[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		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

Date	Revision History	Revision Class	Comments
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.

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 it can regain full network access. NAP allows there to be 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 **Dynamic Host Configuration Protocol (DHCP) clients** and **DHCP servers** to support NAP enforcement through the 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
Statement of Health (SoH)

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. A **network access server (NAS)** operates as a client of 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 a **NAS** include: a VPN server, Wireless Access Point, 802.1x-enabled switch, or **Network Access Protection (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-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary", March 2007.

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

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

[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

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

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

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

1.3 Protocol Overview (Synopsis)

For more information on Network Access Protection (NAP), see [MSDN-NAP]. The Dynamic Host Configuration Protocol (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 as 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 Dynamic Host Configuration Protocol (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-**SoH** option (as specified in sections 2.2.1.1 and 2.2.1.2) of length 1 and data equal to 0 in a DHCPDISCOVER message to determine if 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-Statement of Health (SoH) option of length 3 with data as "NAP" to indicate to the client that the server supports DHCP NAP enforcement.

3. If the client confirms that the server supports DHCP NAP enforcement, then the client asks the NAP agent for the SoH. The DHCP client then selects an offer from one of the DHCP servers that responded (typically the first offer received). If the offer indicated that the server has NAP enabled as explained above, then the client sends a DHCPREQUEST message containing the SoH token it received from the NAP agent in the NAP-SoH option to the server.

4. The DHCP server sends the SoH token received from the client to the **health policy server** for validation. For this, it may use the Remote Access 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 which responds with the network configuration options, as usual, and includes an appropriate SoH-Response (obtained from the health policy server) in the 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 Routes option (as specified in [MS-DHCPE]) that contains the static routes to the NAP remediation servers.

A client that has been quarantined due to non-compliance 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.

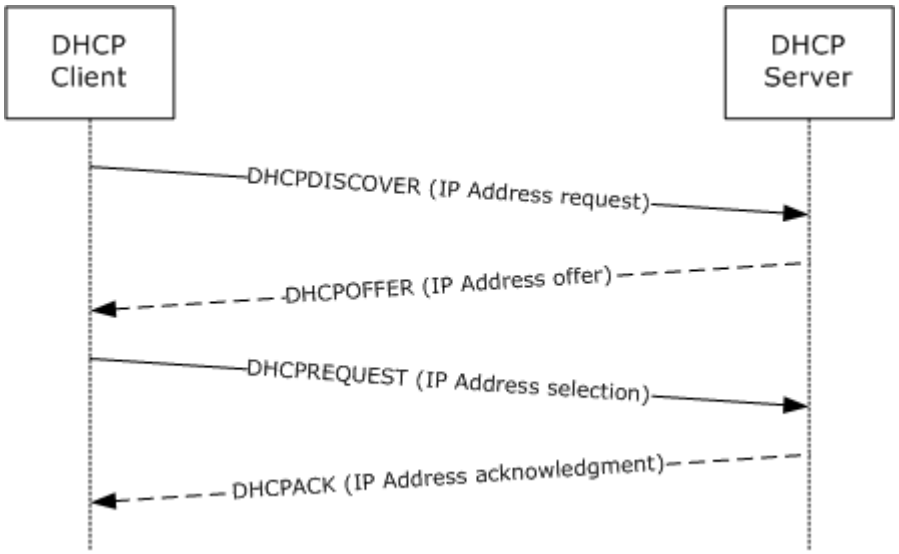


Figure 1: Client request attempt to remedy quarantine state

1.4 Relationship to Other Protocols

The Network Access Protection (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, the DHCP server and the DHCP client must support the extensions defined in [MS-DHCPE].

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.

1.5 Prerequisites/Preconditions

None.

1.6 Applicability Statement

The use of DHCP vendor-specific options for NAP are 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 Network Access Protection (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 2.2.2.

1.8 Vendor-Extensible Fields

This document does not define any vendor-extensible fields.

2 Messages

The following sections specify how messages are encapsulated on the wire.

