PPPEXT Working Group
INTERNET-DRAFT
Category: Informational
Expires: December 25, 2007

Ryan Hurst
Ashwin Palekar
Microsoft Corporation
12 June 2007

Microsoft EAP CHAP Extensions
draft-kamath-pppext-eap-mschapv2-02.txt

Copyright Notice

Abstract

This document defines the Microsoft EAP CHAP Extensions Protocol, Version 2, which encapsulates the MS-CHAPv2 protocol defined in RFC 2759, within EAP as defined in RFC 3748.

Table of Contents

1. Introduction

The Extensible Authentication Protocol (EAP), described in [RFC3748], provides a standard mechanism for support of multiple authentication methods. Through the use of EAP, support for a number of authentication schemes may be added, including smart cards, Kerberos, Public Key, One Time Passwords, and others.

This document defines the Microsoft EAP CHAP Extensions Protocol, Version 2, which encapsulates the MS-CHAP-v2 protocol, defined in [RFC2759], within EAP. As with MS-CHAP-v2, EAP-MSCHAPv2 supports mutual authentication and key derivation. The way EAP-MSCHAPv2 derived keys are used with the Microsoft Point to Point Encryption (MPPE) cipher is described in [RFC3079].

EAP MS-CHAP-V2 provides mutual authentication between peers by piggybacking a peer challenge on the Response packet and an authenticator response on the Success packet.

1.1. Requirements language

In this document, several words are used to signify the requirements of the specification. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in "Key words for use in RFCs to Indicate Requirement Levels" [RFC2119].

1.2. Terminology

This document frequently uses the following terms:

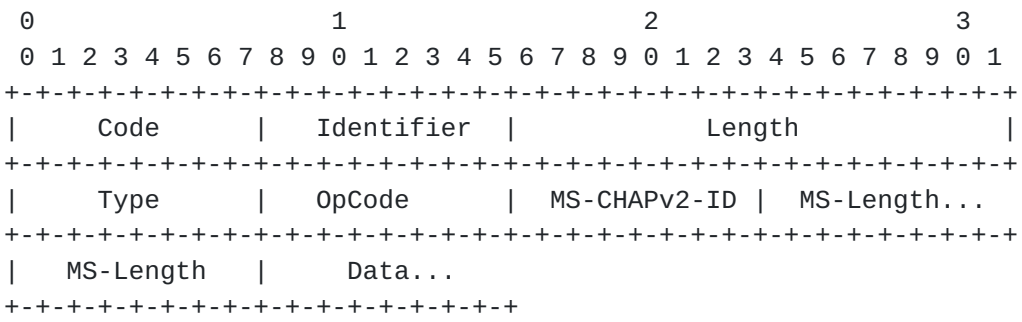
Authenticator
: The end of the link requiring the authentication.

Peer
: The other end of the point-to-point link; the end which is being authenticated by the authenticator.

silently discard
: This means the implementation discards the packet without further processing. The implementation SHOULD provide the capability of logging the error, including the contents of the silently discarded packet, and SHOULD record the event in a statistics counter.

2. EAP MS-CHAP-v2 Packet Format

A summary of the EAP MS-CHAP-V2 packet format is shown below. The fields are transmitted from left to right.



Code

1 - Request
2 - Response

Identifier

The Identifier field is one octet and aids in matching responses with requests.

Length

The Length field is two octets and indicates the length of the EAP packet including the Code, Identifier, Length, Type, OpCode, MS-CHAPv2-ID, MS-Length and Data fields. Octets outside the range of the Length field should be treated as Data Link Layer padding and should be ignored on reception.

Type

26 - EAP MS-CHAP-V2

OpCode

The OpCode field is one octet and identifies the type of EAP MS-CHAP-v2 packet. OpCodes are assigned as follows:

1 Challenge
2 Response
3 Success
4 Failure
7 Change-Password

MS-CHAPv2-ID

The MS-CHAPv2-ID field is one octet and aids in matching MSCHAP-v2 responses with requests. Typically, the MS-CHAPv2-ID field is the same as the Identifier field.

