Internet Engineering Task Force
INTERNET DRAFT

C. Perkins
IBM
22 November 1995

Options for DHCPv6
draft-ietf-dhc-v6opts-00.txt

Status of This Memo

Abstract

The Dynamic Host Configuration Protocol for IPv6 [2] (DHCPv6) provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the "options" field of the DHCPv6 message. The data items themselves are also called "options."

This document specifies the current set of DHCPv6 options. This document will be periodically updated as new options are defined. Each superseding document will include the entire current list of valid options.

Contents

1. Introduction

This document specifies options for use with the Dynamic Host Configuration Protocol for IP version 6, DHVPv6. The full description of DHCPv6 packet formats may be found in the DHCPv6 specification document [2].

This document defines the format of information in the last field of DHCPv6 packets ('options'). The options defined within this document specify a generalized use of this area for giving information useful to a wide class of machines, operating systems and configurations. Sites with a single DHCPv6 server that is shared among heterogeneous clients may choose to define other, site- specific formats for the use of the 'options' field.

Section 2 of this memo describes the formats of DHCPv6 options.

Information on registering new options is contained in section 10. Although option numbers in this document correspond exactly to the same option numbers in the options specification for IPv4 [1], there is no requirement to keep numbering future options in any consistent manner except purely as a matter of editorial and cross-referencing convenience.

2. DHCPv6 Option Field Format

DHCPv6 options have the same format as the BOOTP "vendor extensions" defined in RFC 1497 [9]. Options may be fixed length or variable length. All options begin with a tag octet, which uniquely identifies the option. Fixed-length options without data consist of only a tag octet. Only options 0 and 255 are fixed length. All other options are variable-length with a length octet following the tag octet. The value of the length octet does not include the two octets specifying the tag and length. The length octet is followed by "length" octets of data. In the case of some variable-length options the length field is a constant but must still be specified.

Any options defined subsequent to this document should contain a length octet even if the length is fixed or zero.

All multi-octet quantities are in network byte-order.

Option codes 128 to 254 (decimal) are reserved for site-specific options.

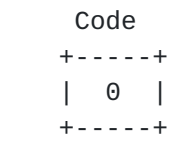
All of the options described in this document will also have their default values specified, if any.

3. Option specifications

3.1. Pad Option

The pad option can be used to cause subsequent fields to align on word boundaries.

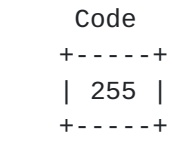
The code for the pad option is 0, and its length is 1 octet.



3.2. End Option

The end option marks the end of valid information in the vendor field. Subsequent octets should be filled with pad options.

The code for the end option is 255, and its length is 1 octet.

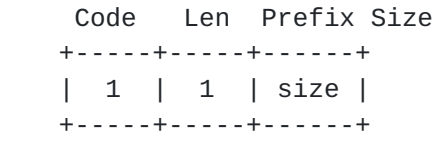


3.3. Routing Prefix size

The routing prefix size option specifies the length of the routing prefix, counting the number of leading 1 bits to be applied to the client's IPv6 address to get the routing prefix.

If both the routing prefix size and the router option are specified in a DHCPv6 reply, the routing prefix size option MUST be first.

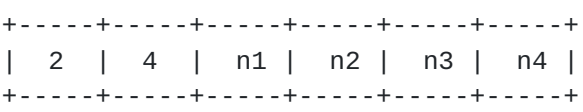
The code for the routing size prefix option is 1, and its length is 1 octet.



3.4. Time Offset

The time offset field specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC). The offset is expressed as a signed 32-bit integer.

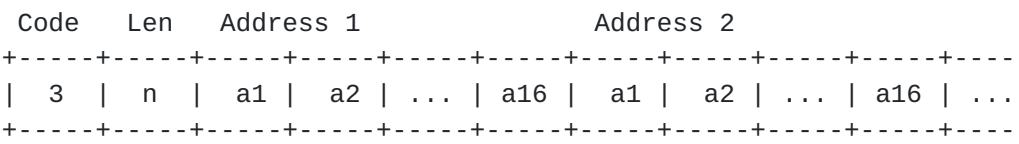
The code for the time offset option is 2, and its length is 4 octets.



