Internet Engineering Task Force
INTERNET DRAFT
Obsoletes RFC 2610
August 13, 2002
Expires in six months

E. Guttman
Sun Microsystems

DHCP Options for Service Location Protocol

draft-guttman-svrloc-rfc2610bis-02.txt

Status of this Memo

Copyright Notice

Abstract

The Dynamic Host Configuration Protocol provides a framework for passing configuration information to hosts on a TCP/IP network. Entities using the Service Location Protocol need to find out the address of Directory Agents in order to transact messages. Another option provides an assignment of scope for configuration of SLP User and Service Agents. This document simplifies and clarifies RFC 2610.

1. Introduction

The Dynamic Host Configuration Protocol [RFC 2131] provides a framework for passing configuration information to hosts on a TCP/IP network. Entities using the Service Location Protocol, Version 2 [RFC 2608] and Service Location Protocol, Version 1 [RFC 2165] need to obtain the address of Directory Agents and Scope configuration. The Service Location Protocol (SLP) provides a default configuration for Scopes and Directory Agents may be discovered using multicast or broadcast. It is useful in a larger deployment to be able to configure SLP Agents using DHCP, so as to centralize the administration and to deploy SLP in networks where multicast routing is not available.

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].

2. Introduction

The DHCP options described below are used to configure Agents using the Service Location Protocol, Version 2 [RFC 2608] and Version 1 [RFC 2165].

The SLP Directory Agent option is used to configure User Agents and Service Agents with the location of Directory Agents in the network.

The SLP Scope Option takes precedence over default scope configuration of SLP agents. The rules for SLPv2 configuration are given elsewhere (in [RFC 2608]) but paraphrased here:

Preference	Mechanism	Requirement level
(1)	Static configuration of scope list	MUST
(2)	Static configuration of DAs *	MUST
(3)	DHCP SLP Scope configuration	SHOULD
(4)	DHCP SLP DA configuration *	SHOULD
(5)	Dynamic discovery (DAAdverts) **	MAY
(6)	Dynamic discovery (SAAdverts) **	MAY
(7)	Use of the scope "DEFAULT"	MUST

Mechanisms of higher preference are used instead of those of lower preference if possible. For example, if there is a static scope list - this is used, but if no static configuration of DAs is available, dynamic DA discovery may be used.

* If no scope is configured by a higher preference mechanism, the scope list is derived from the combined scope list from all DAs whose locations have been given. A SrvRqst is sent to each of these DAs

soliciting a DAAdvert message which contains their scope list.

** Dynamic discovery of DAs using active or passive DA discovery will provide both a list of DAs to use and a scope list. If there are no DAs available, active SA discovery may be used to obtain a list of scopes as well.

2.1 Changes to RFC 2610

The use of the MANDATORY flag is deprecated. The value of the MANDATORY flag MUST be ignored. The effect doing this is that the SLP User Agent or ServiceAgent MAY employ either active or passive multicast discovery of Directory Agents in addition to SLP configuration using DHCP.

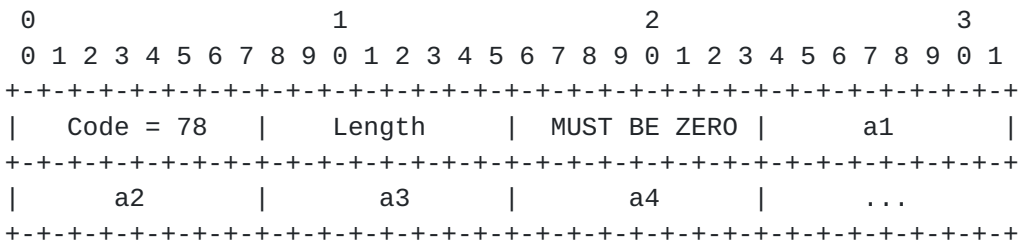
RFC 2610 was not clear about how DAs interpret option 79. DAs MUST ignore option 79 - their scope list MUST be staticly configured.

RFC 2610 was also not clear about how to use scope lists by UAs and SAs. UAs MUST use a proper subset of the scope list delivered in option 79 - that at least one scope from the list, as many as the entire list. SAs MUST use the entire list by default (though a user, administrator or software agent MAY select a subset of the scope list obtained by option 79).

Static configuration is now said to take precedence over DHC configuration.

3. SLP Directory Agent Option

This option specifies the location of one or more SLP Directory Agents.



