[MS-DHCPN]:

Dynamic Host Configuration Protocol (DHCP) Extensions for Network Access Protection (NAP)

Revision Summary

Date	Revision History	Revision Class	Comments
12/18/2006	0.1		Version 0.1 release
3/2/2007	1.0		Version 1.0 release
4/3/2007	1.1		Version 1.1 release
5/11/2007	1.2		Version 1.2 release
6/1/2007	1.2.1	Editorial	Changed language and formatting in the technical content.
7/3/2007	1.2.2	Editorial	Changed language and formatting in the technical content.
7/20/2007	1.2.3	Editorial	Changed language and formatting in the technical content.
8/10/2007	2.0	Major	Updated and revised the technical content.
9/28/2007	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	Changed language and formatting in the technical content.
1/25/2008	4.0.2	Editorial	Changed language and formatting in the technical content.
3/14/2008	4.0.3	Editorial	Changed language and formatting in the technical content.
5/16/2008	4.0.4	Editorial	Changed language and formatting in the technical content.
6/20/2008	4.0.5	Editorial	Changed language and formatting in the technical content.
7/25/2008	4.1	Minor	Clarified the meaning of the technical content.
8/29/2008	4.1.1	Editorial	Changed language and formatting in the technical content.
10/24/2008	4.1.2	Editorial	Changed language and formatting in the technical content.
12/5/2008	4.2	Minor	Clarified the meaning of the technical content.
1/16/2009	4.2.1	Editorial	Changed language and formatting in the technical content.
2/27/2009	4.2.2	Editorial	Changed language and formatting in the technical content.
4/10/2009	4.2.3	Editorial	Changed language and formatting in the technical content.
5/22/2009	4.2.4	Editorial	Changed language and formatting in the technical content.
7/2/2009	4.2.5	Editorial	Changed language and formatting in the technical content.
8/14/2009	4.2.6	Editorial	Changed language and formatting in the technical content.
9/25/2009	4.3	Minor	Clarified the meaning of the technical content.
11/6/2009	4.3.1	Editorial	Changed language and formatting in the technical content.
12/18/2009	4.3.2	Editorial	Changed language and formatting in the technical content.
1/29/2010	4.4	Minor	Clarified the meaning of the technical content.
3/12/2010	4.4.1	Editorial	Changed language and formatting in the technical content.

Date	Revision History	Revision Class	Comments
4/23/2010	4.4.2	Editorial	Changed language and formatting in the technical content.
6/4/2010	4.4.3	Editorial	Changed language and formatting in the technical content.
7/16/2010	5.0	Major	Updated and revised the technical content.
8/27/2010	5.0	None	No changes to the meaning, language, or formatting of the technical content.
10/8/2010	5.0	None	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.
1/7/2011	5.2	Minor	Clarified the meaning of the technical content.
2/11/2011	6.0	Major	Updated and revised the technical content.
3/25/2011	7.0	Major	Updated and revised the technical content.
5/6/2011	7.1	Minor	Clarified the meaning of the technical content.
6/17/2011	8.0	Major	Updated and revised the technical content.
9/23/2011	8.0	None	No changes to the meaning, language, or formatting of the technical content.
12/16/2011	9.0	Major	Updated and revised the technical content.
3/30/2012	9.1	Minor	Clarified the meaning of the technical content.
7/12/2012	9.1	None	No changes to the meaning, language, or formatting of the technical content.
10/25/2012	10.0	Major	Updated and revised the technical content.
1/31/2013	10.0	None	No changes to the meaning, language, or formatting of the technical content.
8/8/2013	11.0	Major	Updated and revised the technical content.
11/14/2013	11.0	None	No changes to the meaning, language, or formatting of the technical content.
2/13/2014	11.0	None	No changes to the meaning, language, or formatting of the technical content.
5/15/2014	12.0	Major	Updated and revised the technical content.
6/30/2015	12.0	None	No changes to the meaning, language, or formatting of the technical content.

Table of Contents

1 Introduction

The Dynamic Host Configuration Protocol (DHCP) is an Internet Engineering Task Force (IETF) standard protocol designed to 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.

Sections 1.8, 2, and 3 of this specification are normative and can contain the terms MAY, SHOULD, MUST, MUST NOT, and SHOULD NOT as defined in [RFC2119]. Sections 1.5 and 1.9 are also normative but do not contain those terms. All other sections and examples in this specification are informative.

1.1 Glossary

The following terms are specific to this document:

DHCP client: The remote procedure call (RPC) clients that use the Dynamic Host Configuration Protocol Server Management Protocol (DHCPM) to configure, manage, and monitor the Dynamic Host Configuration Protocol (DHCP) server.

Dynamic Host Configuration Protocol (DHCP) client: An Internet host using DHCP to obtain configuration parameters such as network addresses.

Dynamic Host Configuration Protocol (DHCP) server: A computer running a DHCP service that offers dynamic configuration of IP addresses and related information to DHCP-enabled clients.

health policy server: An entity in a network that has network policies administered on it and that is capable of validating a **statement of health (SoH)** against the specified policies.

