[MS-RNAP]: Vendor-Specific RADIUS Attributes for Network Access Protection (NAP) Data Structure

Revision Summary

Date	Revision History	Revision Class	Comments
03/14/2007	1.0	Major	Updated and revised the technical content.
04/10/2007	1.1	Minor	Updated the technical content.
05/18/2007	2.0	Major	Replaced normative reference; Clarifications
06/08/2007	2.1	Minor	Updated the technical content.
07/10/2007	2.1.1	Editorial	Revised and edited the technical content.
08/17/2007	2.1.2	Editorial	Revised and edited the technical content.
10/26/2007	3.0	Major	Converted document to unified format.
01/25/2008	3.0.1	Editorial	Revised and edited the technical content.
03/14/2008	4.0	Major	Updated and revised the technical content.
06/20/2008	5.0	Major	Updated and revised the technical content.
07/25/2008	6.0	Major	Updated and revised the technical content.
08/29/2008	7.0	Major	Updated and revised the technical content.
10/24/2008	7.1	Minor	Updated the technical content.
12/05/2008	8.0	Major	Updated and revised the technical content.
01/16/2009	9.0	Major	Updated and revised the technical content.
02/27/2009	9.0.1	Editorial	Revised and edited the technical content.
04/10/2009	9.0.2	Editorial	Revised and edited the technical content.
05/22/2009	9.1	Minor	Updated the technical content.
07/02/2009	9.1.1	Editorial	Revised and edited the technical content.
08/14/2009	9.1.2	Editorial	Revised and edited the technical content.
09/25/2009	9.2	Minor	Updated the technical content.
11/06/2009	9.2.1	Editorial	Revised and edited the technical content.
12/18/2009	10.0	Major	Updated and revised the technical content.
01/29/2010	11.0	Major	Updated and revised the technical content.
03/12/2010	12.0	Major	Updated and revised the technical content.
04/23/2010	12.0.1	Editorial	Revised and edited the technical content.

Date	Revision History	Revision Class	Comments
06/04/2010	12.1	Minor	Updated the technical content.
07/16/2010	12.1	No change	No changes to the meaning, language, or formatting of the technical content.
08/27/2010	12.1	No change	No changes to the meaning, language, or formatting of the technical content.
10/08/2010	12.1	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	12.1	No change	No changes to the meaning, language, or formatting of the technical content.
01/07/2011	12.1	No change	No changes to the meaning, language, or formatting of the technical content.
02/11/2011	13.0	Major	Significantly changed the technical content.

Contents

1 Introduction

The Remote Access Dial In User Service (RADIUS) Protocol (as specified in [RFC2865]) provides authentication, authorization, and accounting (AAA) of **endpoints** in scenarios such as wireless networking, dial-up networking, and virtual private networking (VPN).

RADIUS is an extensible protocol that allows vendors to provide specialized behavior through the use of **vendor-specific attributes (VSAs)** ([RFC2865] section 5.26).

1.1 Glossary

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

Dynamic Host Configuration Protocol (DHCP) scope
Dynamic Host Configuration Protocol (DHCP) server
endpoint
Extensible Authentication Protocol (EAP)
filter
globally unique identifier (GUID)
health registration authority (HRA)
Internet Protocol security (IPsec)
little-endian
Network Access Policy
Network Access Protection (NAP)
network access server (NAS)
RADIUS attribute
RADIUS client
RADIUS server
Remote Access Service (RAS) server
security identifier (SID)
statement of health (SoH)
statement of health response (SoHR)
Transmission Control Protocol (TCP)
User Datagram Protocol (UDP)

The following terms are specific to this document:

Routing and Remote Access Service (RRAS): A **RADIUS client** that provisions routing and remote access service capabilities of a Microsoft Windows operating system.

vendor-specific attribute (VSA): A **RADIUS attribute** (as specified in [RFC2865] section 5.26) whose **Value** field contains a vendor identifier, vendor type, and vendor-defined value.

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.

[CM-HCAP] Cisco Systems and Microsoft Corporation, "Cisco Network Admission Control and Microsoft Network Access Protection Interoperability Architecture", http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/ns617/net_implementation_white_paper0900aecd8051fc24.pdf

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

[IANA-PROTO-NUM] Internet Assigned Numbers Authority, "Protocol Numbers", February 2007, http://www.iana.org/assignments/protocol-numbers

[MS-DTYP] Microsoft Corporation, "Windows Data Types", January 2007.

[MS-HCEP] Microsoft Corporation, "Health Certificate Enrollment Protocol Specification", July 2006.

[MS-MSRP] Microsoft Corporation, "Messenger Service Remote Protocol Specification", July 2006.

[MS-NAPSO] Microsoft Corporation, "Network Policy and Access Services System Overview", August 2009.

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

[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

[RFC2548] Zorn, G., "Microsoft Vendor-Specific RADIUS Attributes", RFC 2548, March 1999, http://www.ietf.org/rfc/rfc2548.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

[RFC2868] Zorn, G., Leifer, D., Rubens, A., et al., "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000, http://www.ietf.org/rfc/rfc2868.txt

[RFC3004] Stump, G., Droms, R., Gu, Y., et al., "The User Class Option for DHCP", RFC 3004, June 2000, http://www.ietf.org/rfc/rfc3004.txt

[RFC5080] Nelson, D., and DeKoK, A., "Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes", RFC 5080, December 2007, http://www.ietf.org/rfc/rfc5080.txt

1.2.2 Informative References

[IEEE802.1X] Institute of Electrical and Electronics Engineers, "IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control", December 2004, http://ieeexplore.ieee.org/iel5/9828/30983/01438730.pdf

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

[MSDN-ANSI-CODEPAGE] Microsoft Corporation, "WideCharToMultiByte", 2006, http://msdn.microsoft.com/en-us/library/aa450989.aspx

[MSDN-MS-SSTP] Microsoft Corporation, "Secure Socket Tunneling Protocol (SSTP) Specification", http://msdn.microsoft.com/en-us/library/cc247338.aspx

[MSFT-NAQC] Microsoft Corporation, "Network Access Quarantine Control in Windows Server 2003", 2004, http://technet.microsoft.com/en-us/library/bb726973.aspx

[RFC1661] Simpson, W., Ed., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994, http://www.ietf.org/rfc/rfc1661.txt

[RFC2882] Mitton, D., Nortel Networks, "Network Access Servers Requirements: Extended RADIUS Practices", RFC 2882, July 2000,http://www.ietf.org/rfc/rfc2882.txt

[RFC3579] Aboba, B., and Calhoun, P., "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003, http://www.ietf.org/rfc/rfc3579.txt

1.3 Overview

The Remote Authentication Dial-In User Service (RADIUS) Protocol, as specified in [RFC2865], provides authentication, authorization, and accounting (AAA) of endpoints in scenarios such as wireless networking, dial-up networking, and virtual private networking (VPN). This document specifies the Microsoft vendor-specific attributes (VSAs) that are passed over RADIUS between the **network access server (NAS)** and the **RADIUS server** to authenticate and authorize connection requests, as well as to configure the level of network access provided by the NAS, and account for usage.

The following figure shows a common deployment model for the RADIUS Protocol.

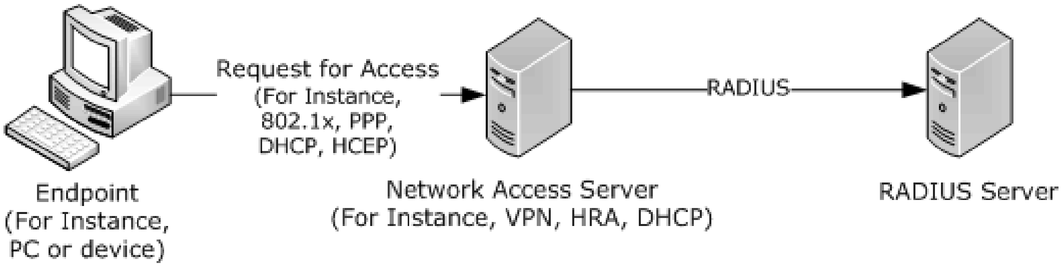

Figure 1: Common RNAP deployment model

An NAS provides network access to endpoints (for example, a client PC or device). An NAS can be a network infrastructure device, such as a switch or a wireless access point, or it can be a server, such as a VPN gateway or dial-up server.

Endpoints initiate communication with an NAS to establish connectivity with a network. A variety of protocols can be used to establish connectivity with a network, such as 802.1x (as specified in [IEEE802.1X]) or Point-to-Point Protocol (PPP) (as specified in [RFC1661]). The NAS then exchanges RADIUS messages with a RADIUS server to authenticate and authorize the endpoint's connectivity to the network. The RADIUS server is configured with policy to accept or reject the endpoint's connectivity request and to instruct the NAS as to the network restrictions to enforce on the endpoint, if appropriate.

The RADIUS Protocol includes an extensibility mechanism that enables NAS vendors and RADIUS server vendors to expose features specific to their products through the use of vendor-specific attributes (VSAs), as specified in [RFC2865] section 5.26.

1.4 Relationship to Other Protocols

The VSAs specified in this document rely on and are transported within the RADIUS Protocol.

Protocols between the client and the **Network Access Protection (NAP)** (for example, PPP [RFC1661], 802.1x [IEEE802.1X], and [MS-HCEP]) relate to the Microsoft VSAs in the following ways:

- Unless otherwise noted, **RADIUS attributes** are sent only between a **RADIUS client** and a RADIUS server. However, some Microsoft RADIUS VSAs may be transported over the protocols between the endpoint and the NAS in addition to being transported over RADIUS. For example, the Health Certificate Enrollment Protocol transports the MS-AFW-Zone attribute, as specified in [MS-HCEP] section 13.

- The Microsoft RADIUS VSAs may affect the operation of the protocols between the endpoint and the NAS. For example, the MS-Quarantine-Grace-Time sets a limit on the time that a client can remain connected through a particular NAS, regardless of the protocol between the client and NAS.

1.5 Prerequisites/Preconditions

The RADIUS Protocol and a set of **Network Access Policies** are configured for use between a NAS and a RADIUS server for the Microsoft VSAs to be used; specifically, an administrator is required to configure a RADIUS shared secret between a NAS and a RADIUS server.

1.6 Applicability Statement

The use of RADIUS VSAs is applicable in those environments where the RADIUS Protocol is used to authenticate and authorize network access requests.

1.7 Versioning and Capability Negotiation

None of the Microsoft RADIUS VSAs described in this document affects the versioning or capability negotiation of the protocols they are transported over. Some of the Microsoft RADIUS VSAs described in this document may not be recognized by a particular type or model of NAS - the behavior of RADIUS client encountering unknown attributes is described in [RFC5080] section 2.5.

See the individual VSAs documented in Message Syntax (section 2.2) for information about version fields.

1.8 Vendor-Extensible Fields

The Microsoft VSAs themselves do not define any additional vendor-extensible fields.

1.9 Standards Assignments

Parameter	Value	Reference
RADIUS VSA type	0x1A	[RFC2865], section 5.26
SMI Network Management Private Enterprise Code for the Vendor ID field	0x00000137	[IANA-ENT]

2 Messages

This protocol references commonly used data types as defined in [MS-DTYP].

2.1 Transport

The RADIUS Protocol, specified in [RFC2865], defines the transport of RADIUS and associated attributes over the **User datagram protocol (UDP)**.

2.2 Message Syntax

2.2.1 Microsoft Vendor-Specific Attributes (VSAs)

The RADIUS Protocol specification [RFC2865] defines attribute type 0x1A as a VSA. This type was defined to allow vendors to extend the RADIUS attribute set. For reference, the format of the standard RADIUS attribute is provided below.

When representing a VSA, the fields MUST be set as follows (for more information, see [RFC2865]).

<table>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>20</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>30</th><th>1</th></tr>
<tr><td colspan="8">Type</td><td colspan="8">Length</td><td colspan="16">Value (variable)</td></tr>
<tr><td colspan="32">...</td></tr>
</table>

Type (1 byte): An 8-bit unsigned integer that MUST be 0x1A, which indicates the type of the **Value** field as vendor-specific.

Length (1 byte): An 8-bit unsigned integer that MUST specify the sum of the lengths of an attribute's **Type**, **Length**, and **Value** fields, in bytes. For vendor-specific RADIUS attributes, the value MUST be at least 9 to account for the **Type**, **Length**, and **Value** fields. The RADIUS client SHOULD ignore the attribute if the value is less than 9.

