

## Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)

### Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

### Copyright Notice

Copyright (C) The Internet Society (2004).

### Abstract

The Dynamic Host Configuration Protocol (DHCP) options for Vendor Class and Vendor-Specific Information can be limiting or ambiguous when a DHCP client represents multiple vendors. This document defines two new options, modeled on the IPv6 options for vendor class and vendor-specific information, that contain Enterprise Numbers to remove ambiguity.

### Table of Contents

1.	Introduction . . . . .	2
1.1.	Conventions Used in This Document. . . . .	2
2.	Supporting Multiple Vendor Instances . . . . .	3
3.	Vendor-Identifying Vendor Class Option . . . . .	3
4.	Vendor-Identifying Vendor-Specific Information Option . . . . .	5
5.	IANA Considerations . . . . .	7
6.	Security Considerations . . . . .	7
7.	References . . . . .	8
7.1.	Normative References . . . . .	8
7.2.	Informative References . . . . .	8
8.	Author's Address . . . . .	8
9.	Full Copyright Statement . . . . .	9

## 1. Introduction

The DHCP protocol for IPv4, RFC 2131 [2], defines options that allow a client to indicate its vendor type (option 60), and the DHCP client and server to exchange vendor-specific information (option 43) [5]. Although there is no prohibition against passing multiple copies of these options in a single packet, doing so would introduce ambiguity of interpretation, particularly if conveying vendor-specific information for multiple vendors. The vendor identified by option 60 defines the interpretation of option 43, which itself carries no vendor identifier. Furthermore, the concatenation of multiple instances of the same option, required by RFC 2131 and specified by RFC 3396 [4], means that multiple copies of options 60 or 43 would not remain independent.

In some circumstances, an implementation may need to support multiple, independently defined forms of vendor-specific information. For example, implementations that must conform to an industry-standard use of DHCPv4, to allow interoperability in a particular technology space, may be required to support the vendor-specific options of that industry group. But the same implementation may also require support for vendor-specific options defined by the manufacturer. In particular, this is an issue for vendors of devices supporting CableLabs [9] standards, such as DOCSIS, CableHome, and PacketCable, as those standards define an industry-specific use for options 60 and 43.

This document defines two new options, modeled on the IPv6 options for vendor class and vendor-specific information defined in RFC 3315 [6], that contain IANA-assigned Enterprise Numbers [3] to remove ambiguity about the interpretation of their contents. If desired, these new options can be used in addition to the current vendor class and vendor information options, whose definition is unaffected by this document.

### 1.1. Conventions Used in This Document

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 BCP 14, RFC 2119 [1].

## 2. Supporting Multiple Vendor Instances

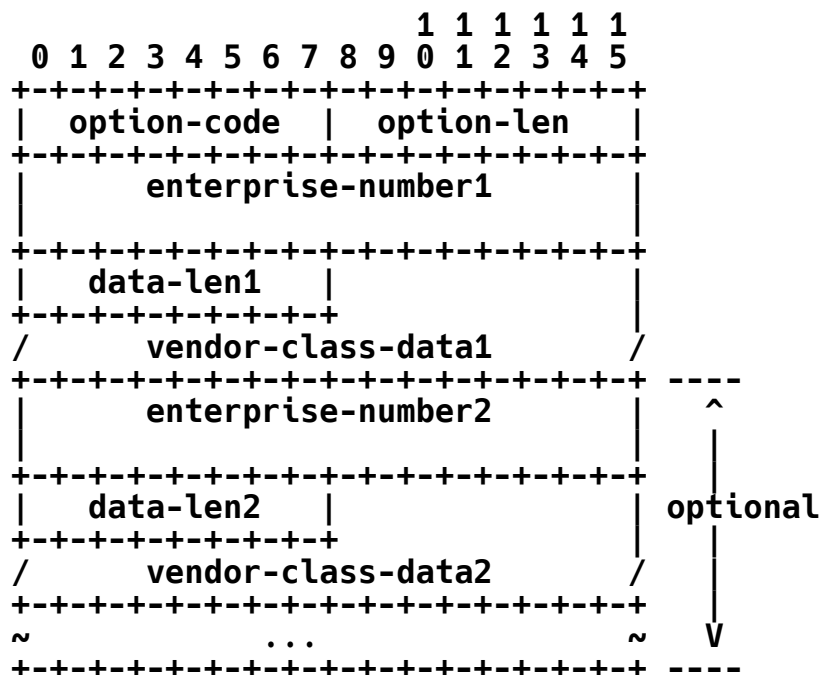
The options defined in this document may each contain data corresponding to more than one vendor. The data portion of each option defined here contains an enterprise number (assigned by IANA [3]), followed by an internal data length, followed by vendor-specific data. This sequence may be repeated multiple times within each option. Because the aggregate of the vendor-specific data for either option may exceed 255 octets, these options are hereby declared to be "concatenation-requiring", as defined by RFC 3396 [4]. As such, for each of the two options defined here, the aggregate of all instances of vendor-specific data is to be considered one long option. These long options can be divided into smaller options for packet encoding in conformance with RFC 3396, on whatever octet boundaries are convenient to the implementation. Dividing on the boundaries between vendor instances is not required but may be convenient for encoding or packet tracing.