Internet Protocol version 4 (IPv4): An Internet protocol that has 32-bit source and destination addresses. IPv4 is the predecessor of IPv6.

Internet Protocol version 6 (IPv6): A revised version of the Internet Protocol (IP) designed to address growth on the Internet. Improvements include a 128-bit IP address size, expanded routing capabilities, and support for authentication (2) and privacy.

little-endian: Multiple-byte values that are byte-ordered with the least significant byte stored in the memory location with the lowest address.

Network Access Protection (NAP): A feature of an operating system that provides a platform for system health-validated access to private networks. **NAP** provides a way of detecting the health state of a network client that is attempting to connect to or communicate on a network, and limiting the access of the network client until the health policy requirements have been met. **NAP** is implemented through quarantines and health checks, as specified in [TNC-IF-TNCCSPBSoH].

network byte order: The order in which the bytes of a multiple-byte number are transmitted on a network, most significant byte first (in big-endian storage). This may or may not match the order in which numbers are normally stored in memory for a particular processor.

statement of health (SoH): A collection of data generated by a system health entity, as specified in [TNC-IF-TNCCSPBSoH], which defines the health state of a machine. The data is interpreted by a Health Policy Server, which determines whether the machine is healthy or unhealthy according to the policies defined by an administrator.

Transmission Control Protocol (TCP): A protocol used with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. TCP handles keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

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

1.2 References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the Errata.

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.

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

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

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

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

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

[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

[TNC-IF-TNCCSPBSoH] TCG, "TNC IF-TNCCS: Protocol Bindings for SoH", version 1.0, May 2007, http://www.trustedcomputinggroup.org/resources/tnc_iftnccs_protocol_bindings_for_soh_version_10/

1.2.2 Informative References

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

[MSDN-GUID] Microsoft Corporation, "GUID structure", http://msdn.microsoft.com/en-us/library/aa373931(VS.85).aspx

[MSDN-NAPAPI] Microsoft Corporation, "NAP Interfaces", http://msdn.microsoft.com/en-us/library/aa369705(v=VS.85).aspx

[MSDN-NAPCORRID] Microsoft Corporation, "GetStringCorrelationId method", http://msdn.microsoft.com/en-us/library/aa369481(v=VS.85).aspx

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

[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

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. The DHCP protocol allows for extensibility by defining new DHCP options. NAP enforcement using DHCP defines new options in order to carry the health state and other control information between the client and server.

The following is an overview of the messages exchanged between the **DHCP client** and server and the details are explained in later sections.

1. The DHCP client sends a NAP **Statement of Health** (NAP-SoH (section 2.2.1.1)) as well as the Correlation ID (NAP-CoID (section 2.2.1.3) within the vendor-specific option ([RFC2132], section 8.4) in a **DHCPDISCOVER** message to determine whether the DHCP server has NAP enabled.

2. A server that is NAP-enabled and receives a **DHCPDISCOVER** message including a NAP Statement of Health (NAP-SoH) will indicate that the server supports NAP by responding with a **DHCPOFFER** including a NAP-SoH, containing the text "NAP" inside the Vendor-Specific option ([RFC2132], section 8.4).

3. 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 includes a NAP-SoH containing the text "NAP" inside the vendor specific option, then the client can send a **DHCPREQUEST** message to the selected server, containing the SoH in the NAP-SoH option encapsulated inside the Vendor-Specific option.

4. The DHCP server sends the SoH token received from the client to the **health policy server** for validation. 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 sends the options to the client that quarantines the client (Section 3.2.5.2.1).

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.

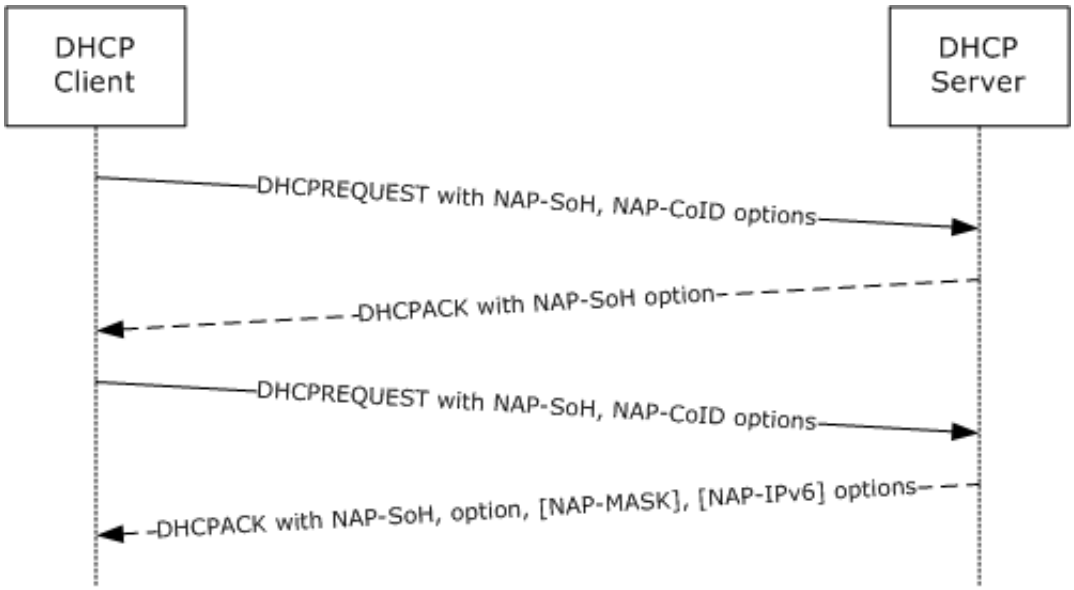

Figure 1: Client request attempt to remedy quarantine state

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**).

