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

Release: Friday, February 4, 2011

Revision Summary

Date	Revision History	Revision Class	Comments
04/10/2007	1.0		Version 1.0 release
05/18/2007	1.2		Version 1.2 release
06/08/2007	1.2.1	Editorial	Edit pass.
07/10/2007	2.0	Major	Updated and revised the technical content.
08/17/2007	3.0	Major	Updated and revised the technical content.
09/21/2007	4.0	Major	Updated and revised the technical content.
10/26/2007	5.0	Major	Updated and revised the technical content.
01/25/2008	5.0.1	Editorial	Revised and edited the technical content.
03/14/2008	5.0.2	Editorial	Revised and edited the technical content.
06/20/2008	5.1	Minor	Updated the technical content.
07/25/2008	5.2	Minor	Updated the technical content.
08/29/2008	5.2.1	Editorial	Revised and edited the technical content.
10/24/2008	5.2.2	Editorial	Revised and edited the technical content.
12/05/2008	6.0	Major	Updated and revised the technical content.
01/16/2009	6.1	Minor	Updated the technical content.
02/27/2009	6.1.1	Editorial	Revised and edited the technical content.
04/10/2009	6.2	Minor	Updated the technical content.
05/22/2009	6.2.1	Editorial	Revised and edited the technical content.
07/02/2009	6.3	Minor	Updated the technical content.
08/14/2009	6.4	Minor	Updated the technical content.
09/25/2009	6.5	Minor	Updated the technical content.
11/06/2009	7.0	Major	Updated and revised the technical content.
12/18/2009	8.0	Major	Updated and revised the technical content.
01/29/2010	9.0	Major	Updated and revised the technical content.
03/12/2010	9.0.1	Editorial	Revised and edited the technical content.
04/23/2010	9.0.2	Editorial	Revised and edited the technical content.

Date	Revision History	Revision Class	Comments
06/04/2010	10.0	Major	Updated and revised the technical content.
07/16/2010	11.0	Major	Significantly changed the technical content.
08/27/2010	11.0	No change	No changes to the meaning, language, or formatting of the technical content.
10/08/2010	11.0	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	12.0	Major	Significantly changed the technical content.
01/07/2011	13.0	Major	Significantly changed the technical content.
02/11/2011	14.0	Major	Significantly changed the technical content.

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, nonstandard options for DHCP [MS-DHCPE], and a set of vendor-specific options, which can be used to authorize a **DHCP server**.

1.1 Glossary

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

Active Directory
Active Directory Domain Services (AD DS)
distinguished name (DN)
domain
Domain Name System (DNS)
Dynamic Host Configuration Protocol (DHCP) client
Dynamic Host Configuration Protocol (DHCP) server
Internet Protocol version 4 (IPv4)
Internet Protocol version 6 (IPv6)
Lightweight Directory Access Protocol (LDAP)
network byte order
original equipment manufacturer (OEM) code page
Transmission Control Protocol (TCP)

The following terms are specific to this document:

Administratively Authorized Server: A **DHCP server** that has been explicitly authorized by an **administrator**.

ADsPath: An LDAP string representation of **distinguished names**.

Authorized Server: A **DHCP server** that has been authorized either administratively or using **Rogue Detection**. Authorized servers respond to both DHCPv4 and DHCPv6 messages.

Classless Static Route: A DHCP option that provides a subnet mask for each entry so that the subnet mask can be other than what would be determined by using the algorithm specified in Internet Protocol STD 5 [RFC791] and Internet Standard Subnetting Procedure STD 5 [RFC950].

Rogue Authorized Server: A **DHCP server** that has been authorized using **Rogue Detection**.

Rogue Aware Server: A **DHCP server** that implements **Rogue Detection**.

Rogue Detection: A mechanism that can be used by a **DHCP server** to validate whether or not it is authorized to lease out addresses to **DHCP** clients.

Unauthorized Server: A **DHCP server** that is not authorized either administratively or using **Rogue Detection**. Unauthorized servers do not respond to either DHCPv4 or DHCPv6 messages.

Validating Server: A **Rogue Aware Server** that is attempting to validate its authorization using **Rogue Detection**.

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

[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", STD 5, 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., et al., "The User Class Option for DHCP", RFC 3004, June 2000, http://www.ietf.org/rfc/rfc3004.txt

[RFC3315] Droms, R., Bound, J., Volz, B., et al., "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

[RFC4702] Stapp, M., Volz, B., and Rekhter, Y., "The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option", RFC 4702, October 2006, http://www.ietf.org/rfc/rfc4702.txt

1.2.2 Informative References

[MS-ADA1] Microsoft Corporation, "Active Directory Schema Attributes A-L", June 2007.

[MS-ADSC] Microsoft Corporation, "Active Directory Schema Classes", July 2006.

[MS-ADTS] Microsoft Corporation, "Active Directory Technical Specification", July 2006.

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

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

[MS-SOH] Microsoft Corporation, "Statement of Health for Network Access Protection (NAP) Protocol Specification", July 2006.

[MSDN-NAP] Microsoft Corporation, "Network Access Protection", http://msdn.microsoft.com/en-us/library/aa369712(VS.85).aspx

[RFC1001] Network Working Group, "Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods", STD 19, 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", STD 19, RFC 1002, March 1987, http://www.ietf.org/rfc/rfc1002.txt

[RFC1035] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, 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

1.3 Overview

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 that 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 no specific standard options or vendor-specific options are defined for hosts running that operating system version, 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 **DHCPREQUEST** 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 server includes 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 preceding steps for other interfaces, if present, for which DHCP is enabled. (See the following figure.) After this is complete, the client can use all TCP/IP services and applications for normal network communications and connectivity to other IPv4 hosts.

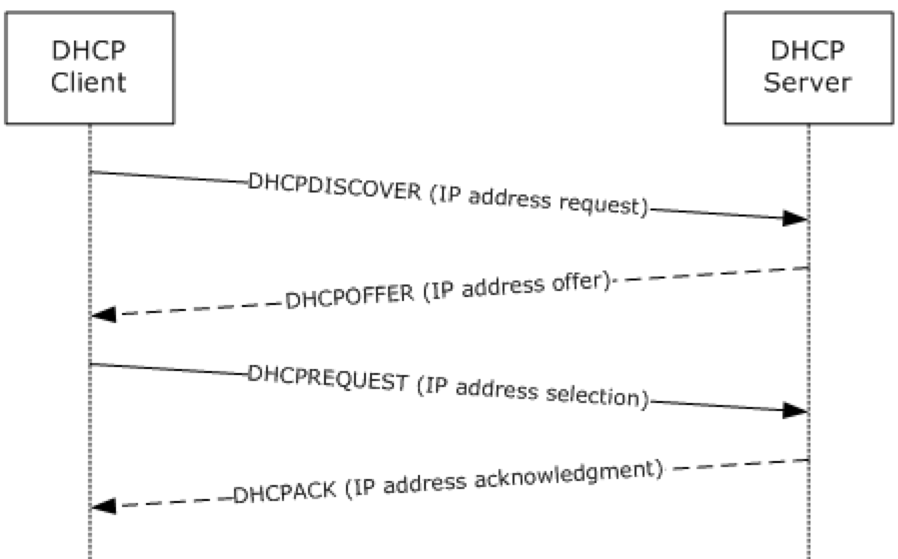

Figure 1: Basic DHCP process

The DHCP client may decline an offer from a DHCP server if it determines 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 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 requires. 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 no specific standard options or vendor-specific options are defined for hosts running that operating system version, 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 the **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 in the preceding steps. It then repeats the preceding steps for other interfaces, if present, for which DHCPv6 is enabled. (See the following figure.) After this is complete, the client can use all TCP/IP services and applications for normal network communications and connectivity to other IPv6 hosts.

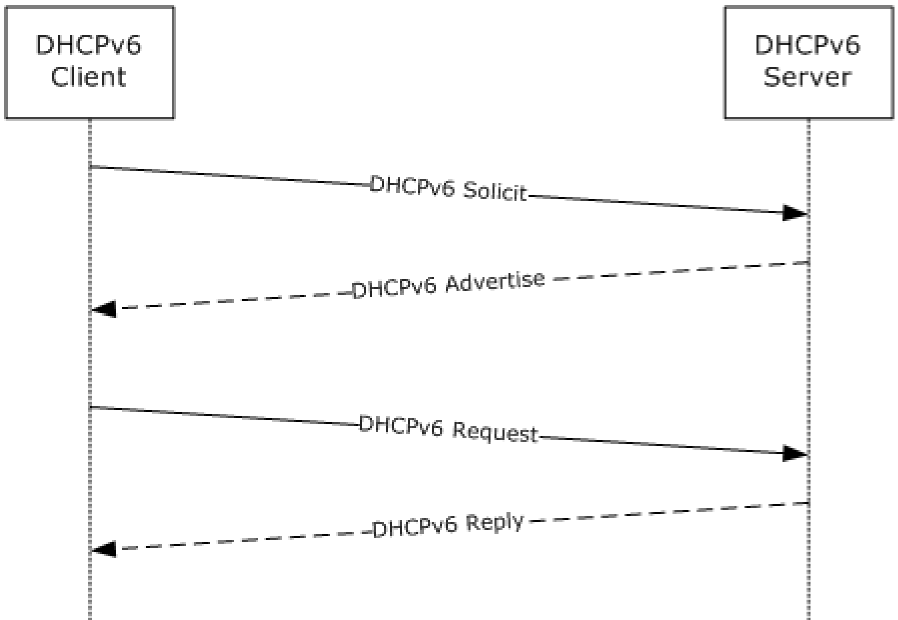

Figure 2: Basic DHCPv6 process

The DHCPv6 client may 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 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 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 of the DHCPv6 protocol overview, see section 3 of [RFC3315].