2.1 Transport

All DHCP extensions used by NAP are transported within DHCP, as specified in [RFC2131] section 4.1 (for DHCPv4) and [RFC3315] section 5.2 (for DHCPv6).

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 multi-byte option fields and values described in this document 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 the DHCP protocol. These vendor-specific options MUST be sent as vendor-specific extensions as part of DHCP option 43, as specified in [RFC2132] section 8.4.

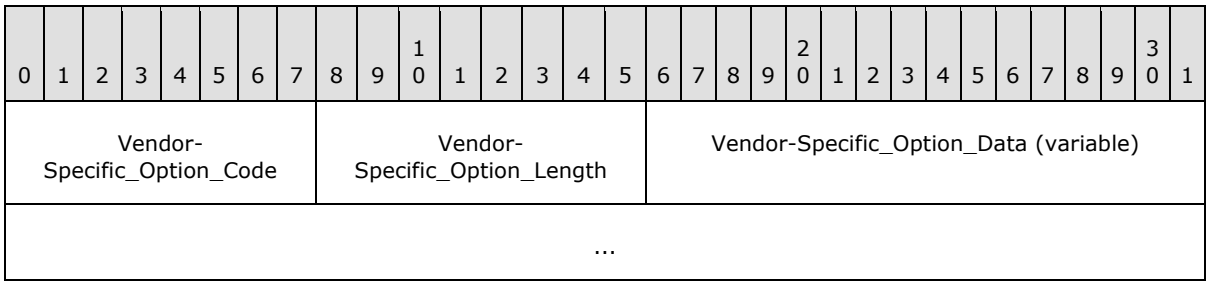
The Microsoft Encoding Long Options Packet, as specified in [MS-DHCPE] section 2.2.7, MUST be used when the cumulative size of all the vendor-specific options being sent in a message exceeds 255 bytes.

2.2.1.1 NAP Statement of Health (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 if 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 Statement of Health (NAP-Soh) Option is defined as follows:



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

Vendor-Specific_Option_Length (1 byte): Variable with a range of 0x00 to 0xFF.

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

No Data: When the Vendor-Specific_Option_Length is zero in a message sent by the server, it indicates that NAP is not enabled on the server.

Zero of length 1: One byte with value 0x00 sent by the client in DHCPDISCOVER, DHCPREQUEST, or DHCPINFORM messages to check if 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.

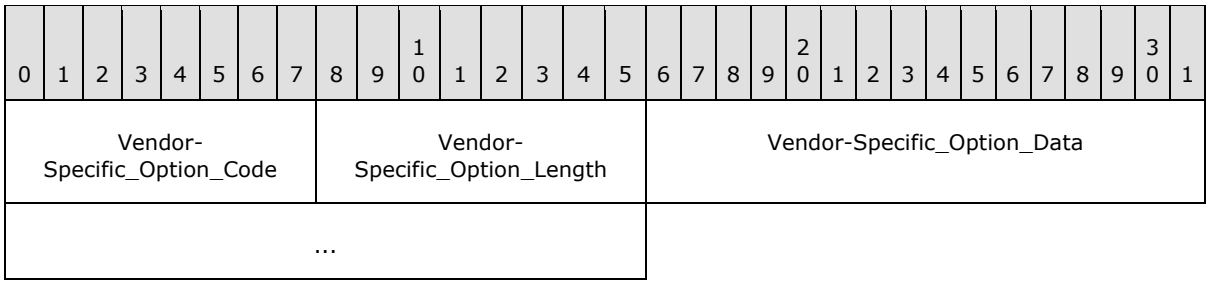
SoH-Response: Binary data of variable length as defined in [MS-SOH] representing the client's quarantine state, sent by the server in DHCPACK messages.

2.2.1.2 NAP Subnet Mask (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 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.