MS-Length

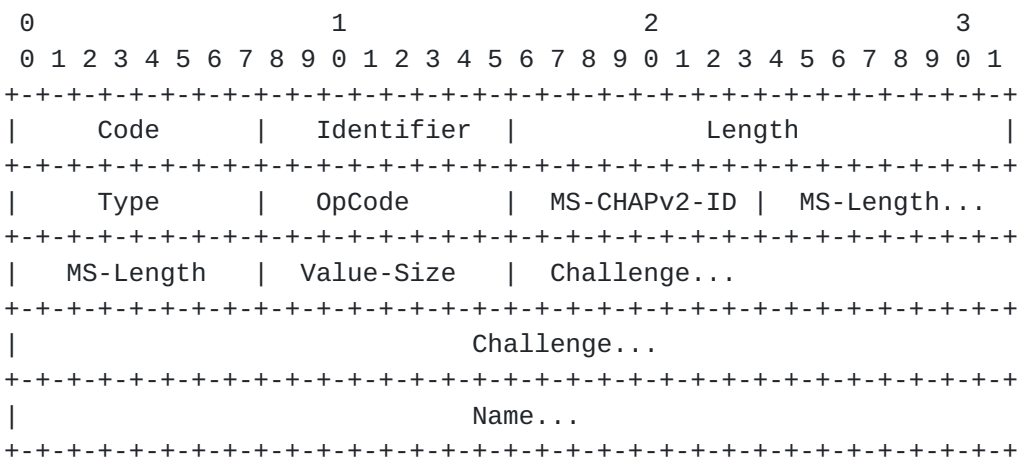
The MS-Length field is two octets and MUST be set to the value of the Length field minus 5.

Data

The format of the Data field is determined by the OpCode field.

2.1. Challenge packet

The Challenge packet is used to begin the EAP MS-CHAP-V2 protocol. The authenticator MUST transmit an EAP Request packet with Type=26, and the OpCode field set to 1 (Challenge). The format of the EAP MS-CHAP-v2 Challenge packet is shown below. The fields are transmitted from left to right.



Code

1 - Request

Identifier

The Identifier field is one octet. The Identifier field MUST be the same if a Request packet is retransmitted due to a timeout while waiting for a Response. Any new (non-retransmission) Requests MUST modify the Identifier field. If a peer receives a duplicate Request for which it has already sent a Response, it MUST resend it's

Response. If a peer receives a duplicate Request before it has sent a Response to the initial Request (i.e. it's waiting for user input), it MUST silently discard the duplicate Request.

Length

The Length field is two octets and indicates the length of the EAP packet including the Code, Identifier, Length, Type, OpCode, MS-CHAPv2-ID, MS-Length, Value-Size, Challenge, and Name fields. Octets outside the range of the Length field should be treated as Data Link Layer padding and should be ignored on reception.

Type

26 - EAP MS-CHAP-V2

OpCode

1 - Challenge

MS-CHAPv2-ID

The MS-CHAPv2-ID field is one octet and aids in matching MSCHAP-v2 responses with requests. Typically, the MS-CHAPv2-ID field is the same as the Identifier field.

MS-Length

The MS-Length field is two octets and MUST be set to the value of the Length field minus 5.

Value-Size

This field is one octet and indicates the length of the Challenge field. Since EAP MS-CHAPv2 utilizes a 16 octet Challenge field, it is set to 0x10 (16 decimal).

Challenge

The Challenge field is 16 octets. The most significant octet is transmitted first. The Challenge MUST be changed each time a Challenge is sent.

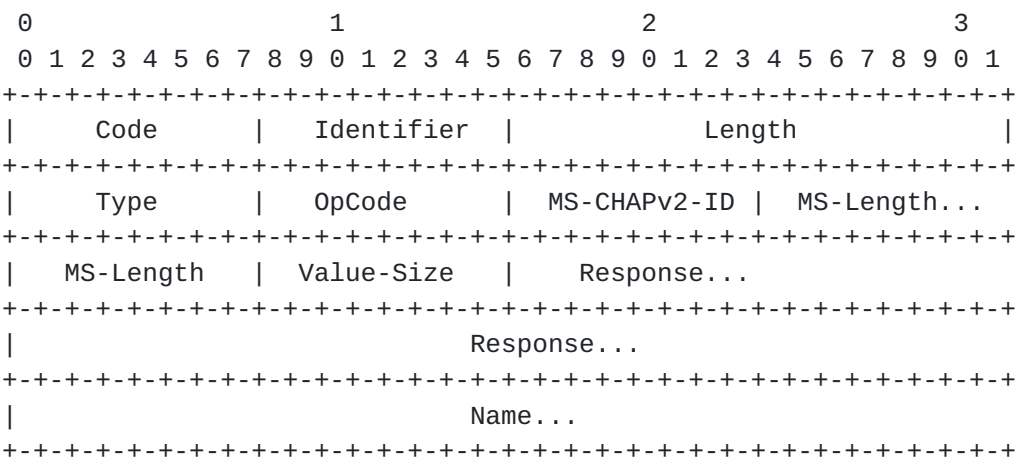
Name

The Name field is one or more octets representing the identification of the system transmitting the packet. There are no limitations on the content of this field. The Name should not be NUL or CR/LF

terminated. The size of the Name field is equal to Length - Value-Size - 10.