5. While selecting the network configuration for a NAP-capable client, the DHCP server uses the **DHCPv4ClassDef** object (a shared ADM element; see [MS-DHCPM] section 3.1.1.8) and follows the processing rules as defined in section 3.2.7.1.

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

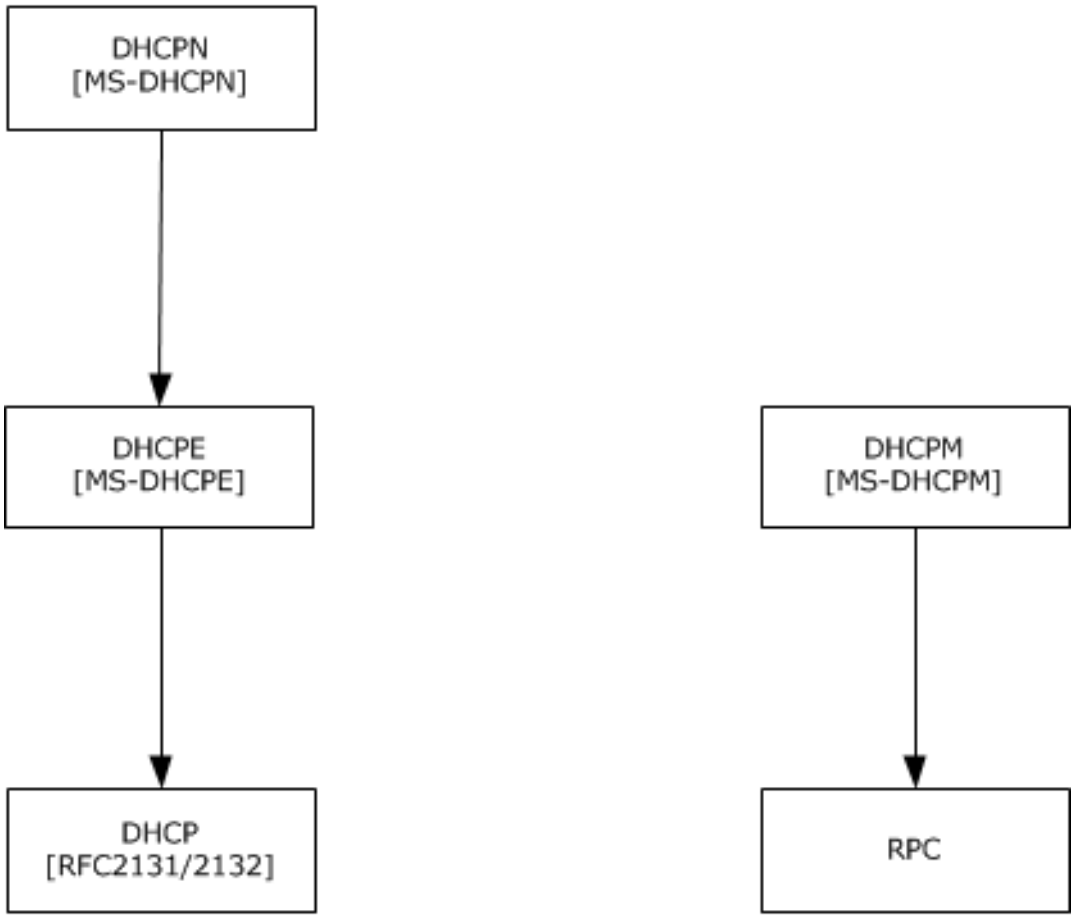

Figure 2: Protocol layering diagram

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.