Value (variable): For Microsoft vendor-specific RADIUS attributes, the value MUST be formatted as described in [RFC2865] section 5.26. For reference, the format is as follows.

<table>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>20</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>30</th><th>1</th></tr>
<tr><td colspan="32">Vendor-ID</td></tr>
<tr><td colspan="8">Vendor-Type</td><td colspan="8">Vendor-Length</td><td colspan="16">Attribute-Specific Value (variable)</td></tr>
<tr><td colspan="32">...</td></tr>
</table>

Vendor-ID (4 bytes): A 32-bit unsigned integer in network byte order, the most significant 8 bits MUST be set to 0 and the remaining 24 bits MUST be set to the SMI code of the vendor taken from [IANA-ENT]. Microsoft VSAs MUST have the **Vendor-ID** field set to 311 (0x00000137).

Vendor-Type (1 byte): An 8-bit unsigned integer that MUST specify the VSA type contained in the **Attribute-Specific Value** field. Microsoft VSA vendor types MUST be set as specified in [RFC2548] and in sections 2.2.1.1 through 2.2.1.27 of this specification.

Vendor-Length (1 byte): An 8-bit unsigned integer that MUST be set to 2 plus the length of **Attribute-Specific Value**. The RADIUS client SHOULD ignore the attribute if Vendor-Length is less than 3.

Attribute-Specific Value (variable): The value of the VSA specified in the **Vendor-Type** field. The format of the **Attribute-Specific Value** field for a given **Vendor-Type** MUST be set as specified in [RFC2548] and in sections 2.2.1.1 through 2.2.1.27 of this specification.

The attribute definitions in the following sections specify the specific parameters relevant to that extension.

2.2.1.1 MS-RAS-Client-Name

MS-RAS-Client-Name is a VSA, as specified in section 2.2.1. It is used to specify the name of the endpoint generating a request.

The fields of the **MS-RAS-Client-Name** VSA MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x22 for **MS-RAS-Client-Name**.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 2 added to the length of the Attribute-Specific **Value** field. Its value MUST be at least 3 and less than 36.

Attribute-Specific Value: This field MUST be the machine name of the endpoint that requests network access, sent in ASCII format, and MUST be null terminated. A valid character set includes the symbols ! @ # $ % ^ & ') (. - _ { } ~ in addition to letters and numbers.<1>

For more information about MS-RAS-Client-Name, see sections 3.1.5.4.1 and 3.2.5.4.1.

2.2.1.2 MS-RAS-Client-Version

MS-RAS-Client-Version is a VSA, as specified in section 2.2.1. It is used to specify the version of the endpoint generating a request.

The fields of the MS-RAS-Client-Version vendor-specific attribute MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x23 for MS-RAS-Client-Version.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 2 added to the length of the Attribute-Specific **Value** field. Its value MUST be at least 3.

Attribute-Specific Value: This field MUST be the ASCII version string of a remote access client; this string MUST be in network byte order.<2>

For more information about MS-RAS-Client-Version, see sections 3.1.5.4.2 and 3.2.5.4.2.

2.2.1.3 MS-Quarantine-IPFilter

MS-Quarantine-IPFilter is a VSA, as specified in section 2.2.1. It is used to specify the set of IP filters to be provisioned for the endpoint associated with a RADIUS Access-Request (as specified in [RFC2865]).

The fields of MS-Quarantine-IPFilter MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x24 for MS-Quarantine-IPFilter.

Vendor-Length: An 8-bit unsigned integer that MUST be set to the length of the Attribute-Specific **Value** field plus 2. Its value MUST be at least 74 to specify at least 1 **filter**. The total length will depend on the number of filter sets and filters in each set.

Attribute-Specific Value: A list of IPv4 filter sets, defined as follows:

The usage of this attribute within Access-Request, Access-Accept, Access-Reject, Access-Challenge and Accounting-Request packets is defined in section 3.1.5.2. If multiple MS-Quarantine-IPFilter VSAs occur in a single RADIUS packet, the Attribute-Specific **Value** field from each MUST be concatenated in the order received to form the full MS-Quarantine-IPFilter value.

										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Version																															
Size																															
FilterSetEntryCount																															
FilterSetEntryList (variable)																															
...																															
FilterSetList (variable)																															
...																															

Version (4 bytes): A 32-bit unsigned integer in **little-endian** byte order that MUST be set to 0x00000001. No other versions are defined. See section 3.1.5.3 for processing details.

Size (4 bytes): A 32-bit unsigned integer in little-endian byte order that MUST specify the size of the VSA field for this VSA, including the version, size, and subsequent filter set data. The size MUST be at least 72, so as to specify at least 1 filter. The total size will depend on the number of filter sets and filters in each set.

FilterSetEntryCount (4 bytes): A 32-bit unsigned integer in little-endian byte order that MUST specify the number of filter set entries. Its value MUST be greater than 0.

FilterSetEntryList (variable): A consecutive list of filter set entries, **FilterSetEntryCount** in number, each of which MUST be formatted as defined below.

										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
InfoType																															

<table>
<tr><td colspan="32">InfoSize</td></tr>
<tr><td colspan="32">FilterSetCount</td></tr>
<tr><td colspan="32">Offset</td></tr>
</table>

InfoType (4 bytes): A 32-bit unsigned integer in little-endian order specifying the type of filters that are contained in the filter set list. The value MUST be one of the following.

Value	Meaning
0xffff0001	Input filter: The filter MUST be applied to IP packets sent from the endpoint to the Network Access Server (NAS).
0xffff0002	Output filter: The filter MUST be applied to IP packets sent from the NAS to the endpoint.
0xffff0009	Site-to-site connection: IP traffic that matches this filter indicates to the NAS that a site-to-site connection MUST be connected and all IP packets matching this filter MUST be routed into the connection.

InfoSize (4 bytes): A 32-bit unsigned integer in little-endian byte order that MUST specify the overall size, in bytes, of the list of filtersets specified by this filter set entry.

FilterSetCount (4 bytes): A 32-bit unsigned integer in little-endian byte order that MUST specify the number of filter sets in this entry. Its value MUST be greater than 0.

Offset (4 bytes): A 32-bit unsigned integer in little-endian byte order that MUST specify the offset of the start of the first filter set of this filter set entry within the Attribute-Specific **Value** of this VSA. Offset values are always multiples of 8 (in other words, a filter set MUST begin at an 8-octet aligned offset within the Attribute-Specific Value). To meet this requirement, any unused octets (holes) within the Attribute-Specific Value before or after a filter set MUST be set to 0 (in other words, padded), as necessary.

FilterSetList (variable): A consecutive list of filter sets equal in number to the value of **FilterSetCount**, each of which MUST be formatted as defined below.

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>1
0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>2
0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>3
0</td><td>1</td></tr>
<tr><td colspan="32">FilterVersion</td></tr>
<tr><td colspan="32">FilterCount</td></tr>
<tr><td colspan="32">ForwardAction</td></tr>
<tr><td colspan="32">FilterList (variable)</td></tr>
<tr><td colspan="32">...</td></tr>
</table>

FilterVersion (4 bytes): A 32-bit unsigned integer in little-endian byte order that MUST be set to 0x00000001. No other versions are defined. For processing details, see section 3.1.5.3.

FilterCount (4 bytes): A 32-bit unsigned integer in little-endian byte order that MUST specify the number of filters. Its value MUST be greater than 0.

ForwardAction (4 bytes): A 32-bit unsigned integer in little-endian byte order that MUST specify the action for the filter. Its value MUST be one of the following.

Value	Meaning
0x00000000	Forward
0x00000001	Drop

FilterList (variable): A consecutive list of filters, equal in number to the value of **FilterCount**, each of which MUST be formatted as defined below:

<table>
<tr><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>1</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>2</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>3</th><th></th></tr>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>0</th><th>1</th></tr>
<tr><td colspan="32">Source Address</td></tr>
<tr><td colspan="32">Source Mask</td></tr>
<tr><td colspan="32">Destination Address</td></tr>
<tr><td colspan="32">Destination Mask</td></tr>
<tr><td colspan="32">Protocol</td></tr>
<tr><td colspan="32">Late Bound</td></tr>
<tr><td colspan="16">Source Port</td><td colspan="16">Destination Port</td></tr>
</table>

Source Address (4 bytes): A 32-bit unsigned integer in network byte order specifying the IPv4 source address for which the filter applies. A value of 0x0000000 in this field denotes ANY.

Source Mask (4 bytes): A 32-bit unsigned integer in network byte order specifying the subnet mask for the source address.

Destination Address (4 bytes): A 32-bit unsigned integer in network byte order specifying the IPv4 destination address for the filter. A value of 0x00000000 in this field denotes ANY.

Destination Mask (4 bytes): A 32-bit unsigned integer in network byte order specifying the subnet mask for the destination address in network byte order.

Protocol (4 bytes): A 32-bit unsigned integer in little-endian byte order specifying the protocol number (such as **TCP** or User Datagram Protocol (UDP)) for the filter. Possible values include the following.

Name	Value
ANY	0x00000000
ICMP	0x00000001
TCP	0x00000006
UDP	0x00000011

The complete list is specified in [IANA-PROTO-NUM].

Late Bound (4 bytes): A 32-bit unsigned integer in little-endian byte order specifying whether the fields in the filter is dynamically replaced by an NAS with values for specific endpoints. Its value MUST be at least one of the following or a bit-wise OR result of two or more such values.

Value	Meaning
0x00000000	No Source or Destination Address or Mask Replacement
0x00000001	Source Address replaceable with a new address
0x00000004	Destination Address replaceable with a new address
0x00000010	Source Address Mask replaceable with a new Mask
0x00000020	Destination Address Mask replaceable with a new Mask

Source Port (2 bytes): If the Protocol is TCP or UDP, this MUST be a 16-bit unsigned integer in network byte order that specifies a port number for the corresponding protocol. If the Protocol is ICMP or ICMPv6, this MUST be a 16-bit unsigned integer in little-endian byte order that specifies a corresponding type indicator for ICMP or ICMPv6. For all other protocol values, this MUST be set to 0 (byte order does not matter).

Destination Port (2 bytes): If the Protocol is TCP or User Datagram Protocol (UDP), this MUST be a 16-bit unsigned integer in network byte order that specifies a port number for the corresponding protocol. If the Protocol is ICMP or ICMPv6, this MUST be a 16-bit unsigned integer in little-endian byte order that specifies a corresponding code indicator for ICMP or ICMPv6. For all other protocol values, this MUST be set to 0 (byte order does not matter).

For more information about MS-Quarantine-IPFilter, see sections 3.1.5.4.3 and 3.2.5.4.3.

2.2.1.4 MS-Quarantine-Session-Timeout

MS-Quarantine-Session-Timeout is a VSA, as specified in 2.2.1. It is used to specify a timeout value used by a **RRAS** server.

The fields of MS-Quarantine-Session-Timeout MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x25.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 6.

Attribute-Specific Value: A 32-bit unsigned integer in network byte order that MUST contain the time in seconds that a restricted VPN connection can remain in a restricted state before being disconnected.

For more information about MS-Quarantine-Session-Timeout, see sections 3.1.5.4.4 and 3.2.5.4.4.

2.2.1.5 MS-User-Security-Identity

MS-User-Security-Identity is a VSA, as specified in section 2.2.1. It is used to specify the **security-identifier (SID)**, as defined in [MS-DTYP] section 2.4.2, of the user requesting access.

The fields of MS-User-Security-Identity MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x28 for MS-User-Security-Identity.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 2 plus the length of the Attribute-Specific **Value** field. Its value MUST be at least 3.

Attribute-Specific Value: This field MUST contain the account SID of the user requesting access in the format of a binary SID used to authenticate a remote access client.

2.2.1.6 MS-Identity-Type

MS-Identity-Type is a VSA, as specified in section 2.2.1. It is used to specify that the RADIUS server MUST process access authorization based on a machine health-check only.

The fields of MS-Identity-Type MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x29.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 6.

Attribute-Specific Value: A 32-bit unsigned integer in network byte order that MUST contain the following value.

Value	Meaning
0x00000001	Indicates to the RADIUS server that this access request message is for a machine health check only and not for authentication.

For more information about MS-Identity-Type, see sections 3.1.5.4.6 and 3.2.5.4.6.

