Network Working Group
Internet-Draft
Expires: July 2, 2002

J. Bound
Compaq Computer Corporation
M. Carney
Sun Microsystems, Inc.
C. Perkins
Nokia Research Center
T. Lemon
Nominum
B. Volz
Ericsson
R. Droms
Cisco Systems

Jan 2002

DNS Configuration Options for DHCPv6
draft-ietf-dhc-dhcpv6-opt-dnsconfig-00.txt

Status of this Memo

Copyright Notice

Abstract

This document describes three options for DNS-related configuration information in DHCPv6: DNS Servers, Domain Name, Domain Search list.

1. Introduction

This document describes three options for configuration information related to Domain Name Service (DNS) [1, 2] in DHCPv6 [5].

2. Requirements

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in RFC 2119 [1]

3. Terminology

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

4. Domain Name Server option

The Domain Name Server option provides a list of one or more IP addresses of DNS servers to which a client's DNS resolver MAY send DNS queries [3]. The DNS servers SHOULD be listed in the order of preference for use by the client resolver.

The format of the Domain Name Server option is:

```
    0                   1                   2                   3
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |      OPTION_DNS_SERVERS       |         option-len            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   |                   DNS server (IP address)                     |
   |                                                               |
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   |                   DNS server (IP address)                     |
   |                                                               |
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                              ...                              |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code: OPTION_DNS_SERVERS

option-length: Length of the 'options' field in octets; must be a

multiple of 16

DNS server: IP address of DNS server

5. Domain Name option

The Domain Name option is used by the server to inform the client of the domain name the client should append to its host name to form the client's fully qualified domain name (FQDN).

The format of the Domain Name option is:

```
    0                   1                   2                   3
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |      OPTION_DOMAIN_NAME       |         option-len            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          domain-name                          |
   |                              ...                              |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code: OPTION_DOMAIN_NAME (tbd)

option-length: Length of the 'domain-name' field in octets

domain-name: Domain name for client

The 'domain-name' MUST be encoded as specified in section "Representation and use of domain names" of the DHCPv6 specification [5].

Local client policy MAY choose to override the domain-name supplied in the Domain-Name option with a locally configured value.

6. Domain Search List option

In some circumstances, it is useful for the DHCP client to be configured with list of domain names to be appended to a host name when resolving DNS name. This document defines a new DHCP option which is passed from the DHCP server to the DHCP client to specify the domain search list used when resolving hostnames with DNS. This option does not apply to other name resolution mechanisms.

The format of the Domain Search option is:

```
       0                   1                   2                   3
       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
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |      OPTION_DOMAIN_LIST       |         option-len            |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                         searchstring                          |
      |                              ...                              |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code: OPTION_DOMAIN_LIST (tbd)

option-length: 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 [5].

Local client policy MAY choose to override the domain search list supplied in the Domain Search List option with a locally configured value.

7. Appearance of these option

The Domain Name Server option MUST appear only in the following messages: Solicit, Advertise, Request, Confirm, Renew, Rebind, Information-Request, Reply.

The Domain Name option MUST appear only in the following messages: Solicit, Advertise, Request, Confirm, Renew, Rebind, Information-Request, Reply.

The Domain Search List option MUST appear only in the following messages: Solicit, Advertise, Request, Confirm, Renew, Rebind, Information-Request, Reply. Note that the Domain Search List option will only appear in a Solicit message if the client has a preferred search list that it is supplying to the server as a hint.

8. Security Considerations

The Domain Name Server option may be used by an intruder DHCP server to cause DHCP clients to send DNS queries to an intruder DNS server.

The results of these misdirected DNS queries may be used to spoof DNS names.

The Domain Name option may be used by an intruder DHCP server to configure a DHCP client with an invalid domain name, which could be used as a denial of service attack.

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.

To avoid attacks through the Domain Name Server option and the Domain Name option, the DHCP client SHOULD use authenticated DHCP (see section "Authentication of DHCP messages" in the DHCPv6 specification [5].

Because the Domain Search List option may be used to spoof DNS name resolution in a way that cannot be detected by DNS security mechanisms like DNSSEC [4], DHCP clients and servers MUST use authenticated DHCP when a Domain Search List option is included in a DHCP message.

9. 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 [5].

References

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

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

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

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

[5] Bound, J., Carney, M., Perkins, C., Lemon, T., Volz, B. and R. Droms (ed.), "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", draft-ietf-dhc-dhcpv6-23 (work in progress), February 2002.

Authors' Addresses

Jim Bound
Compaq Computer Corporation
ZK3-3/W20
110 Spit Brook Road
Nashua, NH 03062-2698
USA

Phone: +1 603 884 0062
EMail: Jim.Bound@compaq.com

Mike Carney
Sun Microsystems, Inc.
Mail Stop: UMPK17-202
901 San Antonio Road
Palo Alto, CA 94303-4900
USA>

Phone: +1 650 786 4171
EMail: mwc@eng.sun.com

Charlie Perkins
Nokia Research Center
Communications Systems Lab
313 Fairchild Drive
Mountain View, CA 94043
USA

Phone: +1 650 625 2503
EMail: charliep@iprg.nokia.com

Nominum

EMail: mellon@nominum.com

Bernie Volz
Ericsson
959 Concord Street
Framingham, MA 01701
USA

Phone: +1 508 875 3162
EMail: bernie.volz@ericsson.com

Ralph Droms
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.