[MS-DHCPE]:
Dynamic Host Configuration Protocol (DHCP) Extensions

Revision Summary

Date	Revision History	Revision Class	Comments
12/18/2006	0.1		MCPP Milestone 2 Initial Availability
03/02/2007	1.0		MCPP Milestone 2
04/03/2007	1.1		Monthly release
05/11/2007	1.2		Monthly release
06/01/2007	2.0	Major	Updated and revised the technical content.

Date	Revision History	Revision Class	Comments
07/03/2007	3.0	Major	Updated and revised the technical content.
07/20/2007	4.0	Major	Updated and revised the technical content.
08/10/2007	5.0	Major	Updated and revised the technical content.
09/28/2007	6.0	Major	Updated and revised the technical content.
10/23/2007	7.0	Major	Updated and revised the technical content.
11/30/2007	7.0.1	Editorial	Revised and edited the technical content.
01/25/2008	7.0.2	Editorial	Revised and edited the technical content.

Table of Contents

1 Introduction

The Dynamic Host Configuration Protocol (DHCP) is an Internet Engineering Task Force (IETF) standard protocol designed to provide a framework for passing configuration information to hosts on a TCP/IP network. See [RFC2131] section 1 for an introduction to this protocol.

This document specifies a set of vendor specific options as well as non-standard options for DHCP (DHCP Extensions).

1.1 Glossary

The following terms are defined in [MS-GLOS]:

Dynamic Host Configuration Protocol (DHCP) Client
Dynamic Host Configuration Protocol (DHCP) Server
Statement of Health (SoH)

The following terms are specific to this document:

Classless Static Routes: A DHCP option that provides a subnet mask for each entry, so that the subnet mask can be other than what would be determined using the algorithm specified in STD 5, [RFC791], and STD 5, [RFC950].

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as described in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

[IANA-ENT] Internet Assigned Numbers Authority, "Private Enterprise Numbers", January 2007, http://www.iana.org/assignments/enterprise-numbers

[MS-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary", March 2007.

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981, http://www.ietf.org/rfc/rfc791.txt

[RFC950] Mogul, J. and Postel, J., "Internet Standard Subnetting Procedure", RFC 950, August 1985, http://www.ietf.org/rfc/rfc950.txt

[RFC951] Croft, B. and Gilmore, J. "BOOTSTRAP Protocol (BOOTP)", RFC 951, September 1985, http://www.ietf.org/rfc/rfc951.txt

[RFC1534] Droms, R., "Interoperation Between DHCP and BOOTP", RFC 1534, October 1993, http://www.ietf.org/rfc/rfc1534.txt

[RFC1812] Baker, F., Ed., "Requirements for IP Version 4 Routers", RFC 1812, June 1995, http://www.ietf.org/rfc/rfc1812.txt

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.ietf.org/rfc/rfc2119.txt

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997, http://www.ietf.org/rfc/rfc2131.txt

[RFC2132] Alexander, S. and Droms, R., "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997, http://www.ietf.org/rfc/rfc2132.txt

[RFC3004] Stump, G., Droms, R., Gu, Y., Vyaghrapuri, R., Demirtjis, A., Beser, B., and Privat, J., "The User Class Option for DHCP", RFC 3004, June 2000, http://www.ietf.org/rfc/rfc3004.txt

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and Carney, M., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003, http://www.ietf.org/rfc/rfc3315.txt

[RFC3442] Lemon, T., Cheshire, S., and Volz, B., "The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4", RFC 3442, December 2002, http://www.ietf.org/rfc/rfc3442.txt

[RFC3925] Littlefield, J., "Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)", RFC 3925, October 2004, http://www.ietf.org/rfc/rfc3925.txt

1.2.2 Informative References

[INTEL-PXE] Intel Corporation, "Preboot Execution Environment", Version 2.1, September 1999, http://download.intel.com/design/archives/wfm/downloads/pxespec.pdf

[MS-DHCPN] Microsoft Corporation, "Dynamic Host Configuration Protocol (DHCP) Extensions for Network Access Protection (NAP)", March 2007.

[MS-SOH] Microsoft Corporation, "Statement of Health for Network Access Protection (NAP) Protocol Specification", January 2007.

[MSDN-DHCP] Microsoft Corporation, "Dynamic Host Configuration Protocol", http://www.microsoft.com/technet/itsolutions/network/dhcp/default.mspx

[MSDN-NAP] Microsoft Corporation, "Network Access Protection", http://www.microsoft.com/technet/network/nap/default.mspx

[RFC1001] Network Working Group, "Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods", RFC 1001, March 1987, http://www.ietf.org/rfc/rfc1001.txt

[RFC1002] Network Working Group, "Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Detailed Specifications", RFC 1002, March 1987, http://www.ietf.org/rfc/rfc1002.txt

[RFC1035] Mockapetris, R., "Domain Names - Implementation and Specification", RFC 1035, November 1987, http://www.ietf.org/rfc/rfc1035.txt

[RFC1534] Droms, R., "Interoperation Between DHCP and BOOTP", RFC 1534, October 1993, http://www.ietf.org/rfc/rfc1534.txt

[RFC3396] Lemon, T. and Cheshire, S., "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)", RFC 3396, November 2002, http://www.ietf.org/rfc/rfc3396.txt

[RFC3442] Lemon, T., Cheshire, S., and Volz, B., "The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4", RFC 3442, December 2002, http://www.ietf.org/rfc/rfc3442.txt

1.3 Protocol Overview (Synopsis)

DHCP uses the following basic steps to automatically configure a network address and configuration information on a **DHCP client**. The application of DHCP discussed here is an illustrative example of an IPv4 network, where the DHCP client and the **DHCP server** are on the same subnet and the client machine has no prior IP address configured on the network interface. DHCP may also be used by a client to obtain configuration parameters (other than the IP address) from the DHCP server. For further details, see section 3.4 of [RFC2131].

1. When the TCP/IP protocol initializes and DHCP has been enabled on any of the client machine's interfaces, the DHCP client sends a DHCPDISCOVER message to find the DHCP servers on the network and to obtain a valid IPv4 address configuration. The DHCP client includes a Vendor-Class Identifier Option that contains "vendor class identifier" information about the host, such as the operating system version.

2. All DHCP servers that receive the DHCPDISCOVER message and have been configured with valid IPv4 address configuration for the client send a DHCPOFFER message back to the DHCP client. The DHCP servers optionally include other configuration information for the client in the DHCPOFFER message, in case the client wants to select the specific configuration information it desires. If configuration information is included, then based on the vendor class identifier that the client included in the message the DHCP servers also include any specific standard options or vendor-specific options appropriate to hosts running that operating system version. If there are no specific standard options or vendor-specific options defined for hosts running that operating system version, the the server ignores the Vendor-Class Identifier Option sent by the client.

3. The DHCP client selects an IPv4 address configuration to use from the DHCPOFFER messages that it receives. The DHCP client then sends a DHCPREQUEST message to the selected DHCP server by using the Server ID option, requesting the use of the selected configuration. The client again includes its vendor class identifier in the message.

4. The DHCPREQUEST message identifies the server that sent the offer that the DHCP client selected. The DHCP servers for which the Server Identifier sent by the client in the DHCP REQUEST does not match the Server ID put the offered IPv4 address back into the available pool of addresses. The selected DHCP server assigns the IPv4 address configuration to the DHCP client and sends a DHCPACK (acknowledgment) message to the DHCP client. The DHCP servers include configuration information, including any specific standard options or vendor-specific options based on the vendor class identifier sent by the client in the DHCPREQUEST message.

The DHCP client computer completes the TCP/IP initialization. It then repeats the above steps for other interfaces, if present, for which DHCP is enabled. Once complete, the client can use all TCP/IP services and applications for normal network communications and connectivity to other IPv4 hosts.

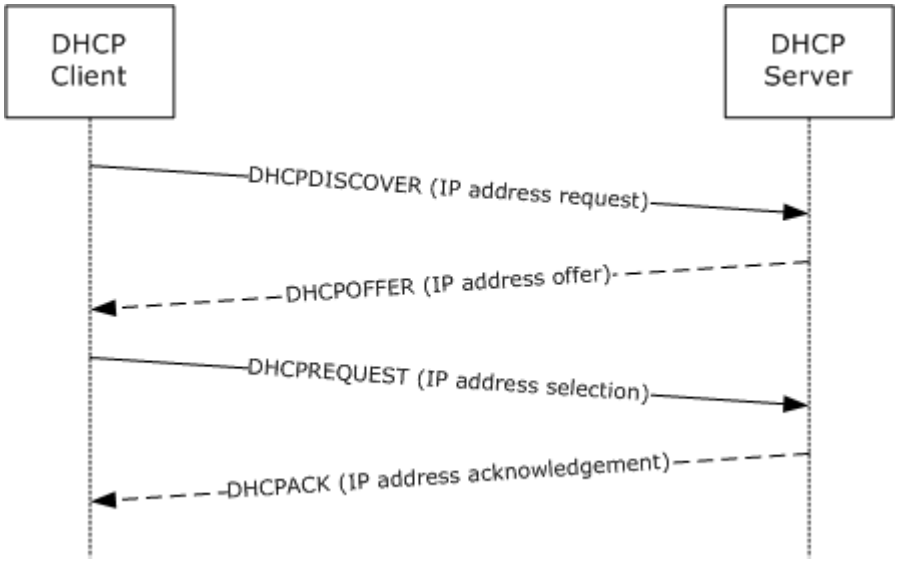


Figure 1: Basic DHCP process

The DHCP client may choose to decline an offer from a DHCP server if it finds that the IP address included in the DHCPOFFER message sent by the server is already in use on that network. If so, the DHCP client sends a DHCPDECLINE message and restarts the configuration process by sending a DHCPDISCOVER message again.