2.2.1.7 MS-Service-Class

MS-Service-Class is a VSA, as specified in section 2.2.1. It is used to specify which group of **DHCP scopes** should supply an IP address to the endpoint requesting access.

The fields of MS-Service-Class MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x2A.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 2 plus the length of the Attribute-Specific **Value** field. Its value MUST be at least 3.

Attribute-Specific Value: The name of a group of DHCP scopes that correspond to the endpoint requesting access. This name string MUST be sent as characters using the code page of the current system (see [MSDN-ANSI-CODEPAGE]). This field MUST only be used when the RADIUS client is a **DHCP server**.

For more information about MS-Service-Class, see sections 3.1.5.4.7 and 3.2.5.4.7.

2.2.1.8 MS-Quarantine-User-Class

MS-Quarantine-User-Class is a VSA, as specified in section 2.2.1. It is used to carry the name of a special DHCP user class, as specified in [RFC3004], called NAP user class.

The fields of MS-Quarantine-User-Class MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x2C.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 2 plus the length of the Attribute-Specific **Value** field. RADIUS client SHOULD ignore the attribute if Vendor-Length is less than 3.

Attribute-Specific Value: This field MUST contain the name of the DHCP user class to be assigned to the endpoint that is requesting access from a DHCP server. The name MUST be sent in ASCII characters with the code page to be the current system Microsoft Windows® ANSI code page (see [MSDN-ANSI-CODEPAGE]) in ANSI format (that is, the string is sent with ANSI code page). For more information about the DHCP option for user class, see [RFC3004].

For more information about MS-Quarantine-User-Class, see sections 3.1.5.4.8 and 3.2.5.4.8.

2.2.1.9 MS-Quarantine-State

MS-Quarantine-State is a VSA, as specified in section 2.2.1. It is used to specify the target restrictive state of the endpoint.

The fields of MS-Quarantine-State MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x2D.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 6.

Attribute-Specific Value: A 32-bit unsigned integer in network byte order that MUST specify the network access level that the RADIUS server authorizes for the endpoint. It MUST be one for the following values.

Value	Meaning
0x00000000	Full access: The endpoint is given full access to the network.
0x00000001	Restricted: The endpoint is given limited access to the network.
0x00000002	On probation: The endpoint is given full access within a limited time period.

For more information about MS-Quarantine-State, see sections 3.1.5.4.9 and 3.2.5.4.9.

2.2.1.10 MS-Quarantine-Grace-Time

MS-Quarantine-Grace-Time is a VSA, as specified in section 2.2.1. It is used to specify the amount of time a host has to conform to network policy.

The fields of MS-Quarantine-Grace-Time MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x2E.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 6.

Attribute-Specific Value: A 32-bit unsigned integer in network byte order that MUST specify the number of seconds since 1/1/1970 UTC (GMT) that the RADIUS server authorizes the endpoint to have full network access. After this time, the endpoint is expected to be authorized to have only restricted access.

For more information about MS-Quarantine-Grace-Time, see sections 3.1.5.4.10 and 3.2.5.4.10.

2.2.1.11 MS-Network-Access-Server-Type

MS-Network-Access-Server-Type is a VSA, as specified in section 2.2.1. It is used to specify the type of a network access server making the request.

The fields of MS-Network-Access-Server-Type MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x2F.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 6.

Attribute-Specific Value: A 32-bit unsigned integer in network byte order that MUST indicate the type of the NAS. The value MUST be interpreted in accordance with the following table:

Value	Meaning
0x00000000	Unspecified
0x00000001	Terminal Server Gateway
0x00000002	**Remote Access Service (RAS) server** (VPN or dial-in)
0x00000003	DHCP server
0x00000005	**Health Registration Authority (HRA)**
0x00000006	Host Credential Authorization Protocol (HCAP) server
All Other Values	A tag value used to identify applicable network access policies on the RADIUS server.

For more information about MS-Network-Access-Server-Type, see sections 3.1.5.4.11 and 3.2.5.4.11.

2.2.1.12 MS-AFW-Zone

MS-AFW-Zone is a VSA, as specified in section 2.2.1. When a network access server (NAS) that understands this attribute receives it, it SHOULD provide it to the endpoint that is requesting access (for example, secure zone, boundary zone, or quaratine zone), to be used as a hint for dynamic selection of a preconfigured **Internet Protocol security (IPsec)** policy by the endpoint.

The fields of MS-AFW-Zone MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x30.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 6.

Attribute-Specific Value: A 32-bit unsigned integer in network byte order that MUST indicate the protection level that the RADIUS server authorizes for the endpoint. It MUST be set to one of the following values.

Value	Meaning
0x00000001	Indicates that the endpoint SHOULD apply an IPsec policy that can require encryption (a boundary policy).
0x00000002	Indicates that the endpoint SHOULD apply an IPsec policy that does not require encryption (an unprotected policy).
0x00000003	Indicates that the endpoint SHOULD apply an IPsec policy that does require encryption (a protected policy).

For more information about MS-AFW-Zone, see sections 3.1.5.4.12 and 3.2.5.4.12.

2.2.1.13 MS-AFW-Protection-Level

MS-AFW-Protection-Level is a VSA, as specified in section 2.2.1. It is used as a hint for dynamic selection of a preconfigured IPsec policy by the endpoint requesting access.

The fields of MS-AFW-Protection-Level MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x31.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 6.

Attribute-Specific Value: A 32-bit unsigned integer in network byte order that MUST indicate the protection level that the RADIUS server authorizes for the endpoint. It MUST be set to one of the following values.

Value	Meaning
0x00000001	Indicates that the certificate payload in the Health Certificate Enrollment Protocol (HCEP) response can be used for signing data.
0x00000002	Indicates that the certificate payload in the HCEP response can be used for signing and encrypting data.

For more information about MS-AFW-Protection-Level, see sections 3.1.5.4.13 and 3.2.5.4.13.

2.2.1.14 MS-Machine-Name

MS-Machine-Name is a VSA, as specified in section 2.2.1. It is used to communicate the machine name of the endpoint requesting network access.

The fields of MS-Machine-Name MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x32.

Vendor-Length: An 8-bit unsigned integer that MUST be set to the length of the Attribute-Specific **Value** field plus 2. Its value MUST be at least 3.

Attribute-Specific Value: An octet string containing characters from Windows ANSI code page (see [MSDN-ANSI-CODEPAGE]) in ANSI format and MUST specify the machine name of the endpoint requesting access.

For more information about MS-Machine-Name, see sections 3.1.5.4.14 and 3.2.5.4.14.

2.2.1.15 MS-IPv6-Filter

MS-IPv6-Filter is a VSA, as specified in section 2.2.1. It is used to limit the inbound and/or outbound access of the endpoint.

The fields of MS-IPv6-Filter MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x33.

Vendor-Length: An 8-bit unsigned integer that MUST be set to the length of the Attribute-Specific **Value** field plus 2. Its value MUST be at least 98, to specify a minimum of 1 filter. The total length will depend on the number of filter sets and filters in each set.

Attribute-Specific Value: A list of IPv6 filter sets, defined as follows.

The usage of this attribute within Access-Request, Access-Accept, Access-Reject, Access-Challenge and Accounting-Request packets is defined in section 3.1.5.2. If multiple MS-IPv6-Filter attributes occur in a single RADIUS packet, the Attribute-Specific **Value** field from each MUST be concatenated in the order received to form the full MS-IPv6-Filter value.

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
Version																															
Size																															
FilterSetEntryCount																															
FilterSetEntryList (variable)																															
...																															
FilterSetList (variable)																															
...																															

Version (4 bytes): A 32-bit unsigned integer in network byte order that MUST be set to 0x00000001. No other versions are defined. For processing details, see section 3.1.5.3.

Size (4 bytes): A 32-bit unsigned integer in network byte order that MUST specify the size of the Attribute-Specific **Value** field for this VSA, including the version, size, and subsequent filter set data. The size MUST be at least 96, so as to specify at least one filter. The total size depends on the number of filter sets and filters in each set.

FilterSetEntryCount (4 bytes): A 32-bit unsigned integer in network byte order that MUST specify the number of filter set entries. Its value MUST be greater than 0.

FilterSetEntryList (variable): A list of consecutive filter set entries, equal in number to the value of **FilterSetEntryCount**, each of which MUST be formatted as defined below.

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
InfoType																															
InfoSize																															
FilterSetCount																															
Offset																															

InfoType (4 bytes): A 32-bit unsigned integer in network byte order specifying the type of filters that are contained in the filter set list. The value MUST be one of the following.

Value	Meaning
0xffff0011	Input filter – The filter NAS MUST be applied to IP packets sent from the endpoint to the NAS.
0xffff0012	Output filter – The filter MUST be applied to IP packets sent from the NAS to the endpoint.

InfoSize (4 bytes): A 32-bit unsigned integer in network byte order specifying the overall size, in bytes, of the list of filter sets specified by this filter set entry.

FilterSetCount (4 bytes): A 32-bit unsigned integer in network byte order specifying the overall size, in bytes, of the list of filter sets specified by this filter set entry.

Offset (4 bytes): A 32-bit unsigned integer in network byte order specifying the offset of start of the first filter set of this filter set entry within the Attribute-Specific **Value** of this VSA. Offset values are always multiples of 8, and a filter set MUST therefore begin at an 8-octet aligned offset within the Attribute-Specific **Value**. To meet this requirement, any unused octets (holes) within the Attribute-Specific **Value** before or after a filter set MUST be set to 0 (padded) as necessary.

FilterSetList (variable): A list of consecutive filter sets, equal in number to the value of **FilterSetCount**, each of which MUST be formatted as defined below.

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
FilterVersion																															
FilterCount																															
ForwardAction																															
FilterList (variable)																															

...

FilterVersion (4 bytes): A 32-bit unsigned integer in network byte order that MUST be set to 0x00000001. No other versions are defined. For processing details, see section 3.1.5.3.

FilterCount (4 bytes): A 32-bit unsigned integer in network byte order specifying the number of filters. Its value MUST be greater than 0.

ForwardAction (4 bytes): A 32-bit unsigned integer in network byte order specifying the action for the filter. Its value MUST be one of the following.

Value	Meaning
0x00000000	Forward
0x00000001	Drop

FilterList (variable): A list of consecutive filters, equal in number to the value of **FilterCount**, each of which MUST be formatted as defined below.

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
Source Address																															
...																															
...																															
...																															
Source Prefix Length																															
Destination Address																															
...																															
...																															
...																															
Destination Prefix Length																															
Protocol																															

Late Bound	
Source Port	Destination Port

Source Address (16 bytes): A 128-bit unsigned integer in network byte order specifying the IPv6 source address for which the filter applies. A value of 0x00000000 in this field MUST denotes ANY.

Source Prefix Length (4 bytes): A 32-bit unsigned integer in network byte order specifying the prefix length for the source address. If this value is set to zero, the NAS MUST use ANY as a source address.

Destination Address (16 bytes): A 128-bit unsigned integer in network byte order that specifies the IPv6 destination address for the filter. A value of zero in this field denotes ANY.

Destination Prefix Length (4 bytes): A 32-bit unsigned integer in network byte order that specifies the Prefix Length for the destination address. If this value is set to zero, the NAS MUST use ANY as a Destination address.

Protocol (4 bytes): A 32-bit unsigned integer in network byte order specifying the protocol number (such as TCP or UDP) for the filter. Possible values include the following.

Name	Value
ANY	0x00000000
ICMP	0x00000001
ICMPv6	0x0000003A
TCP	0x00000006
UDP	0x00000011

Late Bound (4 bytes): A 32-bit unsigned integer in network byte order that indicates if the fields in the filter MAY be dynamically replaced by the NAS with values for specific endpoints. Its value MUST be at least one of the following or a bit-wise OR of two or more such values.

Value	Meaning
0x00000000	No source or destination address or mask replacement
0x00000001	Source address replaceable with a new address
0x00000004	Destination address replaceable with a new address
0x00000010	Source address mask replaceable with a new mask
0x00000020	Destination address mask replaceable with a new mask

Source Port (2 bytes): If the Protocol is TCP or UDP, this MUST be a 16-bit unsigned integer in network byte order that specifies a port number for the corresponding protocol. If the Protocol is ICMP or ICMPv6, this MUST be a 16-bit unsigned integer in network byte order that specifies a corresponding type indicator for ICMP or ICMPv6. For all other protocol values, this MUST be set to 0 (byte order does not matter).

