[MS-DHCPN]:
Dynamic Host Configuration Protocol (DHCP) Extensions for Network Access Protection (NAP)

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft's Open Specification Promise (available here: http://www.microsoft.com/interop/osp) or the Community Promise (available here: http://www.microsoft.com/interop/cp/default.mspx). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Revision Summary

Date	Revision History	Revision Class	Comments
12/18/2006	0.1		MCPP Milestone 2 Initial Availability
03/02/2007	1.0		MCPP Milestone 2
04/03/2007	1.1		Monthly release
05/11/2007	1.2		Monthly release
06/01/2007	1.2.1	Editorial	Revised and edited the technical content.
07/03/2007	1.2.2	Editorial	Revised and edited the technical content.
07/20/2007	1.2.3	Editorial	Revised and edited the technical content.
08/10/2007	2.0	Major	Updated and revised the technical content.
09/28/2007	3.0	Major	Updated and revised the technical content.
10/23/2007	4.0	Major	Updated and revised the technical content.
11/30/2007	4.0.1	Editorial	Revised and edited the technical content.
01/25/2008	4.0.2	Editorial	Revised and edited the technical content.
03/14/2008	4.0.3	Editorial	Revised and edited the technical content.
05/16/2008	4.0.4	Editorial	Revised and edited the technical content.
06/20/2008	4.0.5	Editorial	Revised and edited the technical content.
07/25/2008	4.1	Minor	Updated the technical content.
08/29/2008	4.1.1	Editorial	Revised and edited the technical content.
10/24/2008	4.1.2	Editorial	Revised and edited the technical content.
12/05/2008	4.2	Minor	Updated the technical content.
01/16/2009	4.2.1	Editorial	Revised and edited the technical content.
02/27/2009	4.2.2	Editorial	Revised and edited the technical content.
04/10/2009	4.2.3	Editorial	Revised and edited the technical content.
05/22/2009	4.2.4	Editorial	Revised and edited the technical content.
07/02/2009	4.2.5	Editorial	Revised and edited the technical content.
08/14/2009	4.2.6	Editorial	Revised and edited the technical content.
09/25/2009	4.3	Minor	Updated the technical content.

Date	Revision History	Revision Class	Comments
11/06/2009	4.3.1	Editorial	Revised and edited the technical content.
12/18/2009	4.3.2	Editorial	Revised and edited the technical content.
01/29/2010	4.4	Minor	Updated the technical content.
03/12/2010	4.4.1	Editorial	Revised and edited the technical content.
04/23/2010	4.4.2	Editorial	Revised and edited the technical content.
06/04/2010	4.4.3	Editorial	Revised and edited the technical content.
07/16/2010	5.0	Major	Significantly changed the technical content.
08/27/2010	5.0	No change	No changes to the meaning, language, or formatting of the technical content.
10/08/2010	5.0	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	5.1	Minor	Clarified the meaning of the technical content.
01/07/2011	5.2	Minor	Clarified the meaning of the technical content.
02/11/2011	6.0	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 reduce the administrative burden and complexity of configuring hosts on a **Transmission Control Protocol**/Internet Protocol (TCP/IP)–based network, such as a private intranet.

Network Access Protection (NAP) is a platform that enables an administrator to validate a machine's health before granting it access to the network. It provides for multiple enforcement mechanisms to validate the client's configuration, limit a client's network access, and enable a client to update itself while it has limited connectivity so that it can regain full network access. NAP allows multiple enforcement methods and also provides for new enforcement methods to be developed by different vendors.

This document specifies a set of vendor-class options defined for use by **DHCP clients** and **DHCP servers** to support NAP enforcement through DHCP.

1.1 Glossary

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

Dynamic Host Configuration Protocol (DHCP) client
Dynamic Host Configuration Protocol (DHCP) server
health policy server
Internet Protocol version 4 (IPv4)
Internet Protocol version 6 (IPv6)
little-endian
network byte order
statement of health (SoH)
Transmission Control Protocol (TCP)

The following terms are specific to this document:

Network Access Protection (NAP): A platform that implements system health-validated access in private networks. **NAP** provides a way to detect the health state of a host that is attempting to connect to (or communicate on) a network and to limit the network access of the client until the health policy requirements are met.

Network Access Protection (NAP) agent: A component that maintains the current health state information of the host on which the component is running.

Network Access Server (NAS): A computer server that provides an access service for a user to a network. An **NAS** operates as a client of Remote Authentication Dial-In User Service (RADIUS). The RADIUS client is responsible for passing user information to designated RADIUS servers and then acting on the response returned by the RADIUS server. Examples of an **NAS** include a VPN server, a wireless access point, an 802.1x-enabled switch, and a **NAP** server.

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.

[MS-DHCPE] Microsoft Corporation, "Dynamic Host Configuration Protocol (DHCP) Extensions", March 2007.

[MS-DHCPM] Microsoft Corporation, "Microsoft Dynamic Host Configuration Protocol (DHCP) Server Management Protocol Specification", January 2008.

[MS-RNAP] Microsoft Corporation, "Vendor-Specific RADIUS Attributes for Network Access Protection (NAP) Data Structure", January 2007.

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

[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

[RFC2463] Conta, A., and Deering, S., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", December 1998, http://www.ietf.org/rfc/rfc2463.txt

[RFC2865] Rigney, C., Willens, S., Rubens, A., and Simpson, W., "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000, http://www.ietf.org/rfc/rfc2865.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

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

1.2.2 Informative References

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

[MSDN-CoCreateGuid] Microsoft Corporation, "CoCreateGuid", http://msdn.microsoft.com/en-us/library/ms688568.aspx

[MSDN-DHCP] Microsoft Corporation, "Dynamic Host Configuration Protocol", http://technet.microsoft.com/en-us/network/bb643151.aspx

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

1.3 Overview

For more information about NAP, see [MSDN-NAP]. The DHCP process is as specified in [RFC2131]. For more information, see [MSDN-DHCP].

A synopsis of the basic DHCP messages used by a client to acquire a network address is specified in [MS-DHCPE] section 1.3.

This section provides a synopsis of NAP enforcement using DHCP. It illustrates how a client can send system health information to a DHCP server and can be granted either restricted or normal access to the network, based on its health state.

1. If DHCP NAP enforcement has been enabled on the client, the DHCP client sends a NAP **Statement of Health** (NAP-SoH (section 2.2.1.1)) option, of length 1 and data equal to 0 in a **DHCPDISCOVER** message to determine whether the DHCP server has NAP enabled.

2. If the DHCP server has NAP enabled, it is expected to include in its **DHCPOFFER** message a NAP-SoH option of length 3 with data as "NAP" to indicate to the client that the server supports DHCP NAP enforcement.