The DHCP server may send a DHCPNAK message in response to the client's DHCPREQUEST message if one or more of the desired configuration options sent by the client in that message are unacceptable. In this case, the DHCP client restarts the configuration process by sending a DHCPDISCOVER message again.

The DHCP client may choose to relinquish its lease on the IP address by sending a DHCPRELEASE message to the server.

In some cases, the DHCP client may remember and want to reuse an IP address that was previously allocated by the DHCP server to it. In this case, the client may begin the initialization process by sending a DHCPREQUEST message to the server containing that network address as the "requested IP address". The DHCP server sends a DHCPACK message to the client if it chooses to allow the client to continue to use that IP address. Otherwise, the DHCP server may send a DHCPNAK message to the client.

For further details on the DHCP protocol overview, refer to section 3 of [RFC2131].

DHCPv6 uses the following basic steps to automatically configure a network address on a DHCPv6 client. The application of DHCPv6 discussed here is an illustrative example of an IPv6 network. The DHCPv6 client and the DHCPv6 server are on the same subnet and the client machine has no prior IPv6 address configured on the network interface. DHCPv6 may also be used by a client to obtain configuration parameters (other than the IP address) from the DHCPv6 server. Details are as specified in [RFC3315] sections 1, 18.1.5, and 18.2.5.

1. When the TCP/IP protocol initializes and DHCPv6 has been enabled on any of the client machine's interfaces, the DHCPv6 client sends a DHCPv6 Solicit message to the All_DHCP_Relay_Agents_and_Servers multicast address specified in [RFC3315] to discover the available DHCPv6 servers. The DHCPv6 client includes a Vendor-Class Option that contains information about the host, such as the operating system version.

2. All DHCPv6 servers that receive the DHCPv6 Solicit message from the client and have been configured with valid IPv6 address configuration information for the client send a DHCPv6 Advertise message in response to the DHCPv6 client. The DHCPv6 servers optionally include other configuration information for the client in the DHCPv6 Advertise message, in case the client wants to select the specific configuration information it desires. If configuration information is included, then based on the vendor class information that the client included in the message the DHCPv6 servers also include any specific standard options or vendor-specific options appropriate to hosts running that operating system version. If there are no specific standard options or vendor-specific options defined for hosts running that operating system version, then the DHCPv6 servers ignore the Vendor-Class Option sent by the client.

3. The DHCPv6 client selects an IPv6 address configuration to use from the DHCPv6 Advertise messages that it receives. The DHCPv6 client then sends a DHCP Request message to the selected DHCPv6 server by using the Server Identifier option, requesting the use of the selected configuration. The client again includes a Vendor-Class Option in the message.

4. The DHCPv6 Request message identifies the server that sent the offer that the DHCPv6 client selected. The DHCPv6 servers for which Server Identifier sent by the client in DHCPv6 Request does not match the Server Identifier put the offered IPv6 address back into the available pool of addresses. The selected DHCPv6 server assigns the IPv6 address configuration to the DHCPv6 client and sends a DHCPv6 Reply message with no Status code option or with a Status code option with the value Success to the DHCPv6 client. The DHCPv6 servers include the configuration information, including any specific standard options or vendor-specific options based on the vendor class information sent by the client in the DHCPv6 Request message.

The presence of a Status code option with any value other than Success in a DHCPv6 message from the server to the client is construed as a failure and the DHCPv6 client then restarts the initialization process by sending the DHCPv6 Solicit message again.

The DHCPv6 client computer completes the TCP/IP initialization as described above. It then repeats the above steps for other interfaces, if present, for which DHCPv6 is enabled. Once complete, the client can use all TCP/IP services and applications for normal network communications and connectivity to other IPv6 hosts.

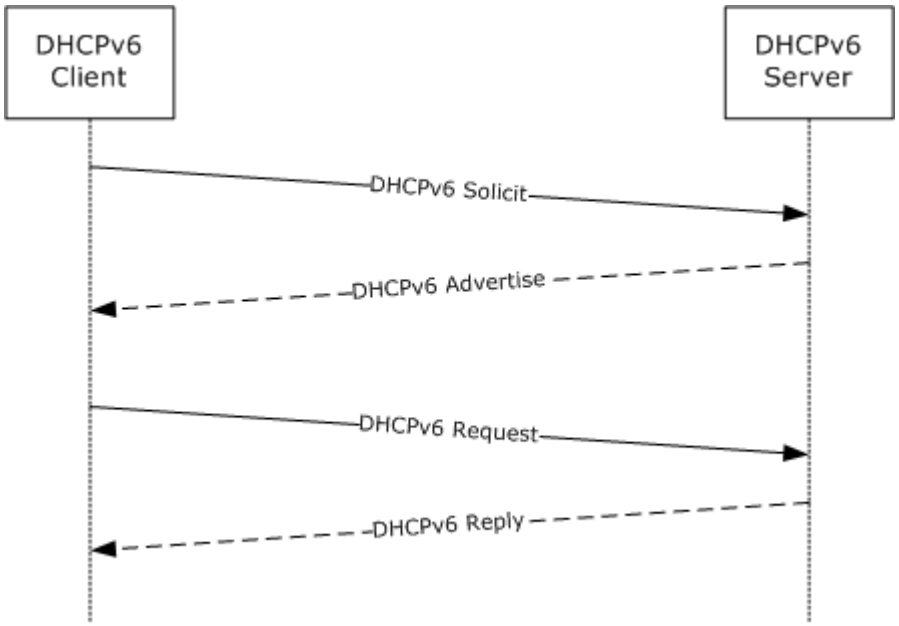


Figure 2: Basic DHCPv6 process

The DHCPv6 client may choose to decline an offer from a DHCP server if it finds that the IPv6 address included in the DHCPv6 Advertise message sent by the server is already in use on that network. If so, the DHCPv6 client sends a DHCPv6 Decline message and restarts the configuration process by sending a DHCPv6 Solicit message again.

The DHCPv6 server may send a DHCPv6 Reply message with a Status Code option with a value other than Success in response to the client's DHCPv6 Request message if one or more of the desired configuration options sent by the client in that message are unacceptable. In this case, the DHCPv6 client restarts the configuration process by sending a DHCPv6 Solicit message again.

The DHCPv6 client may choose to relinquish its lease on the IP address by sending a DHCPv6 Release message to the server.

In some cases, the DHCPv6 client may remember and want to reuse an IP address that was previously allocated by the DHCPv6 server to it. In this case, the client may begin the initialization process by sending a DHCPv6 Renew or Rebind message to the server containing that network address as the "requested IP address". The DHCPv6 server sends a DHCPv6 Reply message with no Status Code option or with a Status Code option with the value of Success to the client if it chooses to allow the client to continue to use that IPv6 address. Otherwise, the DHCPv6 server may send a DHCP Reply message to the client with a value other than Success.

For further details on the DHCPv6 protocol overview, refer to Section 3 of [RFC2131].

1.4 Relationship to Other Protocols

DHCP (as specified in [RFC2131]) is based on the Bootstrap Protocol (BOOTP), as specified in [RFC951]. The format of the DHCP messages is based on the format of the BOOTP messages. The relationship between these two protocols is defined in [RFC1534].

The vendor-specific options specified in this document rely on and are transported within DHCP.

DHCP can be used as one of the enforcement mechanisms defined for Network Access Protection, as described in [MSDN-NAP]. The vendor-specific options used for DHCP-based enforcement of Network Access Protection are defined in [MS-DHCPN], section 1.

The NetBIOS over TCP/IP protocol is defined in [RFC1001] and [RFC1002]. These DHCP RFCs provide only the capability to disable the use of this protocol on client and server machines.

1.5 Prerequisites/Preconditions

None.

1.6 Applicability Statement

The use of these DHCP vendor-specific options are applicable in environments where DHCP is applicable.