Accidental configuration of multiple DHCP servers on a network may cause misconfiguration of DHCP clients. DHCP servers can implement **Rogue Detection** to prevent such accidental configurations. A **Rogue Aware Server** periodically checks whether it is authorized.

Rogue Detection can be implemented using **DHCPINFORM** and/or DHCPv6 Information-Request messages. The following scenarios are valid for Rogue Detection:

Authorization of a DHCPv4 server using DHCPINFORM.

1. A **Validating Server** sends a broadcast **DHCPINFORM** message by sending a DHCPACK message containing the corresponding vendor-specific option with a NULL-terminated string in the option data.
2. A Rogue Aware **Administratively Authorized Server** replies to the **DHCPINFORM** message by sending a **DHCPACK** message with the corresponding vendor-specific option with a NULL-terminated string in the option data.
3. A **Rogue Authorized Server** on the network replies to the **DHCPINFORM** message by sending a **DHCPACK** message containing the corresponding vendor-specific option with a NULL-terminated string in the option data.
4. Any DHCP servers that are not Rogue Aware may reply to the **DHCPINFORM** message by sending a **DHCPACK** message, which does not contain the corresponding vendor-specific option.
5. A Rogue Aware **Unauthorized Server** on the network will not reply to the **DHCPINFORM** message.
6. If a Validating Server receives a **DHCPACK** message from an Administratively Authorized Server, it will consider itself unauthorized.
7. If a Validating Server does not receive a **DHCPACK** message from an Administratively Authorized Server within a stipulated time, it retries sending the **DHCPINFORM** message.
8. If a Validating Server receives a **DHCPACK** message from a Rogue Authorized Server, or a server which is not Rogue Aware, it retries sending the **DHCPINFORM** message.
9. The maximum number of retries is implementation specific. After all retry attempts are exhausted, the Validating Server may consider itself authorized or continue validation using the DHCPv6 Information-Request message.

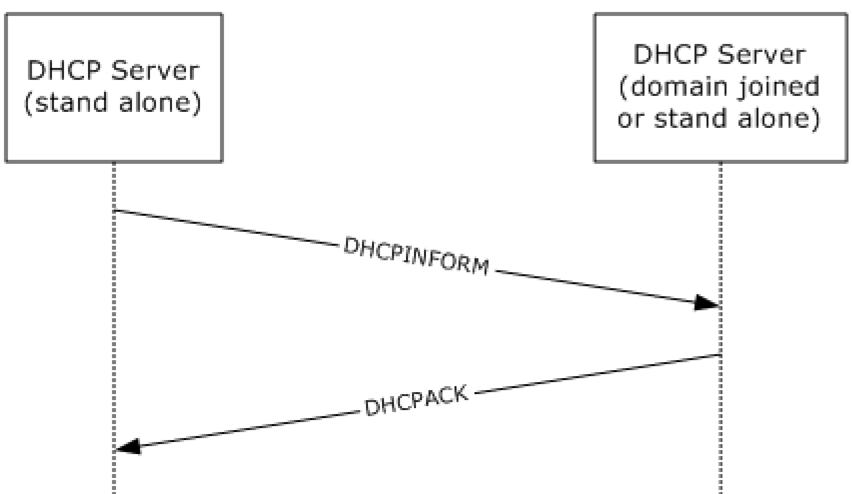

Figure 3: DHCPv4 Server Authorization messages

Authorization of a DHCP server using Information-Request.

1. A Validating Server sends a DHCPv6 Information-Request message containing a designated vendor specific option requesting other Rogue Aware Servers on the network to respond.
2. A Rogue Aware Administratively Authorized Server replies to the DHCPv6 Information-Request message by sending a DHCPv6 **Reply** message containing the corresponding vendor-specific option with a NULL-terminated string in the option data.
3. A Rogue Authorized Server on the network replies to the DHCPv6 Information-Request message by sending a DHCPv6 **Reply** message containing the corresponding vendor-specific option with a NULL-terminated string in the option data.
4. Any DHCP server that is not Rogue Aware may reply to the DHCPv6 Information-Request message by sending a DHCPv6 **Reply** message that does not contain the corresponding vendor-specific option.
5. A Rogue Aware Unauthorized Server on the network will not reply to the DHCPv6 Information-Request message.
6. If a Validating Server receives a DHCPv6 **Reply** message from an Administratively Authorized Server, it will consider itself unauthorized.
7. If a Validating Server does not receive a DHCPv6 **Reply** message from an Administratively Authorized Server within a stipulated time, it retries sending the DHCPv6 Information-Request message.
8. If a Validating Server receives a DHCPv6 **Reply** message from a Rogue Authorized Server, or a server which is not Rogue Aware, it retries sending the DHCPv6 Information-Request message.
9. The maximum number of retries is implementation-specific. After all retry attempts are exhausted, the Validating Server will consider itself authorized.

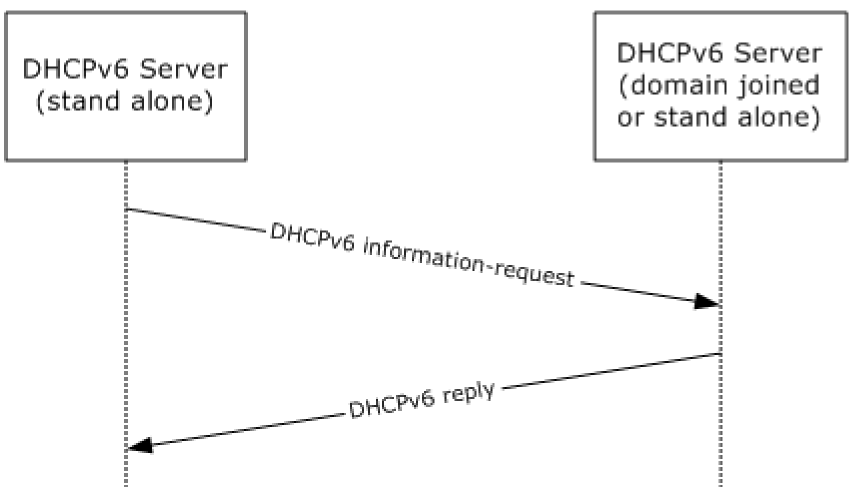

Figure 4: DHCPv6 Server Authorization messages

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 (NAP), as described in [MSDN-NAP]. The vendor-specific options used for DHCP-based enforcement of NAP are defined in [MS-DHCPN] section 1. [MS-DHCPN] affects the contents of DHCP messages when NAP is used.

The NetBIOS over TCP/IP protocol is defined in [RFC1001] and [RFC1002]. The vendor-specific option defined in this specification provides only the capability to disable the use of the NetBIOS over TCP/IP protocol on client and server machines.

1.5 Prerequisites/Preconditions

None.

1.6 Applicability Statement

The use of these DHCP vendor-specific options is applicable in environments where DHCP or DHCPv6 is used.

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 DHCP.

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 DHCPv6 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 2.2.2.

1.9 Standards Assignments

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

2 Messages

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

The following 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 12 (0xC) - Host Name Option

This option, as specified in [RFC2132] section 3.14, specifies the name of the client. As per [RFC2132] section 3.14, the name must follow character set restrictions as specified in [RFC1035]. [RFC1035] Section 2.3.1 gives a "preferred" name syntax that uses letters, digits, and hyphens, but does not state whether this is mandatory . In addition, [RFC1035] does not explain how to ASCII-encode a name if the client has a non-ASCII name, and hence the contents of this option are implementation-specific.<1> It was this ambiguity that led to it being rendered obsolete by DHCP Option Code 81 (section 2.2.7).

2.2.2 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 2.2.3 in the DHCP. A Validating Server MAY include a vendor-class identifier when authorizing itself using Rogue Detection.

When a DHCP message includes a Vendor Class Identifier with one of the values defined in section 2.2.3, 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 2.2.2.1)
0x02	Microsoft Release DHCP Lease on Shutdown Option (section 2.2.2.2)

Value	Meaning
0x03	Microsoft Default Router Metric Base Option (section 2.2.2.3)
0x5E	Rogue Detection Request Option (section 2.2.2.4)
0x5F	Rogue Detection Option (section 2.2.2.5)

In addition, DHCP clients that support **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]. NAP utilizes vendor-specific options as defined in [MS-DHCPN] section 2.2.1.

For information about the format of DHCP Vendor Extensions, see [RFC2132] section 2 and [RFC3315] section 22.

2.2.2.1 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.<2> 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<3> support this option. 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.

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>1
0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>2
0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>3
0</td><td>1</td></tr>
<tr><td colspan="8">Vendor-specific Option Code</td><td colspan="8">Vendor-specific Option Length</td><td colspan="16">Vendor-specific Option Data</td></tr>
<tr><td colspan="16">...</td></tr>
</table>

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): Values are as follows.

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).

2.2.2.2 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<4> support this option.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Vendor-specific Option Code								Vendor-specific Option Length								Vendor-specific Option Data															
...																															

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

2.2.2.3 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<5> support this option.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Vendor-specific Option Code								Vendor-specific Option Length								Vendor-specific Option Data															

...

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<6> be one of the following values.

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.

2.2.2.4 Vendor-Specific Option Code 0x5E - Rogue Detection Request Option

This option is sent by a Validating Server to DHCP servers on the network in a DHCPINFORM message. It is sent as an encapsulated vendor-specific option in option 43 (section 2.2.2).