3. If NAP is enabled for DHCP on the DHCP client, in the **DHCPDISCOVER** message the client will send option 43 in the Parameter request list as well as Vendor-Specific option 43 containing the NAP-CoID (option 222). It will also include option 220 containing the text "Is NAP enabled", within Vendor-Specific option 43. If a server that is NAP enabled receives a **DHCPDISCOVER** message including option 22, containing the text "Is NAP enabled", then it will indicate that the server supports NAP by responding with a **DHCPOFFER** including option 220, containing the text "NAP" inside Vendor-Specific option 43. The client then selects an offer from one of the DHCP servers that responded (typically the first offer received). If the **DHCPOFFER** message corresponding to the selected server indicated that the server is NAP enabled, then the client can send a **DHCPREQUEST** message to the selected server, containing the SoH in the NAP-SoH option by utilizing option 220 encapsulated inside Vendor-Specific option 43. If the client selects a server that does not support NAP, the **DHCPREQUEST** message cannot contain Vendor-Specific option 43.

4. The DHCP server sends the SoH token received from the client to the **health policy server** for validation. To accomplish validation, the DHCP server can use the Remote Authentication Dial-In User Service (RADIUS) [RFC2865], using Microsoft RADIUS Attributes for Network Access Protection [MS-RNAP]. If the client is found to be compliant with the policies, the health policy server informs the DHCP server that responds with the network configuration options, as usual, and includes an appropriate SoH-Response (obtained from the health policy server) in the DHCP acknowledgment (**DHCPACK**) message. If the client is not compliant with the health policies, the DHCP server tells the client to quarantine itself by sending it a default gateway (DHCP option 3, the router option, as specified in [RFC2132] section 3.5) of 0.0.0.0, a subnet mask (DHCP option 1, as specified in [RFC2132] section 3.3) of 255.255.255.255, and a Classless Static Route option (as specified in [MS-DHCPE]) that contains the static routes to the NAP remediation servers.

A client that has been quarantined due to noncompliance with the administrator-defined health policies is expected to remedy its health state and trigger a DHCP Renew. In this event, the client sends its updated SoH to the DHCP server as part of the Renew transaction. If the client is found to be compliant with the health policy, the DHCP server grants the client normal network access by sending the default configuration values for the default gateway and the subnet mask.

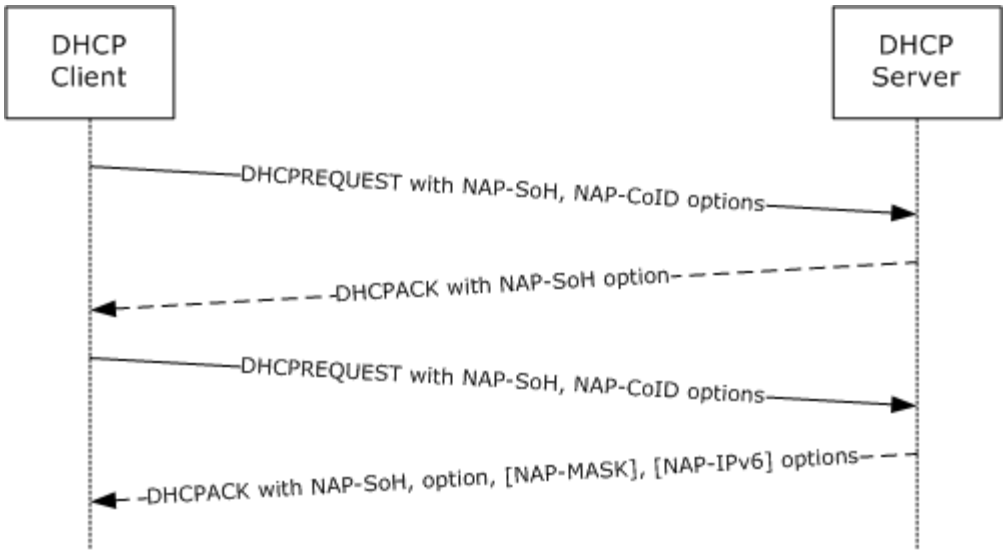


Figure 1: Client request attempt to remedy quarantine state

1.4 Relationship to Other Protocols

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

To use the vendor-specific options for DHCP NAP enforcement, support for the extensions defined in [MS-DHCPE] is required by both the DHCP server and the DHCP client. The relationship between the DHCP protocol elements and the shared ADM elements from [MS-DHCPM] (see [MS-DHCPE] section 1.4) also applies to servers that implement DHCP NAP enforcement.

A DHCP server would typically use these extensions in conjunction with RADIUS [RFC2865] and the Microsoft RADIUS Attributes for Network Access Protection [MS-RNAP], although these extensions do not depend on such. DHCP NAP enforcement can be configured on a DHCP server by using mechanisms specified in [MS-DHCPM] sections 3.1.4.42 through 3.1.4.51. The following is the relationship between [MS-DHCPM]-shared ADM elements and this protocol:

1. DHCP NAP enforcement can be disabled or enabled for a NAP-capable DHCP server by modifying the **DHCPv4ServerConfigInfo.QuarantineOn** element, which is a shared element (see [MS-DHCPM] section 3.1.1.1).
2. If DHCP NAP enforcement is enabled for a NAP-capable DHCP server as described above, it can further be overridden for a specific subnet (selected per [MS-DHCPM] section 1.4 point 1) by modifying the **DHCPv4Scope.ScopeInfo.QuarantineOn** element, which is a shared element (see [MS-DHCPM] section 3.1.1.2).
3. If the DHCP server is able to initialize the local health policy server, it will set the **DHCPv4ServerConfigInfo.QuarRuntimeStatus** element, which is a shared element (see [MS-DHCPM] section 3.1.1.1), to TRUE; else it will set it to FALSE. The value of this element being FALSE indicates that NAP is not enabled at runtime on the DHCP server despite being administratively enabled.

4. Upon processing DHCPREQUEST messages (elaborated in section 3.2.5.2), the DHCP server will update the corresponding **DHCPv4Client** elements, which are shared elements (see [MS-DHCPM] section 3.1.1.7), with information about the client's NAP capability (**DHCPv4Client.QuarantineCapable**), current NAP status (**DHCPv4Client.QuarantineStatus**), and the end time of probation if the client is on probation (**DHCPv4Client.ProbationEnds**).

The following diagram illustrates the layering of the protocol in this section with other protocols in its stack.