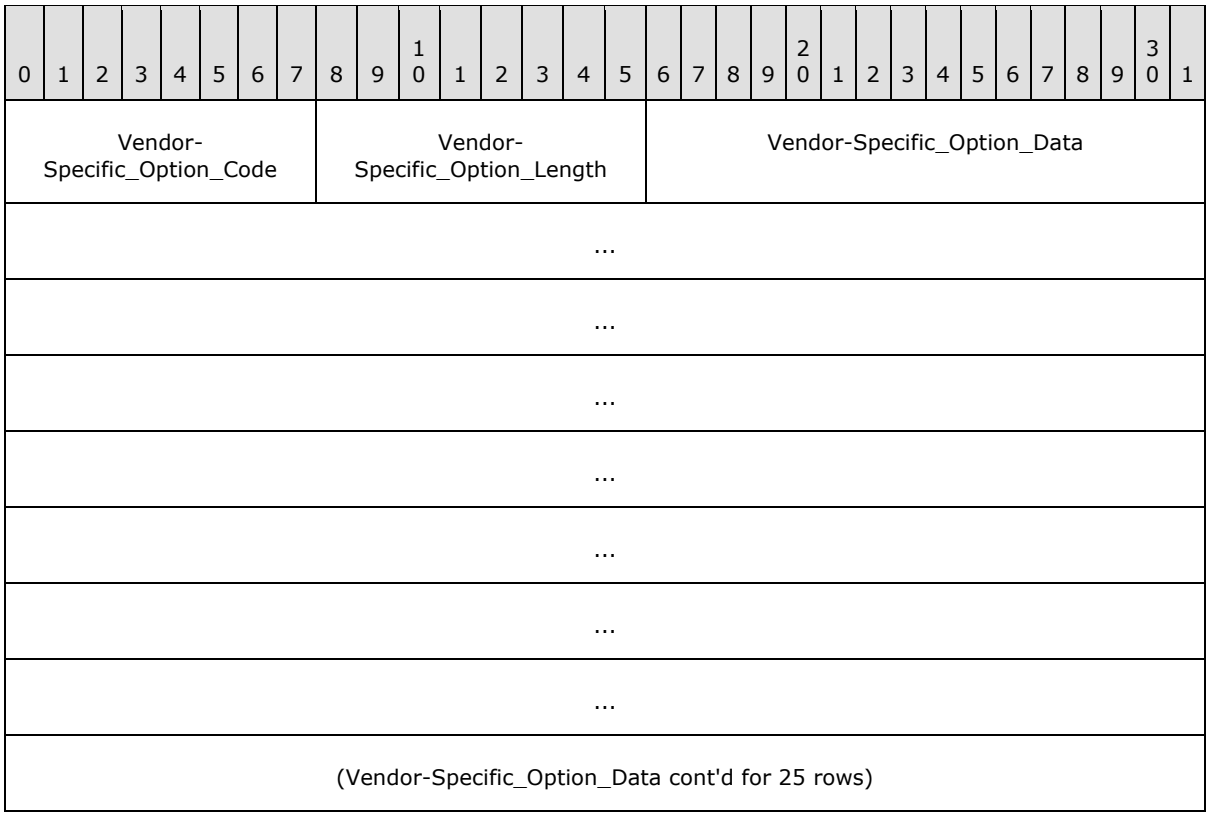
Vendor-Specific_Option_Data (4 bytes): Subnet mask in little-endian byte order.

2.2.1.3 NAP Correlation ID (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 only used 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.

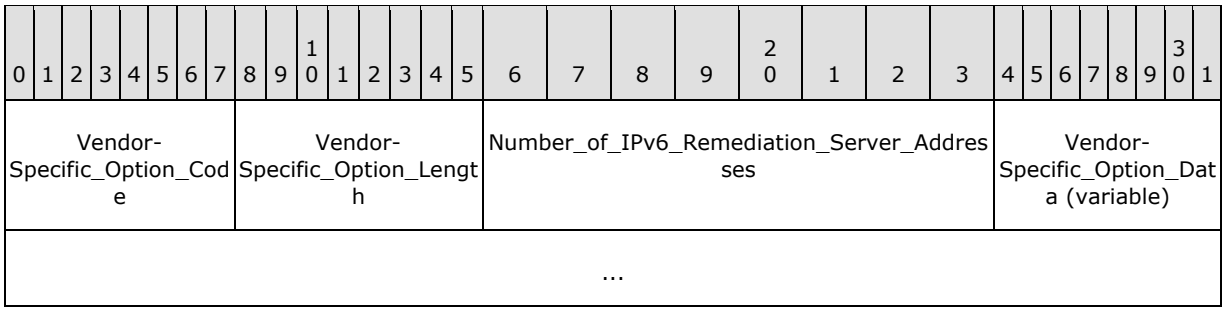
Vendor-Specific_Option_Data (130 bytes): Binary data representing a correlation ID that SHOULD<2> be generated randomly.

