Network Working Group
Internet-Draft
Category: Informational
<draft-ietf-radius-mschap-attr-01.txt>

G. Zorn
Microsoft Corporation
November 1997

RADIUS Attributes for MS-CHAP Support

1. Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress''.

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt'' listing contained in the Internet-Drafts Shadow Directories on ds.internic.net (US East Coast), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim).

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. The distribution of this memo is unlimited. It is filed as <draft-ietf-radius-mschap-attr-01.txt> and expires May 21, 1998. Please send comments to the RADIUS Working Group mailing list (ietf-radius@livingston.com) or to the author (glennz@microsoft.com).

2. Abstract

This document describes a set of vendor-specific RADIUS attributes designed to support the use of Microsoft's proprietary dialect of PPP CHAP (MS-CHAP) in dial-up networks. MS-CHAP is derived from and (where possible) consistent with PPP CHAP [1]; the differences between PPP CHAP and MS-CHAP are significant enough to warrant the definition of new RADIUS attributes, however.

3. Introduction

Microsoft created Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) to authenticate remote Windows workstations, providing the functionality to which LAN-based users are accustomed. Where possible,

MS-CHAP is consistent with standard CHAP, and the differences are easily modularized. Briefly, the differences between MS-CHAP and standard CHAP are:

* MS-CHAP is enabled by negotiating CHAP Algorithm 0x80 in LCP option 3, Authentication Protocol.

* The MS-CHAP Response packet is in a format designed for compatibility with Microsoft Windows NT 3.5, 3.51 and 4.0, Microsoft Windows95, and Microsoft LAN Manager 2.x networking products. The MS-CHAP format does not require the authenticator to store a clear-text or reversibly encrypted password.

* MS-CHAP provides an authenticator-controlled authentication retry mechanism.

* MS-CHAP provides an authenticator-controlled password changing mechanism.

* MS-CHAP defines an extended set of reason-for-failure codes, returned in the Failure packet Message field.

The attributes defined in this document reflect these differences.

4. Specification of Requirements

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT" are to be interpreted as described in [2].

5. Attributes

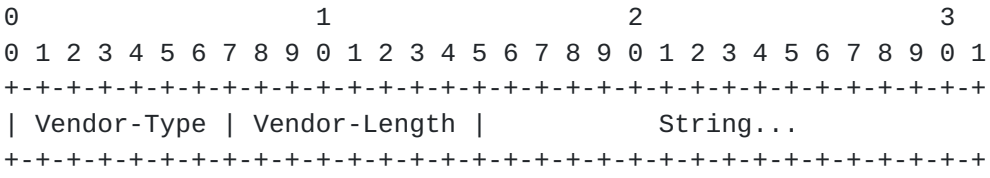
The following sections describe sub-attributes which may be transmitted in one or more RADIUS attributes of type Vendor-Specific [3]. More than one sub-attribute MAY be transmitted in a single Vendor-Specific Attribute; if this is done, the sub-attributes SHOULD be packed as a sequence of Vendor-Type/Vendor-Length/Value triples following the inital Type, Length and Vendor-ID fields. The Length field of the Vendor-Specific Attribute MUST be set equal to the sum of the Vendor-Length fields of the sub-attributes contained in the Vendor-Specific Attribute, plus six. The Vendor-ID field of the Vendor-Specific Attribute(s) MUST be set to decimal 311 (Microsoft).

5.1. MS-CHAP-Challenge

Description

This Attribute contains the challenge sent by a NAS to a Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) user. It MAY be used in both Access-Request and Access-Challenge packets.

A summary of the MS-CHAP-Challenge Attribute format is shown below. The fields are transmitted from left to right.



Vendor-Type
11 for MS-CHAP-Challenge.

Vendor-Length
> 2

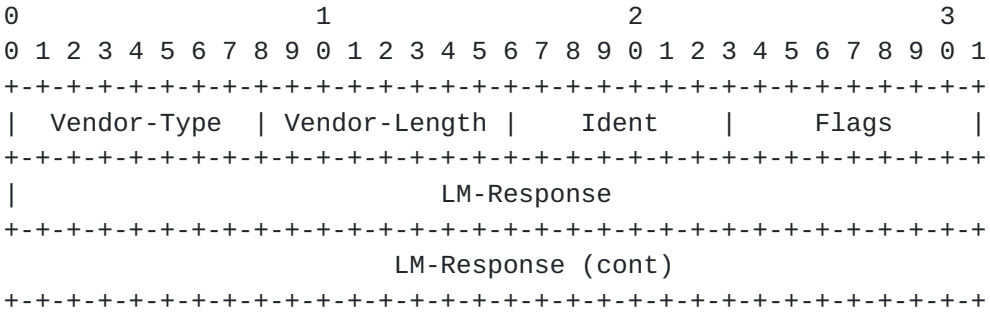
String
The String field contains the MS-CHAP challenge.