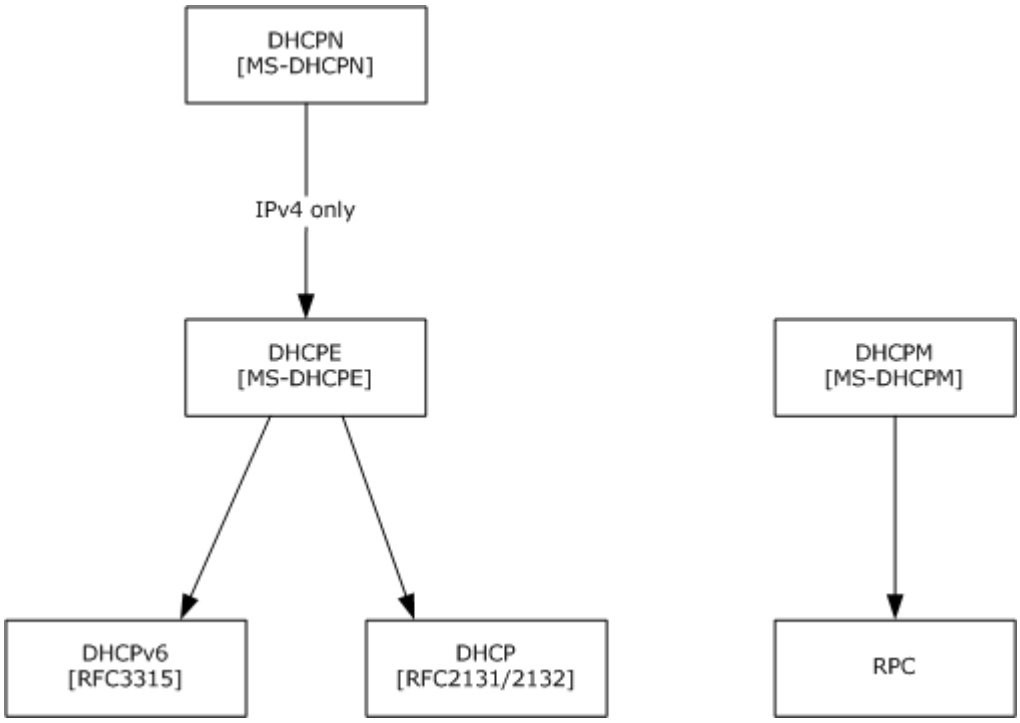


Figure 2: Protocol layering diagram

It may be noted that the current protocol is only implemented using DHCPv4 options and therefore only extends the IPv4-specific functionality of [MS-DHCPE].

The following data flow diagram illustrates the interaction of the server implementation of this protocol with those of other protocols in its stack.

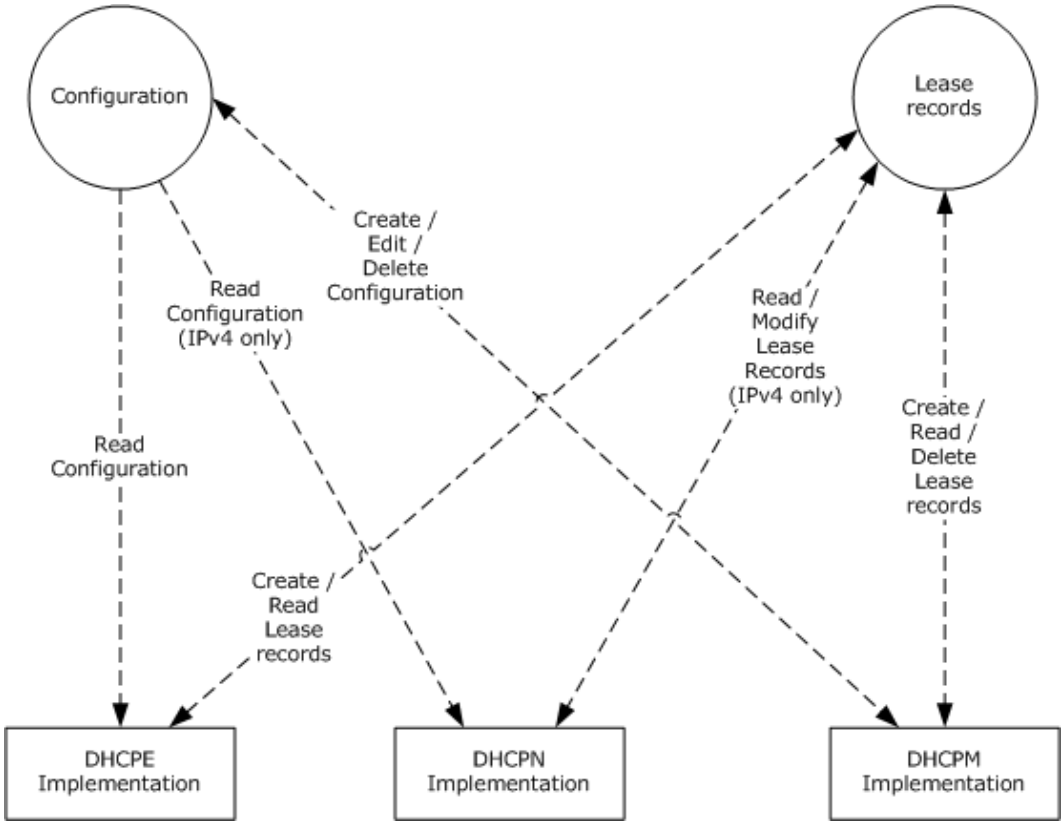


Figure 3: Server-side interaction with related protocols

1.5 Prerequisites/Preconditions

None.

1.6 Applicability Statement

The use of DHCP vendor-specific options for NAP is applicable in environments where DHCP is applicable and where security is not a strict requirement.

1.7 Versioning and Capability Negotiation

The DHCP vendor-specific options used by NAP are not versioned.

DHCP servers and clients identify these vendor-specific options as being DHCP NAP options through the presence of a Vendor Class Identifier option as specified in [MS-DHCPE] section 2.2.3.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.

2 Messages

2.1 Transport

All DHCP extensions used by NAP are transported within DHCP, as specified in [RFC2131] section 4.1 (for DHCPv4).

2.2 Message Syntax

The DHCP extensions used by NAP follow the message format defined for vendor-specific options, as specified in [RFC2132] section 8.4 and [RFC3925] section 6.

All multibyte option fields and values described in this specification are defined to be in **network byte order** unless indicated otherwise.

2.2.1 DHCP Option Code 43 (Microsoft Vendor-Specific Options)

DHCP clients and servers supporting NAP use DHCP vendor-specific options for exchanging NAP-specific information through DHCP. These vendor-specific options MUST be sent as vendor-specific extensions as part of DHCP option 43, as specified in [RFC2132] section 8.4.

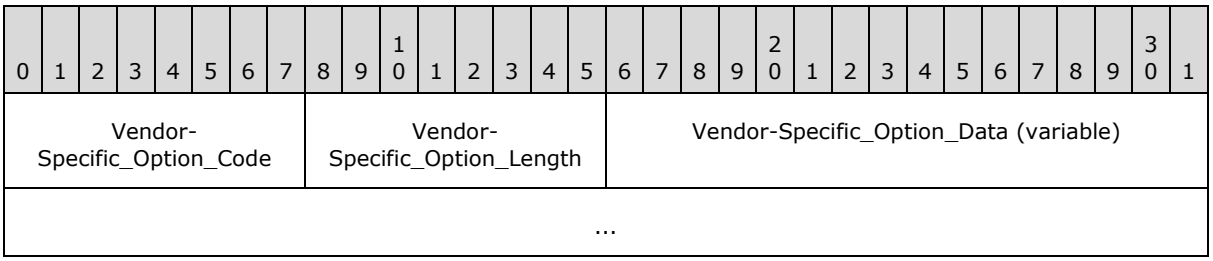
The Microsoft Encoding Long Options Packet, specified in [MS-DHCPE] section 2.2.9, MUST be used when the cumulative size of all the vendor-specific options being sent in a message exceeds 255 bytes.