2.2. Response packet

The format of the EAP MS-CHAP-v2 Response packet is shown below. The fields are transmitted from left to right.



Code

2 - Response

Identifier

The Identifier field is one octet and contains the value included in the EAP Request to which it responds.

Length

The Length field is two octets and indicates the length of the EAP packet including the Code, Identifier, Length, Type, OpCode, MS-CHAPv2-ID, MS-Length, Value-Size, Response, and Name fields. Octets outside the range of the Length field should be treated as Data Link Layer padding and should be ignored on reception.

Type

26 - EAP MS-CHAP-V2

OpCode

2 - Response

MS-CHAPv2-ID

The MS-CHAPv2-ID field is one octet and aids in matching MSCHAP-v2 responses with requests. Typically, the MS-CHAPv2-ID field is the same as the Identifier field.

MS-Length

The MS-Length field is two octets and MUST be set to the value of the Length field minus 5.

Value-Size

This field is one octet and indicates the length of the Response field. It is set to 0x31 (Decimal 49).

Response

The Response field is 49 octets. The most significant octet is transmitted first. It is sub-formatted as follows:

```
16 octets: Peer-Challenge
8 octets: Reserved, must be zero
24 octets: NT-Response
1 octet : Flags
```

The Peer-Challenge field is a 16-octet random number. As the name implies, it is generated by the peer and is used in the calculation of the NT-Response field, below. Peers need not duplicate Microsoft's algorithm for selecting the 16-octet value, but the standard guidelines on randomness [RFC1750] SHOULD be observed.

The NT-Response field is an encoded function of the password, the Name field of the Response packet, the contents of the Peer-Challenge field and the received Challenge as output by the routine GenerateNTResponse() defined in [RFC2759], Section 8.1.

The Windows NT password is a string of 0 to (theoretically) 256 case-sensitive Unicode [UNICODE] characters. Current versions of Windows NT limit passwords to 14 characters, mainly for compatibility reasons; this may change in the future. When computing the NT-Response field contents, only the user name is used, without any associated Windows NT domain name. This is true regardless of whether a Windows NT domain name is present in the Name field (see below).

The Flag field is reserved for future use and MUST be zero.

Whenever a Response packet is received, the authenticator compares the Response Value with its own calculation of the expected value. If the values match, then the authenticator MUST send a Success-Request packet, as described in Section 2.3. If the values do not match, and if the error is retryable, then a Failure-Request packet MUST be sent as described in Section 2.5. If the values do not match, and the error is not retryable, then a Failure-Request packet (described in Section 2.5) SHOULD be sent, or alternatively, the authentication MAY be terminated (as described in Section 2.8) such as by sending an EAP Failure.

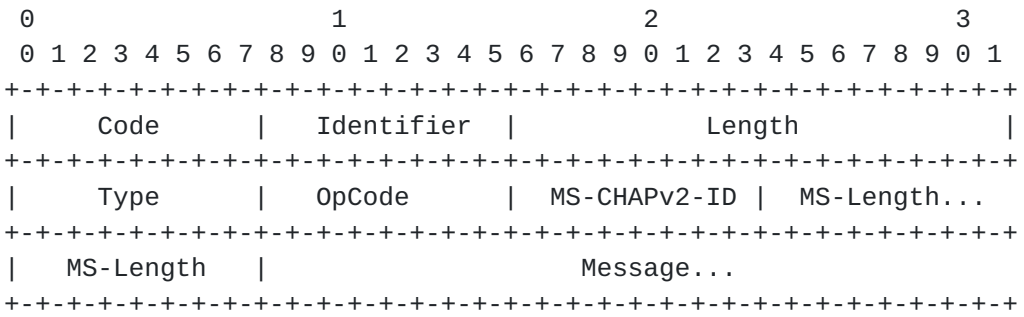
Name

The Name field is a string of 0 to (theoretically) 256 case-sensitive ASCII characters which identifies the peer's user account name. The Windows NT domain name may prefix the user's account name (e.g. BIGCO\johndoe where BIGCO is a Windows NT domain containing the user account johndoe). If a domain is not provided, the backslash should also be omitted, (e.g. johndoe). The Name SHOULD NOT be NUL or CR/LF terminated. The size of the Name field is determined from the Length - Value-Size - 10.