3.5. Router Option

The router option specifies a list of IP addresses for routers on the client's subnet. Routers SHOULD be listed in order of preference.

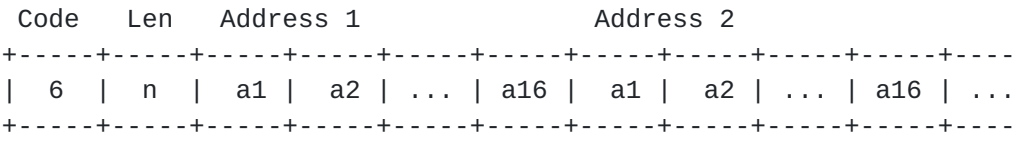
The code for the router option is 3. The minimum length for the router option is 16 octets, and the length MUST always be a multiple of 16.



3.6. Domain Name Server Option

The domain name server option specifies a list of Domain Name System (STD 13, RFC 1035 [5]) name servers available to the client. Servers SHOULD be listed in order of preference.

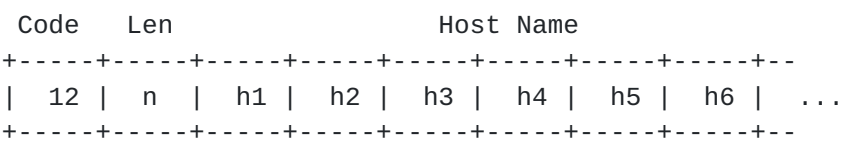
The code for the domain name server option is 6. The minimum length for this option is 16 octets, and the length MUST always be a multiple of 16.



3.7. Host Name Option

This option specifies the name of the client. The name may or may not be a fully qualified domain name (FQDN). See RFC 1035 [5] for character set restrictions.

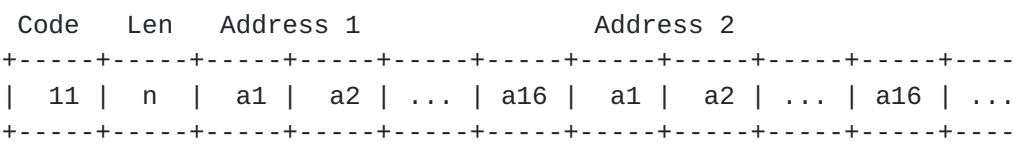
The code for this option is 12, and its minimum length is 1.



3.8. Resource Location Server Option

This option specifies a list of Resource Location servers [12] available to the client. Servers SHOULD be listed in order of preference.

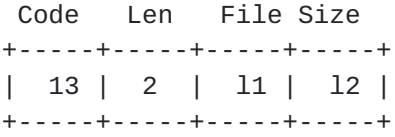
The code for this option is 11. The minimum length for this option is 16 octets, and the length MUST always be a multiple of 16.



3.9. Boot File Size Option

This option specifies the length in 512-octet blocks of the default boot image for the client. The file length is specified as an unsigned 16-bit integer.

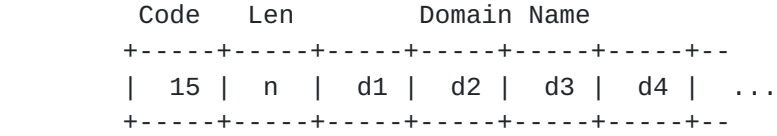
The code for this option is 13, and its length is 2.



3.10. Domain Name

This option specifies the domain name that client should use when resolving hostnames via the Domain Name System.

The code for this option is 15. Its minimum length is 1.



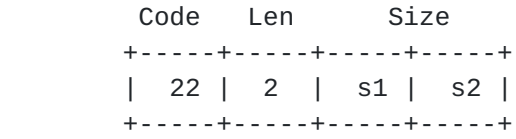
4. IP Layer Parameters per Host

This section details the options that affect the operation of the IP layer on a per-host basis.

4.1. Maximum Datagram Reassembly Size

This option specifies the maximum size datagram that the client should be prepared to reassemble. The size is specified as a 16-bit unsigned integer. The minimum value legal value is 576 [3].