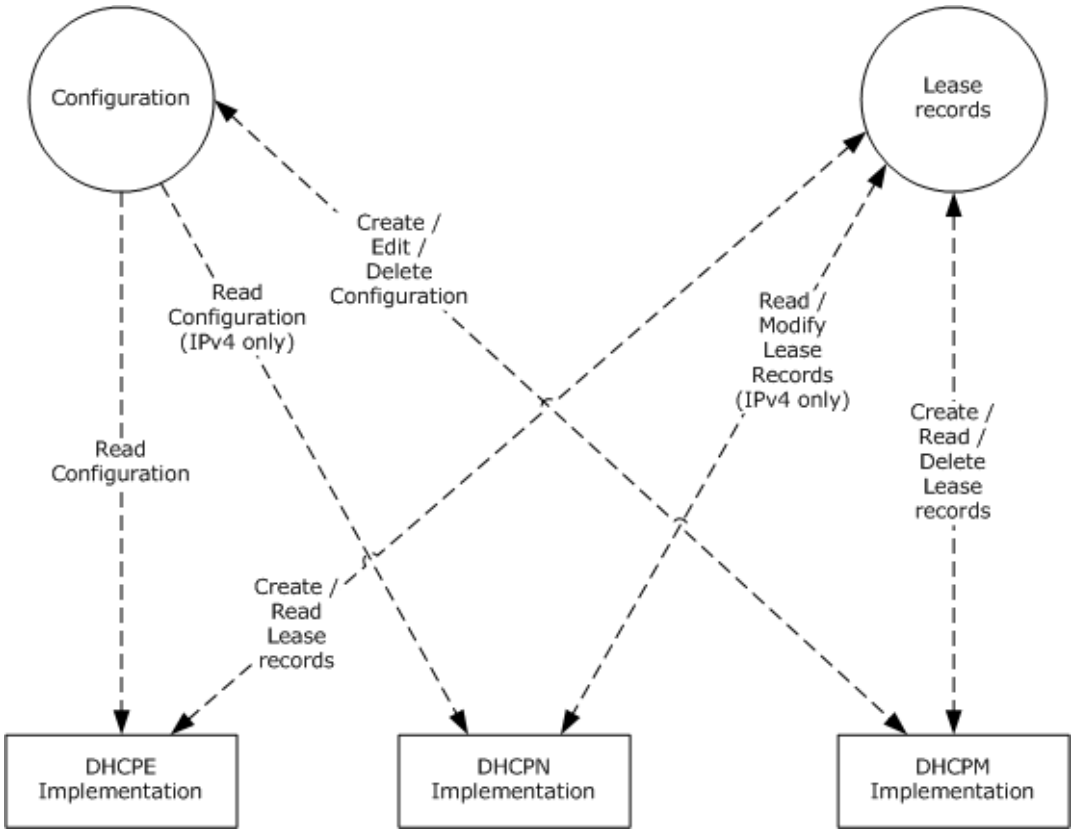

Figure 3: Server-side interaction with related protocols

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.

Supported Transports: [This extension uses [MS-DHCPE] as its sole transport. [MS-DHCPE] extends DHCP [RFC2131]. [MS-DHCPN] does not include support for using [MS-DHCPE] extensions for DHCPv6 [RFC3315] as a transport.

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.

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 (1 byte): This MUST be 220 (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 (0xDE) for NAP-CoID, whose length is 130, and Option 220 (0xDC), whose length is 0. Option 220 (0xDC) with a length of 0 is

included by the client in order to probe whether NAP is enabled on the server. NAP-CoID (option 222 (0xDE)) contains a randomly generated correlation ID to enable end-to-end correlation of NAP transaction between the DHCP client and the DHCP server and is defined in section 2.2.1.3.

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 [TNC-IF-TNCCSPBSoH], representing the client's health state, sent by the client in **DHCPREQUEST** messages.

SoH-Response: Binary data of variable length, as defined in [TNC-IF-TNCCSPBSoH], 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.

<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="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><td colspan="16"></td></tr>
</table>

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.

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 (130 bytes)																
...																															
...																															

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.

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								Number_of_IPv6_Remediation_Server_Addresses								Vendor-Specific_Option_Data (variable)							
...																															

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

The common Abstract Data Model is specified in section 3.3.1.

DHCP clients implementing this protocol 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 specified in [RFC2131] section 3, 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. The NAP-SoH (section 2.2.1.1) option and NAP-CoID (section 2.2.1.3) option are appended to the **DHCPDISCOVER** message packet by calling DhcpAppendVendorSpecificOption ([MS-DHCPE] section 3.1.7.1).

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" or "Yes", 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 "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" or "Yes", 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 "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.

The NAP-SoH (section 2.2.1.1) option and NAP-CoID (section 2.2.1.3) option are extracted from the **DHCPDISCOVER** message packet by calling DhcpExtractVendorSpecificOption ([MS-DHCPE] section 3.1.7.2).

In the **DHCPREQUEST** packet, the NAP-SoH (section 2.2.1.1) option and NAP-CoID (section 2.2.1.3) option are appended by calling DhcpAppendVendorSpecificOption ([MS-DHCPE] section 3.1.7.1).

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 it to the NAP agent. The NAP-SoH (section 2.2.1.1) option is extracted from the **DHCPACK** message by calling DhcpExtractVendorSpecificOption ([MS-DHCPE] section 3.1.7.2). 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 by calling DhcpExtractVendorSpecificOption ([MS-DHCPE] section 3.1.7.2) 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 and DHCPv6 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. If the Subnet Mask and Router options as defined in [RFC2132] sections 3.3 and 3.5 respectively are present in the message the corresponding Subnet Mask and Router IP addresses MUST be configured in the TCP/IP stack. The Microsoft Classless Static Routes option, if present in the message, is processed as specified in [MS-DHCPE] section 3.1.5.2. The NAP-Mask option, if present in the message, MAY<5> 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.