2.2.1.1 NAP-SoH Option

The NAP-SoH vendor-specific option encapsulates the SoH token for transmission to the DHCP server. This option is also used to determine whether the DHCP server is NAP-capable.

This vendor-specific option MUST be encapsulated inside option 43, as specified in [RFC2132] section 8.4.

The NAP-SoH option is defined as follows.



Vendor-Specific_Option_Code (1 byte): This MUST be 0xDC.

Vendor-Specific_Option_Length (1 byte): Length in bytes of the **Vendor-Specific_Option_Data** field.

Vendor-Specific_Option_Data (variable): This MUST contain one of the following:

No Data: A NAP-SoH option of **Vendor-Specific_Option_Length** zero is sent by the client in the **DHCPDISCOVER** message to determine whether NAP is enabled on the server. However, Vendor-Specific Option 43 never has a length of zero. In the **DHCPDISCOVER** message, the Vendor-Specific Option 43 has a length of 134, containing Option 222 for NAP-CoID, whose

length is 130, and Option 220, whose length is 0. Option 220 with a length of 0 is included by the client in order to probe whether NAP is enabled on the server.

Zero of length 1: One byte with value 0x00 sent by the client in **DHCPREQUEST** or **DHCPINFORM** messages to check whether NAP has been enabled on the server.

Data of length 3: With data as string "NAP" in network byte order, sent by the server in **DHCPOFFER** or **DHCPACK** messages to indicate to the client that NAP is enabled on the server.

System SoH: Binary data of variable length, as defined in [MS-SOH], representing the client's health state, sent by the client in **DHCPREQUEST** messages.

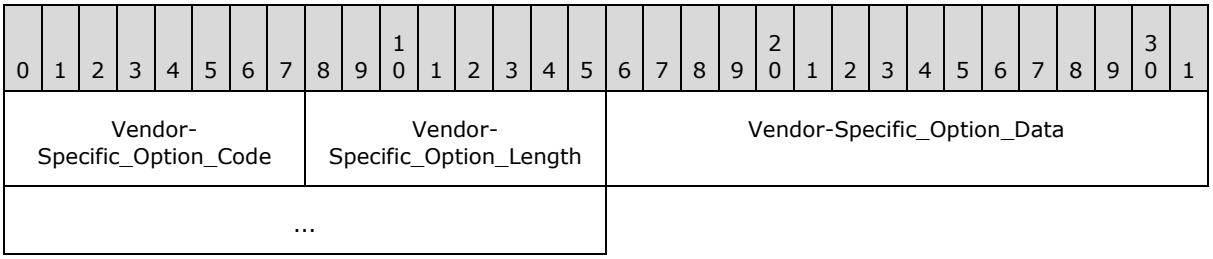
SoH-Response: Binary data of variable length, as defined in [MS-SOH], representing the client's quarantine state, sent by the server in **DHCPACK** messages.

2.2.1.2 NAP-Mask Option

If the DHCP server determines that the DHCP client must be quarantined, it overrides the administrator-configured **IPv4** subnet mask for that subnet and instead sends 255.255.255.255 as the subnet mask in DHCP option 1 (as specified in [RFC2132] section 3.3). In this case, the original subnet mask configured by the administrator MUST be sent as a vendor-specific option to the client in **little-endian** byte order. The original subnet mask MAY be used by clients that do not support classless static routes and that rely on the DHCP Static Route option defined in [RFC2132] for their routing information.<1>

This vendor-specific option MUST be encapsulated inside option 43, as specified in [RFC2132] section 8.4.

The NAP Subnet Mask (NAP-Mask) option is defined as follows.



Vendor-Specific_Option_Code (1 byte): This MUST be 0xDD.

Vendor-Specific_Option_Length (1 byte): This MUST be 0x04.

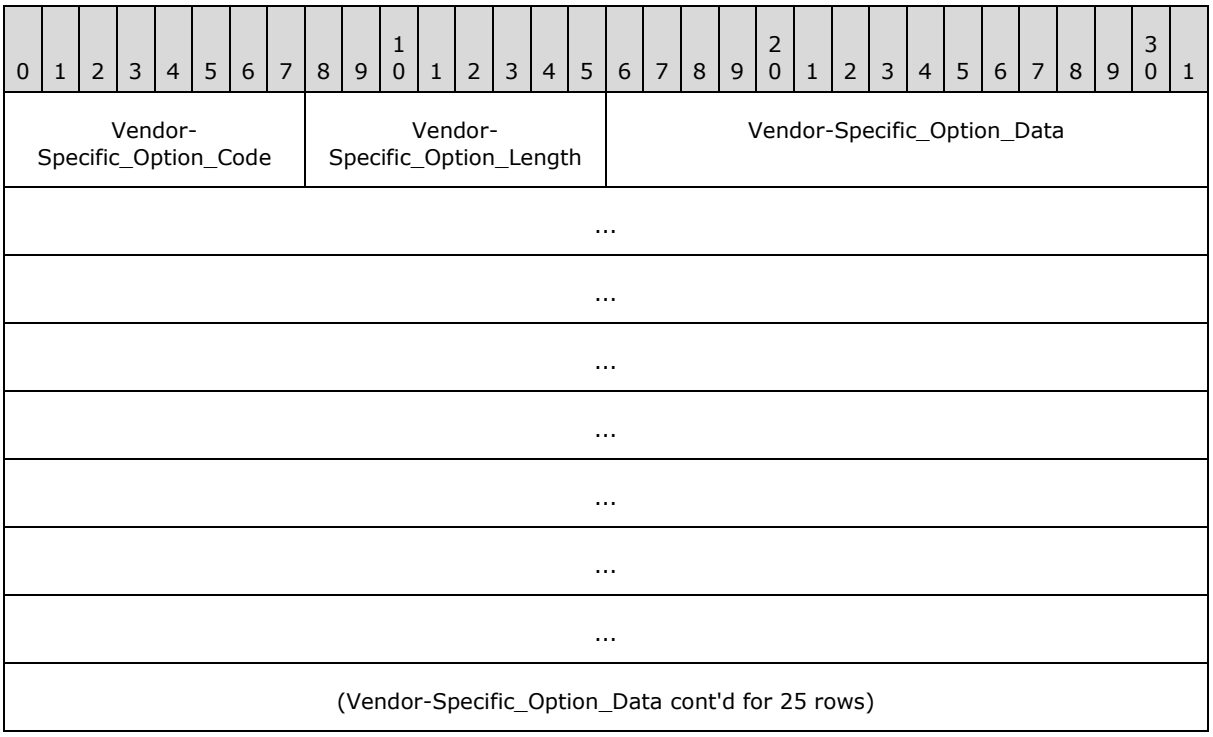
Vendor-Specific_Option_Data (4 bytes): Subnet mask in little-endian byte order.