2.2.1.4 NAP IPv6 Remediation Server List (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 non-zero, then 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" user class predefined on them.

The format for the User Class Option used by clients and servers implementing this specification is defined in [RFC3004] and in [MS-DHCPE] section 2.2.4.

3 Protocol Details

The following sections specify details of the Dynamic Host Configuration Protocol (DHCP) Extensions for Network Access Protection (NAP) specification, including an abstract data model, timers, initialization, higher-layer triggered events, and message processing rules.

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

None beyond those in [MS-DHCPE], section 3.1.2.

3.1.3 Initialization

See section 3.1.3 of [MS-DHCPE] 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 the DHCP protocol, DHCP clients SHOULD NOT attempt to use NAP on unauthenticated wireless networks.

3.1.4.1 Creation and Transmission of 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 one octet and data equal to zero.

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

3.1.4.2 Creation and Transmission of 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, then it MUST include the NAP-SoH option of length one octet and data equal to zero in the DHCPREQUEST message.

If instead the NAP-Capable Server state is set to Yes, then 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 (section 2.2.1.3) in this message.

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

3.1.4.3 Creation and Transmission of the DHCPINFORM Message

Whenever a DHCP client sends a DHCPINFORM message, and its NAP-Capable Server state is set to Unknown, then it MUST include the NAP-SoH option of length one octet, and the data equal to zero in the DHCP INFORMATION-REQUEST (DHCPINFORM) message.

If instead the NAP-Capable Server state is set to Yes, then 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 (section 2.2.1.3) in this message.

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

3.1.5 Message Processing Events and Sequencing Rules

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

3.1.5.1 Receiving a DHCPOFFER Message

If the DHCPOFFER message from the DHCP server contains a NAP-SoH 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 Option (section 2.2.1.3) 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 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, then the client MUST extract the addresses of the IPv6 Remediation servers from the NAP-IPv6 option and block (in any 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 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, then the client MUST block (in any 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, then 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 [RFC2463], and the Microsoft Classless Static Routes option as defined in [MS-DHCPE], 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 received from the DHCP server does not contain a NAP-SoH option, the DHCP client MUST process the message as described in the previous 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 option of length 3 and data as the string "NAP", then 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", then 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<5> be processed as specified in section 3.1.5.2; the client MAY instead ignore the NAP-SoH option and the NAP-IPv6 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 option of length 3 and data as the string "NAP", then 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", then 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.

3.2.2 Timers

None.

3.2.3 Initialization

None.

3.2.4 Higher-Layer Triggered Events

None.

3.2.5 Message Processing Events and Sequencing Rules

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

3.2.5.1 Receiving a DHCPDISCOVER Message

When the DHCP server receives an SoH vendor-specific option with length equal to one octet and data equal to zero, then the DHCP server MUST respond with a DHCPOFFER message that contains a NAP-SoH 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 message from the client contained the SoH token in a NAP-SoH option, the DHCP server 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 is non-compliant with the NAP health policies, then the DHCP server MUST ignore the user class value sent by the client and instead use the default Network Access Protection (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 a value of 0.0.0.0 and the Subnet Mask option (DHCP option 1, as specified in [RFC2132] section 3.3) MUST be set to a value of 255.255.255.255. The Microsoft Classless Static Routes 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, then the DHCP server SHOULD include the NAP-Mask option and it MUST include the IPv6 addresses of the NAP remediation servers in the NAP-IPv6 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.