The SLP Directory Agent Option specifies a list of IP addresses for Directory Agents. Directory Agents MUST be listed in order of preference, if there is an order of preference.

The Length value must include one for the 'MUST BE ZERO' byte and include four for each Directory Agent address which follows. Thus, the Length minus one of the option MUST always be divisible by 4 and has a minimum value of 5.

The address of the Directory Agent is given in network byte order.

The 'MUST BE ZERO' byte MUST be ignored by all interpreting option 78 or 79. Its presence is required for backward compatibility.

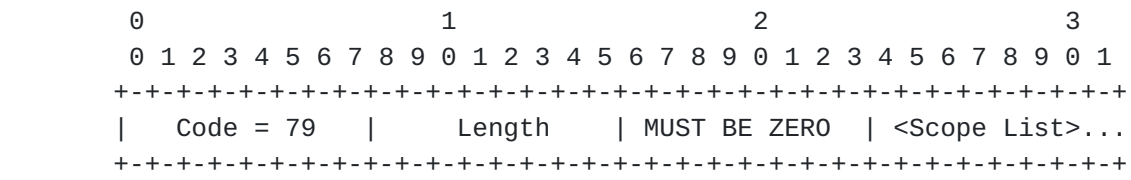
Note that for backward compatibility with some deployed software the Mandatory byte MUST NOT be set to any byte value for which the high order bit (0x80) is set.

The Directory Agents listed in this option MUST be configured with the non-empty subset of the scope list that the Agent receiving the Directory Agent Option is configured with. See the notes below.

The SLPv2 specification [RFC 2608] defines how to use this option.

4. SLP Service Scope Option

The scope list is a comma delimited list which indicates the scopes that a SLP Agent is configured to use.



The Length indicates the number of bytes which follow. Since the Scope-List String is encoded using UTF-8 [RFC 2279] characters, it may be the cast that the Length is not the same as the number of characters in the Scope-List String. The Length value must include one for the "Mandatory" byte.

The 'MUST BE ZERO' byte MUST be ignored by those interpreting option 79.

The Scope List String syntax and usage are defined in the SLPv2 specification [RFC 2608].

4.1. Zero Length Scope-List String Configuration

A SLP Service Scope Option which indicates a Length of 1 (in other words, omitting the <Scope List> string entirely) indicates that the UA or SA SHOULD use dynamic discovery of SLP scopes if possible, or "DEFAULT" if this feature is not implemented.

The UA or SA MAY use the aggregated list of scopes of all known DAs. If no DAs are known, the UA will use SA discovery to determine the list of scopes on the network, as defined in [RFC 2608]. Otherwise, the UA or SA MUST use the scope list "DEFAULT".

5. Security Considerations

If a malicious host is able to insert fraudulent information in DHCPOFFER packets sent to a prospective SLP Agent then the SLP Agent will be unable to obtain service, or may unwittingly be directed to use the incorrect services.

Many opportunities for denial of service exist. A service agent could find that it might rely on fraudulent or otherwise malicious directory agents to advertise its services. DHCPOFFERs could prevent the regular SLP framework from functioning by directing clients to not use multicast, to use nonexistent directory agents and so on.

These difficulties are inherited from the much larger and more serious problem, viz. securing or authenticating any information whatsoever from a DHCP server (or client!) is not possible in common DHCP deployments.

Implementors SHOULD use DHCP Authentication [RFC 3118] to reduce the risk of corrupted SLP boot configuration received via DHCP.

Acknowledgements

Charlie Perkins contributed to RFC 2610. Stuart Cheshire's valuable comments aided in reworking the specification. James Kempf, Roger Holm and Mikael Pahmp did an analysis of scope configuration which showed that the MANDATORY byte greatly complicated the algorithm and was of little utility.

References

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

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

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

See also: E. Guttman, J. Kempf, "Service Location Protocol, Version 2", draft-guttman-svrloc-rfc2608bis-02.txt, August 2002, A work in progress.

[RFC 2615] Veizades, J., Guttman, E., Perkins, C. and S. Kaplan, "Service Location Protocol", RFC 2165, July 1997.

[RFC 2279] Yergeau, F., "UTF-8, a transformation format of unicode
and ISO 10646", RFC 2279, October 1998.

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

Author's Address

Erik Guttman
Sun Microsystems, Inc.
Eichhoelzelstr. 7
74915 Waibstadt, Germany

Phone: +49 6227 356 202
EMail: Erik.Guttman@Sun.Com

Full Copyright Statement

Acknowledgement

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