1.7 Versioning and Capability Negotiation

The guidelines noted in section 8.4 of [RFC2132] to identify the vendor for the vendor-specific options are applicable to this specification.

The Vendor Class Identifier Option defined in [RFC2132] section 9.13 and the Vendor Class Option defined in [RFC3315] section 22.16 contain values used to negotiate which vendor-specific options defined herein are to be sent to the client.

1.8 Vendor-Extensible Fields

DHCP (as specified in [RFC2131]) and DHCPv6 (as specified in [RFC3315] have a provision for vendor-extensible options. These vendor-specific options are used as specified in [RFC2132] and [RFC3315]. The vendor-extensible fields described in this document comply with the provisions defined therein. The vendor-extensible options used by DHCP clients and servers are specified in section 2.2.1.

1.9 Standards Assignments

Parameter	Value	Reference
Private Enterprise Number	311	[IANA-ENT]

2 Messages

The following sections specify how messages are transported and details of message syntax, including common structures, certificate requirements, and common error codes.

2.1 Transport

All DHCP attributes are transported within DHCP, which is transported over the UDP protocol, as specified in [RFC2131] section 4.1 for DHCPv4 and [RFC3315] section 5.2 for DHCPv6.

Parameter	Value	Reference
DHCPv4 server listens for DHCPv4 messages on UDP port.	0x0043	[RFC2131]
DHCPv4 client listens for DHCPv4 messages on UDP port.	0x0044	[RFC2131]
DHCPv6 server listens for DHCPv6 messages on UDP port.	0x0223	[RFC3315] section 5.2
DHCPv6 clients listen for DHCPv6 messages on UDP port.	0x0222	[RFC3315] section 5.2

2.2 Message Syntax

These DHCP extensions use the message format for vendor-specific options, as specified in [RFC2132] section 8.4 and in [RFC3925] section 3.

All option fields and values described in this document are sent in network-byte order unless indicated otherwise.

2.2.1 DHCP Option Code 43 (0x2B) - Vendor-Specific Information Option

DHCP clients request vendor-specific options from the DHCP server by including option code 43 in the Parameter Request List, as specified in [RFC2132] section 8.4.

DHCP clients implementing this specification MUST also include a vendor-class identifier as described in section 2.2.2 in the DHCP message.

When a DHCP message includes a Vendor Class Identifier with one of the values defined in section 2.2.2, the Vendor-Specific Information Option is defined to use the "Encapsulated vendor-specific options" format specified in [RFC2132] section 8.4. This specification defines the following encapsulated vendor-specific option codes:

Value	Meaning
0x01	Microsoft Disable NetBIOS Option (section 2.2.1.1)
0x02	Microsoft Release DHCP Lease on Shutdown Option (section 2.2.1.2)
0x03	Microsoft Default Router Metric Base Option (section 2.2.1.3)

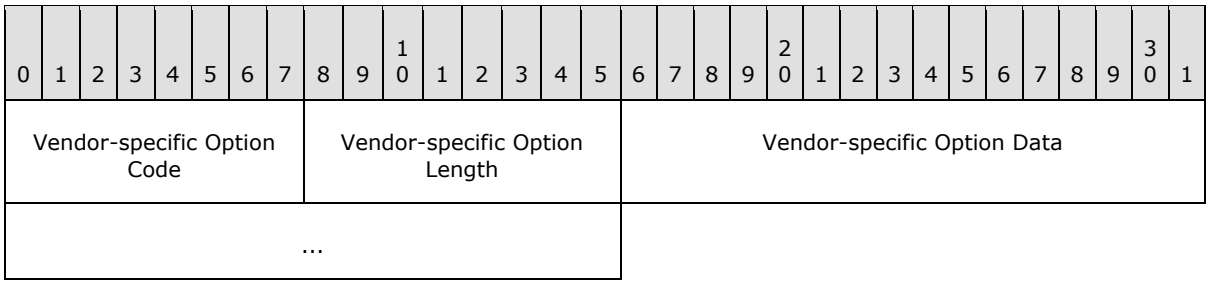
In addition, DHCP clients that support **Network Access Protection (NAP)** also use DHCP vendor-specific options for exchanging NAP-specific information. For an overview of NAP and for more information, see [MS-DHCPN] and [MS-SOH]. These vendor-specific options are also sent as encapsulated vendor-specific options and are defined in [MS-DHCPN], section 2.2.1.

For information about the format of DHCP Vendor Extensions, see [RFC2132] section 2.

2.2.1.1 Vendor-Specific Option Code 0x01 - Microsoft Disable NetBIOS Option

This option is sent by a DHCP server to a DHCP client in a DHCPOFFER or a DHCPACK message.<1> It has no effect on subsequent options in that message or on the DHCPREQUEST message sent by the client to the server.

This option can be used to enable or disable the use of NetBIOS over TCP/IP on the network interface for which the DHCP message was received. DHCP clients SHOULD support this option.<2> If the use of NetBIOS over TCP/IP is disabled on the interface, no NetBIOS over TCP/IP packets can be sent from or received on that interface. If any NetBIOS over TCP/IP packets are sent to the client on that interface, they are silently discarded. This option has no effect on NetBIOS over NetBEUI.



Vendor-specific Option Code (1 byte): This MUST be 0x01.

Vendor-specific Option Length (1 byte): This MUST be 0x04.

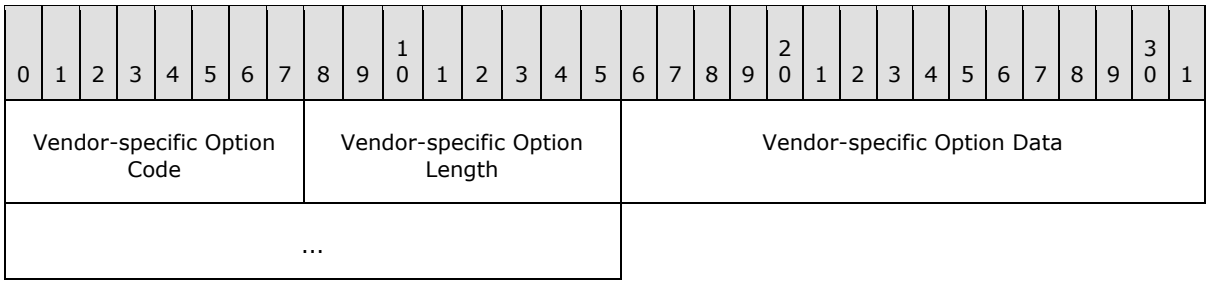
Vendor-specific Option Data (4 bytes): See below for values.

Value	Meaning
0x00000000	Enables NetBIOS over TCP/IP (Default Value) for that network interface.
0x00000001	Ignored (existing behavior unchanged).
0x00000002	Disables NetBIOS over TCP/IP for that network interface.
0x00000003 — 0xFFFFFFFF	Ignored (existing behavior unchanged).

2.2.1.2 Vendor-Specific Option Code 0x02 - Microsoft Release DHCP Lease on Shutdown Option

This option is sent by a DHCP server to a DHCP client in a DHCPOFFER or a DHCPACK message. It has no effect on subsequent options in that message or on the DHCPREQUEST message sent by the client to the server.

This option is used in DHCP messages by the DHCP server for directing the clients to send a DHCPRELEASE on that network interface when the operating system on the client is shutting down. DHCP clients SHOULD<3> support this option.



Vendor-specific Option Code (1 byte): This MUST be 0x02.

Vendor-specific Option Length (1 byte): This MUST be 0x04.

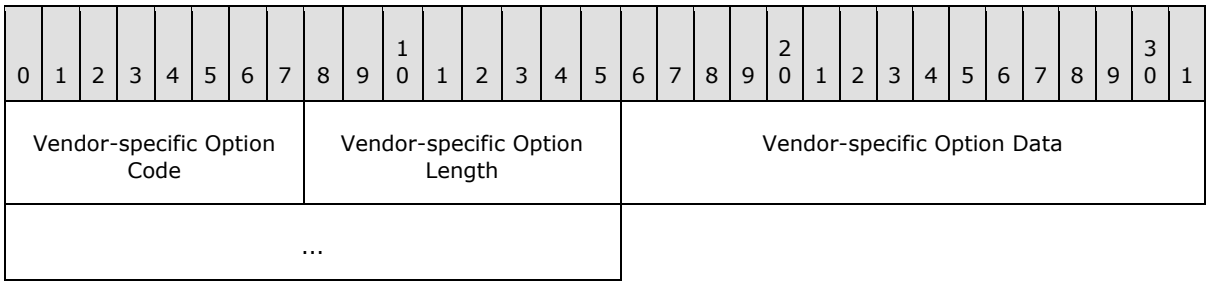
Vendor-specific Option Data (4 bytes): Values are as follows.