The DHCPINFORM message does not contain the vendor-class identifier option (section 2.2.2).

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Vendor-Specific Option Code								Vendor-Specific Option Length																							

Vendor-Specific Option Code (1 byte): This MUST be 94 (0x5E).

Vendor-Specific Option Length (1 byte): This MUST be 0x00.

2.2.2.5 Vendor-Specific Option Code 0x5F – Rogue Detection Reply Option

This option is sent by a Rogue Aware Server to a Validating Server in a DHCPACK message. It is sent in response to an authorization message (see section 2.2.2.4) received in a DHCPINFORM message. It is sent as an encapsulated option in option 43 (section 2.2.2.4).

0	1	2	3	4	5	6	7	8	9	1 0	1	2	3	4	5	6	7	8	9	2 0	1	2	3	4	5	6	7	8	9	3 0	1
Vendor-specific Option Code								Vendor-specific Option Length								Vendor-specific Option Data (variable)															
...																															

Vendor-specific Option Code (1 byte): This MUST be 0x5F.

Vendor-specific Option Length (1 byte): The unsigned length, in bytes, of the **Vendor-specific Option Data** field. The maximum length is 255 bytes.

Vendor-specific Option Data (variable): This is a null-terminated string of length specified in **Vendor-specific Option Length**.

2.2.3 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.

0	1	2	3	4	5	6	7	8	9	1 0	1	2	3	4	5	6	7	8	9	2 0	1	2	3	4	5	6	7	8	9	3 0	1
Option Code								Option Length								Value (variable)															
...																															

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 unsigned 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.

2.2.4 DHCPv6 Option Code 15 (0x000F) - User Class Option

DHCPv6 clients implementing this specification MUST use the message format and semantics specified in [RFC3315] when sending a User Class Option to a DHCPv6 server. The DHCPv6 client MUST send a maximum of only one User Class Option in a DHCPv6 message. This section describes the message format of User Class Option sent by DHCPv6 servers that implement this specification in response to an Option Request from the DHCPv6 client. The format of this option varies from the implementation described in [RFC3315].

DHCPv6 clients MAY<7> request the user classes configured on the DHCPv6 server by sending an Information-request message containing OPTION_ORO (Option 6) with OPTION_USER_CLASS (Option 15) as the ONLY requested option. On receiving the message, the DHCPv6 server SHOULD<8> send a **Reply** message to the DHCPv6 client containing one or more User Class Options (one for each user class configured on the DHCPv6 server) in the format shown as follows. This behavior is an extension of the DHCPv6 protocol defined in [RFC3315]. The DHCPv6 server MUST send the **OPTION_USER_CLASS** with a format described in [RFC3315] when the DHCPv6 server sends the option in response to an OPTION_USER_CLASS received from a DHCPv6 client as described in [RFC3315].

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>20</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>30</td><td>1</td></tr>
<tr><td colspan="16">Option Code</td><td colspan="16">Option Length</td></tr>
<tr><td colspan="16">User Class Data Length</td><td colspan="16">User Class Binary Data Length</td></tr>
<tr><td colspan="32">User Class Binary Data (variable)</td></tr>
<tr><td colspan="32">...</td></tr>
<tr><td colspan="32">Padding (variable)</td></tr>
<tr><td colspan="32">...</td></tr>
<tr><td colspan="16">User Class Name Length</td><td colspan="16">User Class Name (variable)</td></tr>
<tr><td colspan="32">...</td></tr>
<tr><td colspan="16">User Class Description Length</td><td colspan="16">User Class Description (variable)</td></tr>
<tr><td colspan="32">...</td></tr>
</table>

Option Code (2 bytes): This MUST be 15 (0x000F) to indicate User Class Option.

Option Length (2 bytes): The unsigned length, in bytes, of the User Class Option, not including the **Option Code** and **Option Length** fields.

User Class Data Length (2 bytes): Value is variable, depending on the size of **User Class Binary Data**, **User Class Name** and **User Class Description**.

User Class Binary Data Length (2 bytes): Size of **User Class Binary Data** in octets.

User Class Binary Data (variable): Binary data of a User Class set on the DHCPv6 server.

Padding (variable): Padding to align User Class Binary data to 4-byte boundary.

User Class Name Length (2 bytes): Size of **User Class Name** in octets.

User Class Name (variable): Name of a User Class set on the DHCPv6 server.

User Class Description Length (2 bytes): Size of **User Class Description** in octets.

User Class Description (variable): Description of a User Class defined on the DHCPv6 server.

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

A DHCPv6 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.<9>

0	1	2	3	4	5	6	7	8	9	1 0	1	2	3	4	5	6	7	8	9	2 0	1	2	3	4	5	6	7	8	9	3 0	1
Option_Code																Option_Length															
Enterprise_Number																															
Vendor_Class_Data_Length																Vendor_Class_Data_String (variable)															
...																															

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 **Vendor_Class_Data_String**).

Enterprise_Number (4 bytes): MUST be set to 0x00000137 (decimal 311), the Internet Assigned Numbers Authority (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".

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

This section describes the message format of the User Class Option sent by DHCP clients and DHCP servers, 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. The use of this alternate format is indicated by the presence of a Vendor Class Identifier Option (section 2.2.3), which can occur anywhere in the same message.

2.2.6.1 User Class Option Sent by DHCP Client to DHCP Server

DHCP clients MAY<10> send a User Class Option with value selected by the administrator or as explained in the User Class Data tables that follow in all DHCP messages sent by the client. DHCP clients support only one User Class option. For semantics of the usage of DHCP user classes refer to [RFC3004] section 4.

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>1
0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>2
0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>3
0</td><td>1</td></tr>
<tr><td colspan="8">Option Code</td><td colspan="8">Option Length</td><td colspan="16">User_Class_Data (variable)</td></tr>
<tr><td colspan="32">...</td></tr>
</table>

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.

2.2.6.2 User Class Option Sent by DHCP Server to DHCP Client

DHCP clients MAY<11> request the user classes configured on the DHCP server by sending a **DHCPINFORM** message containing OPTION_PARAMETER_REQUEST_LIST (Option 55) with OPTION_USER_CLASS (Option 77) as one of the requested options. On receiving the message, the DHCP server SHOULD<12> send a **DHCPACK** message to the DHCP client containing one or more User Class Options (one for each user class configured on the DHCP server) in the format shown as follows.

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>1
0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>2
0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>3
0</td><td>1</td></tr>
<tr><td colspan="8">Option Code</td><td colspan="8">Option Length</td><td colspan="16">User Class Binary Data Length</td></tr>
<tr><td colspan="32">User Class Binary Data (variable)</td></tr>
<tr><td colspan="16">...</td><td colspan="16">Padding (variable)</td></tr>
</table>

...	
User Class Name Length	User Class Name (variable)
...	
User Class Description Length	User Class Description (variable)
...	

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

Option Length (1 byte): The unsigned length, in bytes, of the User Class Option, not including the **Option Code** and **Option Length** fields.

User Class Binary Data Length (2 bytes): Size of the User Class binary data in octets.

User Class Binary Data (variable): Binary data of a User Class set on the DHCP server.

Padding (variable): Padding to align the User Class binary data to 4-byte boundary.

User Class Name Length (2 bytes): Size of the **User Class Name** in octets.

User Class Name (variable): Name of a User Class set on the DHCP server.

User Class Description Length (2 bytes): Size of the **User Class Description** in octets.

User Class Description (variable): Description of a User Class set on the DHCP server.

2.2.7 DHCP Option Code 81 (0x51) - Client FQDN Option

The client FQDN option is specified in [RFC4702] section 2. [RFC4702] section 2.3.1 states that setting the E bit to 0 indicates that the name is ASCII-encoded, but does not explain how to ASCII encode a name if the client has a non-ASCII name. It then explains that client software may send data intended to be in other character sets, but that support for other character sets is not required. This document clarifies that a client with a non-ASCII name SHOULD always set the E bit to 1, but that a client MAY<13> send its host name in an implementation-specific character set. [RFC4702] section 4 states that DHCP servers SHOULD ignore the client FQDN option if the client's E bit is set to 0 and the servers do not support ASCII encoding. However, [RFC4702] section 2.3.1 states that client software may send data intended to be in other character sets, but that support for other character sets is not required. This specification clarifies that a DHCP server MAY<14> accept other implementation-dependent character sets when the E bit is set to 0.

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

DHCP clients and servers that implement this specification use some nonstandard options in their implementation.

The length and the data format for the Microsoft **Classless Static Route** Option are exactly the same as those specified for the Classless Static Route Option in [RFC3442]; the only difference is that Option Code 249 SHOULD<15> 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, whereas the destination descriptor length is between 1 byte and 5 bytes, depending on the subnet mask. This is described in detail as follows.

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 in any of the messages sent by the client to the server.

<table>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>1
0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>2
0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>3
0</th><th>1</th></tr>
<tr><td colspan="8">Option Code</td><td colspan="8">Option Length</td><td colspan="16">CSR-1 Destination descriptor (variable)</td></tr>
<tr><td colspan="32">...</td></tr>
<tr><td colspan="32">CSR-1 Router IP address</td></tr>
<tr><td colspan="32">CSR-N Destination descriptor (variable)</td></tr>
<tr><td colspan="32">...</td></tr>
<tr><td colspan="32">CSR-N Router IP address</td></tr>
</table>

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

Option Length (1 byte): The unsigned length, in bytes, of the option, not including the **Option Code** and **Option Length** fields.

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.