Destination Port (2 bytes): If the Protocol is TCP or UDP, this MUST be a 16-bit unsigned integer in network byte order that specifies a port number for the corresponding protocol. If the Protocol is ICMP or ICMPv6, this MUST be a 16-bit unsigned integer in network byte order that specifies a corresponding code indicator for ICMP or ICMPv6. For all other protocol values, this MUST be set to 0 (byte order does not matter).

For more information about MS-IPv6-Filter, see sections 3.1.5.4.15 and 3.2.5.4.15.

2.2.1.16 MS-IPv4-Remediation-Servers

MS-IPv4-Remediation-Servers is a VSA, as specified in section 2.2.1. This value is used to specify a list of servers that should be reachable by an endpoint with restricted access so that it may remediate itself.

The fields of MS-IPv4-Remediation-Servers MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x34.

Vendor-Length: An 8-bit unsigned integer that MUST be set to the length of the Attribute-Specific **Value** field plus 2. Only values greater than 6 whose value modulo 4 equals 3 are valid.

Attribute-Specific Value: An 8-bit unsigned integer, which is reserved and which MUST be set to 0 by the RADIUS server, followed by a list of IPv4 addresses that the RADIUS server authorizes a restricted endpoint to access. The list MUST be formatted as a sequential series of 4-octet values. Each of the four-octet values MUST be an IPv4 address in network byte order.

For more information about MS-IPv4-Remediation-Servers, see sections 3.1.5.4.16 and 3.2.5.4.16.

2.2.1.17 MS-IPv6-Remediation-Servers

MS-IPv6-Remediation-Servers is a VSA, as specified in section 2.2.1. This value is used to specify a list of servers that should be reachable by an endpoint with restricted access so that it may remediate itself.

The fields of MS-IPv6-Remediation-Servers MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x35.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 2 plus the length of the Attribute-Specific **Value** field. Only values greater than 18 whose value modulo 16 equals 3 are valid.

Attribute-Specific Value: An 8-bit unsigned integer, which is reserved and which MUST be set to 0 by the RADIUS server, followed by a list of IPv6 addresses that the RADIUS server authorizes a restricted endpoint to access. The list MUST be formatted as a sequential series of 16-octet values. Each of the 16-octet values MUST be an IPv6 address in network byte order.

For more information about MS-IPv6-Remediation-Servers, see sections 3.1.5.4.17 and 3.2.5.4.17.

2.2.1.18 Not-Quarantine-Capable

Not-Quarantine-Capable is a VSA used by a RADIUS client to specify whether an endpoint sent an **SoH** or not, as specified in section 2.2.1.

The fields of Not-Quarantine-Capable MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x36.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 6.

Attribute-Specific Value: A 32-bit unsigned integer in network byte order that MUST indicate whether the endpoint is capable of reporting its state to the NAS. It MUST be one of the following values.

Value	Meaning
0x00000000	The endpoint sent a SoH.
0x00000001	The endpoint did not send an SoH.

For more information about Not-Quarantine-Capable, see sections 3.1.5.4.18 and 3.2.5.4.18.

2.2.1.19 MS-Quarantine-SOH

MS-Quarantine-SOH is a VSA, as specified in 2.2.1. It is used to carry Statement of Health information (as specified in [MS-SOH]).

The fields of MS-Quarantine-SOH MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x37.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 2 plus the length of the Attribute-Specific **Value** field. Its value MUST be at least 12.

Attribute-Specific Value: This field MUST be formatted as a SOH, as specified in [MS-SOH] section 2.2.5.

For more information about MS-Quarantine-SOH, see sections 3.1.5.4.19 and 3.2.5.4.19.

2.2.1.20 MS-RAS-Correlation-ID

The MS-RAS-Correlation-ID is a VSA, as specified in section 2.2.1.

The fields of MS-RAS-Correlation-ID MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x38.

Vendor-Length: An 8-bit unsigned integer that MUST be set to the length of the **globally unique identifier (GUID)** string in the Attribute-Specific value plus 2.

Attribute-Specific Value: A 128-bit unsigned integer that SHOULD specify a GUID and be represented using a curly braced GUID string, as defined in MS-DTYP (section 2.3.2).

2.2.1.21 MS-Extended-Quarantine-State

The MS-Extended-Quarantine-State VSA is used to specify additional information about a restricted access decision by a RADIUS server, as specified in section 2.2.1.

The fields of MS-Extended-Quarantine-State MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x39.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 6.

Attribute-Specific Value: A 32-bit unsigned integer in network-byte order that MUST contain one of the following values.

Value	Meaning
0x00000000	No data
0x00000001	Transition
0x00000002	Infected
0x00000003	Unknown

2.2.1.22 HCAP-User-Groups

HCAP-User-Groups is a VSA used to specify user groups information received over a HCAP interface [CM-HCAP] by a RADIUS client, as specified in section 2.2.1.

The fields of HCAP-User-Groups MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x3A.

Vendor-Length: An 8-bit unsigned integer that MUST be set to the length of the Attribute-Specific **Value** field plus 2. Its value MUST be at least 3.

Attribute-Specific Value: An octet string that contains characters from Windows ANSI code page (for more information, see [MSDN-ANSI-CODEPAGE]) and MUST specify the group name to which an HCAP user belongs (as specified in [MS-HCEP]).

2.2.1.23 HCAP-Location-Group-Name

HCAP-Location-Group-Name is a VSA used to specify location group information received over a HCAP interface [CM-HCAP] by a RADIUS client, as specified in section 2.2.1.

The fields of HCAP-Location-Group-Name MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x3B.

Vendor-Length: An 8-bit unsigned integer that MUST be set to the length of the Attribute-Specific **Value** field plus 2. Its value MUST be at least 3.

Attribute-Specific Value: An octet string that contains characters from Windows ANSI code page (for more information, see [MSDN-ANSI-CODEPAGE]) and MUST specify the location group name for the HCAP entity (as specified in [CM-HCAP]).

2.2.1.24 HCAP-User-Name

HCAP-User-Name is a VSA used to indicate user identity information received over a HCAP interface [CM-HCAP] by a RADIUS client, as specified in section 2.2.1.

The fields of HCAP-User-Name MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x3C.

Vendor-Length: An 8-bit unsigned integer that MUST be set to the length of the Attribute-Specific **Value** field plus 2. Its value MUST be at least 3.

Attribute-Specific Value: An octet string that contains characters from Windows ANSI code page (for more information, see [MSDN-ANSI-CODEPAGE]) and MUST specify the name for the HCAP user (as specified in [CM-HCAP]).

2.2.1.25 MS-User-IPv4-Address

MS-User-IPv4-Address is a VSA used to specify the IPv4 address of the endpoint as known to the RADIUS client, as specified in section 2.2.1.

The fields of MS-User-IPv4-Address MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x3D.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 6.

Attribute-Specific Value: A 32-bit unsigned integer in network byte order that MUST specify the IPv4 address of the machine of the user requesting network access.

2.2.1.26 MS-User-IPv6-Address

MS-User-IPv6-Address is a VSA used to specify the IPv6 address of the endpoint as known to the RADIUS client, as specified in section 2.2.1.

The fields of MS-User-IPv6-Address MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x3E.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 18.

Attribute-Specific Value: A 128-bit unsigned integer in network byte order that MUST specify the IPv6 address of the machine of the user requesting network access.

2.2.1.27 MS-RDG-Device-Redirection

MS-RDG-Device-Redirection is a VSA specifying filters used by a Remote Desktop Gateway, as specified in section 2.2.1.

The fields of MS-RDG-Device-Redirection MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x3F.

Vendor-Length: An 8-bit unsigned integer that MUST be set to 6.

Attribute-Specific Value: A 32-bit unsigned integer in network-byte order (bit 0 is the least significant bit) in which the bits MUST have following meaning.

Bit	Meaning
0	Drives redirection (0: enabled, 1: disabled)
1	Printers redirection (0: enabled, 1: disabled)
2	Serial ports redirection (0: enabled, 1: disabled)
3	Clipboard redirection (0: enabled, 1: disabled)
4	Plug and play devices redirection (0: enabled, 1: disabled)

Bit	Meaning
5-28	<Reserved for additional devices>
29	1: Disable redirection for all devices 0: Device redirection is controlled by bits 0..4
30	1: Enable redirection for all devices 0: Device redirection is controlled, first, by bit 29 and then by bits 0..4
31	<Unused>

When either bit 29 or bit 30 is set to 1, the values for bits 0..4 are ignored.

2.2.2 Microsoft Vendor-Specific Values for RADIUS Attributes

2.2.2.1 Vendor-Specific Value for the Tunnel-Type RADIUS Attribute

In addition to the values specified in [RFC2868], the standard RADIUS attribute Tunnel-Type [RFC2868] is extended to include a value for the Secure Socket Tunneling Protocol (as described in [MS-SSTP]) of 0x013701 in network-byte order. This value was determined using the technique described in [RFC2882], in which "Vendor-Specific Values" are encoded by concatenating the private enterprise ID [IANA-ENT] with an 8-bit unsigned integer value. In this case, a tunnel tag of zero is always used, along with the Microsoft private enterprise ID (0x0137) and an 8-bit unsigned integer value 0x01. As a result, the 4 octet value of the attribute (including the tag) is encoded as 0x00013701.

For more information about using vendor-specific values for the Tunnel-Type RADIUS attribute, see sections 3.1.5.4.28 and 3.2.5.4.28.

3 Protocol Details

3.1 Server Details

3.1.1 Abstract Data Model

The RADIUS Protocol is a stateless protocol, as specified in [RFC2865] section 2.5.

A RADIUS Access-Request is generated by a RADIUS client based on a user request to a NAS. The RADIUS server generates a response containing RADIUS attributes based on the policy settings on the RADIUS server.

3.1.2 Timers

No timers are required. For a discussion of retransmission hints, see the RADIUS Protocol documentation, as specified in [RFC2865].

3.1.3 Initialization

None.

3.1.4 Higher-Layer Triggered Events

The RADIUS exchange is triggered by a request from an NAS.

3.1.4.1 Abstract Interface for Sending a SoHR

SendSoHR: An abstract interface used by the RADIUS server to send a **SoHR** to the PEP server as described in [MS-NAPSO] section 10.3.8. The interface is defined as follows.

```
HRESULT SendSoHR([in] SoHR message);
```

The interface processes the SoHR. If the SoHR permits the connection, it encapsulates the SoHR in an Access-Accept message. If the SoHR does not permit the connection, it encapsulates the SoHR in an Access-Reject message.

3.1.5 Message Processing Events and Sequencing Rules

3.1.5.1 Windows Implementation of RADIUS Attributes

The following section specifies the Microsoft Windows® implementation of RADIUS attributes.<3>

3.1.5.2 Microsoft VSA Support of RADIUS Messages

The RADIUS Protocol standard (as specified in [RFC2865] section 4) defines the messages sent between a RADIUS client and RADIUS server. Each Microsoft VSA is only valid in certain messages as defined in the second table.

The following table defines the meaning of the entries in the second table.

Value	Meaning
0	This attribute MUST NOT be present in packet.
0+	Zero or more instances of this attribute MUST be present in the packet.
0-1	Zero or one instance of this attribute MUST be present in the packet.

Microsoft Vendor-Specific Attribute	Request	Accept	Reject	Challenge	Acct-Request
MS-RAS-Client-Name	0-1	0	0	0	0-1
MS-RAS-Client-Version	0-1	0	0	0	0-1
MS-Quarantine-IPFilter	0	0+	0	0	0+
MS-Quarantine-Session-Timeout	0	0-1	0	0	0-1
MS-User-Security-Identity	0-1	0	0	0	0-1
MS-Identity-Type	0-1	0	0	0	0
MS-Service-Class	0-1	0	0	0	0
MS-Quarantine-User-Class	0	0-1	0	0	0
MS-Quarantine-State	0	0-1	0	0	0
MS-Quarantine-Grace-Time	0	0-1	0	0	0
MS-Network-Access-Server-Type	0-1	0	0	0	0
MS-AFW-Zone	0	0-1	0	0	0
MS-AFW-Protection-Level	0	0-1	0	0	0
MS-Machine-Name	0-1	0	0	0	0-1
MS-IPv6-Filter	0	0+	0	0	0+
MS-IPv4-Remediation-Servers	0	0-1	0	0	0
MS-IPv6-Remediation-Servers	0	0-1	0	0	0
Not-Quarantine-Capable	0	0-1	0	0	0
MS-Quarantine-SoH	0-1	0-1	0	0	0
MS-RAS-Correlation-ID	0-1	0	0	0	0-1
MS-Extended-Quarantine-State	0	0-1	0	0	0
HCAP-User-Groups	0-1	0	0	0	0
HCAP-Location-Group-Name	0-1	0	0	0	0
HCAP-User-Name	0-1	0	0	0	0

Microsoft Vendor-Specific Attribute	Request	Accept	Reject	Challenge	Acct-Request
MS-User-IPv4-Address	0-1	0	0	0	0
MS-User-IPv6-Address	0-1	0	0	0	0
MS-RDG-Device-Redirection	0	0-1	0	0	0

3.1.5.3 Processing RADIUS Attributes

As specified in [RFC2865] section 5, RADIUS clients and RADIUS servers SHOULD<4> ignore VSAs with unknown types.