## 3. Vendor-Identifying Vendor Class Option

A DHCP client may use this option to unambiguously identify the vendor that manufactured the hardware on which the client is running, the software in use, or an industry consortium to which the vendor belongs. The information contained in the per-vendor data area of this option is contained in one or more opaque fields that may identify details of the hardware configuration.

This option may be used wherever Vendor Class Identifier (option 60) may be used, as described in RFC 2131 [2], except for DHCPNAK messages, where other options are not permitted. It is most meaningful in messages from DHCP client to DHCP server (DHCPDISCOVER, DHCPREQUEST, DHCPINFORM).

The format of the V-I Vendor Class option is as follows:



option-code           OPTION\_V-I\_VENDOR\_CLASS (124)

option-len            total length of all following option data in octets

enterprise-numberN    The vendor's 32-bit Enterprise Number as registered with IANA [3]

data-lenN             Length of vendor-class-data field

vendor-class-dataN    Details of the hardware configuration of the host on which the client is running, or of industry consortium compliance

This option contains information corresponding to one or more Enterprise Numbers. Multiple instances of this option may be present and MUST be concatenated in accordance with RFC 3396 [4]. An Enterprise Number SHOULD only occur once among all instances of this option. Behavior is undefined if an Enterprise Number occurs multiple times. The information for each Enterprise Number is treated independently, regardless of whether it occurs in an option with other Enterprise Numbers or in a separate option.

The vendor-class-data comprises a series of separate items, each of which describes some characteristic of the client's hardware configuration or capabilities. Examples of vendor-class-data instances might include the version of the operating system the client is running or the amount of memory installed on the client.

Each instance of the vendor-class-data is formatted as follows:

```

      1 1 1 1 1 1
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+---+---+---+---+---+---+---+---+---+---+
|  data-len  | opaque-data |
+---+---+---+---+---+---+---+---+---+---+
/                               /
+---+---+---+---+---+---+---+---+---+---+

```

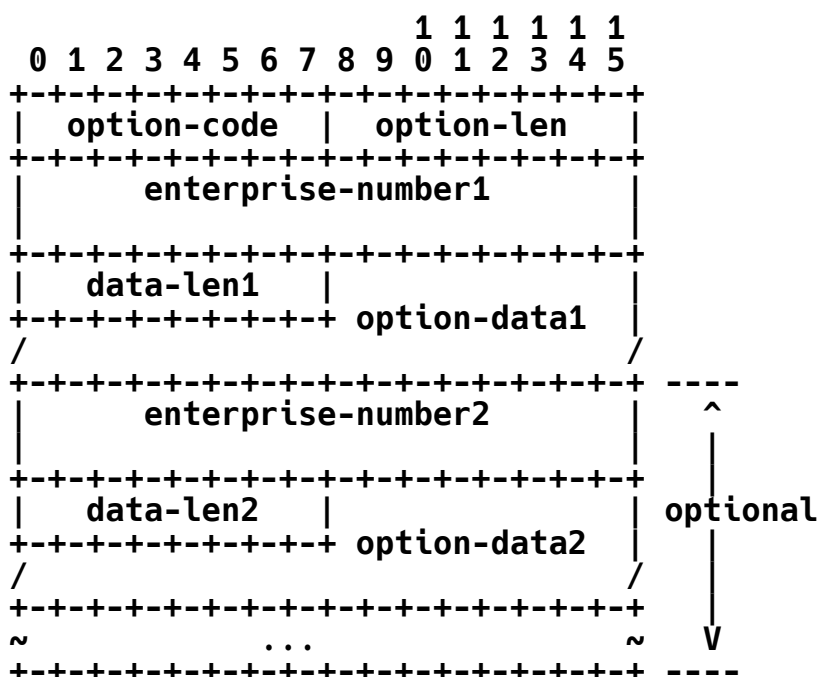
The data-len is one octet long and specifies the length of the opaque vendor class data in network byte order.