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

DHCP standard options are constrained to be of maximum 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.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Option Code								Option Length								Option Data (variable)															
...																															

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

Option Length (1 byte): The unsigned length, in bytes, of the option, not including the **Option Code** and **Option Length** fields.

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.

2.2.10 DHCPv6 Option Code 17 (0x0011) - Vendor Specific Information Option

A DHCPv6 client and server exchange vendor-specific information between themselves. This information is sent in the form of a vendor-specific information option, as specified in [RFC3315] section 22.17.

A Validating Server does not need to include a vendor class option (section 2.2.5) when authorizing itself using Rogue Detection.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Option Code																Option Length															
Enterprise Number																															
Option Data (variable)																															
...																															

Option Code (2 bytes): As specified in [RFC3315] section 22.17, this is used to indicate the Vendor-specific information Option and MUST be 0x0011.

Option Length (2 bytes): Set to the size of **Option Data**, in bytes, plus 4.

Enterprise Number (4 bytes): MUST be set to 0x00000137 (decimal 311), the Internet Assigned Numbers Authority (IANA)–assigned Microsoft Enterprise number [IANA-ENT].

Option Data (variable): This is set to the vendor-specific option data.

When a DHCPv6 message includes a Vendor Class Identifier with the value defined in section 2.2.5, the Vendor-Specific Information Option is defined to use the "Encapsulated vendor-specific options" format specified in [RFC3315] section 22.17. This specification defines the following encapsulated vendor-specific option codes.

Value	Meaning
0x5E	Rogue Detection Request Option
0x5F	Rogue Detection Reply Option

2.2.10.1 Vendor-Specific Option Code 0x5E – Rogue Detection Request Option

This option is sent by a Validating Server to DHCP servers on the network in a DHCPv6 Information-Request message. It is sent as an encapsulated option in option 12 (section 2.2.10).

The DHCPv6 Information-Request message does not need to contain the vendor class identifier option (section 2.2.5).

The DHCPv6 server requests option 94 (0x005E) in the DHCPv6 Information-Request message in the following format.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Vendor-specific Option Code																Vendor-specific Option Length															

Vendor-specific Option Code (2 bytes): This MUST be 94 (0x5E).

Vendor-specific Option Length (2 bytes): This MUST be 0x00.

2.2.10.2 Vendor-Specific Option Code 0x5F – Rogue Detection Reply Option

This option is sent by a Rogue Aware Server to a Validating Server in a DHCPv6 **Reply** message. It is sent in response to option 0x5E (section 2.2.10.1) received in a DHCPv6 Information-Request message. It is sent as an encapsulated option in option 17 (section 2.2.10).

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Vendor-Specific Option Code																Vendor-Specific Option Length															
Vendor-Specific Option Data (variable)																															
...																															

Vendor-Specific Option Code (2 bytes): This MUST be 95 (0x5F).

Vendor-Specific Option Length (2 bytes): The unsigned length in bytes of the **Vendor-Specific Option Data** field. The maximum length is 255 bytes.

Vendor-Specific Option Data (variable): This is a null-terminated string of length specified by **Vendor-Specific Option Length**.

3 Protocol Details

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, except the timers in [RFC2131] and [RFC3315].

The DHCP client MUST follow an exponential backoff model for **DHCPDISCOVER** retransmission, as recommended in [RFC2131] section 4.1. However, [RFC2131] does not specify the actual values, so they are specified here. When the DHCP client attempts to allocate a network address as described in [RFC2131] section 3.1, the DHCP client MUST wait successively for 4, 8, 16, and 32 seconds (its exponential backoff model values) for the server to respond. If no response is received to the fourth **DHCPDISCOVER**, the DHCP client MUST wait 5 minutes before repeating the preceding cycle.

DHCPv6 clients implementing this specification adhere to [RFC3315].

3.1.3 Initialization

DHCP client initialization (as specified in [RFC2131]) and DHCPv6 client initialization (as specified in [RFC3315]) are unchanged by the extensions specified in this document.

3.1.4 Higher-Layer Triggered Events

None.

3.1.4.1 Sending a DHCPDISCOVER, DHCPREQUEST, or DHCPINFORM Message

When sending a **DHCPDISCOVER**, **DHCPREQUEST**, or **DHCPINFORM** message, DHCP clients implementing this specification SHOULD<16> include a Vendor Class Identifier Option formatted as in section 2.2.3 and MAY<17> include a User Class Option formatted as in section 2.2.8. Because 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 2.2.8.

When sending a **DHCPINFORM** message, DHCP clients implementing this specification MAY<18> include an OPTION_PARAMETER_REQUEST_LIST (Option 55) with OPTION_USER_CLASS (Option 77) as one of the requested options.

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 SHOULD<19> include a Vendor Class Option formatted as in section 2.2.5.

When sending an Information-Request message, DHCPv6 clients implementing this specification MAY<20> include an OPTION_ORO (Option 6) with OPTION_USER_CLASS (Option 15) as the only requested option.

3.1.4.3 Sending a DHCP Release or DHCPv6 Release Message

The behavior is same as specified in [RFC2131] section 3.1 for the DHCP **Release** message and [RFC3315] section 18.1.6 for the DHCPv6 **Release** message.

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 is 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<21> instead use the options to choose among offers in any implementation-specific manner.

When sending a **DHCPREQUEST** in response, the DHCP client SHOULD<22> include a Vendor Class Identifier Option formatted as in section 2.2.3 and MAY<23> include a User Class Option formatted as in section 2.2.6. Because 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 2.2.6. The DHCP client SHOULD<24> 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 2.2.2.1.

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 2.2.2.2.

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 2.2.8. 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.

If it contains one or more User Class options (Option 77), the client MUST first check whether each option conforms to the syntax specified in section 2.2.6. If the option does not conform to the syntax, the DHCP client MUST silently discard the complete DHCP message and start the initialization process again. Otherwise, the client uses the information in an implementation-specific manner.

3.1.5.3 Receiving a DHCPv6 Advertise Message

If the DHCPv6 **Advertise** contains any of the V6 options defined in this specification, the client MAY<25> use the options to choose among advertises in any implementation-specific manner.

3.1.5.4 Receiving a DHCPv6 Reply Message

When a DHCPv6 client implementing this specification receives a **Reply** message that contains one or more User Class Options (Option 15), it MUST first check whether the option conforms to the syntax specified in section 2.2.4. If the option does not conform to the syntax, the DHCPv6 client MUST silently discard the option. Otherwise, the DHCPv6 client uses the information in an implementation-specific manner.

3.1.6 Timer Events

DHCP extensions defined in this specification adhere to the RFC standards (as specified in [RFC2131] section 4.4 and in [RFC2132]) for timer events.

The DHCPv6 extensions defined in this specification adhere to the RFC standards (as specified in [RFC3315] section 14 and section 18) 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 or DHCPv6.

3.2.2 Timers

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

3.2.3 Initialization

DHCP/DHCPv6 server initialization (as specified in [RFC2131] and [RFC3315]) is unchanged by 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. The DHCPv6 server processes messages as specified in [RFC3315]. Additional behavior of DHCP and DHCPv6 servers is specified in this section.

3.2.5.1 Receiving a DHCPDISCOVER Message

Increment the **DHCPv4ServerMibInfo.Discovers** element as described in section 1.4, point 10.

Evaluate and apply administrative controls as described in section 1.4, point 6.<26>.

If the **DHCPDISCOVER** message contains a Vendor Class Identifier Option (section 2.2.3) with a value defined in section 2.2.3, the DHCP server SHOULD ignore the Vendor Class Identifier Option and process the message as if the option were not present. The server MAY<27> 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.

If the **DHCPDISCOVER** contains a Client Identifier Option (Option 61) with the field Client-Identifier containing the first four bytes as "RAS", the DHCP server MUST ignore any FQDN Option (Option 81) in the DHCP message and MUST NOT perform DNS registration of A and PTR records on behalf of the DHCP client. For more information, see [RFC4702].

If processing the **DHCPDISCOVER** message results in the server sending a **DHCPOFFER** message to the client, then increment the **DHCPv4ServerMibInfo.Offers** element as described in section 1.4, point 10.

3.2.5.2 Receiving a DHCPREQUEST Message

Evaluate and apply administrative controls as described in section 1.4, point 6.<28>

Increment the **DHCPv4ServerMibInfo.Requests** element as described in section 1.4, point 10.

If the **DHCPREQUEST** message contains a Vendor Class Identifier Option (section 2.2.3) with a value defined in section 2.2.3, the following points illustrate the behavior of the DHCP server:

- The DHCP server MUST include the vendor-specific options defined in section 2.2.2 (if configured to do so by the administrator) in the **DHCPACK** message sent to the clients.
- The DHCP server MUST interpret the User Class Option if it exists<29> in the **DHCPREQUEST** message to contain a single value as defined in section 2.2.6.

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, the Classless Static Route information SHOULD<30> 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 2.2.9.

If processing of the **DHCPREQUEST** message results in the server sending a **DHCPACK** message to the client, then increment the **DHCPv4ServerMibInfo.Acks** element as described in section 1.4, point 10.

If processing of the DHCPREQUEST message results in the server sending a **DHCPNACK** message to the client, then increment the **DHCPv4ServerMibInfo.Nacks** element as described in section 1.4, point 10.

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

If the **DHCPREQUEST** contains a Client Identifier Option (Option 61) with the field Client-Identifier containing the first four bytes as "RAS ", the DHCP server MUST ignore any FQDN Option (Option 81) in the DHCP message and MUST NOT perform DNS registration of A and PTR records on behalf of the DHCP client. For more information, see [RFC4702].