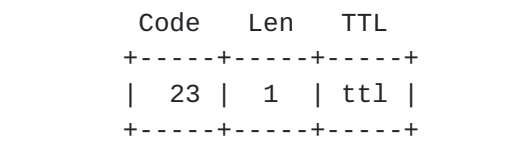
The code for this option is 22, and its length is 2.



4.2. Default IP Time-to-live

This option specifies the default time-to-live that the client should use on outgoing datagrams. The TTL is specified as an octet with a value between 1 and 255.

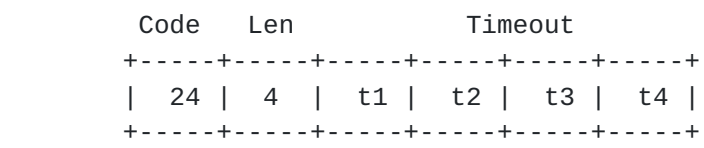
The code for this option is 23, and its length is 1.



4.3. Path MTU Aging Timeout Option

This option specifies the timeout (in seconds) to use when aging Path MTU values discovered by the mechanism defined in RFC 1191 [6]. The timeout is specified as a 32-bit unsigned integer.

The code for this option is 24, and its length is 4.



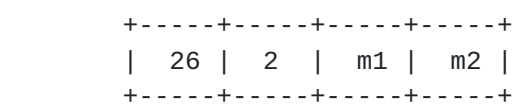
5. IP Layer Parameters per Interface

This section details the options that affect the operation of the IP layer on a per-interface basis. It is expected that a client can issue multiple requests, one per interface, in order to configure interfaces with their specific parameters.

5.1. Interface MTU Option

This option specifies the MTU to use on this interface. The MTU is specified as a 16-bit unsigned integer. The minimum legal value for the MTU is 68.

The code for this option is 26, and its length is 2.



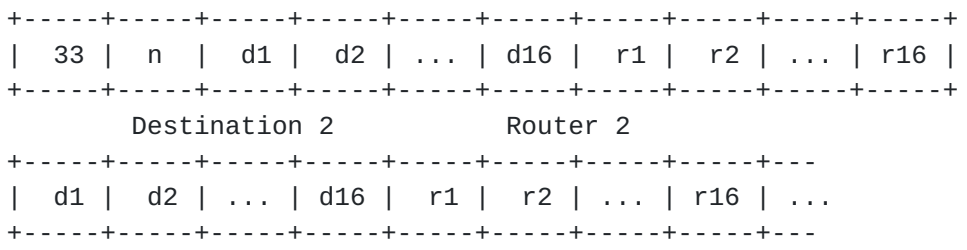
5.2. Static Route Option

This option specifies a list of static routes that the client should install in its routing cache. If multiple routes to the same destination are specified, they are listed in descending order of priority.

The routes consist of a list of IP address pairs. The first address is the destination address, and the second address is the router for the destination.

The default route (0.0.0.0) is an illegal destination for a static route. See section 3.5 for information about the router option.

The code for this option is 33. The minimum length of this option is 32, and the length MUST be a multiple of 16.



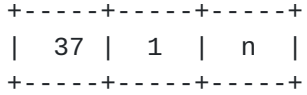
6. TCP Parameters

This section lists the options that affect the operation of the TCP layer on a per-interface basis.

6.1. TCP Default TTL Option

This option specifies the default TTL that the client should use when sending TCP segments. The value is represented as an 8-bit unsigned integer. The minimum value is 1.

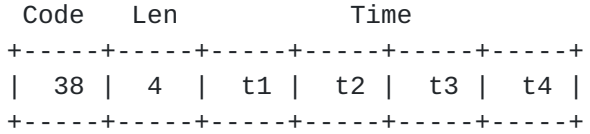
The code for this option is 37, and its length is 1.



6.2. TCP Keepalive Interval Option

This option specifies the interval (in seconds) that the client TCP should wait before sending a keepalive message on a TCP connection. The time is specified as a 32-bit unsigned integer. A value of zero indicates that the client should not generate keepalive messages on connections unless specifically requested by an application.

