. The current value V is multiplied by 33, then the value of the current string byte is added. Each byte in the Service Type string is processed in this manner. The result is contained in the low order 10 bits of V. For example, the following code implements this algorithm:

```
unsigned long slp_hash(const char *pc, unsigned int len) {
    unsigned long h = 0;
    while (len-- != 0) {
        h *= 33;
        h += *pc++;
    }
    return (0x3FF & h); /* round to a range of 0-1023 */
}
```

4.2 SLPv2 Scoping Rules for IPv6

IPv6 provides different scopes for interface address configuration and multicast addresses. A SLPv2 Agent might discover services that it cannot use or not discover services which it could use unless rules are given to prevent this.

Say a SLPv2 UA, for example, could request a service using site-local scope multicast and obtain a service: URL containing a link-local literal address. If the service referred to were not on the same link as the SLPv2 UA, the service could not be reached.

4.2.1 Joining SLPv2 Multicast Groups

A SLPv2 Agent MAY send a multicast message using any scope which it is allowed to (see section 4.2.2). A SA and a DA MUST join all groups to which a SLPv2 Agent may send a message. This ensures that the SA or DA will be able to receive all multicast messages.

Specifically, a SLPv2 Agent MUST NOT join a multicast group which has greater scope for an interface than it is configured with for use with unicast. For example, an interface which is only configured with a link-local address joins groups in scopes with FF01 and FF02. If the interface is configured with a site-local or global address, the scope of all multicast groups joined can be no greater than scope FF05. In this case, SLPv2 SAs and DAs MUST join multicast groups in all the following scopes: FF01 - FF05.

A DA MUST join the SVRLOC-DA group to receive SrvRqst messages requesting DAAdverts.

A SA MUST join the SVRLOC-DA group to receive DAAdvert messages.

A SA MUST join the groups from the Service Location range of group-ids to receive SrvRqst messages. The SA only joins those groups corresponding to services it advertises. For example, a service agent which responds to requests for "service:service-agent" (used for SA discovery), would join groups with the group-id derived from the hash function defined in section 4.1:

```
group-id to join = slp_hash("service:service-agent") + base address
                 = 0x01d8 + FF0X:0:0:0:0:0:1:1000
                 = FF0X:0:0:0:0:0:1:11d8
```

The SA MAY join the SVRLOC group in order to receive SrvTypeRqst and AttrRqst messages; these features are OPTIONAL for the SA to implement.

A UA MAY join the SVRLOC-DA group at any or all of these scopes in order to receive DAAdvert messages.

4.2.2 Sending SLPv2 Multicast Messages

The maximum scope for a SLPv2 multicast message is site-local (FF05).

Multicast SLPv2 messages are sent using a particular scope. An SLPv2 agent MUST issue this request using a source address with a scope no less than the scope of the multicast group.

This prevents, for example, a site-local multicast message being sent from a link-local source address.

A SLPv2 UA with an interface configured with at least one global address could multicast a SrvRqst to any scope up to and including site-local, for instance.

4.2.3 Rules for Message Processing

SLPv2 SAs and DAs MUST determine which scope a service: URL address is in. This may be possible by examining the URL if it contains a numerical IPv6 address. If the URL contains a host name, the SA or DA MUST resolve that name to a set of addresses.

A SLPv2 SA or DA MUST NOT respond to a SrvRqst with a service: URL for a service with an address scope less than the request’s source address scope. The rules are given in Figure 1, below.

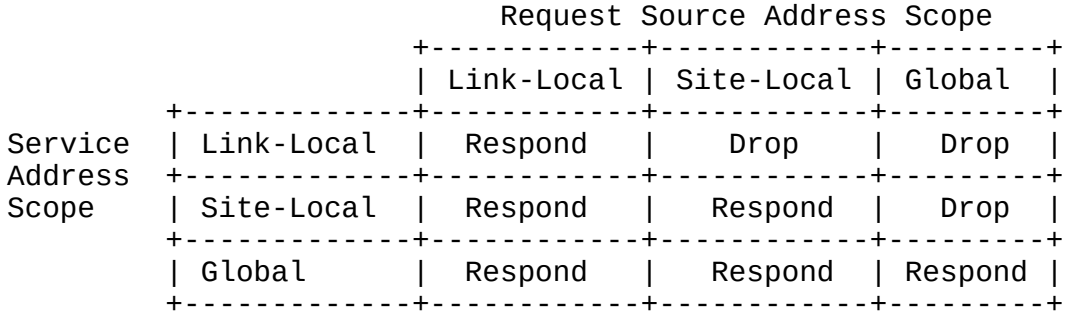

Figure 1: Out-of-Scope Rules

This prevents UAs from being able discover service: URLs for services which cannot be accessed.