3.2.5.3 Receiving a DHCPv6 Message with a Vendor Class Option

DHCPv6 servers implementing this specification MAY<31> 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 DHCPINFORM Message

If the **DHCPINFORM** message does not contain Rogue Detection Request Option (section 2.2.2.4), evaluate and apply administrative controls as described in section 1.4, point 6.<32>

When a DHCP server implementing this specification receives a **DHCPINFORM** message containing an OPTION_PARAMETER_REQUEST_LIST (Option 55) with OPTION_USER_CLASS (Option 77) as one of the requested options, the DHCP server SHOULD<33> send a **DHCPACK** message to the DHCP client containing one or more User Class Options (one for each user class configured on the DHCP Server) in the format specified in section 2.2.6. If the option request is received in a message other than **DHCPINFORM** message, the request is silently ignored.

3.2.5.5 Receiving an Information-Request Message

Increment the **DHCPv6ServerMibInfo.Informs** element as described in section 1.4, point 17.

When a DHCPv6 server implementing this specification receives an Information-Request message containing OPTION_ORO (Option 6) with OPTION_USER_CLASS (Option 15) as the only requested option, the DHCPv6 server SHOULD<34> send a **DHCPACK** message to the DHCPv6 client containing one or more User Class Options (one for each User Class configured on the DHCPv6 server) in the format specified in section 2.2.4. If other options are also requested in the message, the DHCPv6 server MAY<35>respond to the message. If the message is not an Information-Request message, the option request MUST be silently discarded.

If processing of the Information-Request message results in the server sending a DHCPv6 Reply message to the client, then increment the **DHCPv6ServerMibInfo.Replies** element as described in section 1.4, point 17.

3.2.5.6 Receiving a DHCP Message with a User Class Option

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

3.2.5.7 Receiving a DHCP RELEASE Message

Increment the **DHCPv4ServerMibInfo.Releases** element as described in section 1.4, point 10.

Subsequent processing is as specified in [RFC2131] section 4.3.4.

3.2.5.8 Receiving a DHCPv6 Release Message

Increment the **DHCPv6ServerMibInfo.Releases** element as described in section [1.4](), point 17.

The subsequent processing is as specified in [RFC3315] section 18.2.6.

If processing of the Information-Request message results in the server sending a DHCPv6 Reply message to the client, then increment the **DHCPv6ServerMibInfo.Replies** element as described in section 1.4, point 17.

3.2.5.9 Receiving a DHCPDECLINE Message

Increment the **DHCPv4ServerMibInfo.Declines** element as described in section 1.4, point 10.

The subsequent processing is as specified in [RFC2131] section 4.3.3.

If processing of the Information-Request message results in the server sending a DHCPv6 Reply message to the client, then increment the **DHCPv6ServerMibInfo.Replies** element as described in section 1.4, point 17.

3.2.5.10 Receiving a DHCPv6 Solicit Message

Increment the **DHCPv6ServerMibInfo.Solicits** element as described in section 1.4, point 17.

The subsequent processing is as specified in [RFC3315] section 17.2.1.

If processing of the DHCPv6 Solicit message results in the server sending a DHCPv6 Advertise message to the client, then increment the **DHCPv6ServerMibInfo.Offers** element as described in section 1.4, point 17.

3.2.5.11 Receiving a DHCPv6 Request Message

Increment the **DHCPv6ServerMibInfo.Requests** element as described in section 1.4, point 17.

The subsequent processing is as specified in [RFC3315] section 18.2.1.

If processing of the Information-Request message results in the server sending a DHCPv6 Reply message to the client, then increment the **DHCPv6ServerMibInfo.Replies** element as described in section 1.4, point 17.

3.2.5.12 Receiving a DHCPv6 Confirm Message

Increment the **DHCPv6ServerMibInfo.Confirms** element as described in section 1.4, point 17.

The subsequent processing is as specified in [RFC3315] section 18.2.2.

If processing of the Information-Request message results in the server sending a DHCPv6 Reply message to the client, then increment the **DHCPv6ServerMibInfo.Replies** element as described in section 1.4, point 17.

3.2.5.13 Receiving a DHCPv6 Renew Message

Increment the **DHCPv6ServerMibInfo.Renews** element as described in section 1.4, point 17.

The subsequent processing is as specified in [RFC3315] section 18.2.3.

If processing of the Information-Request message results in the server sending a DHCPv6 Reply message to the client, then increment the **DHCPv6ServerMibInfo.Replies** element as described in section 1.4, point 17.

3.2.5.14 Receiving a DHCPv6 Rebind Message

Increment the **DHCPv6ServerMibInfo.Rebinds** element as described in section 1.4, point 17.

The subsequent processing is as specified in [RFC3315] section 18.2.4.

If processing of the Information-Request message results in the server sending a DHCPv6 Reply message to the client, then increment the **DHCPv6ServerMibInfo.Replies** element as described in section 1.4, point 17.

3.2.5.15 Receiving a DHCPv6 Decline Message

Increment the **DHCPv6ServerMibInfo.Declines** element as described in section 1.4, point 17.

The subsequent processing is as specified in [RFC3315] section 18.2.7.

If processing the Information-Request message results in the server sending a DHCPv6 Reply message to the client, then increment the **DHCPv6ServerMibInfo.Replies** element as described in section 1.4, point 17.

3.2.5.16 Receiving a MADCAP DISCOVER Message

Increment the **DHCPv6ServerMibInfo.Declines** element, a shared ADM element, as described in section 1.4, item 17.

The subsequent processing is as specified in [RFC3315] section 18.2.7.

If processing the Information-Request message results in the server sending a DHCPv6 Reply message to the client, then increment the **DHCPv6ServerMibInfo.Replies** element, a shared ADM element, as described in 1.4, item 17.

3.2.5.17 Receiving a MADCAP REQUEST Message

Increment the **DHCPv4ServerMcastMibInfo.Requests** element, a shared ADM element.

The subsequent processing is as specified in [RFC2730] section 2.2.4.

If processing the REQUEST message results in the server sending a MADCAP ACK message to the client, then increment the **DHCPv4ServerMcastMibInfo.Acks** element, a shared ADM element.

3.2.5.18 Receiving a MADCAP RENEW Message

Increment the **DHCPv4ServerMcastMibInfo.Renews** element, a shared ADM element.

The subsequent processing is as specified in [RFC2730] section 2.2.7.

If processing the RENEW message results in the server sending a MADCAP ACK message to the client, then increment the DHCPv4ServerMcastMibInfo.Acks element, a shared ADM.

If processing the RELEASE message results in the server sending a MADCAP NAK message to the client, then increment the **DHCPv4ServerMcastMibInfo.Naks** element, a shared ADM element.

3.2.5.19 Receiving a MADCAP RELEASE Message

Increment the **DHCPv4ServerMcastMibInfo.Releases** element, a shared ADM element.

The subsequent processing is as specified in [RFC2730] section 2.2.8.If processing the RELEASE message results in the server sending a MADCAP ACK message to the client, then increment the DHCPv4ServerMcastMibInfo.Acks element, a shared ADM element.

If processing the RELEASE message results in the server sending a MADCAP NAK message to the client, then increment the **DHCPv4ServerMcastMibInfo.Naks** element, a shared ADM.

3.2.5.20 Receiving a MADCAP GETINFO Message

Increment the **DHCPv4ServerMcastMibInfo.Informs** element, a shared ADM element.

The subsequent processing is as specified in [RFC2730] section 2.2.1.

If processing the GETINFO message results in the server sending a MADCAP ACK message to the client, then increment the **DHCPv4ServerMcastMibInfo.Acks** element, a shared ADM element.

If processing the GETINFO message results in the server sending a MADCAP NAK message to the client, then increment the **DHCPv4ServerMcastMibInfo.Naks** element, a shared ADM element.

3.2.6 Timer Events

The DHCP extensions adhere to the RFC standards ([RFC2131] section 4.4 and in [RFC2132]) for timer events.

The DHCPv6 extensions adhere to the RFC standard ([RFC3315] section 14 and 18) for timer events.

3.2.7 Other Local Events

None.

3.3 Rogue Detection Details

A DHCP server MAY<36> implement the Rogue Detection mechanism. A Rogue Aware Server periodically checks whether it is authorized.<37> This check is done irrespective of the DHCP server authorization state. The time interval between checks MAY<38> vary based on the authorization state.

3.3.1 Authorization of a DHCP server using DHCPINFORM

The following steps describe how a DHCP server can authorize itself using the **DHCPINFORM** message to serve IP addresses.<39>.

1. A Validating Server MUST open **UDP** port 68 on the interfaces bound to the DHCPv4 server. If the server does not contain bound interfaces, the server cannot validate itself.

2. A Validating Server MUST send a broadcast **DHCPINFORM** message to address 255.255.255.255 with the Rogue Detection Request Option (section 2.2.2.4) on all the interfaces bound to the DHCPv4 server.

3. An Administratively Authorized Server<40> that is Rogue Aware SHOULD<41> reply to the **DHCPINFORM** message by sending a **DHCPACK** message containing the Rogue Detection Reply Option (section 2.2.2.5) with a non-empty NULL-terminated string in the option data.

4. A Rogue Authorized Server on the network SHOULD<42> reply to the **DHCPINFORM** message by sending a **DHCPACK** message containing the Rogue Detection Reply Option (section 2.2.2.5) with an empty NULL-terminated string in the option data.

5. Any DHCP server that is not Rogue Aware may reply to the **DHCPINFORM** message by sending a **DHCPACK** message that will however not contain the Rogue Detection Reply Option (section 2.2.2.5).