The code for this option is 38, and its length is 4.



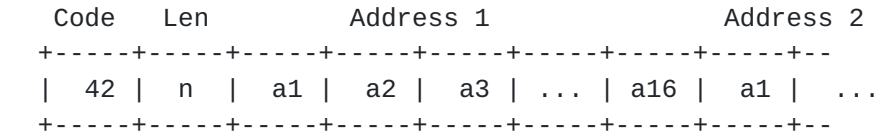
7. Application and Service Parameters

This section details some miscellaneous options used to configure miscellaneous applications and services.

7.1. Network Time Protocol Servers Option

This option specifies a list of IP addresses indicating NTP [4] servers available to the client. Servers SHOULD be listed in order of preference.

The code for this option is 42. Its minimum length is 16, and the length MUST be a multiple of 16.



7.2. Vendor Specific Information

This option is used by clients and servers to exchange vendor-specific information. The information is an opaque object of n octets, presumably interpreted by vendor-specific code on the clients and servers. The definition of this information is vendor specific. The vendor is indicated in the class-identifier option. Servers not equipped to interpret the vendor-specific information sent by a client MUST ignore it (although it may be reported). Clients which do not receive desired vendor-specific information SHOULD make an attempt to operate without it, although they may do so (and announce they are doing so) in a degraded mode.

If a vendor potentially encodes more than one item of information in this option, then the vendor SHOULD encode the option using "Encapsulated vendor-specific options" as described below:

The Encapsulated vendor-specific options field SHOULD be encoded as a sequence of type/length/value fields of identical syntax to the DHCPv6 options field with the following exceptions:

- Codes other than 0 or 255 MAY be redefined by the vendor within the encapsulated vendor-specific extensions field, but SHOULD conform to the tag-length-value syntax defined in section 2.

- Code 255 (END), if present, signifies the end of the encapsulated vendor extensions, not the end of the vendor extensions field. If no code 255 is present, then the end of the enclosing vendor-specific information field is taken as the end of the encapsulated vendor-specific extensions field.

The code for this option is 43 and its minimum length is 1.

```
Code   Len   Vendor-specific information
+-----+-----+-----+-----+---
|  43 |  n  |  i1 |  i2 | ...
+-----+-----+-----+-----+---
```