3.1.5.4 Attributes Details on Server Side

RADIUS servers are responsible for receiving endpoint connection requests from NASs, authenticating the user and/or computer, and authorizing the endpoint. The RADIUS server responds to the NAS with a set of RADIUS attributes that place restrictions on or otherwise specify requirements for the connectivity that the NAS grants the endpoint.

3.1.5.4.1 MS-RAS-Client-Name

When the RADIUS server receives this attribute, it MAY log it.

For more information about this attribute, see section 2.2.1.1.

3.1.5.4.2 MS-RAS-Client-Version

When the RADIUS server receives this attribute, it MAY log it.

For more information about this attribute, see section 2.2.1.2.

3.1.5.4.3 MS-Quarantine-IPFilter

The RADIUS server may send this attribute to an NAS in Access-Accept to specify how to restrict network access for an endpoint.

For the usage details of this filter, see section 3.2.5.4.15. For more information about this attribute, see section 2.2.1.3.

3.1.5.4.4 MS-Quarantine-Session-Timeout

The RADIUS server may send this attribute to an NAS in Access-Accept to specify the time in seconds that a restricted VPN connection can remain in a restricted state before being disconnected.

For more information about this attribute, see section 2.2.1.4.

3.1.5.4.5 MS-User-Security-Identity

Both a user name and user SID can be used to represent the identity of a user who is requesting network access. In most cases, NAS is expected to send a user name to represent the user identity.

NAS may use this attribute as an alternative to the standard RADIUS User-Name attribute [RFC2865], and send a user SID instead of a name to specify the identity of the user who is requesting access.

For more information on this attribute, see 2.2.1.5.

3.1.5.4.6 MS-Identity-Type

This attribute indicates whether a RADIUS server should do only a machine health check (as specified in [MS-SOH]) or not.

A NAS may send this attribute to a RADIUS server in an Access-Request message.

If a RADIUS server receives this attribute and its value is 0x00000001, then the RADIUS server MUST NOT perform authentication; instead, it MUST do a machine health check on this request.

For more information about this attribute, see section 2.2.1.6.

3.1.5.4.7 MS-Service-Class

This attribute carries the name of a service class.

A RADIUS server receiving this attribute knows the service class to which a DHCP client requesting an IP address from a DHCP server belongs.

For more information about this attribute, see section 2.2.1.7.

3.1.5.4.8 MS-Quarantine-User-Class

The RADIUS server may send this attribute to an NAS to specify the name of a special DHCP user class (see [RFC3004]) to which a DHCP client should be assigned.

For more information about this attribute, see section 2.2.1.8.

3.1.5.4.9 MS-Quarantine-State

The RADIUS server may send this attribute to an NAS in Access-Accept to specify the Quarantine state for a user requesting access to this NAS.

For more information about this attribute, see section 2.2.1.9.

3.1.5.4.10 MS-Quarantine-Grace-Time

The RADIUS server may send this attribute to an NAS in Access-Accept to specify an expiration time until an NAS gives full access to an endpoint requesting network access.

For more information about this attribute, see section 2.2.1.10.

3.1.5.4.11 MS-Network-Access-Server-Type

This attribute tells the access type of an NAS. An NAS may send this attribute to RADIUS server to indicate the type of this NAS in an Access-Request message.

For more information about this attribute, see section 2.2.1.11.

3.1.5.4.12 MS-AFW-Zone

This attribute carries the information about the NAP zone (see [MS-HCEP] and [MS-SOH]) in which an endpoint should appear. The RADIUS server may send this attribute in an Access-Accept message to an NAS.

For more information about this attribute, see section 2.2.1.12.

3.1.5.4.13 MS-AFW-Protection-Level

A RADIUS server may send this attribute in an Access-Accept message to an NAS. The NAS in turn sends the message to the endpoint requesting network access.

For more information about this attribute, see section 2.2.1.13.

3.1.5.4.14 MS-Machine-Name

A RADIUS server receiving this attribute learns the machine name. This can be used to determine the machine group to which the user's machine belongs.

For more information about this attribute, see section 2.2.1.14.

3.1.5.4.15 MS-IPv6-Filter

The RADIUS server may send this attribute to an NAS in Access-Accept to define the filters to be applied to the endpoint. It is used only for IPv6 addresses, and MS-Filter [RFC2548] VSA is the corresponding attribute for IPv4 addresses. The structure of MS-Filter is identical to the structure of MS-Quarantine-IPFilter, as specified in section 2.2.1.3.

For more information about this attribute, see 2.2.1.15.

3.1.5.4.16 MS-IPv4-Remediation-Servers

This attribute specifies the IPv4 addresses of the remediation servers. A RADIUS server may send this attribute to an NAS in an Access-Accept message.

For more information about this attribute, see section 2.2.1.16.

3.1.5.4.17 MS-IPv6-Remediation-Servers

This attribute specifies the IPv6 addresses of the rededication servers. A RADIUS server may send this attribute to an NAS in an Access-Accept message.

A RADIUS client that does not implement this attribute or does not support the requested service (restriction of endpoint access to remediation servers) SHOULD ignore this attribute.

For more information about this attribute, see section 2.2.1.17.

3.1.5.4.18 Not-Quarantine-Capable

This attribute indicates whether the endpoint requesting network access is NAP–capable or not. A RADIUS server may send this attribute to an NAS in an Access-Accept message.

For more information about this attribute, see section 2.2.1.18.

3.1.5.4.19 MS-Quarantine-SoH

This attribute carries SoH (as specified in [MS-SOH]) when the **Extensible Authentication Protocol (EAP)**) is not used. The server uses the value of the SoH payload to evaluate the endpoint's compliance to locally configured policy. If an SoH payload is received in the access request, the RADIUS server may return an SoH payload in the access accept message. The value of the payload MUST be the SoHR.

The processing of the SoH message is described in [MS-NAPSO] (section 9).

The process of creating the SoHR is described in [MS-NAPSO] (section 10).

For more information about this attribute, see section 2.2.1.19.

3.1.5.4.20 MS-RAS-Correlation-ID

The RRAS server uses this attribute to match its Access-Requests with RADIUS server responses. When the RADIUS server receives this attribute, it may log it.

For more information about this attribute, see section 2.2.1.20.

3.1.5.4.21 MS-Extended-Quarantine-State

The RADIUS server may send this attribute to a NAS in Access-Accept to specify the additional restricted state information for an endpoint requesting access to this NAS.

For more information about this attribute, see section 2.2.1.21.

3.1.5.4.22 HCAP-User-Groups

If a RADIUS server receives this attribute, it can identify the group to which the user corresponding to the request belongs.

For more information about this attribute, see section 2.2.1.22.

3.1.5.4.23 HCAP-Location-Group-Name

If a RADIUS server receives this attribute, it can identify what location group to which the user's machine corresponding to the request belongs.

For more information about this attribute, see section 2.2.1.23.

3.1.5.4.24 HCAP-User-Name

If a RADIUS server receives this attribute, it can find out the user name corresponding to the request.

For more information about this attribute, see section 2.2.1.24.

3.1.5.4.25 MS-User-IPv4-Address

If a RADIUS server receives this attribute, it can find out the IPv4 address of the endpoint that requested network access.

For more information about this attribute, see section 2.2.1.25.

3.1.5.4.26 MS-User-IPv6-Address

If a RADIUS server receives this attribute, it can find out the IPv6 address of the endpoint that requested network access.

For more information about this attribute, see section 2.2.1.26.

3.1.5.4.27 MS-RDG-Device-Redirection

The RADIUS server may send this attribute to an NAS to specify the device redirection settings for Remote Desktop Gateway.

For more information about this attribute, see section 2.2.1.27.

3.1.5.4.28 Vendor-Specific Value for Tunnel-Type RADIUS Attribute

A RADIUS server MUST process the Tunnel-Type RADIUS attribute as specified in [RFC2868], with one additional constraint: if the value of the Tunnel-Type RADIUS attribute is 0x00013701, it SHOULD be taken as a hint to the RADIUS server that the tunneling protocol supported by the tunnel end-point is SSTP. <5>

For more information about this vendor-specific value for the Tunnel-Type RADIUS attribute, see section 2.2.2.1.

3.1.6 Timer Events

No timer events are required for this protocol.

For a discussion on retransmission hints, see [RFC2865].

3.1.7 Other Local Events

None.

3.2 Client Details

3.2.1 Abstract Data Model

See section 3.1.1.

3.2.2 Timers

No timers are required for this protocol.

For a discussion on retransmission hints, see [RFC2865].

3.2.3 Initialization

None.

3.2.4 Higher-Layer Triggered Events

The RADIUS exchange is triggered by an endpoint request to an NAS for network access.

3.2.4.1 Abstract Interface for Sending a SoH

SendSoH: An abstract interface used by the NAS to send a SoH received from the PEP server as described in [MS-NAPSO] section 7.3.8. The interface is defined as follows.

```
HRESULT SendSoH([in] SoH message);
```

3.2.5 Message Processing Events and Sequencing Rules

3.2.5.1 Windows Implementation of RADIUS Attributes

See section 3.1.5.1.

3.2.5.2 Microsoft VSA Support of RADIUS Messages

See section 3.1.5.2.

3.2.5.3 Processing of RADIUS Attributes

See section 3.1.5.3.

3.2.5.4 Attributes Details on Client Side

An NAS operates as a client of RADIUS. The RADIUS client is responsible for passing user information to its designated RADIUS server, and then acting on the response that is returned.

3.2.5.4.1 MS-RAS-Client-Name

A Microsoft RRAS client sends its client name to identify itself. The RRAS server then uses this attribute to forward this information to the MS-RNAP aware RADIUS server for logging purposes.<6>

For more information about this attribute, see section 2.2.1.1.

3.2.5.4.2 MS-RAS-Client-Version

A Microsoft Routing and Remote Access Service (RRAS) client sends its client version to specify the version of the client generating a request. The RRAS server then uses this attribute to forward this information to Microsoft RADIUS server for accounting purposes.<7>

For more information about this attribute, see section 2.2.1.2.

3.2.5.4.3 MS-Quarantine-IPFilter

This attribute may be sent by a RADIUS server to define the network access scope of the endpoint. It is used only for IPv4 addresses. This attribute defines traffic filters to an NAS for restricting access for a specific network access connection. When an NAS supporting this attribute <8> receives it, the filters defined in this attribute MUST be implemented on the endpoint connection. If multiple MS-Quarantine-IPFilter attributes are contained within a packet, they MUST be in order and they MUST be consecutive attributes in the packet. For the late bound field, this is used to allow an NAS to change a field in the filter after the connection with the endpoint is complete.

For example, the attribute would be configured for "ANY" to be used as the source address. The filter is implemented on the NAS as ANY. When the connection with the endpoint completes and the client is assigned an address, the filter should be replaced with a specific value.

For more information about this attribute, see section 2.2.1.3.

3.2.5.4.4 MS-Quarantine-Session-Timeout

When an NAS receives this attribute, it MAY wait for the time in seconds specified in this attribute before it disconnects a restricted VPN connection.<9>

For more information about this attribute, see section 2.2.1.4.

3.2.5.4.5 MS-User-Security-Identity

Both a user name and user SID can be used to represent the identity of a user requesting network access. In most of the cases, NAS is expected to send user name to represent the user identity.

NAS may use this attribute as an alternative (as opposed to using the standard RADIUS User-Name attribute [RFC2865]) to specifying the identity of the user requesting access by sending the user SID of this user instead of the name.

For more information on this attribute, see 2.2.1.5.