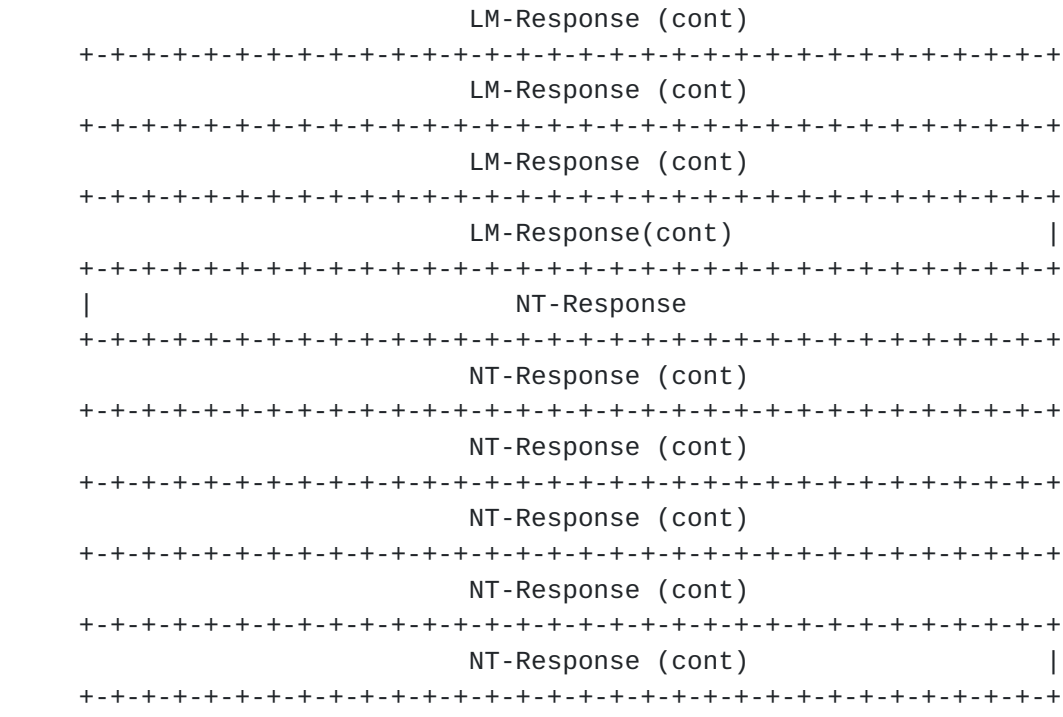
5.2. MS-CHAP-Response

Description

This Attribute contains the response value provided by a PPP Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) user in response to the challenge. It is only used in Access-Request packets.

A summary of the MS-CHAP-Response Attribute format is shown below. The fields are transmitted from left to right.





Vendor-Type
1 for MS-CHAP-Response.

Vendor-Length
52

Ident
Identical to the PPP CHAP Identifier.

Flags
The Flags field is one octet in length. If the Flags field is one (0x01), the NT-Response field is to be used in preference to the LM-Response field for authentication. The LM-Response field MAY still be used (if non-empty), but the NT-Response SHOULD be tried first. If it is zero, the NT-Response field MUST be ignored and the LM-Response field used.

LM-Response
The LM-Response field is 24 octets in length and holds an encoded function of the password and the received challenge. If this field is empty, it SHOULD be zero-filled.

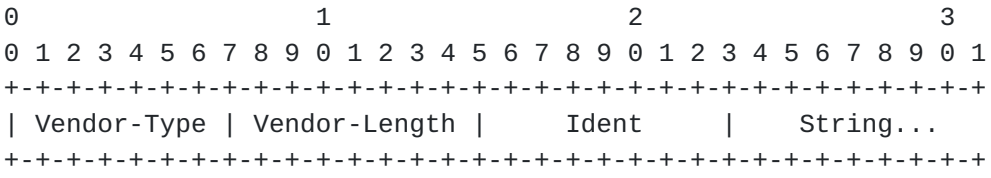
NT-Response
The NT-Response field is 24 octets in length and holds an encoded function of the password and the received challenge. If this field is empty, it SHOULD be zero-filled.