2.2.1.3 NAP-CoID Option

This vendor-specific option is sent by a DHCP client if NAP has been enabled on it. It is used to send a randomly generated correlation ID generated by the client to the DHCP server to enable end-to-end correlation of NAP transactions between a DHCP client and a DHCP server. (This correlation ID is used only for logging.)

This vendor-specific option is encapsulated inside option 43, as specified in [RFC2132] section 8.4.

The NAP Correlation ID (NAP-CoID) option is defined as follows.



Vendor-Specific_Option_Code (1 byte): This MUST be 0xDE.

Vendor-Specific_Option_Length (1 byte): This MUST be 0x82.

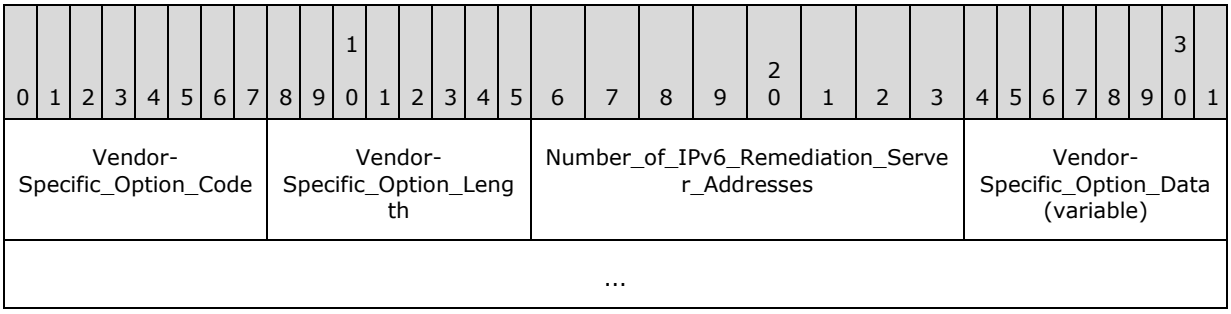
Vendor-Specific_Option_Data (130 bytes): Binary data representing a correlation ID that SHOULD<2> be generated randomly.

2.2.1.4 NAP-IPv6 Option

This vendor-specific option is used to send a list of **IPv6** addresses of NAP remediation servers that the DHCP client can access while it is quarantined.

This vendor-specific option MUST be encapsulated inside option 43, as specified in [RFC2132] section 8.4.

The NAP IPv6 Remediation Server List (NAP-IPv6) option is defined as follows.



Vendor-Specific_Option_Code (1 byte): This MUST be 0xDF.

Vendor-Specific_Option_Length (1 byte): If nonzero, the value is calculated as (N*16 + 1) bytes, where N is the number of IPv6 remediation-server addresses. An option length of zero also indicates zero IPv6 remediation server addresses.

Number_of_IPv6_Remediation_Server_Addresses (1 byte): The number of NAP IPv6 remediation server addresses.

Vendor-Specific_Option_Data (variable): IPv6 addresses of NAP remediation servers in network byte order.

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

This section specifies the user class that is used for NAP.

DHCP servers that support NAP have the "Default Network Access Protection Class" user class with value "MSFT Quarantine" predefined on them (see [MS-DHCPM] section 3.1.1.8).

The format for the User Class option used by clients and servers implementing this specification is defined in [RFC3004] and in [MS-DHCPE] section 2.2.6.

3 Protocol Details

3.1 Client Details

This section specifies the DHCP NAP client behavior.

3.1.1 Abstract Data Model

See section 3.3.1 for common details.

In addition, DHCP clients implementing this specification are required to track the following state:

NAP-Capable Server: State indicating whether the DHCP server with which the client is communicating has NAP Enforcement enabled on it. This information is used to determine whether NAP-specific information should be exchanged with that server in message exchanges. Possible values are "Unknown", "Yes", and "No".

3.1.2 Timers

There are no timers beyond those in [MS-DHCPE] section 3.1.2.

3.1.3 Initialization

See [MS-DHCPE] section 3.1.3 for DHCP client initialization.

3.1.4 Higher-Layer Triggered Events

See [MS-DHCPE] section 3.1.4 for the higher-layer triggered events for the DHCP client.

If DHCP enforcement is enabled for NAP on a DHCP client, the client MUST also trigger a **DHCPDISCOVER** or a DHCP Renew transaction as appropriate whenever the system health state or configuration changes. Due to the vulnerability of DHCP, DHCP clients SHOULD NOT attempt to use NAP on unauthenticated wireless networks.

3.1.4.1 Creating and Transmitting a DHCPDISCOVER Message

Whenever a DHCP client sends a **DHCPDISCOVER** message, the DHCP client implementing this specification MUST indicate its capability to the DHCP server by sending the SoH vendor-specific option with length equal to zero. It MUST also include a NAP-CoID option (section 2.2.1.3) in this message.

In addition, it MUST set its NAP-Capable Server state to "Unknown".

3.1.4.2 Creating and Transmitting a DHCPREQUEST Message During Lease Renewal

Whenever a DHCP client sends a **DHCPREQUEST** message during DHCP lease renewal and its NAP-Capable Server state is set to "Unknown", it MUST include the NAP-SoH (section 2.2.1.1) option of length one octet and data equal to zero in the **DHCPREQUEST** message. It MUST also include a NAP-CoID (section 2.2.1.3) option in this message.

If instead the NAP-Capable Server state is set to "Yes", it MUST retrieve the updated SoH from the **NAP agent** and send the SoH token in the NAP-SoH option in the **DHCPREQUEST** message as specified in section 2.2.1.1. It MUST also include a NAP-CoID option in this message.

If instead the NAP-Capable Server state is set to "No", it MUST send the message without any options defined in this document.

3.1.4.3 Creating and Transmitting a DHCPINFORM Message

Whenever a DHCP client sends a **DHCPINFORM** message and its NAP-Capable Server state is set to "Unknown", it MUST include the NAP-SoH (section 2.2.1.1) option of length one octet and the data equal to zero in the **DHCP INFORMATION-REQUEST (DHCPINFORM)** message. It MUST also include a NAP-CoID (section 2.2.1.3) option in this message.

If instead the NAP-Capable Server state is set to "Yes", it MUST retrieve the updated SoH from the NAP agent and send the SoH token in the NAP-SoH option in the **DHCPINFORM** message as specified in section 2.2.1.1. It MUST also include a NAP-CoID option in this message.

If instead the NAP-Capable Server state is set to "No", it MUST send the message without any options defined in this document.

3.1.5 Processing Events and Sequencing Rules

DHCP message processing is specified in [MS-DHCPE] section 3.1.5, with additional behavior specified in the following sections.