Value	Meaning
0x00000000	Existing behavior of client is unchanged.
0x00000001	Enables client behavior of sending DHCPRELEASE message on operating system shutdown.
0x00000002 — 0xFFFFFFFF	Existing behavior of client is unchanged.

2.2.1.3 Vendor-Specific Option Code 0x03 - Microsoft Default Router Metric Base Option

This option is sent by the DHCP server to the DHCP client in a DHCPOFFER or a DHCPACK message. It has no effect on subsequent options in that message or on the DHCPREQUEST message sent by the client to the server.

This option is used to set the default route metric (as specified in [RFC1812] section 5.2.4.3) for all automatically computed network routes for the network interface on which the DHCP message was received. DHCP clients SHOULD<4> support this option.



Vendor-specific Option Code (1 byte): This MUST be 0x03.

Vendor-specific Option Length (1 byte): This MUST be 0x04.

Vendor-specific Option Data (4 bytes): If zero, clients are to compute a route metric based on link speed. Otherwise this value overrides the automatically calculated metric for the default route for that network interface.

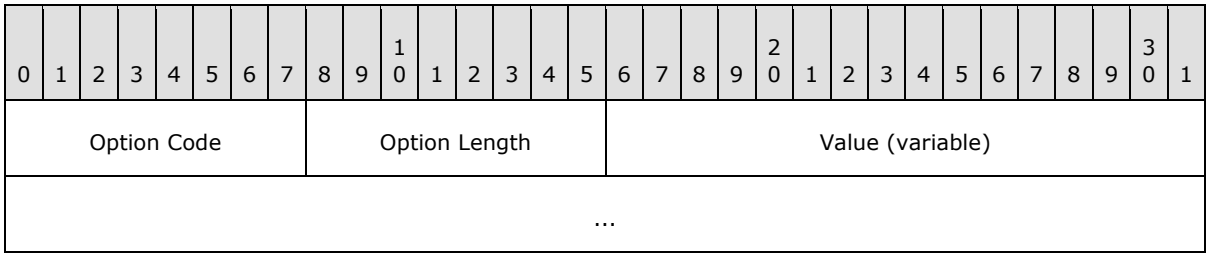
The automatically calculated metric for the default route for DHCP client computers SHOULD be one of the following values:<5>

Value	Meaning
0x0000000A	Greater than 200 Mbps.
0x00000014	Greater than 80 Mbps, and less than or equal to 200 Mbps.
0x00000019	Greater than 20 Mbps, and less than or equal to 80 Mbps.
0x0000001E	Greater than 4 Mbps, and less than or equal to 20 Mbps.
0x00000028	Greater than 500 Kbps, and less than or equal to 4 Mbps.
0x00000032	Less than or equal to 500 Kbps.

2.2.2 DHCP Option Code 60 (0x3C) - Vendor Class Identifier Option

A DHCP client sends vendor information in all DHCP packets that it sends to the DHCP server to indicate the vendor or the version of the operating system running on the client. This information is sent in the form of a vendor-class identifier option, as specified in [RFC2132] section 9.13.

The DHCP servers implementing this specification use the information contained in this option to determine whether a client implements this specification and whether the options defined in this specification should be sent to it. For semantics on the usage of vendor class identifiers, refer to [RFC2132] sections 8.4 and 9.13.



Option Code (1 byte): This MUST be 60 (0x3C) (as specified in [RFC2132] section 9.13) to indicate the Vendor Class Identifier Option.

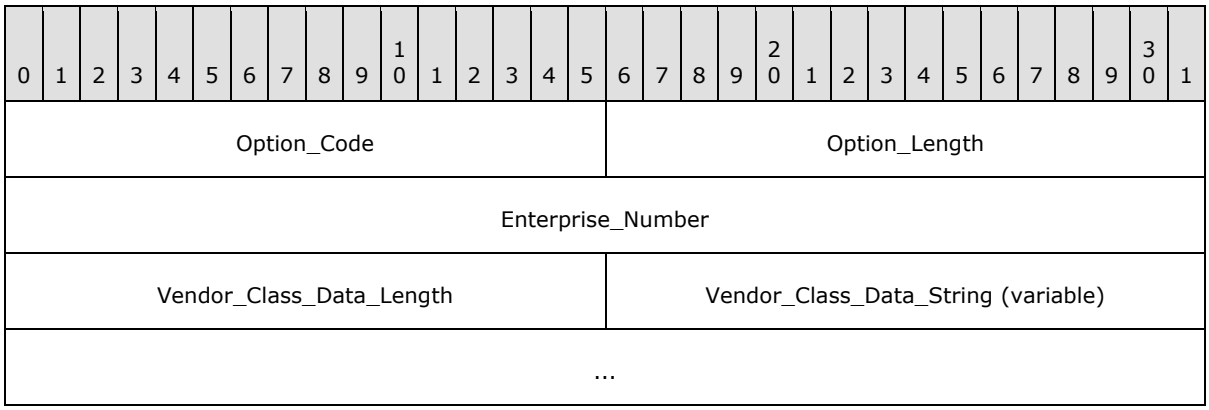
Option Length (1 byte): The length in bytes of the **Value** field.

Value (variable): This MUST be set to one of the following values, where the value shown is encoded as a non-NULL-terminated ASCII string.

Value	Meaning
"MSFT 98"	The client implements this specification but does not understand any encapsulated vendor-specific options.
"MSFT 5.0"	The client implements this specification and understands all encapsulated vendor-specific options defined herein.

2.2.3 DHCPv6 Option Code 16 (0x0010) - Vendor Class Option

A DHCP client sends vendor information in all DHCPv6 packets to the DHCPv6 server This information is sent in the form of a vendor class option, as specified in [RFC3315] section 22.16. An implementation that supports DHCPv6 MUST support this option.<6>



Option_Code (2 bytes): As specified in [RFC3315] section 22, this is used to indicate the Vendor Class option and MUST be 0x0010.

Option_Length (2 bytes): MUST be set to 0x000E (4 + 2 + the size of the **Vendor_Class_Data_String**).

Enterprise_Number (4 bytes): MUST be set to 0x00000137 (decimal 311), the IANA-assigned Microsoft Enterprise number [IANA-ENT].

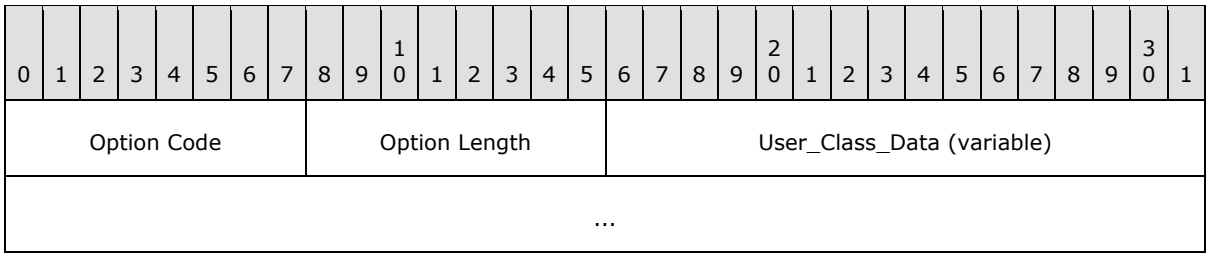
Vendor_Class_Data_Length (2 bytes): The length of the Vendor Class Data String field MUST be set to 0x0008.

Vendor_Class_Data_String (variable): MUST be set to "MSFT 5.0".

2.2.4 DHCP Option Code 77 (0x4D) - User Class Option

This section describes the User Class Option and the values for this option that are predefined on DHCP servers that implement this specification. The format of this option varies from the implementation described in [RFC3004] in that the User Class Data field format is changed and only one User Class value is supported. The use of this alternate format is indicated by the presence of a Vendor Class Identifier Option (section 2.2.2), which can occur anywhere in the same message.

Clients MAY send a User Class Option with values selected by the administrator or as explained in the User Class Data tables below in all DHCP messages sent by the client. For semantics of the usage of DHCP user classes, refer to [RFC3004] section 4.



Option Code (1 byte): MUST be 77 (0x4D) to indicate the User Class Option for DHCP.

Option Length (1 byte): Length in octets of the User Class Data field.

User_Class_Data (variable): The following User Class names SHOULD be used by clients and servers implementing this specification.

Value	Meaning
"BOOTP"	This value MUST be used if the DHCP client is sending a User Class Option in a BOOTP message [RFC1534]. This string is otherwise known as the Default BOOTP Class.
"RRAS.Microsoft"	This value MUST be used if the DHCP client is sending a User Class Option in a message on a dial-up or VPN network interface. This string is otherwise known as the Default Routing and Remote Access Class.
"NAP"	This value is reserved. It MUST NOT be sent by DHCP clients implementing this specification. This string is otherwise known as the Default Network Access Protection Class.

