Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 14, 2008

S. Krishnan
Ericsson

November 11, 2007

Carrying DHCP options over Neighbor Discovery Messages
draft-krishnan-intarea-ra-dhcp-00

Status of this Memo

Copyright Notice

Abstract

DHCP options are used to convey network and host configuration information to the hosts attached to a network. Some networks may wish to configure their routers to advertise these same pieces of information, and might use IPv6 Router Advertisements do distribute these parameters. This document defines a generic neighbor discovery option for carrying DHCP options. This option is carried over IPv6 Router Advertisements.

Table of Contents

1. Requirements notation

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 [RFC2119].

2. Introduction

Router Advertisements (RAs) as defined in [RFC2461] are used to deliver configuration information that is common to several nodes in the same network. The router advertisements are usually multicasted to all nodes in a given network in order to be scalable. The configuration information is contained in Neigbor Discovery (ND) options. DHCP [RFC3315] is used for delivering addressing information and other related configuration information to single clients when they request it. Since there are two mechanisms for delivering common configuration information to a given node, configuration parameters need to be defined under two varying option formats. This leads to duplication of work needed to standardize these options and additional implementation complexity on hosts in order to process these option variants. In order to prevent this duplication, this document proposes a neighbor discovery option that can be used to directly carry any relevant DHCP option.

3. Justification

Recently there has been interest in doing more of DHCP work using Neighbor Discovery (Router Advertisement) messages. This is mainly to accomodate environments where DHCP is not available and the only way of convey configuration information is through RAs. Since DHCP options cannot be carried in RAs this leads to duplicate standardization efforts to develop ND options for options already developed for DHCP. For example consider [RFC5006] that redefines a DNS server address option for RAs that has been defined long ago for DHCP. Not only does this waste valuable time in redundant standardization effort, it also complicates client implementations that need to be able to parse and understand tho incompatible option formats. It also takes away valuable code points away from the neighbor discovery message types (8 bit value). Thus it make sense to define a DHCP carrier option for neighbor discovery messages so that we can reuse DHCP options as necessary without coming up with new neighbor discovery options.

4. Applicability

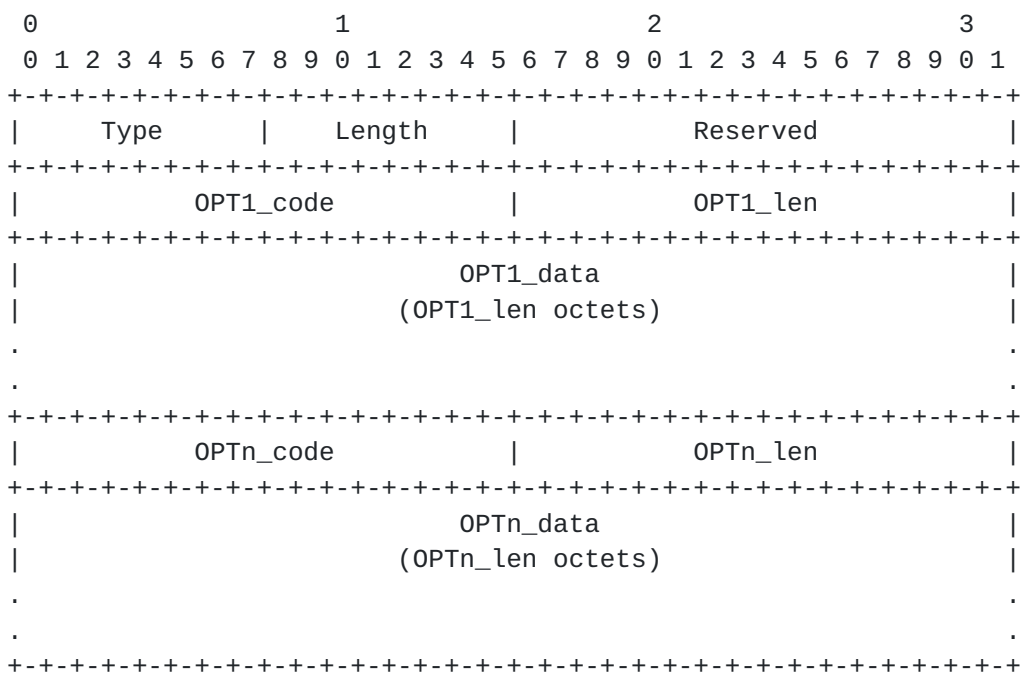
It is possible to carry any DHCP option using the DHCPC option. However, this does not always make sense since there are DHCP options that are client specific and hence are not uniform across all the hosts in the network. The DHCPC option SHOULD NOT be used to carry DHCP options that are client specific. This option can be carried in any neighbor discovery messages.

5. Operation

After a node receives a neighbor discovery that contains a DHCPC option it needs to verify if the DHCPC option length is at least 1 (8 octets). If it is not, the node MUST NOT process the DHCPC option any further and SHOULD log an error message locally. Otherwise it needs to process the embedded DHCP options one at a time as it would if it had received them through a DHCP message. It is entirely possible that the code for processing these options is shared between the neighbor discovery based delivery and DHCP based delivery of these options.

6. DHCP Container(DHCPC) Option

The DHCPC option in Neighbor Discovery messages is used to carry complete DHCP options. There can be more than DHCP option contained in a DHCPC option. The number of contained DHCP options is not explicitly mentioned in the DHCPC. The receiving node MUST process all the contained options



Type

8-bit identifier of the type of option. The option identifier for the DHCPC option will be allocated by the IANA.

Option Length

8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 octets. The value 0 is considered invalid.

OPT1_code

16-bit unsigned integer. The DHCPv6 option code of the first DHCP option that is carried in the DHCPC option.

OPT1_len

16-bit unsigned integer. The length of the option data of the first included DHCP option (excluding the OPT1_code and the

OPT1_len fields)

OPT1_Data

The data field of the first included neighbor discovery option. The contents of this field are determined by the type of the option.

OPT1_code

16-bit unsigned integer. The DHCPv6 option code of the first DHCP option that is carried in the DHCPC option.

OPT1_len

16-bit unsigned integer. The length of the option data of the first included DHCP option (excluding the OPT1_code and the OPT1_len fields)

OPT1_Data

The data field of the first included neighbor discovery option. The contents of this field are determined by the type of the option.

Figure 1: DHCPC layout

7. IANA Considerations

This document defines a new IPv6 neighbor discovery option for carrying DHCP options. IANA is requested to assign the a new neighbor discovery option type in the registry maintained at

http://www.iana.org/assignments/icmpv6-parameters

<TBA> DHCP Carrier Option [RFC-krishnan-intarea-ra-dhcp-00.txt]

The option type 26 is recommended as it is the first unused option type at the time of writing this draft.

8. Security Considerations

The mechanism described in this document provides a method by which one or more DHCP options can be carried using IPv6 Router Advertisement messages. The neighbor discovery messages containing the DHCPC option may be intercepted, modified or replayed in order to communicate false configuration data to the client hosts. In order to prevent these kinds of attacks, it is recommended that SEND [RFC3971] be used.

9. Acknowledgmentes

The author would like to thank Jari Arkko for his detailed review and comments on the earlier versions of this document.

10. Normative References

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

[RFC2461] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[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.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC5006] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Option for DNS Configuration", RFC 5006, September 2007.

Author's Address

Suresh Krishnan
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 x42871
Email: suresh.krishnan@ericsson.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).