5.3. MS-CHAP-Domain

Description

The MS-CHAP-Domain Attribute indicates the Windows NT domain in which the user was authenticated. It MAY be included in both Access-Accept and Accounting-Request packets.

A summary of the MS-CHAP-Domain Attribute format is given below. The fields are transmitted left to right.



Vendor-Type
10 for MS-CHAP-Domain.

Vendor-Length
> 3

Ident
The Ident field is one octet and aids in matching requests and replies.

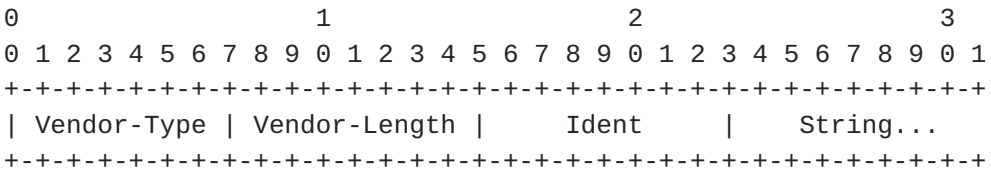
String
This field contains the name in ASCII of the Windows NT domain in which the user was authenticated.

5.4. MS-CHAP-Error

Description

The MS-CHAP-Error Attribute contains error data related to the preceding MS-CHAP exchange. It is only used in Access-Reject packets.

A summary of the MS-CHAP-Error Attribute format is given below. The fields are transmitted left to right.



Vendor-Type
2 for MS-CHAP-Error.

Vendor-Length
> 3

Ident
The Ident field is one octet and aids in matching requests and replies.

String
This field contains up to 48 octets of specially formatted ASCII text, which is interpreted by the authenticating peer. The format of this field is as follows:

"E=eeeeeeeeee R=r C=cccccccccccccccc V=vvvvvvvvvv"

where the "eeeeeeeeee" represents an ASCII representation of a decimal error code of up to 10 digits corresponding to one of the following:

646 ERROR_RESTRICTED_LOGON_HOURS
647 ERROR_ACCT_DISABLED
648 ERROR_PASSWD_EXPIRED
649 ERROR_NO_DIALIN_PERMISSION
691 ERROR_AUTHENTICATION_FAILURE
709 ERROR_CHANGING_PASSWORD

Implementations should deal with codes not on this list gracefully, however. Please note that (unlike PPP CHAP), the receipt of some of these error codes (in particular, the ERROR_PASSWD_EXPIRED code) will modify the subsequent operation of the MS-CHAP protocol. The 'r' is a retry flag (set to '1' if a retry is allowed and '0' otherwise), the "cccccccccccccccc" represents 16 hexadecimal digits ('0'-'F') specifying a new challenge value, and the "vvvvvvvvvv" is a decimal version code signifying the version of MS-CHAP supported by the server.