#### 4. Vendor-Identifying Vendor-Specific Information Option

DHCP clients and servers may use this option to exchange vendor-specific information. Either party may send this option, as needed. Although a typical case might be for a client to send the Vendor-Identifying Vendor Class option, to elicit a useful Vendor-Identifying Vendor-Specific Information Option, there is no requirement for such a flow.

This option may be used in any packets where "other" options are allowed by RFC 2131 [2], specifically DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK, and DHCPINFORM.

The format of the V-I Vendor-specific Information option is as follows:



option-code            `OPTION_V-I_VENDOR_OPTS` (125)

option-len            total length of all following option data in octets

enterprise-numberN    The vendor's registered 32-bit Enterprise Number as registered with IANA [3]

data-lenN            Length of option-data field

option-dataN          Vendor-specific options, described below

The definition of the information carried in this option is vendor specific. The vendor is indicated in the enterprise-number field. This option contains information corresponding to one or more Enterprise Numbers. Multiple instances of this option may be present and MUST be concatenated in accordance with RFC 3396 [4].

An Enterprise Number SHOULD only occur once among all instances of this option. Behavior is undefined if an Enterprise Number occurs multiple times. The information for each Enterprise Number is treated independently, regardless of whether it occurs in an option with other Enterprise Numbers, or in a separate option.

Use of vendor-specific information allows enhanced operation, utilizing additional features in a vendor's DHCP implementation. Servers not equipped to interpret the vendor-specific information sent by a client **MUST** ignore it. Clients that do not receive desired vendor-specific information **SHOULD** make an attempt to operate without it.

The encapsulated vendor-specific option-data field **MUST** be encoded as a sequence of code/length/value fields of identical format to the DHCP options field. The option codes are defined by the vendor identified in the enterprise-number field and are not managed by IANA. Option codes 0 and 255 have no pre-defined interpretation or format. Each of the encapsulated options is formatted as follows:

```

      1 1 1 1 1 1
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| subopt-code | subopt-len |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
/      sub-option-data      /
/                               /
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

subopt-code            The code for the encapsulated option

subopt-len            An unsigned integer giving the length of the  
option-data field in this encapsulated option in  
octets

sub-option-data       Data area for the encapsulated option

## 5. IANA Considerations

The values for the `OPTION_V-I_VENDOR_CLASS` and `OPTION_V-I_VENDOR_OPTS` option codes have been assigned from the numbering space defined for public DHCP Options in RFC 2939 [7].

## 6. Security Considerations

This document in and by itself provides no security, nor does it impact existing security. DHCP provides an authentication and message integrity mechanism, as described in RFC 3118 [8], which may be used if authenticity is required for data carried by the options defined in this document.

## 7. References

### 7.1. Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [2] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.
- [3] IANA, "Private Enterprise Numbers", <<http://www.iana.org/assignments/enterprise-numbers>>.
- [4] Lemon, T. and S. Cheshire, "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)", RFC 3396, November 2002.

### 7.2. Informative References

- [5] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.
- [6] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.
- [7] Droms, R., "Procedures and IANA Guidelines for Definition of New DHCP Options and Message Types", BCP 43, RFC 2939, September 2000.
- [8] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

### URIs

- [9] <<http://www.cablelabs.com/>>

## 8. Author's Address

Josh Littlefield  
Cisco Systems, Inc.  
1414 Massachusetts Avenue  
Boxborough, MA 01719  
USA

Phone: +1 978-936-1379  
EMail: [joshl@cisco.com](mailto:joshl@cisco.com)



## 9. Full Copyright Statement

Copyright (C) The Internet Society (2004).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the IETF's procedures with respect to rights in IETF Documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

## Acknowledgement

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