3.1.5.1 Receiving a DHCPOFFER Message

If the **DHCPOFFER** message from the DHCP server contains a NAP-SoH (section 2.2.1.1) option with length equal to 3 and value equal to the string "NAP", the client MUST set its NAP-Capable Server state to "Yes". In addition, the client MUST send the SoH token in the NAP-SoH option in the **DHCPREQUEST** message as specified in section 2.2.1.1. It MUST also include a NAP-CoID (section 2.2.1.3) option in this message.

Otherwise, the client MUST set its NAP-Capable Server state to "No" and send the **DHCPREQUEST** message without any of the options defined in this document.

3.1.5.2 Receiving a DHCPACK Message in Response to a DHCPREQUEST Message During New Lease Acquisition

If the client has its NAP-Capable Server state set to "Yes" and it receives a **DHCPACK** message that contains a NAP-SoH (section 2.2.1.1) option from the DHCP server, the DHCP client MUST extract the SoH-Response from the NAP-SoH option and pass that to the NAP agent. If the SoH-Response indicates that the client is being quarantined and the NAP-IPv6 option is present in the message, the client MUST extract the addresses of the IPv6 Remediation servers from the NAP-IPv6 option and block (in an implementation-specific<3> way) all inbound and outbound IPv6 traffic on the network interface on which the DHCP message was received except ICMPv6 [RFC2463] and DHCPv6 [RFC3315] traffic and traffic to and from the IPv6 Remediation server addresses. If the client is being quarantined and the NAP-IPv6 option is not present in the message, the client MUST block (in an implementation-specific<4> way) all IPv6 traffic except ICMPv6 and DHCPv6 traffic on the network interface on which the DHCP message was received. If the client is not being quarantined, any NAP-IPv6 option MUST be ignored. (Note that IPv4 is handled through standard behavior of the Router option and the Subnet Mask option as defined in [RFC2132] and the Microsoft Classless Static Route option as defined in [MS-DHCPE] and as discussed in section 3.2.5.2.1; hence only additional behavior for IPv6 is required here.)

If the client has its NAP-Capable Server state set to "Yes" and the **DHCPACK** message NAP-SoHreceived from the DHCP server does not contain an option, the DHCP client MUST process the

message as described in the preceding paragraph as if it contained a NAP-SoH option with **Vendor-Specific_Option_Length** set to zero.

If the client has its NAP-Capable Server state set to "No", the client MUST process the **DHCPACK** message as if none of the options defined in this specification were present in the message.

3.1.5.3 Receiving a DHCPACK Message in Response to a DHCPINFORM Message

If the DHCP client's NAP-Capable Server state is set to "Unknown" and the client receives from the server a **DHCPACK** message that contains the NAP-SoH (section 2.2.1.1) option of length 3 and data as the string "NAP", it MUST set its NAP-Capable Server state to "Yes". In addition, the client MUST discard the **DHCPACK** message and retransmit the **DHCPINFORM** message as specified in section 3.1.4.3. Otherwise, the client MUST set its NAP-Capable Server state to "No" and process the remainder of the **DHCPACK** message as it normally would in the absence of NAP.

If the DHCP client's NAP-Capable Server state is set to "Unknown" and the client receives a **DHCPACK** message from the server that does not contain the NAP-SoH option of length 3 and the data as string "NAP", the client MUST set its NAP-Capable Server state to "No" and process the rest of the message as if none of the options defined in this specification were present in the message.

Otherwise, the message SHOULD be processed as specified in section 3.1.5.2; the client MAY instead ignore the NAP-SoH option and the NAP-IPv6 (section 2.2.1.4) option (if any) and process the message as if they were not present in the message.

3.1.5.4 Receiving a DHCPACK Message in Response to a DHCPREQUEST Message During Lease Renewal

If the DHCP client's NAP-Capable Server state is set to "Unknown" and the client receives from the server a **DHCPACK** message that contains the NAP-SoH (section 2.2.1.1) option of length 3 and data as the string "NAP", it MUST set its NAP-Capable Server state to "Yes". In addition, the client MUST discard the **DHCPACK** message and retransmit the **DHCPREQUEST** message as specified in section 3.1.4.2. Otherwise, the client MUST set its NAP-Capable Server state to "No" and process the remainder of the **DHCPACK** message as it normally would in the absence of NAP.

If the client has its NAP-Capable Server state set to "Unknown" and the client receives from the server a **DHCPACK** message that does not contain the NAP-SoH option of length 3 and data as the string "NAP", the client MUST set its NAP-Capable Server state to "No" and process the rest of the message as if none of the options defined in this specification were present in the message.

Otherwise, the message MUST be processed as specified in section 3.1.5.2.

3.1.6 Timer Events

See section 3.3.6.

3.1.7 Other Local Events

None.

3.2 Server Details

This section specifies the DHCP NAP server behavior.

3.2.1 Abstract Data Model

See section 3.3.1 for the common Abstract Data Model.

This protocol includes the following ADM elements, which are directly accessed from [MS-DHCPM] as specified in [MS-DHCPM] section 3.1.1:

- DHCPv4ServerConfigInfo.QuarantineOn
- DHCPv4ServerConfigInfo.QuarRuntimeStatus
- DHCPv4ServerConfigInfo.QuarDefFail
- DHCPv4Scope.QuarantineOn
- DHCPv4Client.QuarantineCapable
- DHCPv4Client.QuarantineStatus
- DHCPv4Client.ProbationEnds

3.2.2 Timers

None.

3.2.3 Initialization

None.

3.2.4 Higher-Layer Triggered Events

None.

3.2.5 Processing Events and Sequencing Rules

DHCP message processing is specified in [MS-DHCPE] section 3.2.5, with additional behavior specified in the following sections.

3.2.5.1 Receiving a DHCPDISCOVER Message

When a DHCP server that is NAP-enabled (determined per section 1.4 points 1 and 2) receives an SoH vendor-specific option with length equal to one octet and data equal to zero, the DHCP server MUST respond with a DHCPOFFER message that contains a NAP-SoH (section 2.2.1.1) option with length equal to 3 and value equal to "NAP".

3.2.5.2 Receiving a DHCPREQUEST Message

When a DHCP server receives a DHCPREQUEST message, it processes it as specified in [RFC2131] section 4.3.2. As specified there, the presence of a "server identifier" option indicates a new lease acquisition, and the absence of one indicates a lease renewal.

3.2.5.2.1 Receiving a DHCPREQUEST Message for New Lease Acquisition

If the DHCPREQUEST contains a user class option with value "MSFT Quarantine" (see [MS-DHCPM] section 3.1.1.8), that request is considered exempt from quarantine, no further NAP processing is performed on the message, and it is processed per [MS-DHCPE] section 3.2.5.

If the message from the client contained the SoH token in a NAP-SoH (section 2.2.1.1) option, a DHCP server that is NAP-enabled (determined per section 1.4 points 1 and 2) SHOULD extract the SoH token sent by the DHCP client in the message, pass it to the health policy server for validation, and include the SoH-Response received from the health policy server in response to the client in the NAP-SoH option in the DHCPACK message. The SoH-Response can contain information as to whether the client has normal access to the network or whether the client has been quarantined, as specified in [MS-SOH].