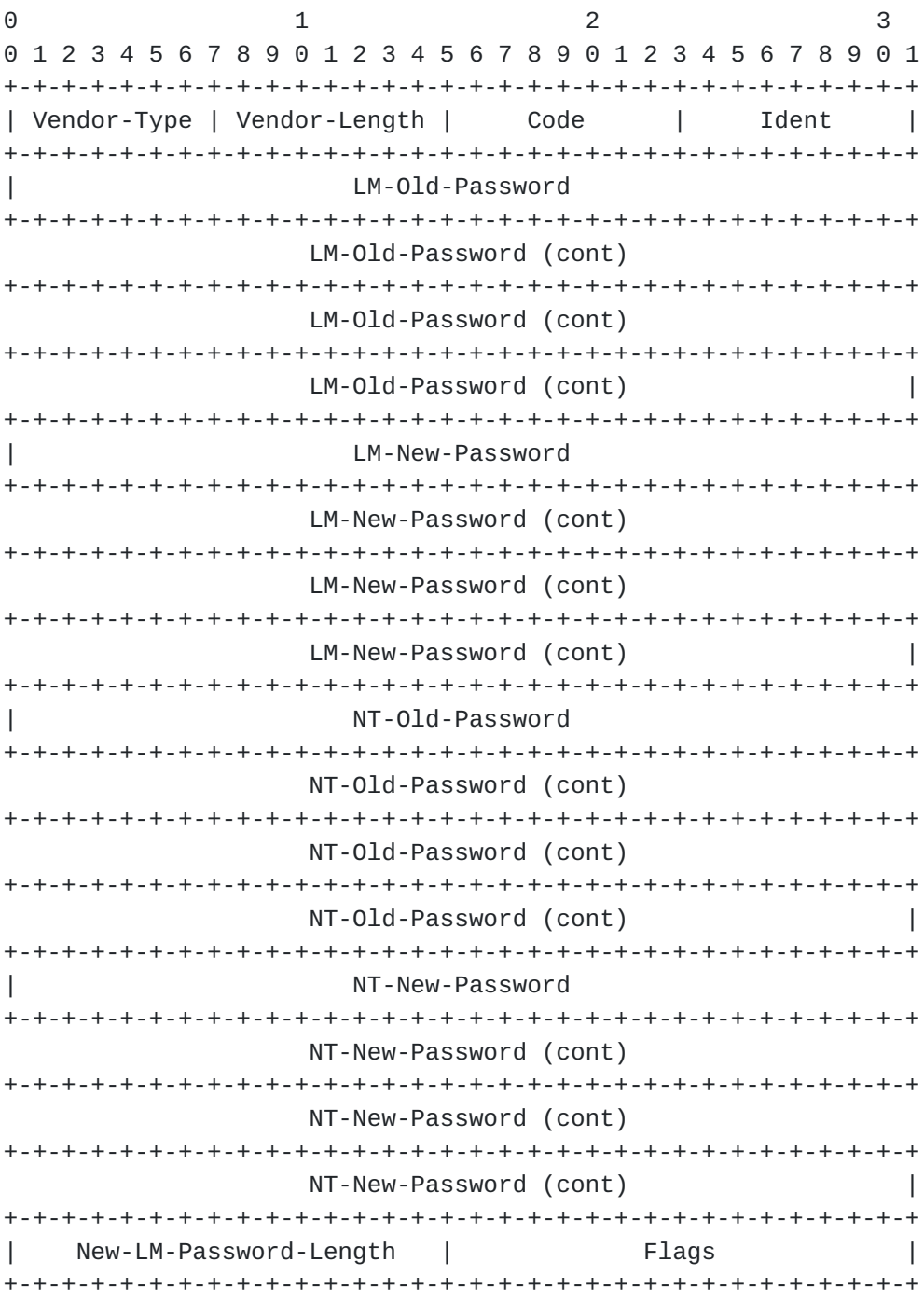
5.5. MS-CHAP-CPW-1

Description

This Attribute allows the user to change their password if it has expired. This Attribute is only used in Access-Request packets, and should only be included if an MS-CHAP-Error attribute was included in the immediately preceding Access-Reject packet, the String field of the MS-CHAP-Error attribute indicated that the

user password had expired, and the MS-CHAP version is less than 2.

A summary of the MS-CHAP-CPW-1 Attribute format is shown below. The fields are transmitted from left to right.



Vendor-Type

3 for MS-CHAP-PW-1

Vendor-Length
72

Code
The Code field is one octet in length. Its value is always 5.

Ident
The Ident field is one octet and aids in matching requests and replies.

LM-Old-Password
The LM-Old-Password field is 16 octets in length. It contains the encrypted Lan Manager hash of the old password.

LM-New-Password
The LM-New-Password field is 16 octets in length. It contains the encrypted Lan Manager hash of the new password.

NT-Old-Password
The NT-Old-Password field is 16 octets in length. It contains the encrypted Lan Manager hash of the old password.

NT-New-Password
The NT-New-Password field is 16 octets in length. It contains the encrypted Lan Manager hash of the new password.

New-LM-Password-Length
The New-LM-Password-Length field is two octets in length and contains the length in octets of the new LAN Manager-compatible password.

Flags
The Flags field is two octets in length. If the least significant bit of the Flags field is one, this indicates that the NT-New-Password and NT-Old-Password fields are valid and SHOULD be used. Otherwise, the LM-New-Password and LM-Old-Password fields MUST be used.