4.2.4 SLPv2 Agents with multiple interfaces

A scope zone, or a simply a zone, is a connected region of topology of a given scope. For example, the set of links connected by routers within a particular site, and the interfaces attached to those links, comprise a single zone of site-local scope. To understand the distinction between scopes and zones, observe that the topological regions within two different sites are considered to be two DIFFERENT zones, but of the SAME scope.

A host which has multiple interfaces attached to different links is by definition is attached to two link-local zones. A host may also be attached to multiple zones of other scopes.

A SLPv2 Agent MUST NOT propagate service advertisements from one zone to another. Another way of saying this is a SLPv2 SA or DA MUST NOT respond to a request from one zone with service information associated with a service in a different zone.

The specific implication of these rules is discussed in the sections which follow.

4.2.4.1 General rules

Service Locations (in SrvReg, SrvRply, AttrRst, SAAdvert or DAAdvert messages) whose locations are literal addresses MUST only be sent to SLP agents located on the same zone.

For example, a service: URL containing a link-local address on link A may be sent in a SLPv2 message on link A, to a link-local destination address only.

Each interface of a multihomed device is potentially on a separate link. It is often difficult to determine whether two interfaces are connected to the same link. For that reason a prudent implementation strategy is to not issue SLP messages containing link-local service locations except on the interface where the service is known to reside.

4.2.4.2 Multihomed UA

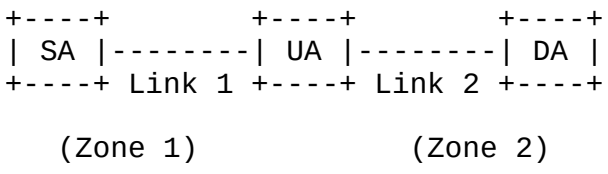

Figure 2: Multihomed UA

In Figure 2 the UA is multihomed. The UA can issue a service request in Zone 1 and discover services on the SA or in Zone 2 and discover services advertised by the DA. For example, if the request is issued from a link-local source address, the SA will only reply with a service available on link 1, the DA only with a service available on link 2.

The UA MUST use active discovery to detect DAs before issuing multicast requests, as per SLPv2 [2]. The UA MUST issue requests using increasing multicast scopes starting at FF01 and increasing to a maximum scope of FF05, to solicit DAAdvertisements. Note the restrictions in Section 4.2.2.

If the UA is unable to discover any DAs using multicast discovery, it may issue site-local scope (FF05) or less multicast requests. (Note that the source address of the request must be of at least the scope of the multicast, as described in section 4.2.2.)

If the UA wishes to discover all services, it must issue requests into both Zone 1 and 2.

4.2.4.3 Multihomed SA

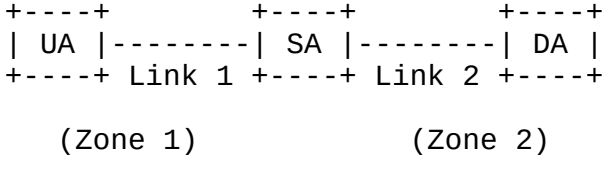

Figure 3: Multihomed SA

In Figure 3, the SA is multihomed. The SA may receive a request from the UA on Link 1 (Zone 1). The SA MUST NOT return service information for services offered on a different zone as a request. For example, the UA could discover services offered in Zone 1 not Zone 2.

The SA may receive a DAAdvert on Link 2 (Zone 2). The SA MUST NOT send a service registration to the DA for a service which is present in Zone 1. The SA MUST register a service with the DA which is present in Zone 2.

The SA MUST NOT include an address in a SAAdvert message which is sent on a zone where the address is not valid. For example, the SA MUST NOT send a SAAdvert onto link 2, if the SAADvert contains a service: URL with a literal link-local scoped IPv6 address for Link 1.