If the SoH-Response from the health policy server indicates that the client request should be rejected, the incoming DHCPREQUEST message is not processed any further and no response is sent to the DHCP client.

If the SoH-Response from the health policy server indicates that the client is noncompliant with the NAP health policies, the DHCP server MUST ignore the user class value sent by the client and instead use the default NAP user class. That is, the network configuration options sent to the client MUST be selected from the default NAP user class (instead of the default user class or the client-provided user class). In addition, it overrides three option values. The Router option (DHCP option 3, as specified in [RFC2132] section 3.3) MUST be set to the value 0.0.0.0, and the Subnet Mask option (DHCP option 1, as specified in [RFC2132] section 3.3) MUST be set to the value 255.255.255.255. The Microsoft Classless Static Route option (as specified in [MS-DHCPE]) MUST be configured with static routes to the IPv4 addresses of the NAP remediation servers. Also, if the DHCP client is being quarantined, the DHCP server SHOULD include the NAP-Mask (section 2.2.1.2) option, and it MUST include the IPv6 addresses of the NAP remediation servers in the NAP-IPv6 (section 2.2.1.4) option if configured to do so on the server. If there are no IPv6 addresses of the NAP remediation servers, the DHCP server SHOULD NOT include the NAP-IPv6 option in the message.

If the DHCP server is unable to get a response from the health policy server (for example, if no response is received from the RADIUS server [RFC2865]), the processing will happen as configured in the **DHCPv4ServerConfigInfo.QuarDefFail** element, which is a shared element (see [MS-DHCPM] section 3.1.1.1). If the value of this element is set to NOQUARANTINE, the client will have normal access to the network. If the value is set to DROPPACKET, the behavior is the same as if the health policy server indicated that the client request should be rejected. If the value is set to RESTRICTEDACCESS, the client will be considered noncompliant with the NAP health policies.

3.2.5.2.2 Receiving a DHCPREQUEST Message During Lease Renewal

If the message from the client contains the NAP-SoH (section 2.2.1.1) option of length equal to one octet and with data equal to zero, a server that is NAP-enabled (determined per section 1.4 points 1 and 2) MUST respond with a DHCPACK message containing the NAP-SoH option of length 3 and data as the string "NAP". The remaining options in the DHCPACK message SHOULD be the same as would be sent to a client that is not capable of supporting NAP.

Otherwise, the message MUST be processed as specified in section 3.2.5.2.1.

3.2.5.3 Receiving a DHCPINFORM Message

The DHCPINFORM message SHOULD<5> be processed as specified in section 3.2.5.2.2; a DHCP server that is NAP-enabled (determined per section 1.4 points 1 and 2) MAY instead respond back to a DHCPINFORM message from the client containing the SoH token in the NAP-SoH option with a DHCPACK message containing a NAP-SoH option containing the non-null-terminated string "NAP" of length 3 in network byte order.

3.2.6 Timer Events

None.

3.2.7 Other Local Events

None.

3.3 Common Details

3.3.1 Abstract Data Model

The DHCP extensions for NAP adhere to the RFC standards as specified in [RFC2131] and [RFC2132]. The state machine and data model are defined in [RFC2131] section 4.4.

3.3.2 Timers

There are no timers beyond those specified in [MS-DHCPE].

3.3.3 Initialization

The DHCP extensions for NAP adhere to the RFC standards for initialization, as specified in [RFC2131] and [RFC2132].

3.3.4 Higher-Layer Triggered Events

Events that can trigger DHCP transactions are specified in [MS-DHCPE] section 3.1.4.

3.3.5 Processing Events and Sequencing Rules

The nonstandard mechanism for encoding long options using option 250, as specified in [MS-DHCPE], MUST be used during the exchange of any Microsoft vendor-specific NAP options if the length of the data to be sent exceeds 255 bytes.

3.3.6 Timer Events

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

3.3.7 Other Local Events

None.

4 Protocol Examples

The DHCP extensions for NAP adhere to the RFC standards for protocol exchanges as specified in [RFC2131] and [RFC2132].

This section explains the DHCP message exchanges between DHCP clients and DHCP servers for DHCP NAP enforcement.

4.1 Message Exchanges During New Lease Acquisition

A DHCP transaction for acquiring a new IP address that involves NAP enforcement starts with the **DHCPDISCOVER** message as described in section 3.1.4.1. The following figure represents such a transaction.

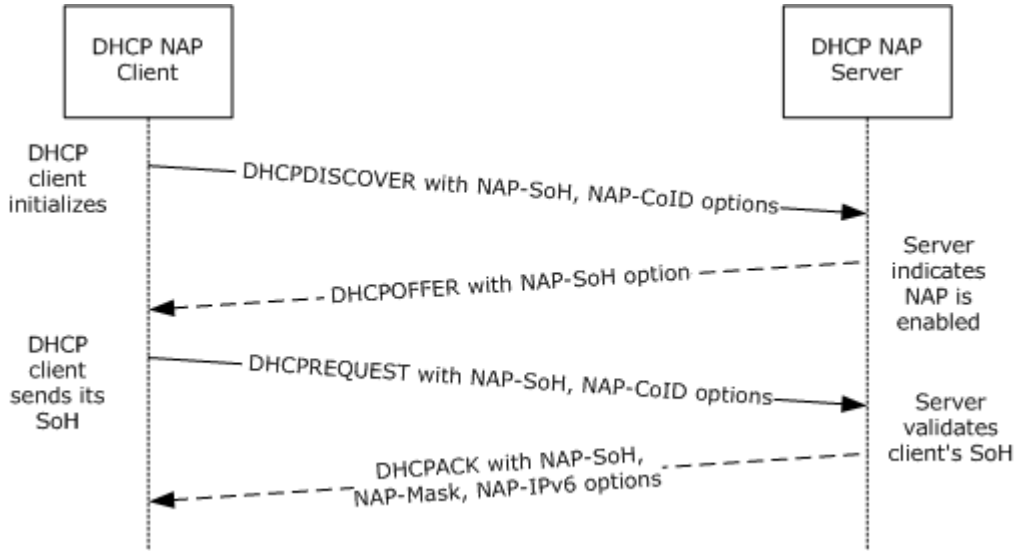


Figure 4: DHCP new lease acquisition process

The subsequent messages between the client and the server include the **DHCPOFFER**, **DHCPREQUEST**, and **DHCPACK** messages. (See sections 3.1.5.1, 3.1.5.2, 3.2.5.1, and 3.2.5.2.)

4.2 Message Exchanges During DHCP Information Request

A DHCP transaction for acquiring IP configuration options that involves NAP enforcement consists of the **DHCPINFORM** and **DHCPACK** messages as specified in sections 3.1.4.3, 3.1.5.3, and 3.2.5.3. The following figure demonstrates such a transaction.