3.2.5.2.2 Receiving a DHCPREQUEST Message during lease renewal

If the message from the client contains the NAP-SoH option of length equal to one octet and with data equal to zero, then the server 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<6> be processed as specified in section 3.2.5.2.2; the DHCP server 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 adheres 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

None beyond those specified in [MS-DHCPE].

3.3.3 Initialization

The DHCP Extensions for NAP specification 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 Message Processing Events and Sequencing Rules

The non-standard 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 adheres 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 adheres 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

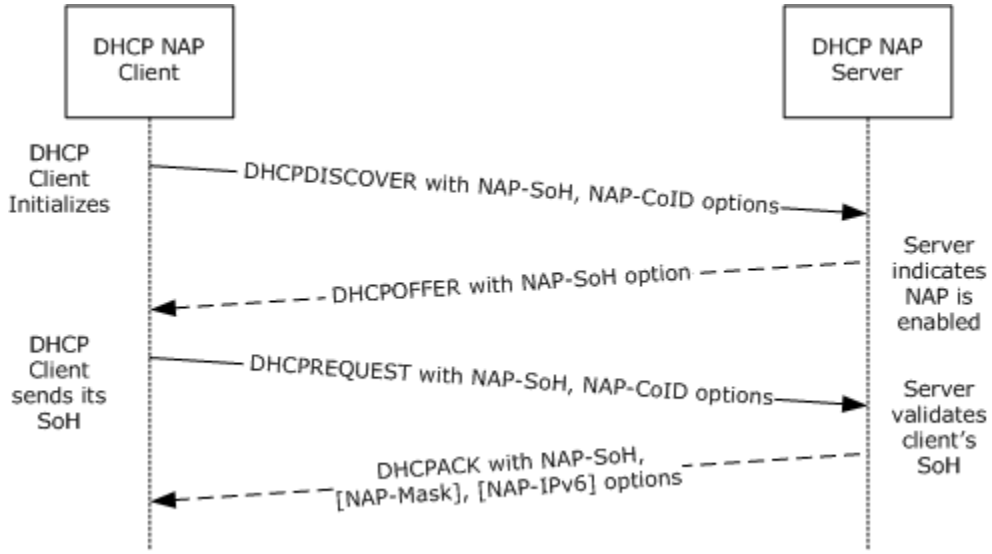


Figure 2: DHCP new lease acquisition process

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 subsequent messages between the client and the server include the DHCPOFFER, DHCPREQUEST and the 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

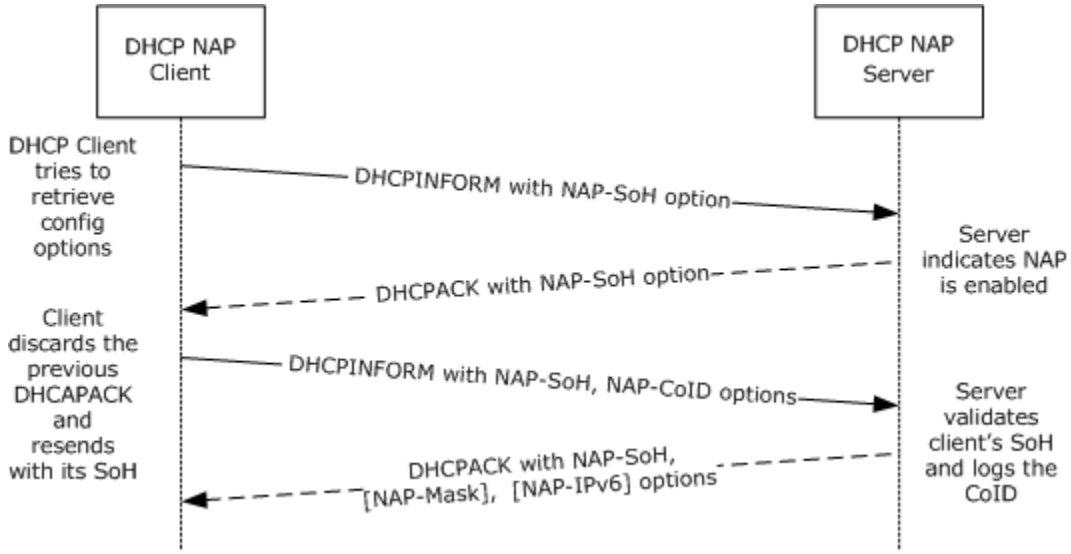


Figure 3: DHCP client request

A DHCP transaction for acquiring IP configuration options that involves NAP enforcement consists of the DHCPINFORM and the DHCPACK messages as specified in sections 3.1.4.3, 3.1.5.3 and 3.2.5.3).