If the client has its NAP-Capable Server state set to "Yes" and the **DHCPACK** message received from the DHCP server does not contain a NAP-SoH option, the DHCP client MUST process the message only for the Subnet Mask and Router options, the Microsoft Classless Static Routes (section 3.1.5.2) option, and the NAP-Mask option, as described in the preceding paragraph.

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 either of length 3 and data as the string "NAP" or of length greater than 3, it MUST set its NAP-Capable Server state to "Yes". The NAP-SoH (section 2.2.1.1) option is extracted from the **DHCPACK** message by calling DhcpExtractVendorSpecificOption ([MS-DHCPE] section 3.1.7.2). In addition, the client MUST discard the **DHCPACK** message and retransmit the **DHCPINFORM** message with the updated SoH message ([TNC-IF-TNCCSPBSoH]) retrieved by calling DhcpClientGetSoH (section 3.1.7.1) and sending the SoH token in the NAP-SoH option. It MUST also include a NAP-CoID option (section 2.2.1.3) in this message.

The NAP-SoH option and NAP-CoID option are appended to the DHCPINFORM message packet by calling DhcpAppendVendorSpecificOption ([MS-DHCPE] section 3.1.7.1) with appropriate parameters provided as input.

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 or contains the NAP-SoH option of length 3 or less, but the data as string is not "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.

If the DHCP client's NAP-Capable Server state is set to "Yes" or "No", the message SHOULD be processed as specified in section 3.1.5.2. However, if the client has its NAP-Capable Server state set to "Yes" and receives a DHCPACK message in response to a DHCPINFORM message, the client MAY<6> 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 either of length 3 and data as the string "NAP" or of length greater than 3, it MUST set its NAP-Capable Server state to "Yes". The NAP-SoH (section 2.2.1.1) option is extracted from the **DHCPACK** message by calling DhcpExtractVendorSpecificOption ([MS-DHCPE] section 3.1.7.2). In addition, the client MUST discard the **DHCPACK** message and retransmit the **DHCPREQUEST** message with the updated SoH message ([TNC-IF-TNCCSPBSoH]) retrieved by calling DhcpClientGetSoH (section 3.1.7.1) and sending the SoH token in the NAP-SoH option. It MUST also include a NAP-CoID option (section 2.2.1.3) in this message.

The NAP-SoH option and NAP-CoID option are appended to the DHCPINFORM message packet by calling DhcpAppendVendorSpecificOption ([MS-DHCPE] section 3.1.7.1) with appropriate parameters provided as input.

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 or contains the NAP-SoH option of length 3 or less, but the data as string is not "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.

If the DHCP client's NAP-Capable Server state is set to "Yes" or "No", 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

3.1.7.1 DhcpClientGetSoH

If DHCP is NAP-capable, the DHCP client uses this method to get the SoH message (see [TNC-IF-TNCCSPBSoH]) to be sent as payload of NAP-SoH Option (section 2.2.1.1). The SoH SHOULD be obtained by calling INapEnforcementClientBinding::GetSoHRequest, which is part of the NAP EC API, to set the SoH message on the connection, and then calling the INapEnforcementClientConnection::GetSoHRequest, also part of the NAP EC API, to retrieve the SoH as an opaque buffer.

3.2 Server Details

This section specifies the DHCP NAP server behavior.

3.2.1 Abstract Data Model

The common Abstract Data Model is specified in section 3.3.1.

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
- DHCPv4Scope.ScopeInfo.SubnetMask
- DHCPv4Client.QuarantineCapable
- DHCPv4Client.QuarantineStatus
- DHCPv4Client.ProbationEnds

3.2.2 Timers

Health Check Timeout: This timer is initialized whenever the DHCP server sends the SoH to the health policy server after receiving the DHCPREQUEST message as described in section 3.2.5.2.1. The timer is stopped when the health policy server responds with an SoH Response.

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 a **DHCPDISCOVER** message, it extracts the NAP-SoH (section 2.2.1.1) and NAP-CoID (section 2.2.1.3) options from the message packet by calling DhcpExtractVendorSpecificOption ([MS-DHCPE] section 3.2.7.3). If the SoH vendor-specific option has length 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", and the NAP-CoID (section 2.2.1.3) option as it is in the **DHCPDISCOVER** message packet. The NAP-SoH (section 2.2.1.1) and NAP-CoID (section 2.2.1.3) options are appended to the DHCPOFFER message packet by calling DhcpAppendVendorSpecificOption ([MS-DHCPE] section 3.2.7.1).

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.

The NAP-SoH (section 2.2.1.1) option and NAP-CoID (section 2.2.1.3) option are extracted from the **DHCPREQUEST** message packet by calling DhcpExtractVendorSpecificOption ([MS-DHCPE] section 3.1.7.2).

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.

Otherwise, the NAP-SoH (section 2.2.1.1) and NAP-CoID (section 2.2.1.3) options are extracted from the message packet by calling DhcpExtractVendorSpecificOption ([MS-DHCPE] section 3.2.7.3). 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, and initialize the Health Check Timeout timer to 2 seconds. The NAP-SoH (section 2.2.1.1) is appended to the DHCPACK message packet by calling DhcpAppendVendorSpecificOption ([MS-DHCPE] section 3.2.7.1). 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 [TNC-IF-TNCCSPBSoH].