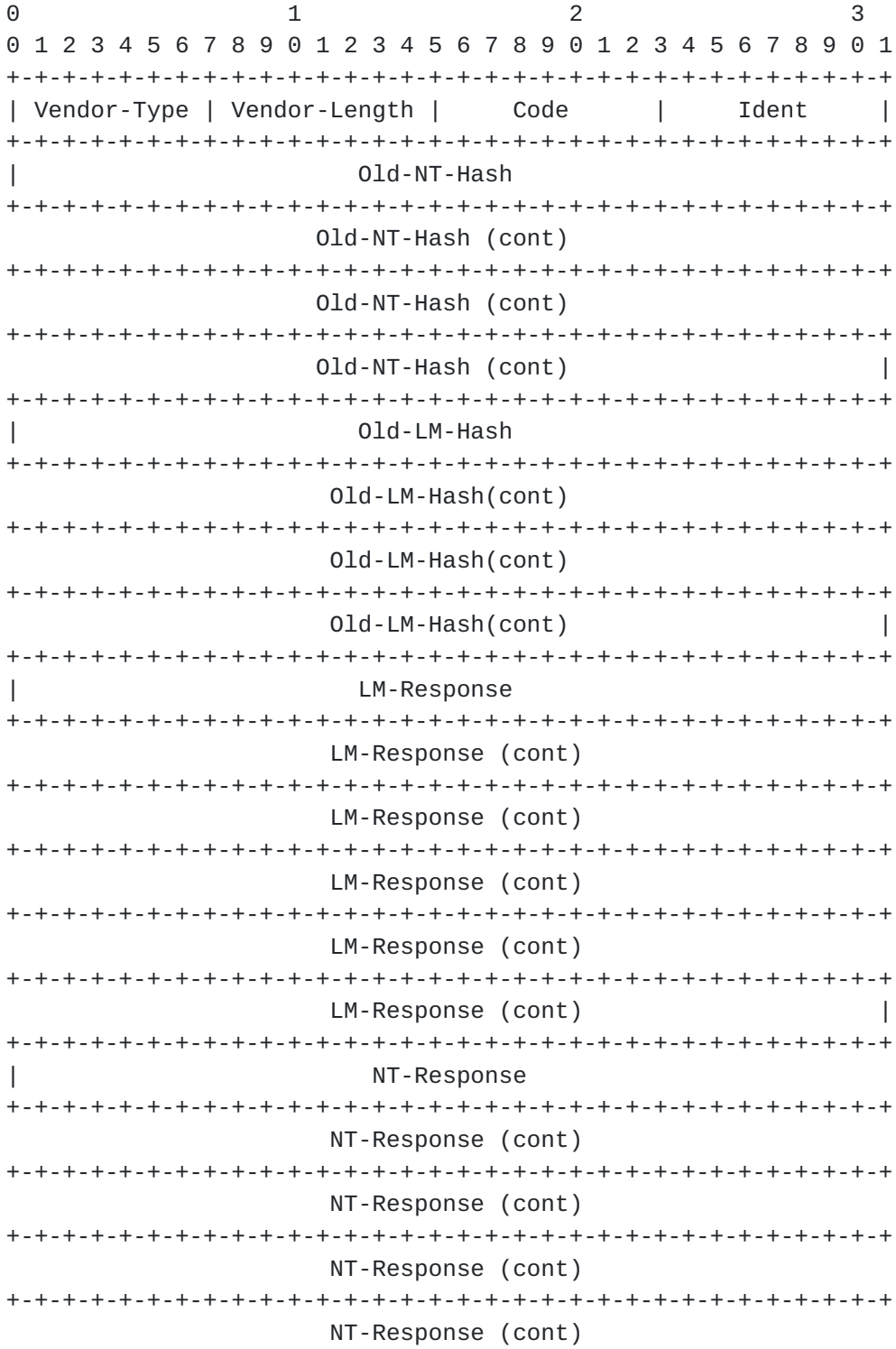
5.6. MS-CHAP-CPW-2

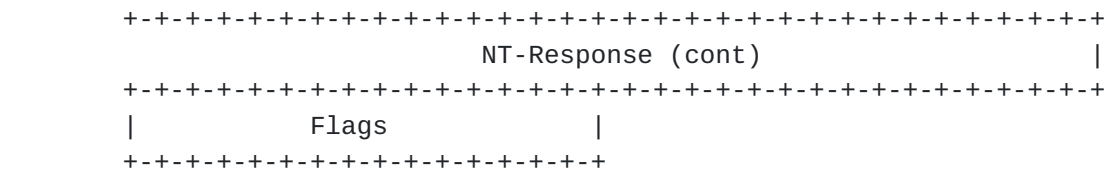
Description

This Attribute allows the user to change their password if it has expired. This Attribute is only used in Access-Request packets, and should only be included if an MS-CHAP-Error attribute was included in the immediately preceding Access-Reject packet, the String field of the MS-CHAP-Error attribute indicated that the

user password had expired, and the MS-CHAP version is 2 or greater.

A summary of the MS-CHAP-CPW-2 Attribute format is shown below. The fields are transmitted from left to right.





Vendor-Type
4 for MS-CHAP-PW-2

Vendor-Length
86

Code
6

Ident
The Ident field is one octet and aids in matching requests and replies. The value of this field MUST be identical to that in the Ident field in all instances of the MS-CHAP-LM-Enc-PW, MS-CHAP-NT-Enc-PW and MS-CHAP-PW-2 attributes contained in a single Access-Request packet.