6. An Unauthorized Server which is Rogue Aware will not reply to the **DHCPINFORM** message.

7. If a Validating Server receives a **DHCPACK** message from an Administratively Authorized Server, it will consider itself unauthorized.

8. If a Validating Server does not receive a **DHCPACK** message from an Administratively Authorized Server within a stipulated time<43>, it retries sending the **DHCPINFORM** message.

9. If a Validating Server receives a **DHCPACK** message from a Rogue Authorized Server or a server which is not Rogue Aware, it retries sending the **DHCPINFORM** message.

10. The maximum number of retries is implementation-specific<44>. When all attempts are exhausted, the Validating Server MAY<45> consider itself authorized or continue validation using the DHCPv6 Information-Request message.

3.3.2 Authorization of a DHCP server using DHCPv6 Information-Request

Authorization of a DHCP server using DHCPv6 Information-Request message is done when the IPv4 protocol is uninstalled or disabled on the interfaces. If, in the DHCP server authorization scenario using **DHCPINFORM** message a DHCP server does not receive any **DHCPACK** messages from an Administratively Authorized Server after all the retry attempts are exhausted, the DHCP server attempts authorization using the Information-Request message. The following steps describe how a DHCP server authorizes itself using Information-Request to serve IP addresses.<46>

1. A Validating Server MUST open UDP port 546 on the interfaces bound to the DHCPv6 server. If the server does not contain bound interfaces then server cannot validate itself.

2. A Validating Server MUST send a DHCPv6 Information-Request message with the Rogue Detection Request Option (section 2.2.10.1) on all the interfaces bound to the DHCPv6 server.

3. An Administratively Authorized Server<47> which is Rogue Aware SHOULD<48> reply to the DHCPv6 INFORMATION-REQUEST message by sending a DHCPv6 **Reply** message containing the Rogue Detection Reply Option (section 2.2.10.2) with a non-empty null-terminated string in the option data.

4. A Rogue Authorized Server on the network SHOULD<49> reply to the DHCPv6 INFORMATION-REQUEST message by sending a DHCPv6 **Reply** message containing the Rogue Detection Reply Option (section 2.2.10.2) with an empty null-terminated string in the option data.

5. Any DHCP server that is not Rogue Aware may reply to the DHCPv6 INFORMATION-REQUEST message by sending a DHCPv6 **Reply** message that will however not contain the corresponding vendor specific option.

6. An Unauthorized Server on the network which is Rogue Aware will not reply to the DHCPv6 INFORMATION-REQUEST message.

7. If a Validating Server receives a DHCPv6 **Reply** message from an Administratively Authorized Server, it will consider itself unauthorized.

8. If a Validating Server does not receive a DHCPv6 **Reply** message from an Administratively Authorized Server within a stipulated time<50>, it retries sending the DHCPv6 INFORMATION-REQUEST message.

9. If a Validating Server receives a DHCPv6 **Reply** message from a Rogue Authorized Server or a server which is not Rogue Aware, it retries sending the DHCPv6 INFORMATION-REQUEST message.

10. The maximum number of retries is implementation specific<51>. After all retry attempts are exhausted, the Validating Server will consider itself authorized.

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 prevent 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 2.2.2.1, to the DHCP clients.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Vendor-specific Option Code = 0x01								Vendor-specific Option Length = 0x04								Vendor-specific Option Data = 0x0000															
0x0002																															

2. The DHCP client joins the network and sends a **DHCPDISCOVER** message that includes a Vendor Class Identifier Option. For instance, the DHCP client sends the vendor class as "MSFT 5.0".

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Option Code = 0x3C								Option Length = 0x08								Value = "MS"															
"FT 5"																															
".0"																															

3. The DHCP server ignores the Vendor Class Identifier Option and responds with a **DHCPOFFER** message. It does not include any option defined in this specification in the **DHCPOFFER** message. The DHCP client accepts the offer by sending a **DHCPREQUEST** message again that includes 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 previously shown.

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

In another example, an administrator wants DHCP 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 2.2.2.2, to the DHCP clients.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Vendor-specific Option Code = 0x02								Vendor-specific Option Length = 0x04								Vendor-specific Option Data = 0x0000															
0x0001																															

2. The DHCP client joins the network and sends a **DHCPDISCOVER** message that includes a Vendor Class Identifier Option. For instance, the DHCP client may send the vendor class as "MSFT 5.0".

3. The DHCP server ignores the Vendor Class Identifier Option and responds with a **DHCPOFFER** message. It does not include any option defined in this specification in the **DHCPOFFER** message. The DHCP client accepts the offer by sending a **DHCPREQUEST** message again that includes a 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 2 as previously shown.

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

In another example, an administrator wants to change the router metric used by DHCP 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 2.2.2.3, to the DHCP clients.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Vendor-specific Option Code = 0x03								Vendor-specific Option Length = 0x04								Vendor-specific Option Data = 0x0000															
0x000A																															

2. The DHCP client joins the network and sends a **DHCPDISCOVER** message that includes a Vendor Class Identifier Option with, for example, the value "MSFT 5.0".

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

5. The DHCP 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 previously.
2. The DHCPv6 client joins the local network and sends a DHCPv6 **Solicit** message that includes a Vendor Class Option (section 2.2.5). For instance, the DHCPv6 client sends the vendor-class data as "MSFT 5.0".

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Option_Code = 0x0010																Option_Length = 0x000E															
Enterprise_Number = 0x00000137																															
Vendor_Class_Data_Length = 0x0008																Data String = "MS"															
"FT 5"																															
".0"																															

3. The DHCPv6 server ignores the Vendor Class Option and responds with a DHCPv6 **Advertise** message. The DHCPv6 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 DHCPv6 client in the DHCPv6 **Request** message and sends the appropriate standard options to the DHCPv6 client in the DHCPv6 **Reply** message. Depending on the DHCPv6 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 DHCPv6 client receives and applies the option information sent by the DHCPv6 server.

In another example, an administrator wants to send specific information to DHCP clients on the local network when the administrator sends 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 subpacket with the value "BOOTP" (as described in section 2.2.6) in the DHCP message sent by the DHCP client. If the message contains this user-class subpacket, the DHCP server is configured to respond with the desired information that the administrator wants to send to the DHCP client.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Option Code = 0x4D								Option Length = 0x06								Value Length = 0x05								Value = "B"							
"OOTP"																															

2. DHCP 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 subpacket with the value "BOOTP" as previously shown. Thus, if the DHCP server is configured as explained previously, the DHCP 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 option code 121, used in [RFC3442].

In another example, say that an administrator wants to send Vendor-specific Information through DHCP to a DHCP client on the local network as DHCP Vendor-Specific Information Option 43 (0x2B). However, this information, when encapsulated in Option 43 as per [RFC2132], is 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 DHCP client joins the network and sends a **DHCPDISCOVER** message that includes a Vendor Class Identifier Option with, for example, the value "MSFT 5.0".

3. The DHCP server ignores the Vendor Class Identifier Option and responds with a **DHCPOFFER** message. It does not include any option defined in this specification in the **DHCPOFFER** message. The DHCP client accepts the offer by sending a **DHCPREQUEST** 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 the Vendor-Specific Information option with the desired value as configured by the administrator, while formatting it as described in section 2.2.9, 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.

<table>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>20</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>30</th><th>1</th></tr>
<tr><td colspan="8">DHCP Option Code = 0x2B</td><td colspan="8">Length = 0xFF</td><td colspan="16">First 255 bytes of option data</td></tr>
<tr><td colspan="32">...</td></tr>
<tr><td colspan="8">...</td><td colspan="8">DHCP Option Code 250 - Long Options Packet = 0xFA</td><td colspan="8">Length = 0xFF</td><td colspan="8">...</td></tr>
<tr><td colspan="32">Second 255 bytes (bytes 256-510) of option data</td></tr>
<tr><td colspan="32">...</td></tr>
<tr><td colspan="16">...</td><td colspan="8">DHCP Option Code 250 - Long Options Packet = 0xFA</td><td colspan="8">Length = 0x5A</td></tr>
<tr><td colspan="32">Last 90 bytes of option data</td></tr>
<tr><td colspan="32">...</td></tr>
</table>

5. DHCP clients on the local network that initiate a DHCP transaction with the preceding 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 the options as described in section 2.2.9.

The following example demonstrates the use of User Class option when a user wants to see all User Classes configured on DHCP server by an administrator.

1. The administrator configures a User Class on the DHCP server with name as "test", description as "desc" and binarydata as "123".

2. When a DHCP client gets connected in this network, the client gets the IP and other configuration information from the DHCP server.

3. The user instructs the DHCP client in an implementation-specific manner to retrieve all User Classes on the DHCP server. The DHCP client sends a **DHCPINFORM** packet containing the Option 55 to the DHCP server requesting Option 77, shown as follows.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Option Code = 55								Option Length = 1 byte								Option Requested = 77															

4. In the reply to the **DHCPINFORM** packet, the server sends **DHCPACK** with the Option 77 record in it. The format of the option record is as follows.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Option Code = 77								Option Length = 30 bytes								User Class Binary Data Length = 3															
'1'								'2'								'3'								'\0' (Padding)							
User Class Name Length= 10(0x0A)																'\0'								'T'							
'\0'								'E'								'\0'								'S'							
'\0'								'T'								'\0'								'\0'							
User Class Description Length= 10(0x0A)																'\0'								'D'							
'\0'								'E'								'\0'								'S'							
'\0'								'C'								'\0'								'\0'							

5 Security

5.1 Security Considerations for Implementers

All of the security considerations that are applicable to DHCP (as described in [RFC2131] section 7) and DHCPv6 (as described in [RFC3315] section 23) apply to the implementation of this specification.