3.2.5.2.2 Processing the SoH-Response from the Health Policy Server

The SoH-Response from the health policy server as well as the type of the encapsulating RADIUS server packet received comes as part of RADIUS [RFC2865] and the Microsoft RADIUS Attributes for Network Access Protection [MS-RNAP]. If the SoH-Response from the health policy server is encapsulated in a RADIUS server packet of type Access-Reject as specified in section 4.3 of [RFC2865], the incoming DHCPREQUEST message is not processed any further and no response is sent to the DHCP client.

If the RADIUS server packet is of type Access-Accept as specified in section 4.2 of [RFC2865], this will trigger the creation of a DHCPACK containing the SoH-Response and the NAP-CoID (section 2.2.1.3) option as it was received in the DHCPREQUEST message packet. The NAP-SoH (section 2.2.1.1) and NAP-CoID (section 2.2.1.3) options are appended to the DHCPACK message packet by calling DhcpAppendVendorSpecificOption ([MS-DHCPE] section 3.2.7.1). 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 [TNC-IF-TNCCSPBSoH].

If, in the SoH-Response from the health policy server, the **qState** field of the **MS-Quarantine-State** attribute ([TNC-IF-TNCCSPBSoH] section 3.8.2) is 3, the client is noncompliant with the NAP health policies. In such a case, the DHCP server MUST ignore the user class value sent by the client and instead use the "Default Network Access Protection Class" ([MS-DHCPM] section 3.1.1.8) 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). The option values corresponding to the "Default Network Access Protection Class" ([MS-DHCPM] section 3.1.1.8) user class are obtained by using the procedure DhcpGetNetworkConfigurationForClient (section 3.2.7.1). 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 MUST be configured with static routes to the IPv4 addresses of the NAP remediation servers by calling DhcpAppendCSROption ([MS-DHCPE] section 3.2.7.2).

Also, if the DHCP client is being quarantined, the DHCP server SHOULD include the **DHCPv4Scope.ScopeInfo.SubnetMask** element, which is a shared element (see [MS-DHCPM] section 3.1.1.2) (as specified in [RFC2132] section 3.3) in the NAP-Mask (section 2.2.1.2) option. It MUST also include the IPv6 addresses of the NAP remediation servers in the NAP-IPv6 (section 2.2.1.4) option if the addresses are received in the **Attribute-Specific Value** field of the MS-IPv6-Remediation-Servers attribute ([MS-RNAP] section 2.2.1.17) of the encapsulating RADIUS packet. The NAP-Mask (section 2.2.1.2) option and NAP-IPv6 (section 2.2.1.4) option are appended to the DHCPACK message packet by calling DhcpAppendVendorSpecificOption ([MS-DHCPE] section 3.2.7.1). 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 SoH-Response from the health policy server indicates that the client is compliant with the NAP health policies, the DHCPREQUEST is processed as a normal DHCPREQUEST and the network configuration (option values) is to be sent to the client as specified in section 1.4 (point 5).

3.2.5.2.3 No SoH-Response Received Within Health Check Timeout

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.

3.2.5.2.4 Receiving a DHCPREQUEST Message During Lease Renewal

When a DHCP server receives a **DHCPREQUEST** message, it extracts the NAP-SoH (section 2.2.1.1) and NAP-CoID (section 2.2.1.3) options from the message packet by calling DhcpExtractVendorSpecificOption ([MS-DHCPE] section 3.2.7.3). If the NAP-SoH (section 2.2.1.1) option is of length equal to one octet and its data is 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" and the NAP-CoID (section 2.2.1.3) option as it is in the DHCPREQUEST message packet. 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. The NAP-

SoH (section 2.2.1.1) and NAP-CoID (section 2.2.1.3) options are appended to the DHCPACK message packet by calling DhcpAppendVendorSpecificOption ([MS-DHCPE] section 3.2.7.1).

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<7> be processed as specified in section 3.2.5.2.4; when a DHCP server that is NAP-enabled (determined per section 1.4 points 1 and 2) receives a DHCPINFORM message, it extracts the NAP-SoH (section 2.2.1.1) and NAP-CoID (section 2.2.1.3) options from the message packet by calling DhcpExtractVendorSpecificOption ([MS-DHCPE] section 3.2.7.3).

It SHOULD 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 and the NAP-CoID (section 2.2.1.3) option as it is in the DHCPINFORM message packet. The NAP-SoH (section 2.2.1.1) is appended to the DHCPACK message packet by calling DhcpAppendVendorSpecificOption ([MS-DHCPE] section 3.2.7.1).

3.2.6 Timer Events

Health Check Timeout: When this timer expires, it denotes a period in which the DHCP server has sent the SoH to the health policy server but has not received a corresponding SoH-Response. The following are the tasks to be performed when this timer expires:

- Invoke the processing rules in section 3.2.5.2.3, No SoH-Response Received Within Health Check Timeout.