Old-NT-Hash
The Old-NT-Hash field is 16 octets in length. It contains the old Windows NT password hash encrypted with the new Windows NT password hash.

Old-LM-Hash
The Old-LM-Hash field is 16 octets in length. It contains the old Lan Manager password hash encrypted with the new Windows NT password hash.

LM-Response
The LM-Response field is 24 octets in length and holds an encoded function of the password and the received challenge. If this field is empty, it SHOULD be zero-filled.

NT-Response
The NT-Response field is 24 octets in length and holds an encoded function of the password and the received challenge. If this field is empty, it SHOULD be zero-filled.

Flags
The Flags field is two octets in length. If the least significant bit (bit 0) of this field is one, the NT-Response field is to be used in preference to the LM-Response field for authentication. The LM-Response field MAY still be used (if present), but the NT-Response SHOULD be tried first. If least significant bit of the

field is zero, the NT-Response field MUST be ignored and the LM-Response field used instead. If bit 1 of the Flags field is one, the Old-LM-Hash field is valid and SHOULD be used. If this bit is set, at least one instance of the MS-CHAP-LM-Enc-PW attribute MUST be included in the packet.

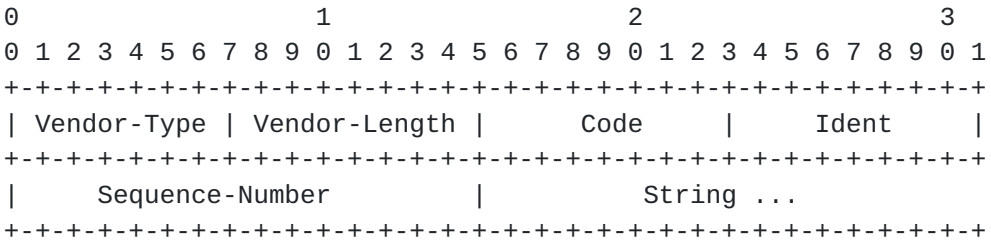
5.7. MS-CHAP-LM-Enc-PW

Description

This Attribute contains the new Windows NT password encrypted with the old LAN Manager password hash. The encrypted Windows NT password is 516 octets in length; since this is longer than the maximum lengtth of a RADIUS attribute, the password must be split into several attibutes for transmission. A 2 octet sequence number is included in the attribute to help preserve ordering of the password fragments.

This Attribute is only used in Access-Request packets, in conjunction with the MS-CHAP-CPW-2 attribute. It should only be included if an MS-CHAP-Error attribute was included in the immediately preceding Access-Reject packet, the String field of the MS-CHAP-Error attribute indicated that the user password had expired, and the MS-CHAP version is 2 or greater.

A summary of the MS-CHAP-LM-Enc-PW Attribute format is shown below. The fields are transmitted from left to right.



Vendor-Type
5 for MS-CHAP-LM-Enc-PW

Vendor-Length
> 6

Code
6. Code is the same as for the MS-CHAP-PW-2 attribute.

Ident
The Ident field is one octet and aids in matching requests and

replies. The value of this field MUST be identical in all instances of the MS-CHAP-LM-Enc-PW, MS-CHAP-NT-Enc-PW and MS-CHAP-PW-2 attributes which are present in the same Access-Request packet.

Sequence-Number
The Sequence-Number field is two octets in length and indicates which "chunk" of the encrypted password is contained in the following String field.

String
The String field contains a portion of the encrypted password.

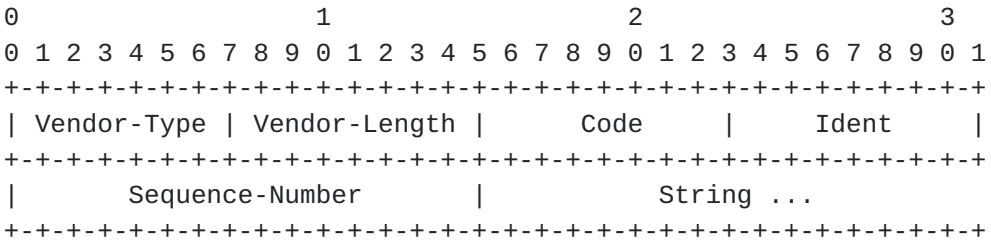
5.8. MS-CHAP-NT-Enc-PW

Description

This Attribute contains the new Windows NT password encrypted with the old Windows NT password hash. The encrypted Windows NT password is 516 octets in length; since this is longer than the maximum lengtth of a RADIUS attribute, the password must be split into several attibutes for transmission. A 2 octet sequence number is included in the attribute to help preserve ordering of the password fragments.