2.2.5 DHCP Option Code 249 (0xF9) - Microsoft Classless Static Route Option

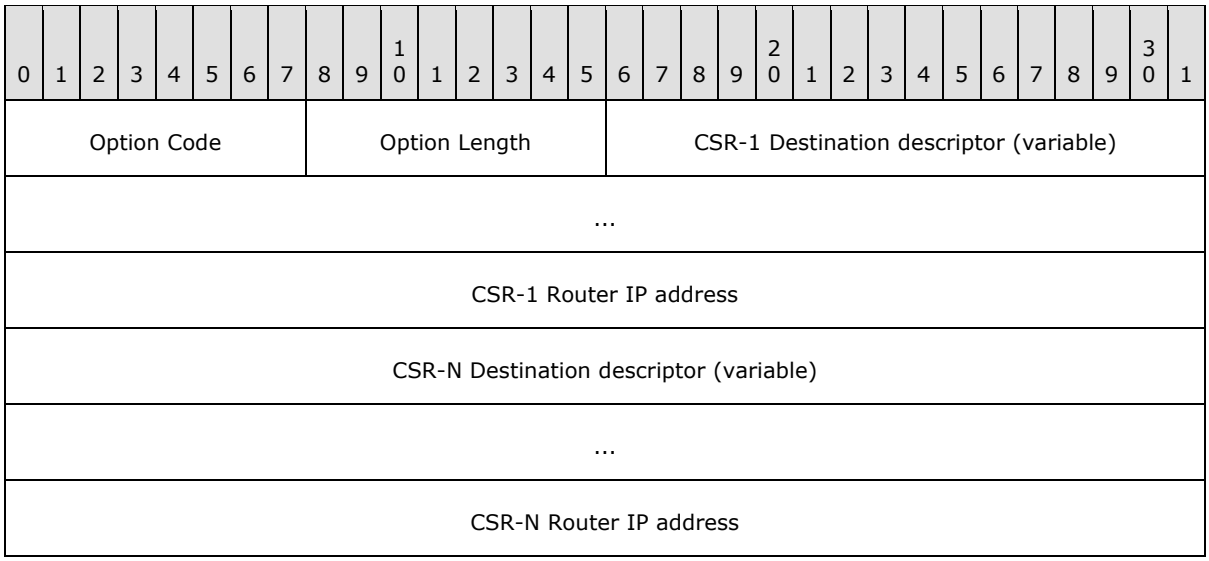
DHCP clients and servers that implement this specification use some non-standard options in their implementation.

The option-length and the option-data format for the Microsoft **Classless Static Route** option is exactly the same as that specified for the Classless Static Route option in [RFC3442]; the only difference is that Option Code 249 MAY<7> be used instead of or in addition to Option Code 121.

Multiple routes can be sent using the option. Each classless route consists of the Destination descriptor and Router IP address elements. The number of routes included in the option can be determined by processing the option data.

Note that the router IP address is of length 4 bytes while the destination descriptor length is between 1 byte and 5 bytes, depending on the subnet mask. This is described in detail below.

This option is sent by the DHCP server to the DHCP client in the DHCPOFFER or the DHCPACK message. It has no effect on subsequent options in that message or any of the messages sent by the client to the server.



Option Code (1 byte): This MUST be 249 (0xF9).

Option Length (1 byte): Value is variable, depending on the number of classless routes being sent, with a maximum of 255 bytes. This is determined as the sum of the length of the subnet mask, the destination descriptor, and the router IP address of all of the classless routes being sent through the option.

In the value portion for Option 249, each route is encoded as comprising three elements: subnet mask, destination descriptor, and router address. The encoding of the option is same as that specified in [RFC3442] for the CSR option.

CSR-1 Destination descriptor (variable): This is determined in exactly the same way described on the destination descriptor specified on page 4 of [RFC3442].

CSR-1 Router IP address (4 bytes): The IPv4 address of the next-hop router that can be used to reach the destination.

CSR-N Destination descriptor (variable): This is determined in exactly the same way as the destination descriptor specified on Page 4 of [RFC3442].

CSR-N Router IP address (4 bytes): The IPv4 address of the next-hop router that can be used to reach the destination.

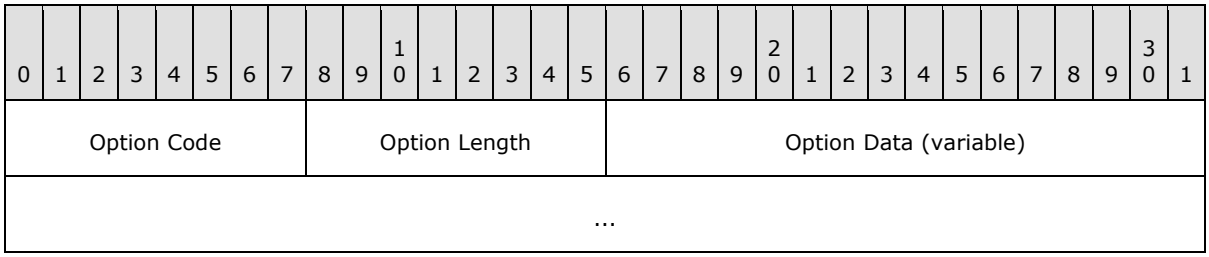
2.2.6 DHCP Option Code 250 (0xFA) - Microsoft Encoding Long Options Packet

The DHCP standard options are constrained to be of size 255 bytes due to the length of the 8-bit option length field that the protocol defines.

In the case where the option data for any of the DHCP option values exceeds 255 bytes in length, implementations of this specification do not follow [RFC3396] section 5. Instead, Option Code 250 is used to encode the excess data over 255 bytes. Option Code 250 repeats immediately after the option being encoded as many times as necessary to encode the remaining data.

For instance, if the Option Data for a given Option Code X is 600 bytes, the DHCP client or DHCP server sends Option X with 255 bytes of data, immediately followed by Option 250 with another 255 bytes of data, and then again Option 250 with the remaining 90 (=600-255-255) bytes of data.

Option 250 is encoded by DHCP clients and servers in the same format as the following standard DHCP options.



Option Code (1 byte): This MUST be 250 (0xFA).

Option Length (1 byte): The value is variable, depending on the size of the data in the long option being encoded, with a maximum of 255.

Option Data (variable): This field contains the continuation of the data of the previous option, which was too long to be contained in that option.

3 Protocol Details

The following sections specify protocol details including common details, abstract data model, timers, initialization, higher-layer triggered events, and message processing rules.

3.1 Client Details

3.1.1 Abstract Data Model

These DHCP Extensions comply with the data store (as defined in [RFC2131] section 2.1). The state machine and data model for DHCP are defined in [RFC2131] section 4.4. The data model for DHCPv6 is similar and is defined by [RFC3315].

In addition, DHCP clients also maintain the following state per network interface:

Release DHCP Lease on Shutdown Flag: This flag indicates whether the client will send a DHCPRELEASE when it shuts down.

Enable NetBIOS Flag: This flag indicates whether the host has NetBIOS enabled or disabled on the interface.

3.1.2 Timers

None beyond those in [RFC2131] and [RFC3315].

The DHCP client MUST follow an exponential backoff model for DHCPDISCOVER retransmission, as recommended in section 4.1 of [RFC2131]. However, [RFC2131] does not specify the actual values, so they are specified here. After a Media Sense event, the DHCP client MUST wait successively for 4, 8, 16, and 32 seconds for the server to respond, as its exponential backoff model values. If there is no response received to the 4th DHCPDISCOVER, the DHCP client MUST wait for five minutes before repeating the above cycle.

Note that the above means that DHCP clients implementing this specification do not follow section 17.1.2 of [RFC3315]. The retransmission behavior for DHCPv6 Solicit messages follows the same behavior as that described above for DHCPDISCOVER messages in DHCPv4.

3.1.3 Initialization

DHCP client initialization (as specified in [RFC2131]and [RFC3315]) is unchanged by DHCP extensions specified in this document.

3.1.4 Higher-Layer Triggered Events

There are no higher-layer triggered events that are specific to DHCP extensions described in this specification.

3.1.4.1 Sending a DHCPDISCOVER, Renew, or DHCPINFORM message

When sending a DHCPDISCOVER, Renew, or DHCPINFORM message, DHCP clients implementing this specification MUST include a Vendor Class Identifiers Option formatted as in section 2.2.2 and MAY<8> include a User Class Option formatted as in section 2.2.5. Since this specification supports only one user class value in this packet, the client MUST conform to the guidelines for the user class data defined in section 2.2.5.

3.1.4.2 Sending a DHCPv6 Solicit, Request, or Information-Request message

When sending a DHCPv6 Solicit, Request, or Information-Request message, DHCPv6 clients implementing this specification MUST include a Vendor Class Option formatted as in section 2.2.4.