3.2.5.4.6 MS-Identity-Type

This attribute indicates whether or not a RADIUS server should do only a machine health check, as specified in [MS-SOH]. An NAS may send this attribute to a RADIUS server in an Access-Request message. If an NAS sends this attribute to a RADIUS server and its value is 0x00000001, then this NAS requests that this RADIUS server do only a machine health check and not do any authentication.

For more information about this attribute, see section 2.2.1.6.

3.2.5.4.7 MS-Service-Class

This attribute carries the name of the service class corresponding to the client requesting access.

An NAS may send this attribute to a RADIUS server. When configured to support Network Access Protection (NAP), the DHCP server SHOULD send this attribute in an Access-Request to the RADIUS server. For more information about this attribute, see section 2.2.1.7.

3.2.5.4.8 MS-Quarantine-User-Class

This attribute is to be consumed by a DHCP RADIUS client only; if received by other network access servers, it SHOULD be silently discarded. When a DHCP RADIUS client receives this attribute, it MAY assign the DHCP client to the DHCP user class, as specified in [RFC3004].

3.2.5.4.9 MS-Quarantine-State

When a network access server (NAS) receives this attribute, it assigns the restrictive state specified by this attribute (see [MS-SOH]) to the endpoint requesting access.

This attribute indicates the level of network access that the RADIUS server authorizes to the endpoint.

When a MS-RNAP aware DHCP server receives this attribute from a MS-RNAP aware RADIUS server in an Access-Accept message, it gives access rights accordingly to the endpoint requesting network access (for example, gives full access or restricted access).

If the value of the MS-Quarantine-State VSA indicates a restricted state, the RADIUS client MUST restrict the endpoint's network connectivity accordingly to locally configured policy and according to the following rules:

- The VPN server and Dial-up server MUST block all IP packets from the endpoint except for those specified in the MS-IPv4-Remediation-Servers (see section 3.2.5.4.16) and MS-IPv6-Remediation-Servers (see section 3.2.5.4.17) VSAs (if received).

- The DHCP server MUST assign host-specific routes to the DHCP client for the IP addresses specified in the MS-IPv4-Remediation-Servers (see section 3.2.5.4.16) and MS-IPv6-Remediation-Servers (see section 3.2.5.4.17) VSAs (if received). The DHCP server MUST NOT assign the client a default gateway.
- The health registration authority (HRA) MUST NOT issue a certificate to the endpoint.

If the value of the MS-Quarantine-State VSA is either "Full Access" or "On Probation", the RADIUS client MUST NOT restrict the network connectivity of the endpoint.

If the value of the MS-Quarantine-State VSA is "On Probation", the RADIUS client MUST do the following:

- The VPN or Dial-Up Server MUST disconnect the endpoint after the time specified in the MS-Quarantine-Grace-Time elapses.
- The DHCP server MUST ensure that the DHCP lease expires for the endpoint before or at the same time specified in the MS-Quarantine-Grace-Time (see section 3.2.5.4.10) VSA.
- The HRA MUST ignore this attribute.

For more information about this attribute, see section 2.2.1.9.

3.2.5.4.10 MS-Quarantine-Grace-Time

When a NAS receives this attribute in an Access-Accept message, it MUST on expiration give full access to an endpoint requesting network access until the time specified by this attribute expires.

For more information about this attribute, see section 2.2.1.10.

3.2.5.4.11 MS-Network-Access-Server-Type

This attribute carries the type information of an NAS.

An NAS may send this attribute to RADIUS server to indicate the type of NAS in an Access-Request message.

For more information about this attribute, see section 2.2.1.11.

3.2.5.4.12 MS-AFW-Zone

This attribute carries the information about the NAP zone (see [MS-HCEP] and [MS-SOH]) that an endpoint should be in.

This attribute is only for RADIUS clients that are configured to support IPsec policies. When a network access server (NAS) that understands this attribute receives it, it SHOULD decide which zone to put an endpoint to (for example, secure zone, boundary zone, or quarantine zone), and then it SHOULD send the decision of the zone to the endpoint using a mechanism that is understood by both NAS and the endpoint (for example, HCEP, as documented in [MS-HCEP] section 3.2.5.2). The NAS accordingly applies a different IPsec policy to this endpoint.

For more information about this attribute, see section 2.2.1.12.

3.2.5.4.13 MS-AFW-Protection-Level

A NAS that receives this attribute from the RADIUS server in an Access-Accept MUST send it to the endpoint that is requesting network access.

This attribute is only for RADIUS clients that are configured to support IPsec policies. When a NAS that understands this attribute receives it, it SHOULD set the protection level accordingly based on the value of this attribute and indicate to the endpoints requesting network access the protection level they should use.

For more information about this attribute, see section 2.2.1.13.

3.2.5.4.14 MS-Machine-Name

A NAS MAY use this attribute to pass the machine name of the endpoint requesting network access to a RADIUS server, which may then use this information to make an authentication or authorization decision.<10>

This attribute MAY be sent to a RADIUS server when MS-Quarantine-SOH (as specified in section 2.2.1.19) is not sent to a RADIUS server.

For more information about this attribute, see section 2.2.1.14.

3.2.5.4.15 MS-IPv6-Filter

This attribute may be sent by a RADIUS server to define the network access scope of the endpoint. It is used only for IPv6 addresses and MS-Filter, [RFC2548] VSA is the corresponding attribute for IPv4 addresses. The structure of MS-Filter is identical to the structure of MS-Quarantine-IPFilter, as specified in section 2.2.1.3.<11> This attribute defines traffic filters to an NAS for restricting access for a specific network access connection. When an NAS supporting this attribute receives it, the filters defined in this attribute MUST be implemented on the endpoint connection. If multiple MS-IPv6-Filter attributes are contained within a packet, they MUST be in order and they MUST be consecutive attributes in the packet.

Only the Microsoft Routing and Remote Access Service (RRAS) RADIUS client supports this attribute when configured to support RQS/RQC. If received by other RADIUS clients, it is silently discarded.

For the late bound field, this is used to allow an NAS to change a field in the filter after the connection with the endpoint is complete. For example, the attribute could be configured for "ANY" to be used as the source address. The filter is implemented on the NAS as ANY. When the connection with the endpoint completes and the client is assigned an address, the filter could be replaced with a specific value.

For more information about this attribute, see section 2.2.1.15.

3.2.5.4.16 MS-IPv4-Remediation-Servers

This attribute specifies the IPv4 addresses of the remediation servers. The first 8-bit unsigned integer, which is reserved and set to 0 by the RADIUS server, MAY be ignored by the RADIUS client.

When a NAS that understands this attribute receives it, it SHOULD<12> authorize a restricted endpoint to access the IPv4 addresses carried in this attribute.

If the RADIUS client does not support this attribute or does not support the required service (restricting the endpoint's access to remediation servers either via configuration (for example, DHCP) or filtering (for example, RRAS)), then it SHOULD ignore this attribute.

For more information about this attribute, see section 2.2.1.16.

3.2.5.4.17 MS-IPv6-Remediation-Servers

This attribute specifies the IPv6 addresses of the remediation servers. The first 8-bit unsigned integer, which is reserved and set to 0 by the RADIUS server, MAY be ignored by the RADIUS client.

When a NAS that understands this attribute receives it, it SHOULD authorize a restricted endpoint to access the IPv6 addresses carried in this attribute.

A RADIUS client that does not implement this attribute or does not support the requested service (restriction of endpoint access to remediation servers) SHOULD ignore this attribute.

For more information about this attribute, see section 2.2.1.17.

3.2.5.4.18 Not-Quarantine-Capable

This attribute indicates whether or not the endpoint requesting network access is Network Access Protection (NAP)–capable.

When an NAS receives this attribute from a MS-RNAP aware RADIUS server, it can determine if the endpoint requesting networking access sent an SoH. An NAS supporting the VSAs specified in this document which receives a Not-Quarantine-Capable Attribute with a value indicating that the SoH was not sent (0x000001) SHOULD NOT send NAP-related information to the endpoint.

A RADIUS client that does not implement this attribute or does not support the requested service (restriction of access based on NAP-capability) SHOULD ignore this attribute.

For more information about this attribute, see section 2.2.1.18.

3.2.5.4.19 MS-Quarantine-SoH

This attribute carries a SoH (as specified in [MS-SOH]) information when EAP is not used.

An RADIUS client can forward the SoH (as specified in [MS-SOH]) that is provided by the client to a MS-RNAP aware RADIUS server in Access-Request by this attribute, which contains an EAP-TLV-TYPE of vendor-specific TLV and is a MS-SOH-Payload-TLV that contains the SoH (as specified in [MS-SOH]).

For more information about this attribute, see section 2.2.1.19.

3.2.5.4.20 MS-RAS-Correlation-ID

An NAS uses this attribute in RADIUS [RFC2865] Access-Request or Accounting-Request messages for correlation of log events.<13>

For more information about this attribute, see section 2.2.1.20.

3.2.5.4.21 MS-Extended-Quarantine-State

When a NAS receives this attribute, it MUST assign the extended Quarantine state specified by this attribute, as specified in [MS-SOH], to the client requesting access. This attribute is used in NAP scenarios.

This attribute further qualifies the level of network access that the RADIUS server authorizes to the endpoint. When a network access server receives this attribute from a RADIUS server in an Access-Accept message, it MAY combine the value of this attribute with the value of MS-Quarantine-State attribute in an implementation specific manner.<14>

For more information about this attribute, see section 2.2.1.21.

3.2.5.4.22 HCAP-User-Groups

An NAS may use this attribute to pass the group name of the user requesting network access to a RADIUS server, which may then use this information to make authentication or authorization decisions.

For more information about this attribute, see section 2.2.1.22.

3.2.5.4.23 HCAP-Location-Group-Name

An NAS may use this attribute to pass the location group name of the endpoint requesting network access to a RADIUS server, which may then use this information to make authentication or authorization decisions.

For more information about this attribute, see section 2.2.1.23.

3.2.5.4.24 HCAP-User-Name

An NAS may use this attribute to pass the name of the user requesting network access to a RADIUS server, which may then use this information to make authentication or authorization decisions.

For more information about this attribute, see section 2.2.1.24.

3.2.5.4.25 MS-User-IPv4-Address

An NAS may use this attribute to pass the IPv4 address of the endpoint requesting network access to a RADIUS server, which may then use this information to make authentication or authorization decisions.<15>

For more information about this attribute, see section 2.2.1.25.

3.2.5.4.26 MS-User-IPv6-Address

An NAS may use this attribute to pass the IPv6 address of the endpoint requesting network access to a RADIUS server, which may then use this information to make authentication or authorization decisions.<16>

For more information about this attribute, see section 2.2.1.27.

3.2.5.4.27 MS-RDG-Device-Redirection

This attribute is for Microsoft Remote Desktop Gateway only. Other NAS devices SHOULD silently discard this attribute. When Microsoft Remote Desktop Gateway receives this attribute, it MUST disable or enable the device redirection functionality based on the bits that are set in the attribute. For the meaning of the bits, see section 2.2.1.27.

When bit 29 (disable all devices) is set, the device redirection functionality MUST be disabled for all the devices regardless of the value of bit 30 (enable all devices) and bits 0–4 (disable a particular device). When bit 29 is not set but bit 30 is set, device redirection functionality for all the devices MUST be enabled regardless of the value of bits 0–4.

For more information about this attribute, see section 2.2.1.27.

3.2.5.4.28 Vendor-Specific Value for Tunnel-Type RADIUS Attribute

A RADIUS client MUST process the Tunnel-Type RADIUS attribute as specified in [RFC2868], with one additional constraint: A VPN server that supports the Secure Socket Tunneling Protocol (SSTP) SHOULD use the vendor-specific value 0x00013701 for the RADIUS Tunnel-Type attribute in Access-Requests sent to a RADIUS server, indicating that the tunnels configured by it are as described in [MS-SSTP]. <17>

For more information about this vendor-specific value for the Tunnel-Type RADIUS attribute, see section 2.2.2.1.

3.2.6 Timer Events

No timer events are required for this protocol.

For a discussion on retransmission hints, see [RFC2865].

3.2.7 Other Local Events

None.

4 Protocol Examples

The following sections describe several operations as used in common scenarios to illustrate the function of the RADIUS Protocol.