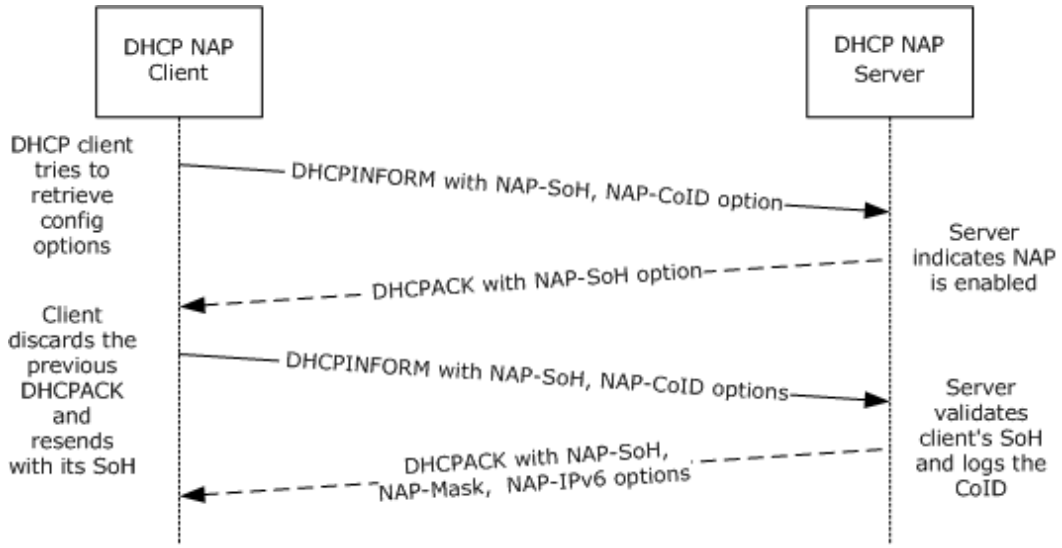


Figure 5: DHCP client request

4.3 Message Exchanges During DHCP Lease Renewal

A DHCP transaction for renewing an IP address lease that involves NAP enforcement consists of the **DHCPREQUEST** and **DHCPACK** messages as described in sections 3.1.4.2, 3.1.5.4, and 3.2.5.2.2. The following figure demonstrates such a transaction.

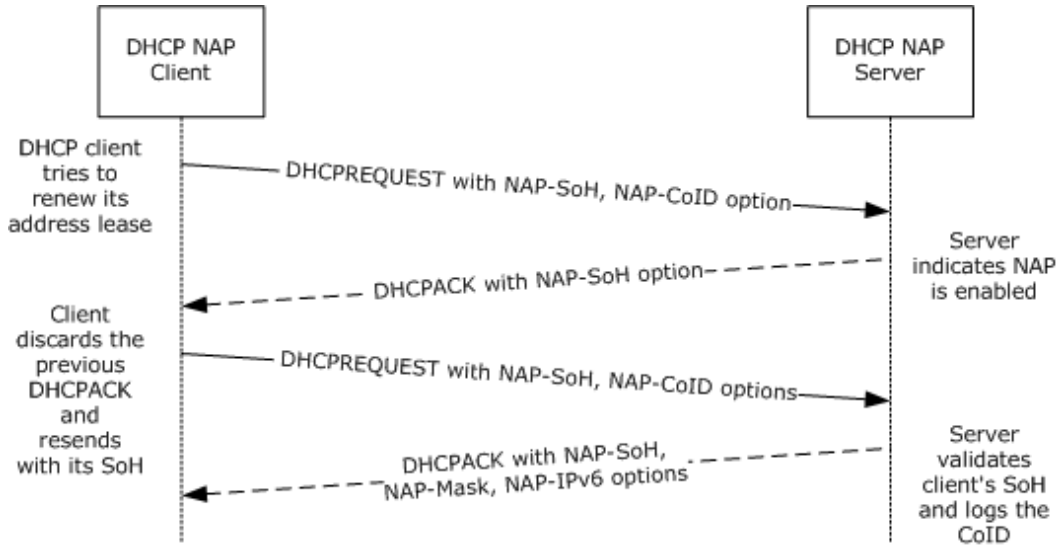


Figure 6: DHCP lease renewal process

5 Security

5.1 Security Considerations for Implementers

All of the security considerations applicable to DHCP, as specified in [RFC2131] section 7, apply to this specification. In addition, the security considerations described in [MS-SOH] section 5.1 also apply to this specification.

Because DHCP is inherently insecure (as noted in section 7 of [RFC2131]), DHCP NAP enforcement also inherits these security vulnerabilities. In addition, clients can easily bypass the connection restrictions in the case that they do not comply with administrative policies. Hence, DHCP-based enforcement for NAP should be treated as being inherently insecure.

Also, as specified in section 3.1.4, DHCP clients do not send the NAP-SoH (section 2.2.1.1) packet in DHCP messages to the DHCP server on unauthenticated wireless networks.

It is also recommended that DHCP servers implementing these protocol extensions record the NAP transaction correlation ID if included by the client in the DHCP messages for that transaction (possibly by logging it).

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:

- Windows® XP operating system Service Pack 3 (SP3)
- 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 2.2.1.2: The NAP Subnet Mask (NAP-Mask) packet sent by the DHCP server is not used by the Windows clients supporting DHCP NAP enforcement.

<2> Section 2.2.1.3: Windows DHCP clients supporting DHCP NAP enforcement use the method specified in [MSDN-CoCreateGuid] to generate a NAP transaction correlation identifier that to a very high degree of certainty is unique.

<3> Section 3.1.5.2: Windows DHCP clients use the Windows Firewall to block IPv6 traffic on the network interface when the client is being quarantined.

<4> Section 3.1.5.2: Windows DHCP clients use the Windows Firewall to block IPv6 traffic on the network interface when the client is being quarantined.

<5> Section 3.2.5.3: Windows DHCP servers do not extract the SoH token from the NAP-SoH (section 2.2.1.1) option sent by the client or pass the SoH to the health policy server.

7 Change Tracking

This section identifies changes that were made to the [MS-DHCPN] 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	60523 Added text to the diagram captioned "Protocol layering diagram" and to the body of the section to clarify that the DHCPN protocol only extends the DHCPE protocol over IPv4. Added text to the diagram captioned "Server-side interaction with related protocols" to clarify that the DHCPN protocol only interacts with IPv4-specific configuration and leases managed by [MS-DHCPM].	Y	Content updated.
2.1 Transport	60523 Clarified that the DHCP extensions used by NAP are transported within DHCP only for DHCPv4.	Y	Content updated.
3.1.5.2 Receiving a DHCPACK Message in Response to a DHCPREQUEST Message During New Lease Acquisition	60523 Added a reference to [RFC3315] and changed a reference from [RFC2463] to [RFC2132].	Y	Content updated.

8 Index

T

V