This Attribute is only used in Access-Request packets, in conjunction with the MS-CHAP-CPW-2 attribute. It should only be included if an MS-CHAP-Error attribute was included in the immediately preceding Access-Reject packet, the String field of the MS-CHAP-Error attribute indicated that the user password had expired, and the MS-CHAP version is 2 or greater.

A summary of the MS-CHAP-NT-Enc-PW Attribute format is shown below. The fields are transmitted from left to right.



Vendor-Type
6 for MS-CHAP-NT-Enc-PW

Vendor-Length

> 6

Code
6. Code is the same as for the MS-CHAP-PW-2 attribute.

Ident
The Ident field is one octet and aids in matching requests and replies. The value of this field MUST be identical in all instances of the MS-CHAP-LM-Enc-PW, MS-CHAP-NT-Enc-PW and MS-CHAP-PW-2 attributes which are present in the same Access-Request packet.

Sequence-Number
The Sequence-Number field is two octets in length and indicates which "chunk" of the encrypted password is contained in the following String field.

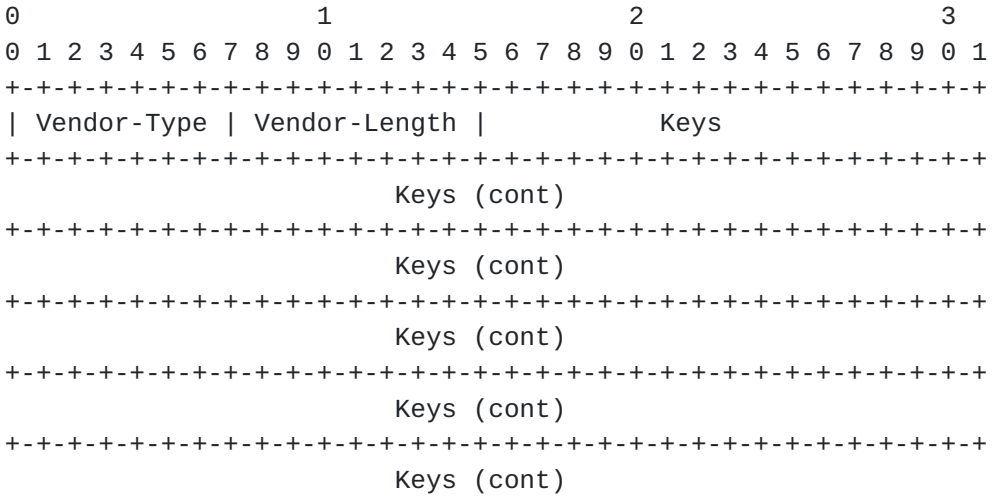
String
The String field contains a portion of the encrypted password.

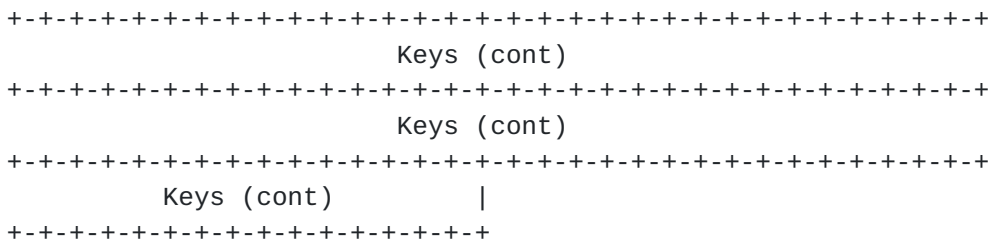
5.9. MS-CHAP-MPPE-Keys

Description

The MS-CHAP-MPPE-Keys Attribute contains two session keys for use by the Microsoft Point-to-Point Encryption Protocol (MPPE). This Attribute is only included in Access-Accept packets. Note that the keys are generative session keys; no processing need be done by the RADIUS client before using the keys in the MPPE protocol.

A summary of the MS-CHAP-MPPE-Keys Attribute format is given below. The fields are transmitted left to right.