3.2.7 Other Local Events

3.2.7.1 DhcpGetNetworkConfigurationForClient

The DHCP server uses this method to get the network configuration for a NAP-capable client by following the steps below.

Wherever the client message contains a user class option ([RFC3004]) and there exists a **DHCPv4ClassDef** object (a shared ADM element; see [MS-DHCPM] section 3.1.1.8) whose **DHCPv4ClassDef.ClassData** and **DHCPv4ClassDef.ClassDataLength** match the user class option data, then any parameter values configured in **DHCPv4Reservation.DHCPv4ResvOptValuesList**, **DHCPv4Scope.DHCPv4ScopeOptValuesList**, or **DHCPv4ServerOptValueList** with the corresponding **DHCPv4ClassDef.ClassName** in the **DHCPv4OptionValue.UserClass** (a shared ADM element; see [MS-DHCPM] section 3.1.1.11) will be selected in preference to parameters configured without a ClassName in any list. The overall order of selecting a configured default value is:

1. **DHCPv4OptionValue** with matching ClassName configured in the **DHCPv4Reservation.DHCPv4ResvOptValuesList** for a **DHCPv4Reservation** matching the client hardware address ([RFC2131] section 2) / client identifier ([RFC2132] section 9.14).

2. **DHCPv4OptionValue** with matching ClassName configured in the **DHCPv4Scope.DHCPv4ScopeOptValuesList** for a **DHCPv4Scope** selected as outlined above.

3. **DHCPv4OptionValue** with matching ClassName configured in the **DHCPv4ServerOptValueList**.

4. **DHCPv4OptionValue** with no ClassName configured in the **DHCPv4Reservation.DHCPv4ResvOptValuesList** for a **DHCPv4Reservation** matching the client hardware address ([RFC2131] section 2) / client identifier ([RFC2132] section 9.14).

5. **DHCPv4OptionValue** with no ClassName configured in the **DHCPv4Scope.DHCPv4ScopeOptValuesList** for a **DHCPv4Scope** selected as outlined above.

6. **DHCPv4OptionValue** with no ClassName configured in the **DHCPv4ServerOptValueList**.

The Subnet Mask option (DHCP option 1, as specified in [RFC2132] section 3.3) is overridden and MUST be set to the value from the **DHCPv4Scope.ScopeInfo.SubnetMask** ADM element as defined in [MS-DHCPM] section 3.1.1.2.

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.

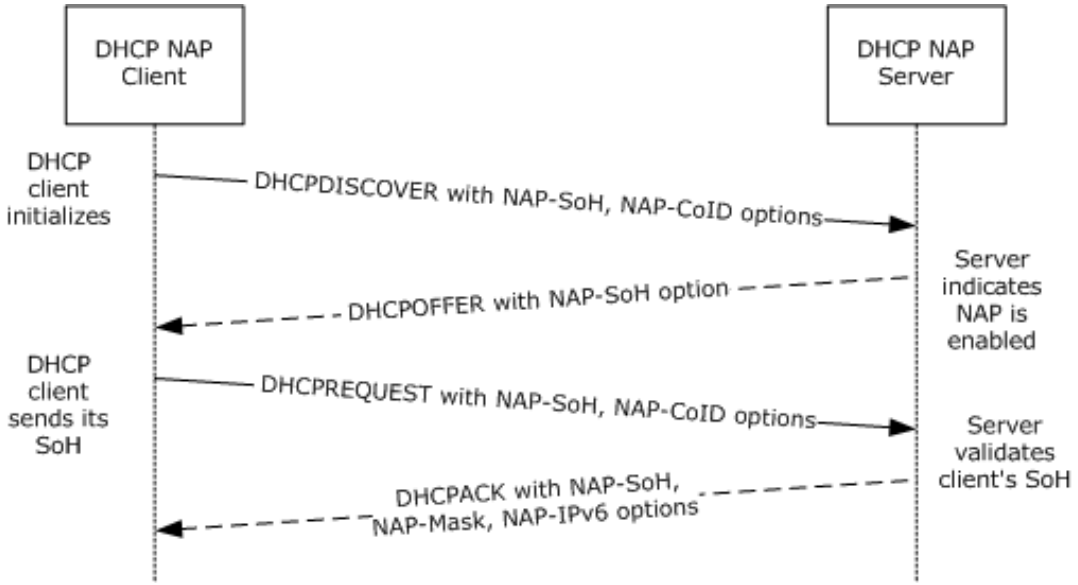

Figure 4: DHCP new lease acquisition process

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.