2.3. Success Request packet

If the value received in the Response field of the EAP MS-CHAP-V2 Response packet is equal to the expected value, then the implementation MUST transmit an EAP MS-CHAP-V2 Request packet with the OpCode field set to 3 (Success).

The format of the EAP MS-CHAP-v2 Success Request packet is shown below. The fields are transmitted from left to right.



Code

1 - Request

Identifier

The Identifier field is one octet. The Identifier field MUST be the same if a Request packet is retransmitted due to a timeout while waiting for a Response. Any new (non-retransmission) Requests MUST modify the Identifier field. If a peer receives a duplicate Request for which it has already sent a Response, it MUST resend it's Response. If a peer receives a duplicate Request before it has sent a Response to the initial Request (i.e. it's waiting for user input), it MUST silently discard the duplicate Request.

Length

The Length field is two octets and indicates the length of the EAP packet including the Code, Identifier, Length, Type, OpCode, MS-CHAPv2-ID, MS-Length, and Message fields. Octets outside the range of the Length field should be treated as Data Link Layer padding and should be ignored on reception.

Type

26 - EAP MS-CHAP-V2

OpCode

3 - Success

MS-CHAPv2-ID

The MS-CHAPv2-ID field is one octet and aids in matching MSCHAP-v2 responses with requests. Typically, the MS-CHAPv2-ID field is the same as the Identifier field.

MS-Length

The MS-Length field is two octets and MUST be set to the value of the Length field minus 5.

Message

The Message field contains a 42-octet authenticator response string and a printable message. The format of the message field is illustrated below.

"S=<auth_string> M=<message>"

The <auth_string> quantity is a 20 octet number encoded in ASCII as 40 hexadecimal digits. The hexadecimal digits A-F (if present) MUST

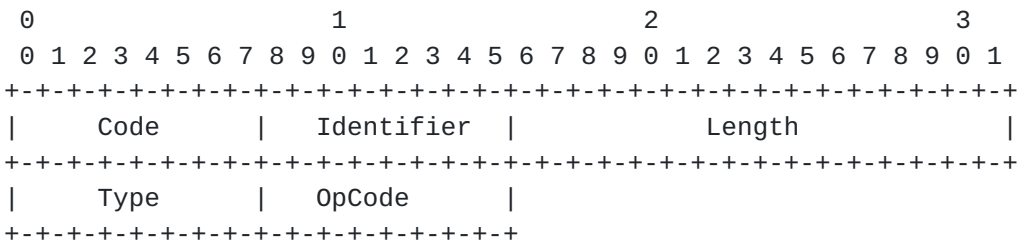
be uppercase. This number is derived from the challenge from the Challenge packet, the Peer-Challenge and NT-Response fields from the Response packet, and the peer password as output by the routine GenerateAuthenticatorResponse() defined in [RFC2759], Section 8.7. The authenticating peer MUST verify the authenticator response when a Success packet is received. The method for verifying the authenticator is described in [RFC2759], section 8.8. If the authenticator response is either missing or incorrect, the peer MUST end the session without sending a response.

The <message> quantity is human-readable text in the appropriate charset and language [RFC2484].

2.4. Success Response packet

In the peer successfully validates the EAP MS-CHAP-V2 Success Request packet sent by the authenticator, then it MUST respond with an EAP MS-CHAP-V2 Success Response packet with the OpCode field set to 3 (Success).

The format of the EAP MS-CHAP-v2 Success Response packet is shown below. The fields are transmitted from left to right.



Code

2 - Response

Identifier

The Identifier field is one octet and contains the value included in the EAP Request to which it responds.