3.1.4.3 Sending BOOTP messages

DHCP clients implementing this specification MUST send BOOTP messages if and only if DHCP is being used in a Preboot Execution Environment (see [INTEL-PXE]). Also, BOOTP messages MUST NOT be sent over dial-up or VPN network interfaces. Also, DHCP clients MUST NOT send the Default_Network_Access_Protection_Class in the User Class Option on dial-up or VPN interfaces.

3.1.5 Message Processing Events and Sequencing Rules

DHCP clients process DHCP messages as specified in [RFC2131] sections 3 and 4, with additional behavior as specified in this section.

If the length or the data of the field of any of the options in a DHCP message received by clients implementing this specification are inconsistent, the DHCP client MUST silently discard the DHCP message, and restart the initialization process.

3.1.5.1 Receiving a DHCPOFFER

If the DHCPOFFER contains any of the options defined in this specification, these options SHOULD be ignored; the client MAY instead use the options to choose among offers in any implementation-specific manner.

When sending a DHCPREQUEST in response, the client MUST include a Vendor Class Identifier Option formatted as in section 2.2.2, and MAY<9> include a User Class Option formatted as in section 2.2.4. Since this specification supports only one user class value in this packet, the client MUST conform to the guidelines for the user class data defined in section 2.2.4. The client SHOULD<10> include both options 121 and 249 in the parameter request list in this message.

3.1.5.2 Receiving a DHCPACK

When a DHCP client implementing this specification receives a DHCPACK that contains a Vendor-Specific Information Option, it MUST be processed as follows.

If it contains a Microsoft Disable NetBIOS Option, the DHCP client MUST update its NetBIOS Enabled Flag for the interface over which the DHCPACK was received, as indicated in section 2.2.1.1.

If it contains a Microsoft Release DHCP Lease on Shutdown Option, the DHCP client MUST update its Release DHCP Lease on Shutdown Flag for the interface over which the DHCPACK was received, as indicated in section 2.2.1.2.

If it contains a Microsoft Router Base Metric Option, the value for this option from the DHCPACK message MUST be applied by the client for the default routes on that interface.

If it contains a Microsoft Classless Static Route Option, the client MUST first check whether the option conforms to the syntax specified in section 2.2.5. If any of the parameters in this DHCP option are invalid or incomplete, the DHCP client MUST silently discard the complete DHCP message and start the initialization process again. Otherwise, the specified routes MUST be inserted into the routing table in the TCP/IP stack.

3.1.6 Timer Events

The DHCP Extensions adhere to the RFC standards (as specified in [RFC2131] section 4.4 and in [RFC2132]) for Timer Events.

3.1.7 Other Local Events

On System Shutdown, if its Release DHCP Lease on Shutdown Flag is set, the DHCP client MUST send a DHCPRELEASE message for all IP addresses obtained through DHCP.

3.2 Server Details

3.2.1 Abstract Data Model

These DHCP Extensions comply with the data store (as defined in [RFC2131] section 2.1). The state machine and data model for DHCP are defined in [RFC2131] section 4.4. The data model for DHCPv6 is similar and is defined by [RFC3315]. The extensions defined in this specification do not require any change to the state machine or the data model of DHCP.

3.2.2 Timers

None beyond those in [RFC2131] and [RFC3315].

3.2.3 Initialization

DHCP server initialization (as specified in [RFC2131] and [RFC3315]) is unchanged by DHCP extensions specified in this document.

3.2.4 Higher-Layer Triggered Events

None.

3.2.5 Message Processing Events and Sequencing Rules

DHCP servers process DHCP messages as specified in [RFC2131] sections 3 and 4, with additional behavior as specified in this section.

3.2.5.1 Receiving a DHCPDISCOVER message

If the DHCPDISCOVER contains a Vendor Class Identifier Option (section 2.2.2) with a value defined in section 2.2.2, the DHCP server SHOULD ignore the Vendor Class Identifier Option and process the message as if the option were not present. The server MAY instead include any standard option or vendor-specific option defined in this specification in its response (if configured to do so by the administrator) in the DHCPOFFER message sent to the clients.

3.2.5.2 Receiving a DHCPREQUEST message

If the DHCPREQUEST contains a Vendor Class Identifier Option (section 2.2.2) with a value defined in section 2.2.2, the DHCP server MUST include the vendor-specific options defined in section 2.2.1.1 (if configured to do so by the administrator) in the DHCPACK message sent to the clients. In this case, the DHCP server MUST interpret the User Class Option if it exists<11> in the DHCPREQUEST message to contain a single value as defined in section 2.2.4.

When the DHCP server receives a request for Option 249, but not for Option 121 in the Parameter Request List, the Classless Static Route information MUST be returned to the DHCP client in Option 249. If the Parameter Request List contains a request for both Options 121 and 249, then the Classless Static Route information SHOULD<12> be returned to the DHCP client in Option 121 only.

The DHCP server MUST format any option values that are longer than 255 bytes as defined in section 2.2.6.

The remainder of the DHCPREQUEST message MUST be processed as specified by [RFC2131] and [RFC2132].

3.2.5.3 Receiving a DHCPv6 Message with a Vendor Class Option

DHCP servers implementing this specification MAY<13> simply ignore the Vendor Class Option sent in the DHCPv6 messages by the client; the server SHOULD instead return the relevant options configured for clients with the specified vendor class information as specified by [RFC3315].

3.2.5.4 Receiving a DHCP Message with a User Class Option

If the option length or any of the values in the option are inconsistent with the data sent, DHCP servers implementing this specification MUST silently discard the DHCP message from the client.

3.2.6 Timer Events

The DHCP Extensions adhere to the RFC standards (as specified in [RFC2131] section 4.4 and in [RFC2132]) for Timer Events.

3.2.7 Other Local Events

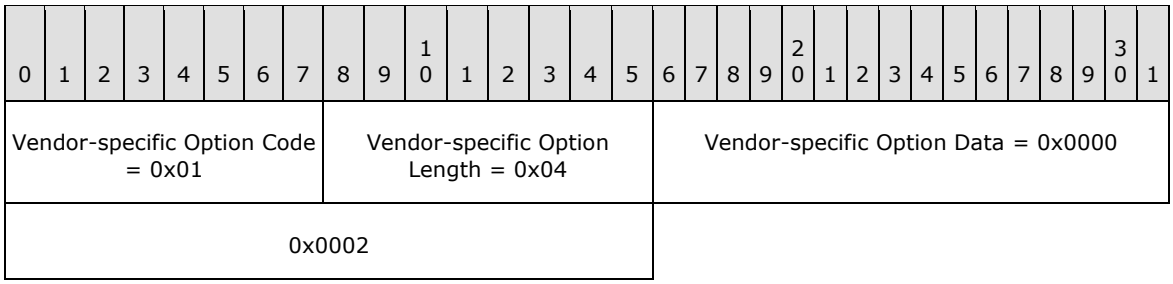
None.

4 Protocol Examples

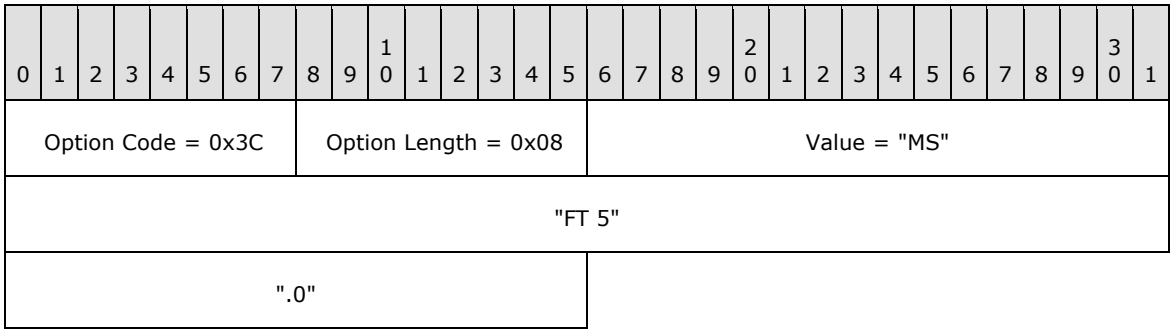
The message exchanges described for DHCP are specified in [RFC2131] section 3. Message exchanges for DHCPv6 are specified in [RFC3315]. The message sequences and the operation of DHCP (as specified in [RFC2131] section 4.1) and DHCPv6 (as specified in [RFC3315]) are unchanged by DHCP Extensions.

In this example, an administrator wants to disable clients from using NetBIOS-over-TCP/IP on the local network.

1. The administrator configures the DHCP server to send vendor-specific option number 1 with option value as 2, as specified in section 2.2.1.1, to the clients.



2. The client joins the network and sends a DHCPDISCOVER message including a Vendor Class Identifier Option. For instance, say the client sends the vendor-class as "MSFT 5.0".