5.2 Index of Security Parameters

None.

6 Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs:

- Microsoft Windows® 98 operating system
- Microsoft Windows® 2000 operating system
- Microsoft Windows® Millennium Edition operating system
- Windows® XP operating system
- Windows Server® 2003 operating system
- Windows Vista® operating system
- Windows Server® 2008 operating system
- Windows® 7 operating system
- Windows Server® 2008 R2 operating system

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that the product does not follow the prescription.

<1> Section 2.2.1: All Windows DHCP clients send the host name encoded using the **original equipment manufacturer (OEM) code page** that was installed as the current system code page at system boot time in Option 12. All Windows DHCP servers treat the host name as being encoded using the OEM code page that was installed on the DHCP server as the current system code page at system boot time.

<2> Section 2.2.2.1: Windows DHCP servers send this option in the **DHCPOFFER** and **DHCPACK** messages, if configured to do so by the administrator.

<3> Section 2.2.2.1: Windows 98 and Windows Millennium EditionDHCP clients do not support this option.

<4> Section 2.2.2.2: Windows 98 and Windows Millennium Edition DHCP clients do not support this option.

<5> Section 2.2.2.3: Windows 98 and Windows Millennium Edition DHCP clients do not support this option.

<6> Section 2.2.2.3: 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 Millennium Edition, Windows 2000, Windows XP, and Windows XP SP1 clients.

Release: Friday, February 4, 2011

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)

<7> Section 2.2.4: Windows 7 and Windows Server 2008 R2 DHCPv6 clients request the User Classes defined on Windows DHCPv6 server whenever a user tries to set the User Class for the DHCPv6 client by executing "Ipconfig /setuseridclass6" or whenever a user tries to see the User Classes defined on DHCPv6 server by executing "Ipconfig /showuseridclass6". DHCPv6 clients on Windows Vista SP1 and Windows Server 2008 do not support the User Class Option.

<8> Section 2.2.4: Windows Server 2008 R2 sends one or more User Class Options depending on whether one or more User Classes are configured on the DHCP server. DHCPv6 server on Windows Server 2008 does not support User Class Option.

<9> Section 2.2.5: DHCPv6 Client support is implemented in Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2. DHCPv6 server support is available in Windows Server 2008 and Windows Server 2008 R2.

<10> Section 2.2.6.1: By default, Windows DHCP 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.

<11> Section 2.2.6.2: DHCP clients request the User Classes defined on the Windows DHCP server whenever a user tries to set the User Class for the DHCP client by executing "Ipconfig /setuserid" or whenever a user tries to see the User Classes defined on the DHCP server by executing "Ipconfig /showuserid"

<12> Section 2.2.6.2: Windows Server sends on or more User Class Options depending on whether one or more User Classes are configured on the DHCP server.

<13> Section 2.2.7: All Windows DHCP clients send FQDNs in Option 81 with the E bit set to 0 by default, but can be configured to send with the E bit set to 1. When sending with the E bit set to 0, the host name is encoded using the OEM code page that was installed as the current system code page at system boot time. When sending with the E bit set to 1, the host name is encoded using **UTF-8** encoding.

<14> Section 2.2.7: Windows DHCP servers treat FQDNs with the E bit set to 0 in Option 81 as being encoded using the OEM code page that was installed on the DHCP server as the current system code page at system boot time. FQDNs with the E bit set to 1 are treated as being encoded using UTF-8 encoding.

<15> Section 2.2.8: Windows XP and Windows Server 2003 DHCP clients and servers 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, Windows Server 2008, Windows 7 and Windows Server 2008 R2 DHCP clients use both Option 121 and Option 249.

<16> Section 3.1.4.1: All Windows DHCP clients include Vendor Class Identifier Option (Option 60) in **DHCPDISCOVER**, **DHCPREQUEST**, and **DHCPINFORM** messages.

<17> Section 3.1.4.1: By default, Windows DHCP 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.

Windows DHCP clients using BOOTP to boot from the network send the Default BOOTP class (as defined in section 2.2.6) as their user class.

<18> Section 3.1.4.1: DHCP clients request the User Classes defined on Windows DHCP server whenever a user tries to set the User Class for the DHCP client by executing "Ipconfig /setuserid" or whenever a user tries to see the User Classes defined on DHCP server by executing "Ipconfig /showuserid"

<19> Section 3.1.4.2: All Windows DHCPv6 clients include a Vendor Class Option (Option 16) in DHCPv6 **Solicit**, **Request**, and Information-Request messages.

<20> Section 3.1.4.2: Windows 7 and Windows Server 2008 R2 DHCPv6 clients request the User Classes defined on Windows DHCPv6 server whenever a user tries to set the User Class for the DHCPv6 client by executing "Ipconfig /setuserid6" or whenever a user tries to see the User Classes defined on DHCPv6 server by executing "Ipconfig /showuserid6". DHCPv6 clients on Windows Vista and Windows Server 2008 do not support the User Class Option.

<21> Section 3.1.5.1: Windows DHCP clients parse each of the options in the **OFFER** received and silently discard the message if any of the options do not conform to the syntax. If the DHCP client has requested a particular IP Address, it chooses the **OFFER** which has value of allocated IP address same as the requested IP address.

<22> Section 3.1.5.1: All Windows DHCP clients include a Vendor Class Identifier Option (Option 60) in **DHCPDISCOVER**, **DHCPREQUEST**, and **DHCPINFORM** messages.

<23> Section 3.1.5.1: By default, Windows DHCP 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.

Windows DHCP clients using BOOTP to boot from the network send the Default BOOTP class (as defined in section 2.2.6) as their user class.

<24> Section 3.1.5.1: Windows XP and Windows Server 2003 DHCP clients request only option code 249 in the Parameter Request List. Windows DHCP clients request both option code 121 and option code 249 in the Parameter Request List.

<25> Section 3.1.5.3: Windows DHCPv6 clients parse each of the options in the ADVERTISE received and silently discard the message if any of the options do not conform to the syntax.

<26> Section 3.2.5.1: Administrative controls are implemented only by the Windows Server 2008 R2 DHCP server.

<27> Section 3.2.5.1: Windows DHCP Servers includes all the standard and requested options in the reply.

<28> Section 3.2.5.2: Administrative controls are implemented only by the Windows Server 2008 R2 DHCP server.

<29> Section 3.2.5.2: Windows DHCP 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.

<30> Section 3.2.5.2: Windows 2000, Windows Server 2003, and Windows Vista, DHCP servers send the Classless Static Route information to clients in Option 249, even if the client requests both option code 121 and option code 249. Windows Server 2008 and Windows Server 2008 R2 send 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.

<31> Section 3.2.5.3: Windows DHCP servers ignore the Vendor Class Option.

<32> Section 3.2.5.4: Administrative controls are implemented only by the Windows Server 2008 R2.

<33> Section 3.2.5.4: Windows Server sends one or more User Class Options depending on whether one or more User Classes are configured on the DHCP server.

<34> Section 3.2.5.5: Windows Server 2008 R2 DHCPv6 server sends one or more User Class Options depending on whether one or more User Classes are configured on the DHCPv6 server. DHCPv6 server on Windows Server 2008 does not support User Class Option.

<35> Section 3.2.5.5: Windows Server 2008 R2 DHCPv6 server sends one or more User Class Options depending on whether one or more User Classes are configured on the DHCPv6 server. DHCPv6 server on Windows Server 2008 does not support User Class Option.

<36> Section 3.3: DHCP server on Windows 2000 Server, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2 implement Rogue Detection.

<37> Section 3.3: An authorization check is performed after every one hour by default by DHCP server on Windows 2000 Server, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2. The time interval after which the authorization check should be done is configurable and the minimum time interval is 5 minutes.

<38> Section 3.3: The time interval after which the authorization check is done does not vary based on the authorization state of a DHCP server on Windows 2000 Server, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2.

<39> Section 3.3.1: Windows 2000 Server, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2 use Rogue Detection for authorization of a DHCP server which is not domain joined.

<40> Section 3.3.1: For Windows 2000 Server, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2, a DHCP server can be administratively authorized using the mechanism specified in Appendix B.

<41> Section 3.3.1: DHCP servers on Windows 2000 Server, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2 do not reply if there are no subnets configured on the DHCPv4 server.

<42> Section 3.3.1: DHCP servers on Windows 2000 Server, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2 do not reply if there are no subnets configured on the DHCPv4 server.

<43> Section 3.3.1: Windows 2000 Server, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2 waits for 2 seconds after sending **DHCPINFORM** message to receive **DHCPACK** messages when validating DHCP server authorization using Rogue Detection.

<44> Section 3.3.1: The maximum number of retries for sending **DHCPINFORM** message in Rogue Detection mechanism is 4 for DHCP servers on Windows 2000 Server, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2.

<45> Section 3.3.1: In Rogue Detection, after all retry attempts of sending **DHCPINFORM** message are exhausted, DHCP servers on Windows 2000 Server and Windows Server 2003 considers itself authorized. DHCP servers on Windows Server 2008 and Windows Server 2008 R2 continues validation using DHCPv6 Information-Request.

<46> Section 3.3.2: Windows 2000 Server, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2 use Rogue Detection for servers not domain joined.

<47> Section 3.3.2: A DHCP server can be administratively authorized using the mechanism specified in Appendix B for Windows 2000 Server, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2.