4.1 VPN Connection with RQC/RQS Quarantine

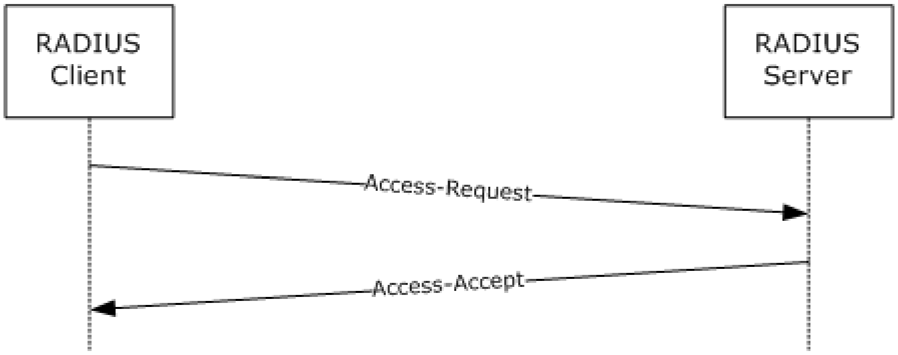

Figure 2: VPN Connection with RQC/RQS Quarantine example

In this example, a RAS server is configured as a RADIUS client to use RADIUS as the authentication, authorization, and accounting protocol to a RADIUS server. Based on the data known to RAS, the RAS server formulates an Access-Request packet as follows:

- Attribute 0: NAS Identifier = NAS Computer Name
- Attribute 1: MS-RAS-Client-Name = MSRAS-0-<NAS Client ComputerName>
- Attribute 2: MS-RAS-Client-Version = MSRASV5.20
- Attribute 3: NAS-IP-Address = IP address of the RAS server
- Attribute 4: Service-Type = Framed OR Callback Framed
- Attribute 5: Framed-Protocol = PPP
- Attribute 6: NAS-port = Port number
- Attribute 7: NAS-port-Type = Virtual
- Attribute 8: Calling-Station-ID = NAS client IP address
- Attribute 9: Tunnel-Type = PPTP/L2TP/SSTP
- Attribute 10: Tunnel-Medium-Type = IP
- Attribute 11: Tunnel-Client-Endpt = NAS client IP address
- Attribute 12: MS-RAS-Version = MSRASV5.20

This is forwarded to the RADIUS server. The RADIUS server authenticates and authorizes the request. Based on the RADIUS server configuration, it responds with an Access-Accept packet with the following attributes:

- Attribute 0: MS-Quarantine-State = 0 [Full access]

- Attribute 1: MS-Quarantine-Session-Timeout = Time in seconds
- Attribute 2: MS-Quarantine-IPFilter = List of IPv4 traffic filters
- Attribute 3: MS-Filter = List IPv4 traffic filters
- Attribute 4: MS-IPv6-Filter = List IPv6 traffic filters
- Attribute 5: Tunnel-Type = List of tunnel types (PPTP/L2TP)

Note: Attributes 5 would be in the Access-Accept packet, provided they are set in the Settings placeholder other than the Conditions place holder for the relevant Network Policy configured on a RADIUS server.

For more information on RQC/RQS Quarantine, see [MSFT-NAQC].

4.2 Health Registration Authority (HRA)

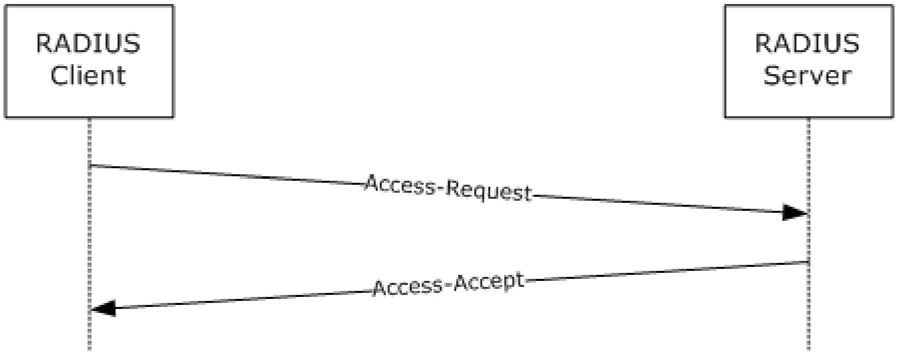

Figure 3: Health Registration Authority (HRA) example

In this example, an HRA is configured as a RADIUS client to use RADIUS as the authentication, authorization, and accounting protocol to a RADIUS server. Based on data collected from the access client, the HRA formulates an Access-Request packet as follows:

- Attribute 0: MS-Network-Access-Server-Type = 5 HRA
- Attribute 1: Acct-Session-Id = Transaction-id
- Attribute 2: Service-Type = Authorize-only
- Attribute 3: MS-Identity-Type = Machine health check
- Attribute 4: NAS-Port-Type = Ethernet
- Attribute 5: MS-Attribute-Machine-Name = fqdn client name in ASCII characters with ANSI code page.
- Attribute 6: MS-SoH-Payload-Type = SoH blob
- Attribute 7: NAS-Identifier-Type = HCS server fqdn name in ASCII characters with the code page to be the current system Microsoft Windows® ANSI code page (see [MSDN-ANSI-CODEPAGE]).
- Attribute 8: NAS-Ip-Address = Server address

This is forwarded to the RADIUS server where the RADIUS server authenticates and authorizes the request. Based on the RADIUS server configuration, it responds with an Access-Accept packet with the following attributes:

- Attribute 0: MS-Quarantine-State = Full access
- Attribute 1: MS-AFW-Zone = Non-Boundary
- Attribute 2: MS-AFW-Protection-Level = Encrypted

4.3 DHCP NAP

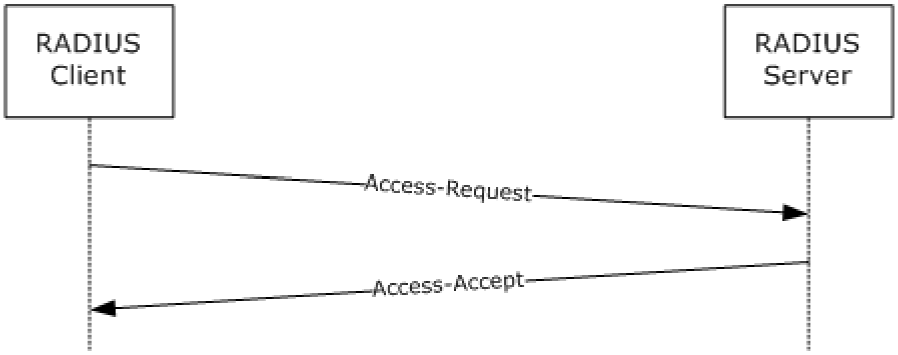

Figure 4: DHCP NAP example

In this example, a DHCP Server is configured as a RADIUS client to use RADIUS as the authentication, authorization, and accounting protocol to a RADIUS server. Based on data collected from the endpoint, the DHCP Server formulates an Access-Request packet as follows:

- Attribute 0: MS-Network-Access-Server-Type = 3 (DHCP)
- Attribute 1: Acct-Session-Id = Transaction-id
- Attribute 2: Service-Type = Authorize-only
- Attribute 3: MS-Identity-Type = Machine health check
- Attribute 4: NAS-Port-Type = Ethernet
- Attribute 5: MS-Attribute-Machine-Name = fqdn client name in ANSI
- Attribute 6: MS-SoH-Payload-Type = SoH blob
- Attribute 7: NAS-Identifier-Type = HCS server fqdn name in ANSI
- Attribute 8: NAS-Ip-Address = Server address
- Attribute 9: MS-Service-Class = DHCP service class

This is forwarded to the RADIUS server where the RADIUS server authenticates and authorizes the request. Based on the RADIUS server configuration, it responds with an Access-Accept packet with the following attributes:

- Attribute 0: MS-Quarantine-State = Full access
- Attribute 1: MS-IPv4-Remediation-Servers = List of IPv4 addresses

- Attribute 2: MS-Quarantine-User-Class = User class

4.4 VPN NAP

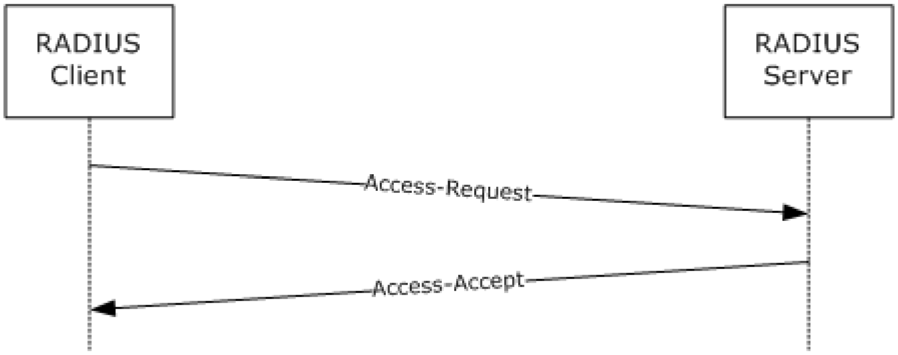

Figure 5: VPN NAP example

In this example, a RAS server is configured as a RADIUS client to use RADIUS as the authentication, authorization, and accounting protocol to a RADIUS server. Based on the data known to RAS, RAS server formulates an Access-Request packet as follows:

- Attribute 0: NAS Identifier = NAS computer name
- Attribute 1: NAS-IP-Address = IP address of the RAS server
- Attribute 2: Service-Type = Framed OR Callback Framed
- Attribute 3: Framed-Protocol = PPP
- Attribute 4: NAS-port = Port number
- Attribute 5: NAS-port-Type = Virtual
- Attribute 6: Calling-Station-Id = NAS client IP address
- Attribute 7: Tunnel-Type = PPTP/L2TP/SSTP
- Attribute 8: Tunnel-Medium-Type = IP
- Attribute 9: Tunnel-Client-Endpt = NAS client IP address
- Attribute 10: MS-RAS-Version = MSRASV5.20
- Attribute 11: MS-Network-Access-Server-Type = 2 [RAS]

This is forwarded to the RADIUS server. The RADIUS server authenticates and authorizes the request. Based on the RADIUS server configuration, it responds with an Access-Accept packet with the following attributes:

- Attribute 0: MS-Quarantine-State = 1 [Restricted Access]
- Attribute 1: MS-Quarantine-Session-Timeout = Time in seconds
- Attribute 2: MS-Filter = List IPv4 traffic filters (the structure of MS-Filter is identical to the structure of MS-Quarantine-IPFilter, as specified in section 2.2.1.3.

- Attribute 3: MS-IPv6-Filter = List IPv6 traffic filters
- Attribute 4: MS-IPv4-Remediation-Servers= List of IPv4 Addresses
- Attribute 5: MS-IPv6-Remediation-Servers= List of IPv6 Addresses
- Attribute 6: Tunnel-Type = List of tunnel types (PPTP/L2TP)

Note: Attributes 6 would be in the Access-Accept packet, provided they are set in the Settings place holder other than the Conditions place holder for the relevant Network Policy configured on RADIUS server.

5 Security

5.1 Security Considerations for Implementers

The Microsoft RADIUS VSAs rely on the security of the RADIUS Protocol in which they are transported. There are many security considerations for the RADIUS Protocol, as specified in [RFC2865] section 8 and [RFC3579] section 4. It is best to deploy RADIUS over IPsec (as specified in [RFC3579] section 4.2) to mitigate the potential attacks against RADIUS alone.

Recommendations exist to mitigate most of the attacks against RADIUS. However, it cannot be assumed that these recommendations are universally deployed. As a result, in some environments, it is possible for an attacker to tamper with or spoof the RADIUS VSAs.

Implementers should perform validation checks against all VSAs received to prevent remote protocol parsing attacks. These validation checks will include, but are not necessarily limited to, the following:

1. Ensuring that the VSA lengths fit within the containing RADIUS attribute.
2. Ensuring that the VSA lengths fit within the RADIUS packet itself.
3. Ensuring that all field values fall within acceptable ranges.