Length

6

Type

26 - EAP MS-CHAP-V2

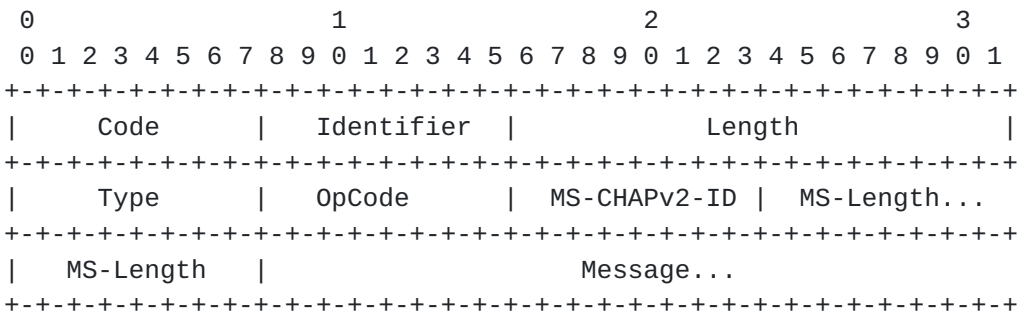
OpCode

3 - Success

2.5. Failure Request packet

If the Value received in a Response is not equal to the expected value, and the error is retryable, then the implementation MUST transmit an EAP MS-CHAP-v2 Request packet with the OpCode field set to 4 (Failure). If the error is not retryable, then the implementation SHOULD transmit an EAP MS-CHAP-v2 Failure Request packet, or it MAY terminate the authentication (e.g. send an EAP Failure packet). The former approach is preferable, since this enables the cause of the error to be communicated.

The format of the EAP MS-CHAP-v2 Failure Request packet is shown below. The fields are transmitted from left to right.



Code

1 - Request

Identifier

The Identifier field is one octet. The Identifier field MUST be the same if a Request packet is retransmitted due to a timeout while waiting for a Response. Any new (non-retransmission) Requests MUST modify the Identifier field. If a peer receives a duplicate Request for which it has already sent a Response, it MUST resend it's Response. If a peer receives a duplicate Request before it has sent a Response to the initial Request (i.e. it's waiting for user input), it MUST silently discard the duplicate Request.

Length

The Length field is two octets and indicates the length of the EAP packet including the Code, Identifier, Length, Type, OpCode, MS-CHAPv2-ID, MS-Length, and Message fields. Octets outside the range of the Length field should be treated as Data Link Layer padding and should be ignored on reception.

Type

26 - EAP MS-CHAP-V2

OpCode

4 - Failure

MS-CHAPv2-ID

The MS-CHAPv2-ID field is one octet and aids in matching MSCHAP-v2 responses with requests. Typically, the MS-CHAPv2-ID field is the same as the Identifier field.

MS-Length

The MS-Length field is two octets and MUST be set to the value of the Length field minus 5.

Message

The Message field format is:

"E=eeeeeeeeee R=r C=cccccccccccccccccccccccccccccccc V=vvvvvvvvvv M=<msg>"

where

The "eeeeeeeeee" is the ASCII representation of a decimal error code corresponding to one of those listed below, though implementations should deal with codes not on this list gracefully. The error code need not be 10 digits long.

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

The "r" is a single character ASCII flag set to '1' if a retry is

allowed, and '0' if not. Typically, errors 646, 647, and 649 are non-retryable (R=0). When the authenticator sets this flag to '1' it disables short timeouts, expecting the peer to prompt the user for new credentials and resubmit the response. The "ccccccccccccccccccccccccccccccc" is the ASCII representation of a hexadecimal challenge value. This field MUST be exactly 32 octets long and MUST be present.

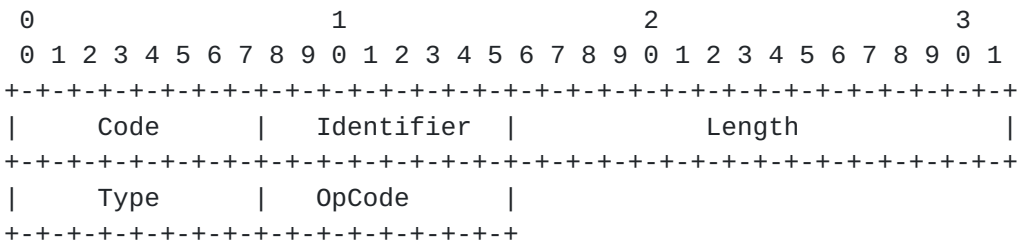
The "vvvvvvvvvv" is the ASCII representation of a decimal version code (need not be 10 digits) indicating the password changing protocol version supported on the server. For EAP MS-CHAP-V2, this value MUSTalways be 3.

<msg> is human-readable text in the appropriate charset and language [RFC2484].

2.6. Failure Response packet

When the peer receives a Failure Request packet that is retryable (R=1), the authentication MAY be retried. For example, a new Response packet, or Change Password packet MAY be sent. In these cases a Failure Response packet is not sent.

However, if the EAP MS-CHAPv2 Failure Request is non-retryable (R=0), then the peer SHOULD transmit an EAP MS-CHAP-v2 Response packet with the OpCode field set to 4 (Failure). The format of the EAP MS-CHAP-v2 Failure Response packet is shown below. The fields are transmitted from left to right.