<48> Section 3.3.2: Windows 2000 Server, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2 DHCP servers reply even if there are no subnets configured on the DHCPv6 server.

<49> Section 3.3.2: Windows 2000 Server, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2 DHCP servers reply even if there are no subnets configured on the DHCPv6 server.

<50> Section 3.3.2: Windows 2000 Server, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2 wait 2 seconds after sending DHCPv6 INFORMATION-REQUEST message to receive DHCPv6 **Reply** messages when validating DHCP server authorization using Rogue Detection.

<51> Section 3.3.2: The maximum number of retries for sending DHCPv6 INFORMATION-REQUEST messages in Rogue Detection is 4 for Windows 2000 Server, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2 DHCP servers.

7 Appendix B: Administrative Authorization of Windows DHCP server

The information in this section is applicable to the following Microsoft products:

- Microsoft Windows® 2000 Server operating system
- Windows Server® 2003 operating system
- Windows Server® 2008 operating system
- Windows Server® 2008 R2 operating system

7.1 Windows DHCP Server Authorization in Domain Joined Scenario

A domain joined Microsoft Windows® server with DHCP server deployed can validate itself. Authorization mechanism of a DHCP server in a domain joined scenario is as follows:

- A domain joined DHCP server is authorized by a domain administrator in **Active Directory Domain Services (AD DS)**. Any DHCP server which is domain joined and is required to service DHCP clients must have an **AD** object in the Active Directory.
- The DHCP server validates its authorization in AD DS every hour. It uses **LDAP** protocol [MS-ADTS] for the purpose of communicating with the Active Directory and validating whether it is authorized to serve IP addresses.
- When installed in a multiple forest environment, DHCP servers seek authorization from within. Once authorized, DHCP servers in a multiple forest environment lease IP addresses to all reachable clients.

7.2 DHCP Server AD DS Path and Objects

A domain joined DHCP server is authorized in the Active Directory Domain Services (AD DS). The "DhcpRoot" object and <DHCP server name> objects, which are of type "dhcpClass" [MS-ADSC] are added in the AD DS. The attribute "dhcpServers" and other mandatory attributes of the class "dhcpClass" are also updated in the AD DS. The section below describes the "dHCPClass" objects, their attribute values in different conditions, and the containers in AD DS.

7.3 Active Directory Path for dhcpClass Objects

The **ADsPath** where the dHCPClass [MS-ADSC] objects are stored is:

"LDAP://<domain name>/CN=NetServices, CN=Services, CN=Configuration [,DC=<domain component1> [,DC=<domain component2>] …]"

Format of the "dhcpServers" attribute of "dHCPClass"

The "dhcpServers" [MS-ADA1] attribute of the "dHCPClass" object MUST be updated with the value defined below.

"i<server ip address>$rcn=<relative ADsPath Name>$f<flags>$s<server name>$"

The following table provides the specifics of the string.

Field	Description	Examples
server ip address	IPv4 address of the DHCP server which is being authorized	"57.60.41.211"
relative ADsPath Name	Relative LDAP Path name of the object in which the attribute "dhcpServer" is being updated.	"dhcpserver.contoso.com"
Flags	Unused field. This is set to 0.	0x00000000
server name	Server name of the DHCP server which is being authorized.	"dhcpserver.contoso.com"

The server ip address field takes an IPv4 address only. In an IPv6 scenario where the IPv4 is uninstalled or disabled, the DHCP server adds itself to the AD DS with the server name of the DHCPv6 server and a fixed IP address of 255.0.0.1.

The following table specifies the characters in the "dhcpServers" attribute value string.

Value	Meaning
L'$'	A field separator.
L'i'	Precedes an IP address.
L'r'	Precedes a relative AD Path.
L'f'	Precedes a flag entry
L's'	Precedes a server entry

7.4 Mandatory Attribute Values for the DHCPRoot Object

The mandatory attributes of the "dHCPClass" class SHOULD be updated with values mentioned below when creating a "DhcpRoot" object.

OBJECT ATTRIBUTES	Value
dhcpUniqueKey	0
dhcpType	0
dhcpIdentification	L"This is a server"
dhcpFlags	0
instanceType	0x04

7.5 Mandatory Attribute Values for the <DHCP server> Object

The mandatory attributes of the "dHCPClass" class SHOULD be updated with values mentioned below when creating a <Dhcp server> object.

OBJECT ATTRIBUTES	Value
dhcpUniqueKey	0

OBJECT ATTRIBUTES	Value
dhcpType	1
dhcpIdentification	L"DHCP Server Object"
dhcpFlags	0
instanceType	0x04

7.6 Unauthorization Filter

To unauthorize a DHCP server, the server object added in AD DS MUST be removed. The server object to be deleted is identified by the "dhcpServers" attribute value. The filter [MS-ADTS] required to identify the server object corresponding to the specific DHCP server is described below.

"(&(objectCategory=dHCPClass)(&(dhcpServers=i<server ip address>$*)(dhcpServers=*s<server name>$*)))"

7.7 Validation Filter

The filter [MS-ADTS] required to validate DHCP server authorization in AD DS is described below.

"(&(objectCategory=dHCPClass)(|(dhcpServers=i<server ip address>$*)(dhcpServers=*s<server name>$*)))"

7.8 Authorizing a DHCP Server in Active Directory Domain Services

A DHCP server that is domain joined is authorized by a domain administrator in the AD DS.

The authorization MUST first check to see if a "CN=DhcpRoot" object is present in the AD DS in the ADsPath.

If it is not found it MUST be created in the AD DS using the following:

- Object Relative Distinguished Name: CN= "DhcpRoot"
- Object Class: "dHCPClass" (defined in the AD schema [MS-ADSC])

When creating "DhcpRoot" object, the "dHCPClass" attributes SHOULD be updated.

Once the object "DhcpRoot" exists, a new object by the name of the DHCP server authorizing itself in AD DS MUST be created.

The LDAP ADsPath of the new object MUST be specified using the following:

- Object Distinguished Name = <server name>
- Object Class = "dHCPClass"

When creating DHCP server object to authorize in AD DS, the "dHCPClass" attributes SHOULD be updated.

The new server object attribute "dhcpServers" MUST be updated.

7.9 Unauthorizing a DHCP Server from Active Directory Domain Services

A DHCP server is unauthorized from AD DS when the "dHCPClass" object corresponding to the server is deleted from the AD DS.

The filter required to unauthorize a DHCP server MUST be based on its IP address and server name as specified above under section Unauthorization Filter.

This filter matches a "dHCPClass" object with the "dhcpServers" attribute matching "i<server ip address>$" and "s<server name>$". Only one such object matches the filter. Delete that object from the AD DS.

7.10 Validating DHCP Server Authorization in Active Directory Domain Services

A domain joined DHCP server verifies if it is authorized to service DHCP clients. It validates itself in AD DS.

A DHCP server MUST verify if the "DhcpRoot" object exists in the AD DS. If the object is not present, the server MUST work as a non-authorized DHCP server. A DHCP server MUST make a filter query to verify if it is authorized in the AD DS. If the query succeeds, the DHCP server is authorized, otherwise it is not.

The filter required to validate if a DHCP server is authorized MUST be based on a server IP address or server name.

This filter MUST match any "dHCPClass" objects with "dhcpServers" attribute matching "i<server IP address>$" or "s<server name>$".

8 Change Tracking

This section identifies changes that were made to the [MS-DHCPE] protocol document between the January 2011 and February 2011 releases. Changes are classified as New, Major, Minor, Editorial, or No change.

The revision class **New** means that a new document is being released.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements or functionality.
- An extensive rewrite, addition, or deletion of major portions of content.
- The removal of a document from the documentation set.
- Changes made for template compliance.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **Editorial** means that the language and formatting in the technical content was changed. Editorial changes apply to grammatical, formatting, and style issues.

The revision class **No change** means that no new technical or language changes were introduced. The technical content of the document is identical to the last released version, but minor editorial and formatting changes, as well as updates to the header and footer information, and to the revision summary, may have been made.

Major and minor changes can be described further using the following change types:

- New content added.
- Content updated.
- Content removed.
- New product behavior note added.
- Product behavior note updated.
- Product behavior note removed.
- New protocol syntax added.
- Protocol syntax updated.
- Protocol syntax removed.
- New content added due to protocol revision.
- Content updated due to protocol revision.
- Content removed due to protocol revision.
- New protocol syntax added due to protocol revision.

- Protocol syntax updated due to protocol revision.
- Protocol syntax removed due to protocol revision.
- New content added for template compliance.
- Content updated for template compliance.
- Content removed for template compliance.
- Obsolete document removed.

Editorial changes are always classified with the change type **Editorially updated.**

Some important terms used in the change type descriptions are defined as follows:

- **Protocol syntax** refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.
- **Protocol revision** refers to changes made to a protocol that affect the bits that are sent over the wire.

The changes made to this document are listed in the following table. For more information, please contact protocol@microsoft.com.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Change type
1.4 Relationship to Other Protocols	60187 Added the DHCPv4ServerMcastMibInfo element.	Y	Content updated.
3.2.5.16 Receiving a MADCAP DISCOVER Message	60187 Added section.	Y	New content added.
3.2.5.17 Receiving a MADCAP REQUEST Message	60187 Added section.	Y	New content added.
3.2.5.18 Receiving a MADCAP RENEW Message	60187 Added section.	Y	New content added.
3.2.5.19 Receiving a MADCAP RELEASE Message	60187 Added section.	Y	New content added.
3.2.5.20 Receiving a MADCAP GETINFO Message	60187 Added section.	Y	New content added.

9 Index