The SA performs active DA discovery, as described in SLPv2 [2]. The SA MUST issue requests using multicast scope FF02 to solicit DAAdvertisements. If the SA has a site-local or global source address, it MUST reissue the request with increasing scopes up to a maximum scope of FF05. Active DA discovery must be attempted in both Zone 1 and 2. This ensures that the SA will discover as many DAs in its scope as possible.

4.2.4.4 Multihomed DA

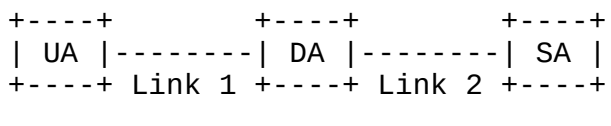

Figure 4: Multihomed DA

In Figure 4, the DA is multihomed. The DA MUST keep track of which interface registrations were made on. The DA MUST prevent a registration from the SA which contains a service information valid in one zone from being discovered in another zone. For example, services registered by the SA in Zone 2 would not be discoverable by the UA in Zone 1.

Care must be taken when issuing DAAdverts. The DA must respond to active DA discovery requests using the same scope as the request. For instance, if the SA issues a SrvRqst message for service type "service:directory" from a link-local source address, the DA MUST respond with a link-local (link 2) source address.

The DA MUST multicast unsolicited DAAdverts on each interface using link-local and site-local source addresses, unless it is only configured with a link-local address. In that case, the DA MUST issue DAAdverts with link-local scope only.

The DA URL MUST contain the address of the greatest scope the DA is configured with in the zone. For instance, if the DA is configured with a link-local, site-local and global address in Zone 2, it would use the global address in the DA URL (as a literal IPv6 address).

5. IANA Considerations

The IPv6 multicast group-id range FF05::1:1000 - FF05::1:13FF was previously assigned by IANA in RFC 2375 for use by SLP [10].

This document defines how the range of addresses FF0X::1:1000 - FF0X::1:13FF is used. IANA has assigned this range of addresses for use by Service Location Protocol.

This document fully defines the multicast addresses that this protocol will use. There is no requirement for the IANA to establish a registry to assign additional addresses.

6. Security Considerations

User Agents and Directory Agents MAY ignore all unauthenticated Service Location messages when a valid IPSec association exists.

Service Agents and Directory Agents MUST be able to use the IP Authentication and IP Encapsulating Security Payload for issuing and processing Service Location messages whenever an appropriate IPSec Security Association exists [13].

SLP allows digital signatures to be produced to allow the verification of the contents of messages. There is nothing in the Modifications for IPv6 document which weakens or strengthens this technique.

Acknowledgments

Thanks to Dan Harrington, Jim Wood and Alain Durand, Thomas Narten, Dave Thaler and Erik Nordmark for their reviews of this document. John Veizades contributed to the original version of this document. The hash function is modified from a code fragment attributed to Chris Torek. Text on Scope Zones is taken from writing by Steve Deering, Brian Haberman and Brian Zill.

References

[1] Bradner, S., "The Internet Standards Process -- Version 3", BCP 9, RFC 2026, October 1996.

[2] Guttman, E., Perkins, C., Veizades, J. and M. Day, "Service Location Protocol, Version 2", RFC 2608, June 1999.

[3] Veizades, J., Guttman, E., Perkins, C. and S. Kaplan, "Service Location Protocol", RFC 2165, June 1997.

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

[5] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, November 1987.

Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, November 1987.

[6] Guttman, E., Perkins, C. and J. Kempf, "Service Templates and URLs", RFC 2609, July 1999.

[7] Berners-Lee, T., Fielding, R. and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[8] Hinden, R. and B. Carpenter, "Format for Literal IPv6 Addresses in URL's", RFC 2732, December 1999.

[9] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 1998.

[10] Hinden, R. and S. Deering, "IPv6 Multicast Address Assignments", RFC 2375, July 1997.

[11] Meyer, D., "Administratively Scoped IP Multicast", RFC 2365, July 1998.

[12] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.

[13] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

Author's Address

Erik Guttman
Sun Microsystems
Eichhoelzelstr. 7
74915 Waibstadt, Germany

Phone: +49 7263 911701
EMail: Erik.Guttman@germany.sun.com

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.