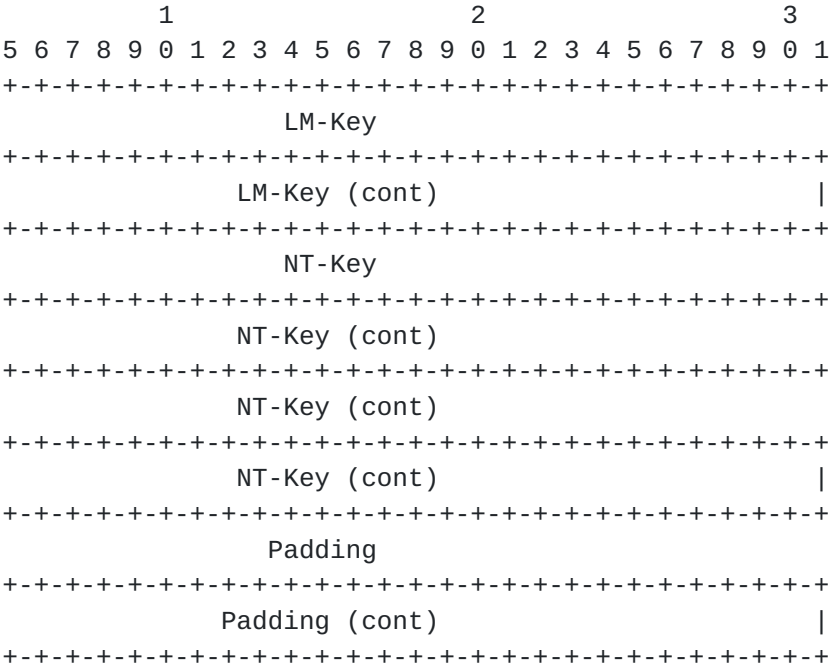




Vendor-Type
12 for MS-CHAP-MPPE-Keys.

Vendor-Length
34

Keys
The Keys field consists of two logical sub-fields: the LM-Key and the NT-Key. The LM-Key is eight octets in length and is derived from the first eight bytes of the hashed LAN Manager password. The NT-Key sub-field is sixteen octets in length and is derived from the first sixteen octets of the hashed Windows NT password. The format of the plaintext Keys field is illustrated in the following diagram:



The Keys field MUST be encrypted by the RADIUS server using the same method defined for the User-Password Attribute [3]. Note that the padding is required because the method referenced above requires the field to be encrypted to be a multiple of sixteen octets in length.

6. Table of Attributes

The following table provides a guide to which of the above attributes may be found in which kinds of packets, and in what quantity.

Request	Accept	Reject	Challenge	Acct-Request	#	Attribute
0+	0	0	0+	0	11	MS-CHAP-Challenge
0+	0	0	0	0	1	MS-CHAP-Response
0	0+	0	0	0+	10	MS-CHAP-Domain
0	0	0+	0	0	2	MS-CHAP-Error
0+	0	0	0	0	3	MS-CHAP-CPW-1
0+	0	0	0	0	4	MS-CHAP-CPW-2
0+	0	0	0	0	5	MS-CHAP-LM-Enc-PW
0+	0	0	0	0	6	MS-CHAP-NT-Enc-PW
0	0+	0	0	0	12	MS-CHAP-MPPE-Keys

The following table defines the meaning of the above table entries.

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

7. Security Considerations

MS-CHAP, like PPP CHAP, is susceptible to dictionary attacks. User passwords should be chosen with care, and be of sufficient length to deter easy guessing. Although the scheme used to protect the Keys field of the MS-CHAP-MPPE-Keys Attribute is believed to be relatively secure on the wire, RADIUS proxies will decrypt and re-encrypt the field for forwarding. Therefore, the MS-CHAP-MPPE-Keys attribute SHOULD NOT be used on networks where untrusted RADIUS proxies reside.

8. Acknowledgements

Thanks to Carl Rigney (cdr@livingston.com), Narendra Gidwani (nareng@microsoft.com), Steve Cobb (stevec@microsoft.com), Pat Calhoun (pcalhoun@usr.com), Dave Mitton (dmitton@baynetworks.com), Paul Funk (paul@funk.com), Gurdeep Singh Pall (gurdeep@microsoft.com) and Don Rule (donaldr@microsoft.com) for useful suggestions and editorial feedback.

9. Expiration Date

This document expires May 21, 1998.

10. Chair's Address

The RADIUS Working Group can be contacted via the current chair:

Carl Rigney
Livingston Enterprises
4464 Willow Road
Pleasanton, California 94588

Phone: +1 510 426 0770
E-Mail: cdr@livingston.com

11. Author's Address

Questions about this memo can also be directed to:

Glen Zorn
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052

Phone: +1 425 703 1559
FAX: +1 425 936 7329
EMail: glennz@microsoft.com

12. References

[1] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997

[3] Rigney, C., et. al., "Remote Access Dial In User Service", RFC 2138, April 1997