Network Working Group
Internet-Draft
Expires: August 29, 2003

R. Droms (ed.)
Cisco Systems

February 28, 2003

DNS Configuration options for DHCPv6
draft-ietf-dhc-dhcpv6-opt-dnsconfig-03.txt

Status of this Memo

Copyright Notice

Abstract

This document describes DHCPv6 options for passing a list of available DNS resolvers and a domain search list to a client.

1. Introduction

This document describes two options for passing configuration information related to Domain Name Service (DNS) [1, 6] in DHCPv6 [2].

2. Terminology

The key words MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD,

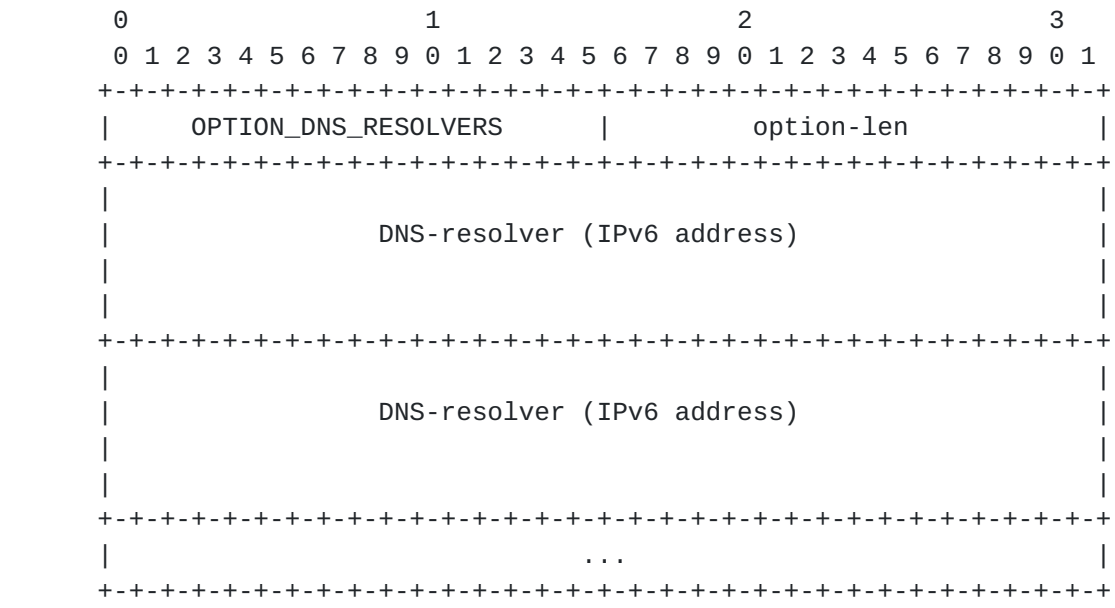
SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL in this document are to be interpreted as described in RFC2119 [3].

This document uses terminology specific to IPv6 and DHCPv6 as defined in section "Terminology" of the DHCP specification [2].

3. DNS Resolver option

The DNS Resolver option provides a list of one or more IPv6 addresses of DNS recursive resolvers to which a client's DNS resolver MAY send DNS queries [1]. The DNS servers are listed in the order of preference for use by the client resolver.

The format of the DNS Resolver option is:



option-code: OPTION_DNS_RESOLVERS (tbd)

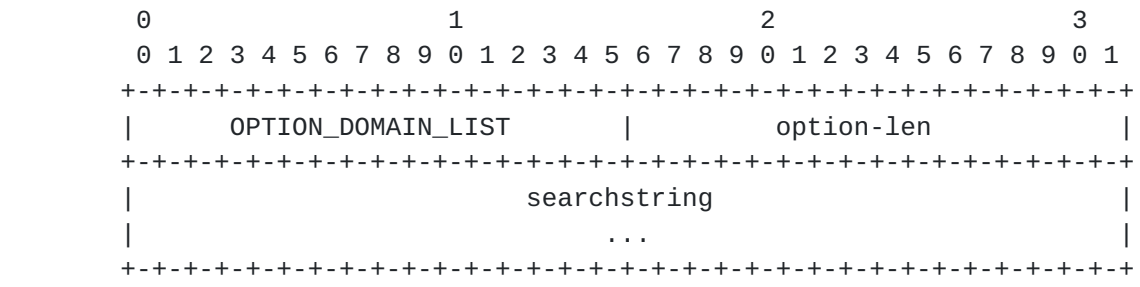
option-len: Length of the list of DNS resolvers in octets; must be a multiple of 16

DNS-server: IPv6 address of DNS resolver

4. Domain Search List option

The Domain Search List option specifies the domain search list the client is to use when resolving hostnames with DNS. This option does not apply to other name resolution mechanisms.