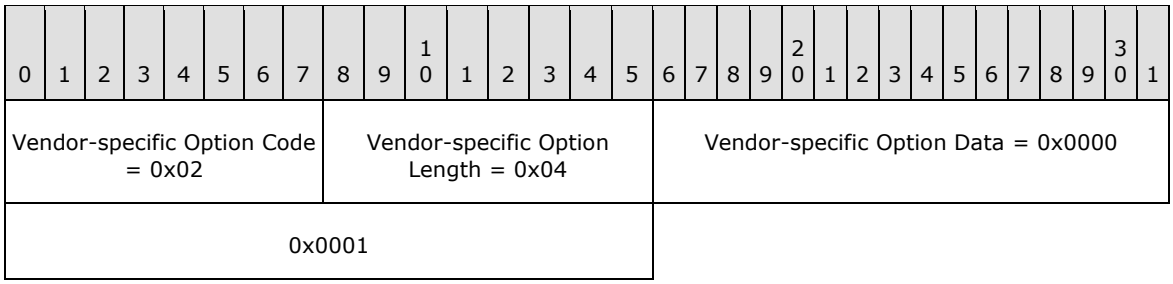
3. The server ignores the Vendor Class Identifier Option and responds with a DHCPOFFER. It does not include any option defined in this specification in the DHCPOFFER. The client accepts the offer by sending a DHCREQUEST message again including the Vendor Class Identifier Option as before.

4. The DHCP server recognizes the value in the Vendor Class Identifier Option in the DHCP message from the client, and sends a DHCPACK message that includes vendor-specific option number 1 as shown above.

5. The client will receive this vendor-specific option from the DHCP server and disable the use of NetBIOS-over-TCP/IP.

Another example is when an administrator wants clients on the local network to release the DHCP address lease when the machine is shut down.

1. The administrator can configure the DHCP server to send vendor-specific option number 2 with value 1, as described in section 2.2.1.2, to the clients.



2. The client joins the network and sends a DHCPDISCOVER messsage including a Vendor Class Identifier Option. For instance, the client may send the vendor-class as "MSFT 5.0".

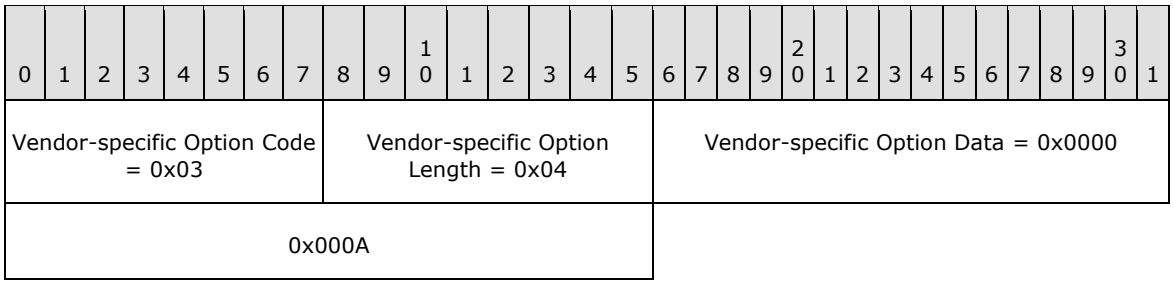
3. The server ignores the Vendor Class Identifier Option and responds with a DHCPOFFER. It does not include any option defined in this specification in the DHCPOFFER. The client accepts the offer by sending a DHCPREQUEST message again including a Vendor Class Identifier Option as before.

4. The DHCP server recognizes the value in the Vendor Class Identifiers Option in the DHCP message from the client, and sends a DHCPACK message that includes vendor-specific option number 2 as shown above.

5. The client will receive this vendor-specific option from the DHCP server will release its DHCP address lease when the machine is shut down.

Another example is when an administrator wants to change the router metric used by clients connecting to the local network.

1. The administrator configures the DHCP server to send vendor-specific option number 3 with the desired routing metric (say 10), as specified in section 2.2.1.3, to the clients.



2. The client joins the network and sends a DHCPDISCOVER message including a Vendor Class Identifier Option with value as, say, "MSFT 5.0".

3. The server ignores the Vendor Class Identifier Option and responds with a DHCPOFFER. It does not include any option defined in this specification in the DHCPOFFER. The client accepts the offer by sending a DHCPREQUEST message again including a Vendor Class Identifier Option as before.

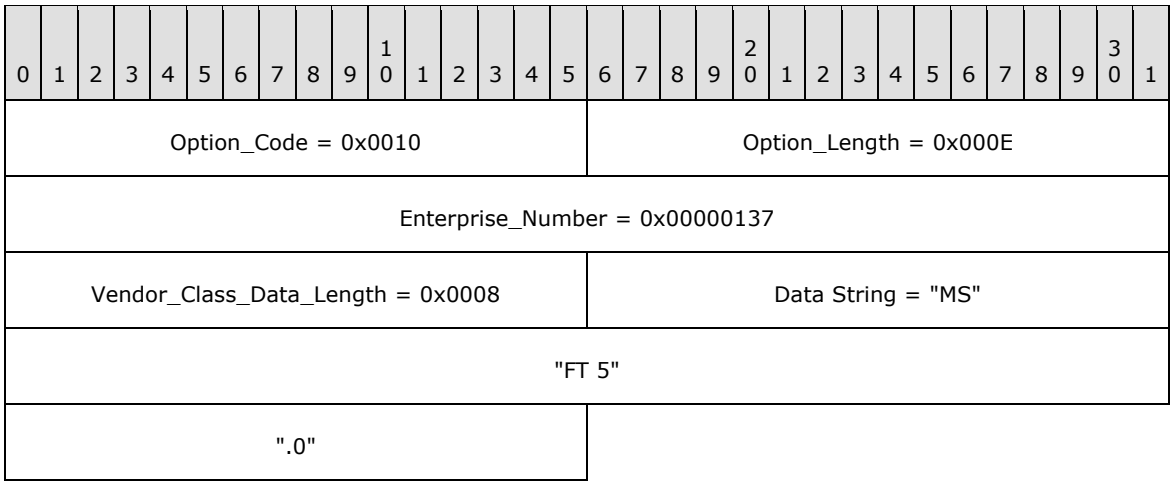
4. The DHCP server recognizes the Vendor Class Identifier Option in the DHCP message from the client, and sends a DHCPACK message that includes vendor-specific option number 3 as shown above.

5. The client will receive this vendor-specific option from the DHCP server and use the appropriate router-metric value (in this example 10) as specified by the DHCP server on that network interface.

If an administrator wants to send vendor-specific information to clients through DHCPv6 on the local network, this can be done based on the vendor class identifier:

1. The administrator configures the DHCPv6 server to send the desired information to clients if the vendor-class identifier received from the client is "MSFT 5.0" as described above.

2. The client joins the local network and sends a DHCPv6 Solicit message including a Vendor Class Option (section 2.2.3). For instance, the client sends the vendor-class data as "MSFT 5.0".



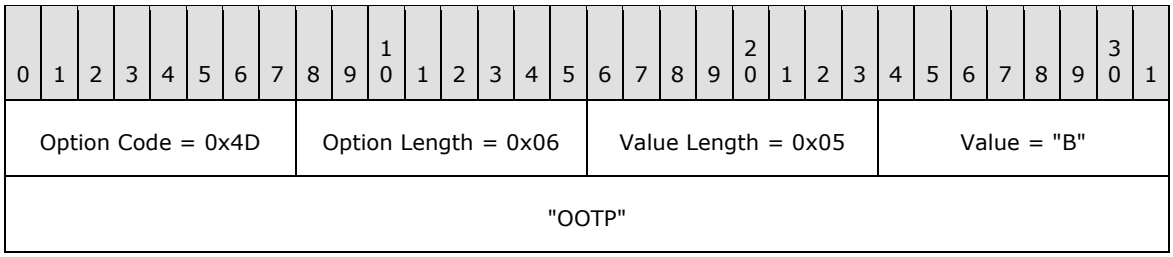
3. The server ignores the Vendor Class Option and responds with a DHCPv6 Advertise. The client accepts the offer by sending a DHCPv6 Request message, again including a Vendor Class Option as before.

4. The DHCPv6 server interprets the vendor-class identifier sent by the client in the DHCPv6 Request message, and sends the appropriate standard options to the client in the DHCPv6 Reply message. Depending on the server configuration, the option values selected by the server for inclusion in the Reply message may be based on the Vendor Class Option value sent by the client in the Request message.

5. The client receives and applies the option information sent by the server.

Another example is when an administrator wants to send specific information to clients on the local network when they send the DHCP message as a BOOTP message.