In addition, implementers can support a mode of operation wherein RADIUS will not be sent or received unless protected by IPsec, as specified in [RFC3579] section 4.2.<18>

5.2 Index of Security Parameters

Security parameter	Section
MS-User-Security-Identity	2.2.1.5

6 Appendix A: Product Behavior

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

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

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

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

<1> Section 2.2.1.1: Windows endpoints always use the format MS-RAS-x-<RAS Client Computer Name> (for example, MS-RAS-0-Laptop where "Laptop" is the name of the computer). The value of x is either 0 or 1, where 0 indicates that the messenger service is not running on the endpoint machine and 1 indicates that the messenger service is running. This information is useful to decide whether the Microsoft RRAS Administrator can send messages to the user by using messenger service. (This is a UI/API option to "Send Messages to User" in Windows NT, Windows 2000, Windows XP, and Windows Server 2003.) Also note that this service is deprecated in Windows Server 2008 and Windows Vista and PPP always sends "MSRAS-0<>" on a Windows Vista client. For Windows Messenger Service, see [MS-MSRP].

<2> Section 2.2.1.2: For Windows XP, the **Attribute-Specific Value** is "MSRASV5.10" and for Windows Vista, this value is "MSRASV5.20"

<3> Section 3.1.5.1: The Remote Authentication Dial-In User Service (RADIUS) Protocol standard, as specified in [RFC2865], defines RADIUS attributes. One of the attributes in [RFC2865] section 5.26 defines a VSA for use by implementers to extend the attribute set. Microsoft has created a number of VSAs for use with RADIUS to support authenticated network access. Some of these VSAs are as specified in [RFC2548]. The remaining VSAs will be documented in section 2.2.1 of this document. The following table shows what RADIUS VSAs are implemented in the various versions of Windows:

Windows Server						
Microsoft VSA	**Reference**	**Section**	**Windows Server 2000**	**Windows Server2003**	**Windows Server2008**	**Windows Server 2008 R2**
MS-CHAP-Response	[RFC2548]	2.1.3	X	X	X	X
MS-CHAP-Domain	[RFC2548]	2.1.4	X	X	X	X
MS-CHAP-Error	[RFC2548]	2.1.5	X	X	X	X
MS-CHAP-CPW-1	[RFC2548]	2.1.6	X	X	X	X
MS-CHAP-CPW-2	[RFC2548]	2.1.7	X	X	X	X
MS-CHAP-LM-Enc-PW	[RFC2548]	2.1.8	X	X	X	X
MS-CHAP-NT-Enc-PW	[RFC2548]	2.2	X	X	X	X
MS-CHAP2-Response	[RFC2548]	2.3.2	X	X	X	X
MS-CHAP2-Success	[RFC2548]	2.3.3	X	X	X	X
MS-CHAP2-CPW	[RFC2548]	2.3.4	X	X	X	X
MS-CHAP-MPPE-Keys	[RFC2548]	2.4.1	X	X	X	X
MS-MPPE-Send-Key	[RFC2548]	2.4.2	X	X	X	X
MS-MPPE-Recv-Key	[RFC2548]	2.4.3	X	X	X	X
MS-MPPE-Encryption-Types	[RFC2548]	2.4.4	X	X	X	X
MS-MPPE-Encryption-Policy	[RFC2548]	2.4.5	X	X	X	X
MS-BAP-Usage	[RFC2548]	2.5.1	X	X	X	X
MS-Link-Utilization-Threshold	[RFC2548]	2.5.2	X	X	X	X

Windows Server						
MS-Link-Drop-Time-Limit	[RFC2548]	2.5.3	X	X	X	X
MS-Old-ARAP-Password	[RFC2548]	2.6.1	X			
MS-New-ARAP-Password	[RFC2548]	2.6.2	X			
MS-ARAP-PW-Change-Reason	[RFC2548]	2.6.3	X			
MS-ARAP-Challenge	[RFC2548]	2.6.4	X			
MS-RAS-Vendor	[RFC2548]	2.7.1	X	X	X	X
MS-RAS-Version	[RFC2548]	2.7.2	X	X	X	X
MS-Filter	[RFC2548]	2.7.3	X	X	X	X
MS-Acct-Auth-Type	[RFC2548]	2.7.4	X	X	X	X
MS-Acct-EAP-Type	[RFC2548]	2.7.5	X	X	X	X
MS-Primary-DNS-Server	[RFC2548]	2.7.6	X	X	X	X
MS-Secondary-DNS-Server	[RFC2548]	2.7.7	X	X	X	X
MS-Primary-NBNS-Server	[RFC2548]	2.7.8	X	X	X	X
MS-Secondary-NBNS-Server	[RFC2548]	2.7.9	X	X	X	X
MS-RAS-Client-Name	This document	MS-RAS-Client-Name (section 2.2.1.1)		X	X	X
MS-RAS-Client-Version	This document	MS-RAS-Client-Version (section 2.2.1.2)		X	X	X
MS-	This	MS-		X	X	X

Windows Server						
Quarantine-IPFilter	document	Quarantine-IPFilter (section 2.2.1.3)				
MS-Quarantine-Session-Timeout	This document	MS-Quarantine-Session-Timeout (section 2.2.1.4)		X	X	X
MS-Identity-Type	This document	MS-Identity-Type (section 2.2.1.6)			X	X
MS-Service-Class	This document	MS-Service-Class (section 2.2.1.7)			X	X
MS-Quarantine-User-Class	This document	MS-Quarantine-User-Class (section 2.2.1.8)			X	X
MS-Quarantine-State	This document	MS-Quarantine-State (section 2.2.1.9)			X	X
MS-Quarantine-Grace-Time	This document	MS-Quarantine-Grace-Time (section 2.2.1.10)			X	X
MS-Network-Access-Server-Type	This document	MS-Network-Access-Server-Type (section 2.2.1.11)			X	X
MS-AFW-Zone	This document	MS-AFW-Zone (section 2.2.1.12)			X	X
MS-AFW-Protection-Level	This document	MS-AFW-Protection-Level (section 2.2.1.13)			X	X
MS-Machine-Name	This document	MS-Machine-Name (section 2.2.1.14)			X	X
MS-IPv6-	This	MS-IPv6-			X	X

Windows Server						
Filter	document	Filter (section 2.2.1.15)				
MS-IPv4-Remediation-Servers	This document	MS-IPv4-Remediation-Servers (section 2.2.1.16)			X	X
MS-IPv6-Remediation-Servers	This document	MS-IPv6-Remediation-Servers (section 2.2.1.17)			X	X
Not-Quarantine-Capable	This document	Not-Quarantine-Capable (section 2.2.1.18)			X	X
MS-Quarantine-SOH	This document	MS-Quarantine-SOH (section 2.2.1.19)			X	X
MS-RAS-Correlation-ID	This document	MS-RAS-Correlation-ID (section 2.2.1.20)			X	X
MS-Extended-Quarantine-State	This document	MS-Extended-Quarantine-State (section 2.2.1.21)			X	X
HCAP-User-Groups	This document	HCAP-User-Groups (section 2.2.1.22)			X	X
HCAP-Location-Group-Name	This document	HCAP-Location-Group-Name (section 2.2.1.23)			X	X
HCAP-User-Name	This document	HCAP-User-Name (section 2.2.1.24)			X	X
MS-User-IPv4-Address	This document	MS-User-IPv4-Address (section 2.2.1.25)			X	X

Windows Server						
MS-User-IPv6-Address	This document	MS-User-IPv6-Address (section 2.2.1.26)			X	X
MS-RDG-Device-Redirection	This document	MS-RDG-Device-Redirection (section 2.2.1.27)			X	X
MS-Tunnel-Type	This document	MS-Tunnel-Type (section 2.2.2.1)				X

<4> Section 3.1.5.3: Microsoft RADIUS clients and RADIUS servers ignore VSAs in the following conditions:

- A VSA is received in a RADIUS message by a RADIUS client or RADIUS server that it is not supported per the preceding table. For example, A Not-Quarantine-Capable VSA should not be sent to a RADIUS server in an Access-Request message, so if a RADIUS server receives such an attribute in an Access-Request message, it ignores it.
- A VSA is received by a RADIUS client or RADIUS server with invalid data (for example, a RADIUS client receives a Not-Quarantine-Capable VSA with a length of 2).
- A VSA is received with a VSA with an unknown vendor ID/vendor type combination (for example, a RADIUS client receives a VSA with the vendor ID set to 0x00000137 and a vendor-type set to 0xAA).

<5> Section 3.1.5.4.28: Only Windows Server 2008 R2 RADIUS servers support this vendor-specific value for the RADIUS Tunnel-Type Attribute.

<6> Section 3.2.5.4.1: When configured to support NAP, the Microsoft RRAS server sends this attribute in an Access-Request to the RADIUS server.

<7> Section 3.2.5.4.2: When configured to support NAP, the MS-RNAP aware RRAS server sends this attribute in an Access-Request to the RADIUS server.

<8> Section 3.2.5.4.3: Only the Microsoft RRAS RADIUS client supports this attribute when configured to support RQS/RQC; if received by a HRA or DHCP server acting as a RADIUS client, it is silently discarded.

<9> Section 3.2.5.4.4: Only the Microsoft RRAS server RADIUS client supports this attribute when configured to support RQS/RQC; if received by an HRA or DHCP RADIUS client, it is silently discarded.

For RQS/RQC, see section VPN Connection with RQC / RQS quarantine (section 4.1).

<10> Section 3.2.5.4.14: When configured to support NAP, the Microsoft RRAS, DHCP, and HRA RADIUS client send this attribute in an Access-Request to a RADIUS server.

<11> Section 3.2.5.4.15: When Windows is operating as an NAS in a RAS server or VPN server role, the late bound flag uses the late bound flag in the following way:

1. An endpoint initiates a connection to an NAS.

2. The NAS forwards the connection request to the RADIUS server using an access-request message.

3. The RADIUS server processes the request and returns an access-accept which contains the MS-IPv6-Filter attribute with a list of filters.

4. The NAS implements the filter list for the endpoint connection and begins filtering traffic.

5. The NAS and endpoint complete the connection request and the endpoint receives IP address information for the RAS connection.

6. The NAS uses the IP addresses to alter the implemented filter list for the client connection. The filter list, if modified, based on the Late Bound flag is as follows:

   - 0x00000001: The source address is replaced with the address assigned to the endpoint.

   - 0x00000004: This is not implemented in Windows.

   - 0x00000010: The source prefix is replaced with 64.

<12> Section 3.2.5.4.16: Only the Microsoft RRAS server and DHCP servers acting as RADIUS clients support this attribute when configured to support NAP; if received by an HRA RADIUS client, it is silently discarded.

<13> Section 3.2.5.4.20: The Microsoft RRAS server sends this attribute in Access-Request and Accounting-Request messages to the RADIUS server. This attribute can be sent by any RADIUS client, not just RRAS.

<14> Section 3.2.5.4.21: No existing Microsoft product acting as a RADIUS client uses this VSA.

<15> Section 3.2.5.4.25: The Microsoft HCAP server sends this attribute in Access-Request messages to the RADIUS server.

Microsoft HCAP allows you to integrate your Microsoft NAP solution with Cisco Network Access Control, and the endpoint's IPv4 address obtained from Cisco Network Access Control is put into this attribute by Microsoft HCAP.

<16> Section 3.2.5.4.26: The Microsoft HCAP server sends this attribute in Access-Request messages to the RADIUS server.

Microsoft HCAP allows you to integrate your Microsoft NAP solution with Cisco Network Access Control, and the endpoint's IPv6 address obtained from Cisco Network Access Control is put into this attribute by Microsoft HCAP.

<17> Section 3.2.5.4.28: Only Windows Server 2008 R2 VPN servers support this vendor-specific value for the RADIUS Tunnel-Type Attribute.

<18> Section 5.1: Windows does not support such a mode. However, IPsec can be configured on Windows to ensure equivalent behavior.

7 Change Tracking

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Section	Tracking number (if applicable) and description	Major change (Y or N)	Change type
1.2.1 Normative References	63763 Added [MS-NAPSO] reference.	Y	Content updated.
2.2.1.20 MS-RAS-Correlation-ID	60625 Updated content regarding the length of "Vendor-Length" and specified how the GUID was to be represented.	Y	Content updated.
3.1.4 Higher-Layer Triggered Events	63699 Updated content to specify that a RADIUS exchange is triggered by a request from an NAS.	Y	Content updated.
3.1.4.1 Abstract Interface for Sending a SoHR	56946 Added section.	Y	New content added.
3.1.5.4.19 MS-Quarantine-SoH	63763 Added links to appropriate sections in [MS-NAPSO] regarding processing and creating the SoHR task.	Y	Content updated.
3.2.4.1 Abstract Interface for Sending a SoH	56945 Added section.	Y	New content added.

8 Index