The format of the Domain Search List option is:



option-code: OPTION_DOMAIN_LIST (tbd)

option-len: Length of the 'searchstring' field in octets

searchstring: The specification of the list of domain names in the Domain Search List

The list of domain names in the 'searchstring' MUST be encoded as specified in section "Representation and use of domain names" of the DHCPv6 specification [2].

5. Appearance of these options

The Domain Name Server option MUST NOT appear in other than the following messages: Solicit, Advertise, Request, Renew, Rebind, Information-Request, Reply.

The Domain Search List option MUST NOT appear in other than the following messages: Solicit, Advertise, Request, Renew, Rebind, Information-Request, Reply.

6. Security Considerations

The DNS Resolver option may be used by an intruder DHCP server to cause DHCP clients to send DNS queries to an intruder DNS resolver. The results of these misdirected DNS queries may be used to spoof DNS names.

To avoid attacks through the DNS Resolver option, the DHCP client SHOULD require DHCP authentication (see section "Authentication of DHCP messages" in the DHCPv6 specification) before installing a list of DNS resolvers obtained through authenticated DHCP .

The Domain Search List option may be used by an intruder DHCP server to cause DHCP clients to search through invalid domains for

incompletely specified domain names. The results of these misdirected searches may be used to spoof DNS names. Note that support for DNSSEC [4] will not avert this attack, because the resource records in the invalid domains may be legitimately signed.

The degree to which a host is vulnerable to attack via an invalid domain search option is determined in part by DNS resolver behavior. RFC1535 [7] contains a discussion of security weaknesses related to implicit as well as explicit domain searchlists, and provides recommendations relating to resolver searchlist processing. Section 6 of RFC1536 [5] also addresses this vulnerability, and recommends that resolvers:

1. Use searchlists only when explicitly specified; no implicit searchlists should be used.

2. Resolve a name that contains any dots by first trying it as an FQDN and if that fails, with the names in the searchlist appended.

3. Resolve a name containing no dots by appending with the searchlist right away, but once again, no implicit searchlists should be used.

In order to minimize potential vulnerabilities it is recommended that:

1. Hosts implementing the domain search option SHOULD also implement the searchlist recommendations of RFC1536, section 6.

2. Where DNS parameters such as the domain searchlist or DNS servers have been manually configured, these parameters SHOULD NOT be overridden by DHCP.

3. A host SHOULD require the use of DHCP authentication (see section "Authentication of DHCP messages" in the DHCPv6 specification) prior to accepting a domain search option.

7. IANA Considerations

IANA is requested to assign an option code to these options from the option-code space defined in section "DHCPv6 Options" of the DHCPv6 specification [2].

8. Acknowledgments

This option was originally part of the DHCPv6 specification, written

by Jim Bound, Mike Carney, Charlie Perkins, Ted Lemon, Bernie Volz and Ralph Droms.

The analysis of the potential attack through the domain search list is taken from the specification of the DHCPv4 Domain Search option, RFC3397 [8].

Thanks to Rob Austein, Alain Durand, Peter Koch, Tony Lindstrom and Pekka Savola for their contributions to this document.

9. Changes from draft-ietf-dhc-dhcpv6-opt-dnsconfig-02.txt

This document includes the following changes in response to comments made during the dhc/dnsext WG last call:

- Combined RFC2119 reference and reference to DHCPv6 specification into one "Terminology" section; added explicit normative reference to DHCPv6 specification.
- Changed name of "Domain Name Server" option to "DNS Resolver" option.
- Clarified and corrected filed names and descriptions of fields in the option format diagrams.
- Reworded "Appearance of these options" for clarity; removed Confirm from list of messages in which the options can appear.
- Clarified the type of attack that can be mounted through the Domain Search List option by copying text from RFC3997

Normative References

[1] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[2] Bound, J., Carney, M., Perkins, C., Lemon, T., Volz, B. and R. Droms (ed.), "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC XXXX, TBD 2003.

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

[4] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[5] Kumar, A., Postel, J., Neuman, C., Danzig, P. and S. Miller, "Common DNS Implementation Errors and Suggested Fixes", RFC

1536, October 1993.

Normative References

[6] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[7] Gavron, E., "A Security Problem and Proposed Correction With Widely Deployed DNS Software", RFC 1535, October 1993.

[8] Aboba, B. and S. Cheshire, "Dynamic Host Configuration Protocol (DHCP) Domain Search Option", RFC 3397, November 2002.

Author's Address

Ralph Droms (ed.)
Cisco Systems
250 Apollo Drive
Chelmsford, MA 01824
USA

Phone: +1 978 497 4733
EMail: rdroms@cisco.com

Full Copyright Statement

Acknowledgement

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