1. In this case, the administrator can configure the DHCP server to look for the User-Class option containing a User-Class sub-packet with the value "BOOTP" (as described in section 2.2.4) in the DHCP message sent by the client. If the message contains this user-class sub-packet, then the DHCP server is configured to respond with the desired information that the administrator wants to send to the client.



2. Clients that send a DHCP message as a BOOTP message (see [RFC1534] section 2) will include a User-Class option in the message containing the User-Class sub-packet with the value "BOOTP" as shown above. Thus, if the DHCP server is configured as explained above, the client will receive the desired information in the response from the server.

As an example of the use of the Microsoft Classless Static Route option, see the examples on pages 4 and 5 of [RFC3442], with the only difference being that the code used for this option is 249 instead of Code 121 used in [RFC3442].

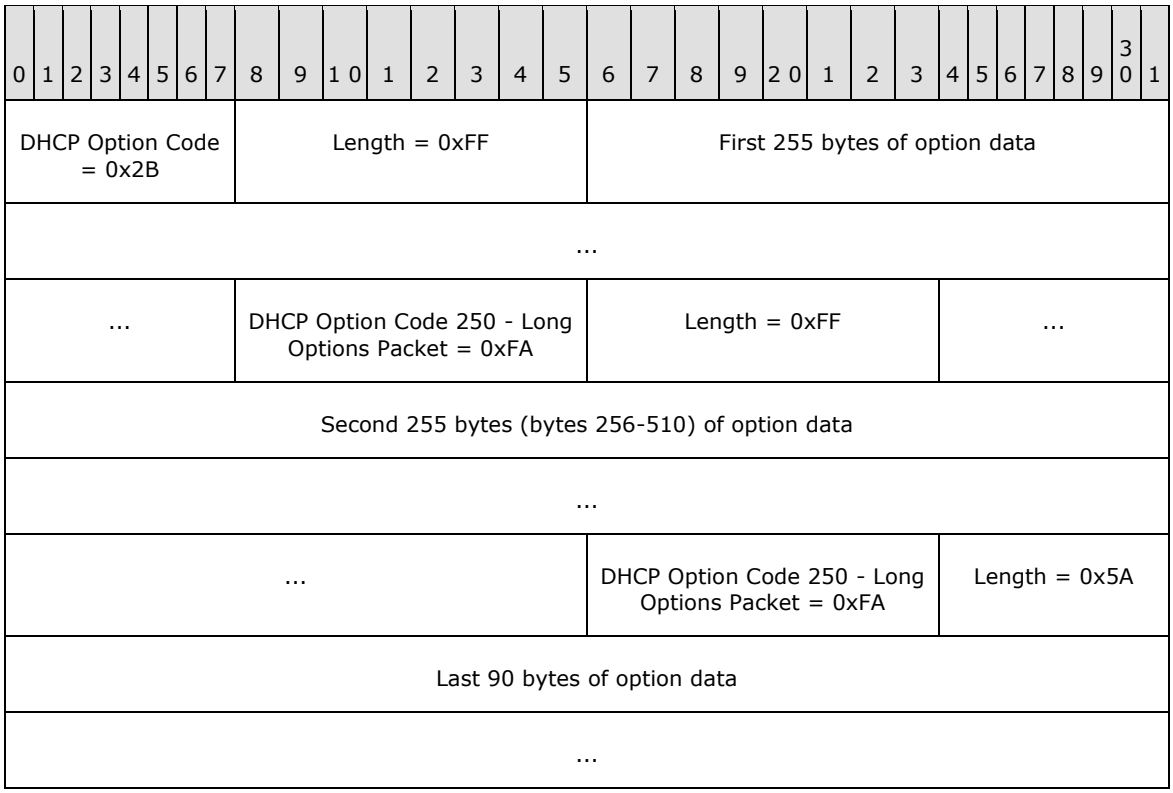
In another example, say an administrator wants to send vendor-specific information through DHCP to clients on the local network as DHCP Vendor Specific Information option 43 (0x2B). However, this information when encapsulated in option 43 as per [RFC2132] is of size 600 bytes, exceeding the 255 byte limit of a DHCP option length.

1. The administrator configures the DHCP server to send vendor-specific options to the client.

2. The client joins the network and sends a DHCPDISCOVER message including a Vendor Class Identifier Option with value as, say, “MSFT 5.0”.

3. 3. The server ignores the Vendor Class Identifier Option and responds with a DHCPOFFER. It does not include any option defined in this specification in the DHCPOFFER. The client accepts the offer by sending a DHCPREQUEST message again including the Vendor Class Identifier Option as before.

4. 4. The DHCP server recognizes the value in the Vendor Class Identifier Option in the DHCP message from the client, and sends a DHCPACK message that includes the Vendor Specific Information option with the desired value as configured by the administrator, while formatting it as described in section 2.2.6, by sending option 43 (0x2B) of size 255 bytes, followed by option 250 with the next 255 bytes, and then again option 250 with the remaining 90 bytes.



5. DHCP clients on the local network that initiate a DHCP transaction with the above server will thus receive the -configured vendor-specific information that exceeds 255 bytes. Similarly, standard option values that exceed 255 bytes can also be sent to clients by formatting it as described in section 2.2.6.

5 Security

The following section specifies security considerations for implementers of the DHCP Extensions.

5.1 Security Considerations for Implementers

All of the security considerations that are applicable to DHCP (as described in [RFC2131] section 7 and [RFC3315] section 23) apply to implementation of this specification.

5.2 Index of Security Parameters

None.

6 Appendix A: Windows Behavior

The information in this specification is applicable to the following versions of Windows:

- Windows 98
- Windows Me
- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008

Exceptions, if any, are noted below. Unless otherwise specified, any statement of optional behavior in this specification prescribed using the terms SHOULD or SHOULD NOT implies Windows behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that Windows does not follow the prescription.

<1> Section 2.2.1.1: Windows DHCP servers do not send this option in the DHCPOFFER message. If configured by the administrator, they send this option in the DHCPACK message only.

<2> Section 2.2.1.1: Windows 98 and Windows MeDHCP clients do not support this option.

<3> Section 2.2.1.2: Windows 98 and Windows MeDHCP clients do not support this option.

<4> Section 2.2.1.3: Windows 98 and Windows MeDHCP clients do not support this option.

<5> Section 2.2.1.3: By default (if not overridden by this option), the TCP/IP stack instead computes the route metric based on link speed as follows for Windows 98, Windows Me, Windows 2000, Windows XP, and Windows XP SP1 clients:

Link speed	Metric
Greater than 200 Mbps	0x0000000A (10)
Greater than 20 Mbps, and less than or equal to 200 Mbps	0x00000014 (20)
Greater than 4 Mbps, and less than or equal to 20 Mbps	0x0000001E (30)
Greater than 500 Kbps, and less than or equal to 4 Mbps	0x00000028 (40)
Less than or equal to 500 Kbps	0x00000032 (50)

<6> Section 2.2.3: DHCPv6 Client support is implemented in Windows Vista and Windows Server 2008. DHCPv6 server support is available only in Windows Server 2008.

<7> Section 2.2.5: All Windows DHCP clients and servers prior to Windows Vista and Windows Server 2008 use Option Code 249 for requesting and sending Classless Static Routes (CSRs) instead of Option Code 121, as specified in [RFC3442]. These clients and servers ignore Option 121 if included in a DHCP message.

Windows Vista and Windows Server 2008 DHCP clients use both Option 121 and Option 249.

<8> Section 3.1.4.1: By default, WindowsDHCP clients do not send the User Class Option in the DHCP messages. Users can configure any data string value to be sent as the user class value by the DHCP client to the server.

WindowsDHCP clients using BOOTP to boot from the network send the Default BOOTP class (as defined in section 2.2.4) as their user class.

<9> Section 3.1.5.1: By default, WindowsDHCP clients do not send the User Class Option in the DHCP messages. Users can configure any data string value to be sent as the user class value by the DHCP client to the server.

WindowsDHCP clients using BOOTP to boot from the network send the Default BOOTP class (as defined in section 2.2.4) as their user class.

<10> Section 3.1.5.1: All WindowsDHCP clients prior to Windows Vista only request option code 249 in the Parameter Request List. WindowsDHCP clients request both option code 121 and option code 249 in the Parameter Request List.

<11> Section 3.2.5.2: WindowsDHCP servers interpret all unrecognized User classes (including cases where the client sends a User Class Option of length zero or where the client does not send the User Class Option) to be the Default User class.

<12> Section 3.2.5.2: All WindowsDHCP servers prior to Windows Server 2008 send the classless static route information to clients in Option 249 even if the client requests both option code 121 and 249. Windows Server 2008 sends the classless static route information to clients in Option 121 if the client requests both option code 121 and option code 249 in the Parameter Request List.

<13> Section 3.2.5.3: WindowsDHCP servers ignore the Vendor Class Option.

7 Index

T

V

W