4.3 Message Exchanges During DHCP Lease Renewal

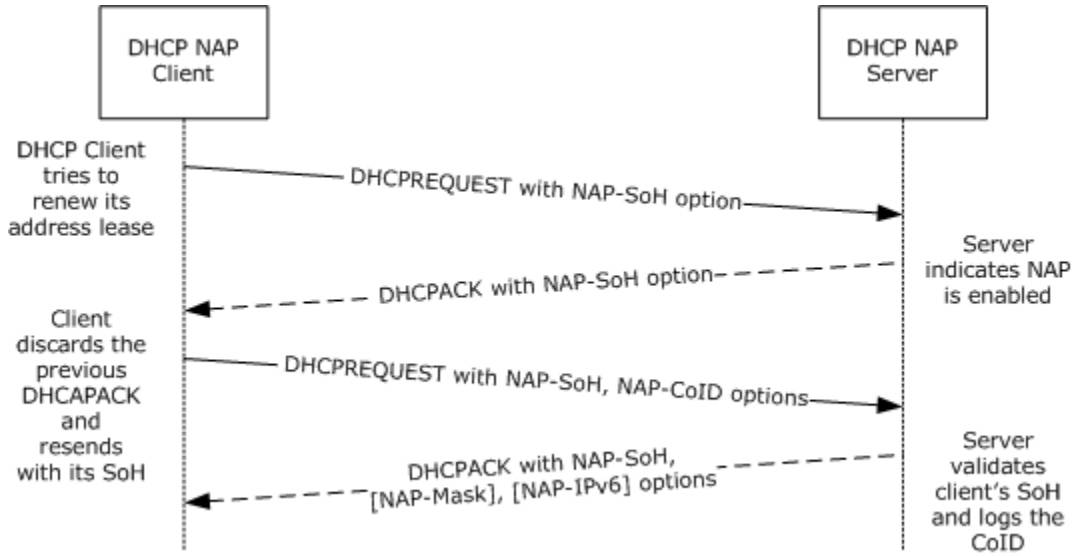


Figure 4: DHCP lease renewal process

A DHCP transaction for renewing an IP address lease involves NAP enforcement consists of the DHCPREQUEST and the DHCPACK messages as described in sections 3.1.4.2, 3.1.5.4 and 3.2.5.2.2).

5 Security

The following sections specify security considerations for administrators of the Dynamic Host Configuration Protocol (DHCP) Extensions for Network Access Protection (NAP).

5.1 Security Considerations for Implementers

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

Since the DHCP protocol as described in [RFC2131] 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 Packet in DHCP messages to the DHCP server on unauthenticated wireless networks.

It is also recommended that DHCP servers implementing this specification 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: Windows Behavior

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

- Windows XP SP3
- Windows Vista
- Windows Server 2008

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

<1> Section 2.2.1.2: The NAP Subnet Mask packet (NAP-Mask) 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-GUID] to generate a NAP transaction Correlation Identifier which to a very high degree of certainty is unique.

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

<5> Section 3.1.5.3: WindowsDHCP clients do not pass the SoH-Response sent by the DHCP server to the NAP Agent. Instead they ignore the NAP-SoH option and the NAP-IPv6 option (if any), and process the message as if this option were not present in the message. As a result, they do not block the IPv6 traffic on the network interface since they cannot determine if the client needs to be quarantined or not.

<6> Section 3.2.5.3: Windows DHCP servers do not extract the SoH token from the NAP-SoH option sent by the client or pass the SoH to the health policy server.

7 Index

T

V

W