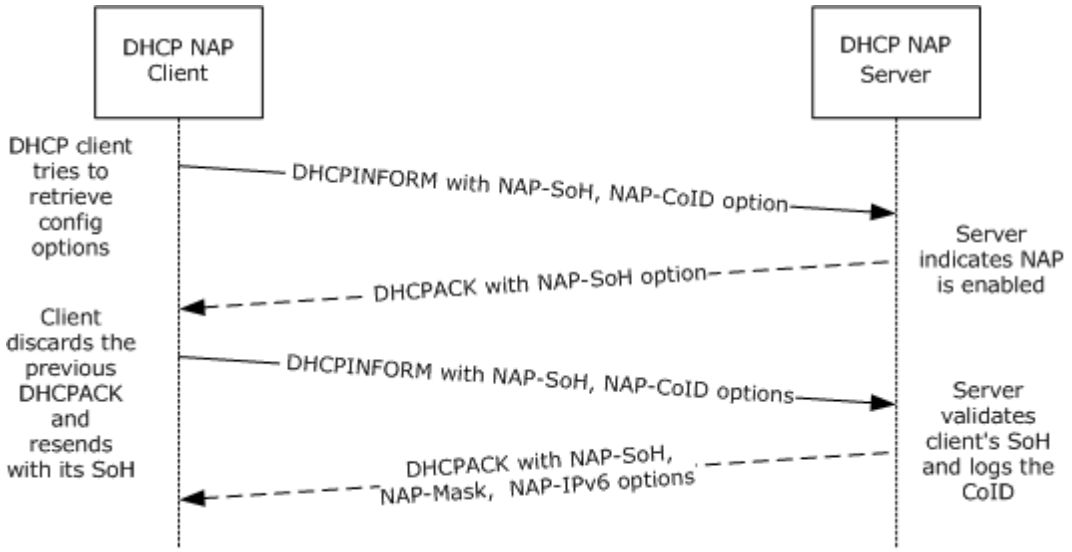

Figure 5: DHCP client request

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 3.2.5.2.4. The following figure demonstrates such a transaction.

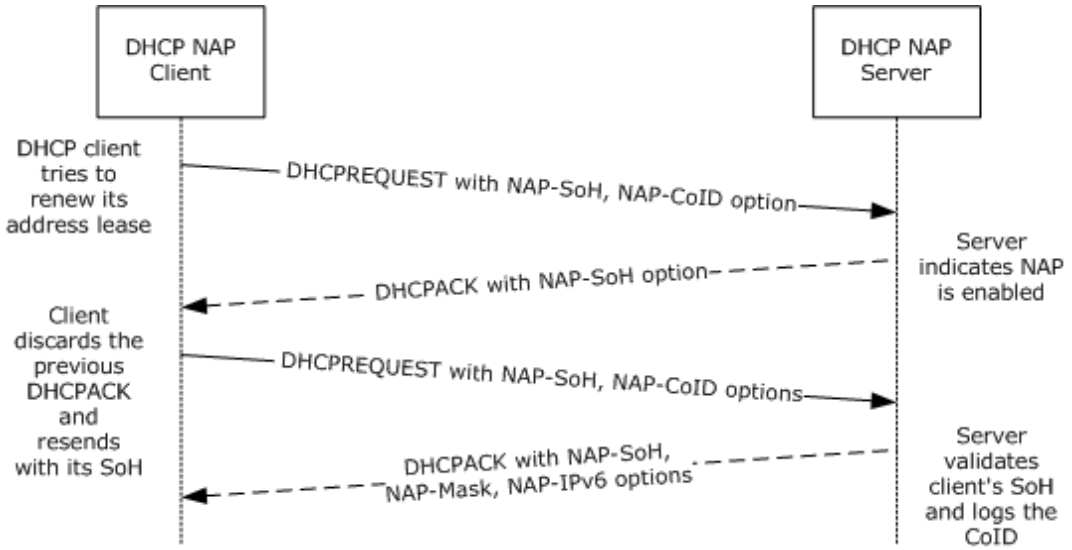

Figure 6: DHCP lease renewal process

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 [TNC-IF-TNCCSPBSoH] 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
- Windows 8 operating system
- Windows Server 2012 operating system
- Windows 8.1 operating system
- Windows Server 2012 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 NAP EC API ([MSDN-NAPAPI], and [MSDN-NAPCORRID]) to generate a NAP transaction correlation identifier that to a very high degree of certainty is unique. The correlation identifier generated by [MSDN-NAPCORRID] is a combination of the string representation of a GUID [MSDN-GUID] and a time stamp.

The string representation of the GUID [MSDN-GUID] is "{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}". The string representation of the time stamp is "YYYY-MM-DD HH:MM:SS.LLLZ", which represents the sequence year, month, date, hours, minutes, seconds, milliseconds, and the character "Z". The two string references are combined together to form the string representation of the correlation identifier, as follows:"{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX} – YYYY-MM-DD HH:MM:SS.LLLZ"

This combination is a 65-character Unicode string, which is equivalent to 130 bytes.

<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 3.1.5.2: The NAP Subnet Mask (NAP-Mask) packet (see 2.2.1.2) sent by the DHCP server is not used by Windows clients supporting DHCP NAP enforcement.

<6> Section 3.1.5.3: Windows DHCP servers do not ignore the NAP-SoH option (section 2.2.1.1) or the NAP-IPv6 (section 2.2.1.4) option sent by the client.

<7> 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

No table of changes is available. The document is either new or has had no changes since its last release.

8 Index

M

N

O

P

R

S

T

V