When encapsulated vendor-specific extensions are used, the information bytes 1-n have the following format:

```
 Code   Len   Data item        Code   Len   Data item       Code
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|  T1 |  n  |  d1 |  d2 | ... |  T2 |  n  |  D1 |  D2 | ... | ... |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

7.3. X Window System Font Server Option

This option specifies a list of X Window System [11] Font servers available to the client. Servers SHOULD be listed in order of preference.

The code for this option is 48. The minimum length of this option is 16 octets, and the length MUST be a multiple of 16.

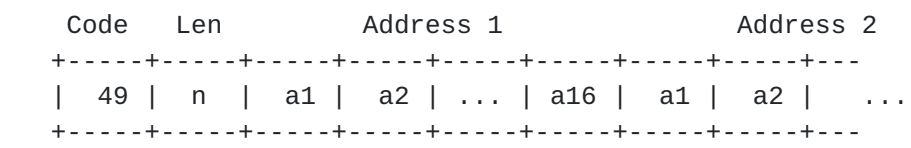
```
 Code   Len         Address 1               Address 2
+-----+-----+-----+-----+-----+-----+-----+-----+---
|  48 |  n  |  a1 |  a2 | ... | a16 |  a1 |  a2 |   ...
+-----+-----+-----+-----+-----+-----+-----+-----+---
```

7.4. X Window System Display Manager Option

This option specifies a list of IP addresses of systems that are running the X Window System Display Manager [11] and are available to the client.

Addresses SHOULD be listed in order of preference.

The code for the this option is 49. The minimum length of this option is 16, and the length MUST be a multiple of 16.



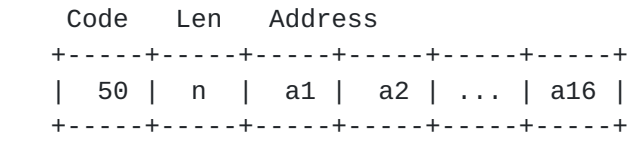
8. DHCPv6 Extensions

This section details the options that are specific to DHCPv6.

8.1. Requested IP Address

This option is used in a DHCPv6 [2] client request (DISCOVER) to allow the client to request that a particular IP address be assigned.

The code for this option is 50, and its length is 16.

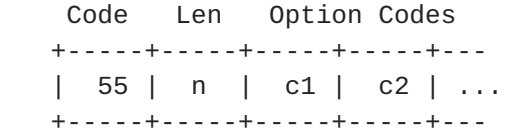


8.2. Parameter Request List

This option is used by a DHCPv6 client to request values for specified configuration parameters. The list of requested parameters is specified as n octets, where each octet is a valid DHCPv6 option code as defined in this document.

The client MAY list the options in order of preference. The DHCPv6 server is not required to return the options in the requested order, but MUST try to insert the requested options in the order requested by the client.

The code for this option is 55. Its minimum length is 1.

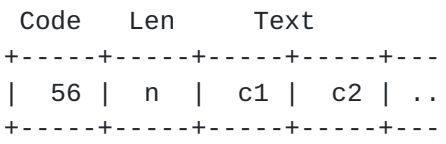


8.3. Message

This option is used by a DHCPv6 server to provide an error message to a DHCPv6 client in a CONF-RESPONSE message in the event of a failure.

A client may use this option in a CONF-RESPONSE message to indicate the why the client declined the offered parameters. The message consists of n octets of NVT ASCII [8] text, which the client may display on an available output device.

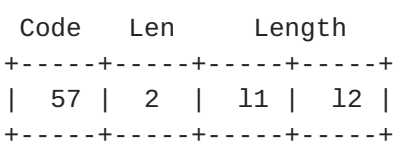
The code for this option is 56 and its minimum length is 1.



8.4. Maximum DHCPv6 Message Size

This option specifies the maximum length DHCPv6 message that it is willing to accept. The length is specified as an unsigned 16-bit integer. A client may use the maximum DHCPv6 message size option in DISCOVER or CONF-REQUEST messages, but should not use the option in CONF-RESPONSE messages (see [2] for DISCOVER, CONF-REQUEST, and CONF-RESPONSE message formats).

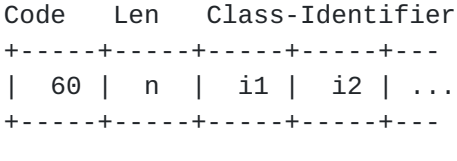
The code for this option is 57, and its length is 2. The minimum legal value is 576 octets.



8.5. Class-identifier

This option is used by DHCPv6 clients to optionally identify the type and configuration of a DHCPv6 client. The information is a string of n octets, interpreted by servers. Vendors and sites may choose to define specific class identifiers to convey particular configuration or other identification information about a client. For example, the identifier may encode the client's hardware configuration. Servers not equipped to interpret the class-specific information sent by a client MUST ignore it (although it may be reported).

The code for this option is 60, and its minimum length is 1.

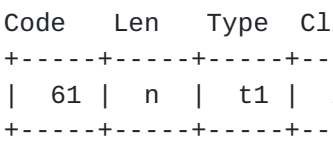


8.6. Client-identifier

This option is used by DHCPv6 clients to specify their unique identifier. DHCPv6 servers use this value to index their database of address bindings. This value is expected to be unique for all clients in an administrative domain.

It is expected that this field will typically contain a hardware type and hardware address, but this is not required. Current legal values for hardware types are defined in [10].

The code for this option is 61, and its minimum length is 2.



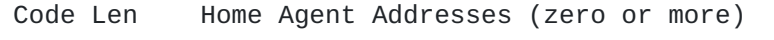
8.7. Mobile Home Address Option

When this option is present in a client request message, the DHCPv6 server is asked to send an appropriate home address to the mobile host. The DHCPv6 server, in its corresponding offering message, will insert the requested address into the usual place for requested IP addresses. The DHCPv6 server will typically notify the mobile host of (one of) its home agents' addresses, as configured by the local administration to be associated with the address given to the mobile host. That home agent's IP address is inserted in the data field of the mobile home address option.

It is anticipated that the mobile-IP working group will approve one of the current proposals for allowing a mobile host, with its already known mobile home address, to dynamically discover the location of a home agent serving the home address. In that case, the DHCPv6 server may be configured to send out mobile home addresses and expect that the mobile host discover the home agent's address by whichever method is approved by the working group.

It is also anticipated that many installations will allow several home agents to serve the same mobile home addresses, for redundancy or load sharing. For this reason, we have also allowed for the possibility that the DHCPv6 server may wish to insert multiple home agent addresses in the mobile home address option.

The format of the mobile home address option is as follows:



```
+----+----+ - -+ - -+-----+ - --+ - -+ - -+ - -+
| 68 | n  | a1 | a2 | ... | a16 | ...
+----+----+ - -+ - -+-----+ - --+ - -+ - -+ - -+
```

The code for the mobile home address option is 68. The length is 16 octets multiplied by the number of home agents supplied in the option, which may be zero or more. It is expected that the usual length will be sixteen octets, containing a single home agent's address.

9. Neighbor Discovery Extensions

This section contains option definitions for specifying parameters that are useful with IPv6 Neighbor Discovery [7].

10. Extensions

Additional generic data fields may be registered by contacting:

Internet Assigned Numbers Authority (IANA)
USC/Information Sciences Institute
4676 Admiralty Way
Marina del Rey, California 90292-6695

or by email as: iana@isi.edu

Implementation specific use of undefined generic types (including those in the range 69-127) may conflict with other implementations, and registration is required.

11. Acknowledgements

Quite a bit of this internet draft is copied directly from RFC1533 [1], written by Steve Alexander and Ralph Droms.

12. Security Considerations

Security issues are not discussed in this memo. However, there is an urgent need to define some security protocol for use with DHCPv6, since otherwise malicious parties could create numerous denial-of-service style attacks based on depleting available server resources or providing corrupted or infected data to unsuspecting clients.

References

[1] S. Alexander and R. Droms. DHCP Options and BOOTP Vendor Extensions. RFC 1533, October 1993.

[2] J. Bound. Dynamic Host Configuration Protocol for IPv6. draft-ietf-dhc-dhcpv6-03.txt -- work in progress, November 1995.

[3] R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. draft-ietf-ipngwg-ipv6-spec-02.txt - work in progress, June 1995.

[4] D. Mills. Network Time Protocol (Version 3). RFC 1305, March 1992.

[5] P. Mockapetris. DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION. RFC 1035, November 1987.

[6] J. Mogul and S. Deering. Path MTU Discovery. RFC 1191, November 1990.

[7] T. Narten, E. Nordmark, and W. Simpson. IPv6 Neighbor Discovery. draft-ietf-ipngwg-discovery-03.txt -- work in progress, November 1995.

[8] J. Postel and J. Reynolds. Telnet Protocol Specification. RFC 854, May 1983.

[9] J. Reynolds. BOOTP Vendor Information Extensions. RFC 1497, August 1993.

[10] J. Reynolds and J. Postel. Assigned Numbers. RFC 1700, October 1994.

[11] R. Scheifler. FYI On the X Window System. RFC 1198, January 1991.

[12] J. Veizades, S. Kaplan, and E. Guttman. Service Location Protocol. draft-ietf-svrloc-protocol-07.txt - work in progress, October 1995.

Chair's Addresses

The working group can be contacted via the current chair:

Ralph Droms
Computer Science Department
323 Dana Engineering
Bucknell University
Lewisburg, PA 17837

Phone: (717) 524-1145
EMail: droms@bucknell.edu

Author's Address

Questions about this memo can be directed to:

Charles Perkins
Room J1-A25
T. J. Watson Research Center
IBM Corporation
30 Saw Mill River Rd.
Hawthorne, NY 10532

Work: +1-914-784-7350
Fax: +1-914-784-7007
E-mail: perk@watson.ibm.com