Code

2 - Response

Identifier

The Identifier field is one octet and contains the value included in the EAP Request to which it responds.

Length

6

Type

26 - EAP MS-CHAP-V2

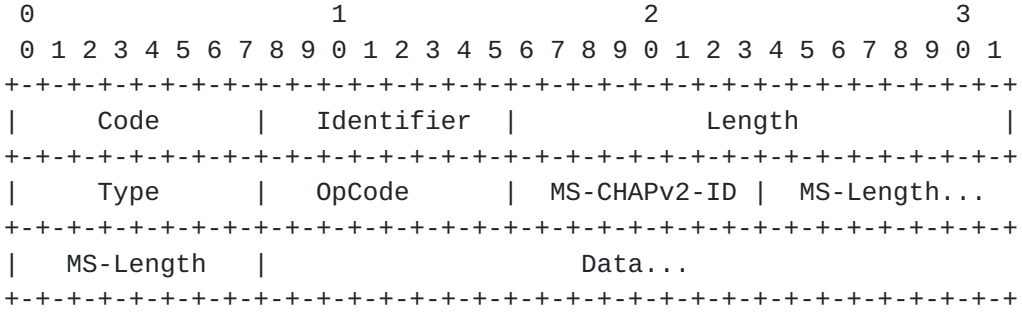
OpCode

4 - Failure

2.7. Change-Password packet

The Change-Password packet does not appear in either standard CHAP or MS-CHAP-V1. It allows the peer to change the password on the account specified in the preceding Response packet. The Change-Password packet should be sent only if the authenticator reports ERROR_PASSWD_EXPIRED (E=648) in the Message field of the Failure packet.

The format of the EAP MS-CHAP-v2 Change Password packet is shown below. The fields are transmitted from left to right.



Code

2 - Response

Identifier

The Identifier field is one octet and aids in matching responses with requests. The value is the Identifier of the received Failure packet to which this packet responds.

Length

The Length field is two octets and indicates the length of the EAP packet including the Code, Identifier, Length, Type, OpCode, MS-

CHAPv2-ID, MS-Length and Data fields. Octets outside the range of the Length field should be treated as Data Link Layer padding and should be ignored on reception. For the Change Password packet, the length = 591.

Type

26 - EAP MS-CHAP-V2

OpCode

7 - Change Password

MS-CHAPv2-ID

The MS-CHAPv2-ID field is one octet and aids in matching MSCHAP-v2 responses with requests. Typically, the MS-CHAPv2-ID field is the same as the Identifier field.

MS-Length

The MS-Length field is two octets and MUST be set to the value of the Length field minus 5.

Data

The Data field is 582 octets in length, and is subdivided as follows:

```
     516 octets : Encrypted-Password
      16 octets : Encrypted-Hash
      16 octets : Peer-Challenge
       8 octets : Reserved
      24 octets : NT-Response
       2-octet  : Flags
```

Encrypted-Password

The Encrypted-Password field is 516 octets in length, and contains the PWBLOCK form of the new Windows NT password encrypted with the old Windows NT password hash, as output by the NewPasswordEncryptedWithOldNtPasswordHash() routine defined in [RFC2759], Section 8.9.

Encrypted-Hash

The Encrypted-Hash field is 16 octets in length and contains the old Windows NT password hash encrypted with the new Windows NT password hash, as output by the

OldNtPasswordHashEncryptedWithNewNtPasswordHash() routine, defined in [RFC2759], Section 8.12.

Peer-Challenge

The Peer-Challenge field is 16 octets in length, and contains a 16-octet random quantity, as described in the Response packet description.

Reserved

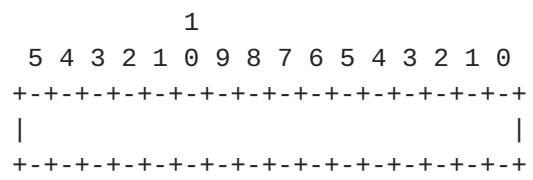
8 octets, must be zero.

NT-Response

The NT-Response field is 24 octets in length and is as described in the Response packet description. However it is calculated on the new password and the challenge received in the Failure packet.

Flags

The Flags field is two octets in length. It is a bit field of option flags where 0 is the least significant bit of the 16-bit quantity. The format of this field is illustrated in the following diagram:



Bits 0-15
Reserved, always clear (0).

2.8. Alternative failure behavior

Rather than sending a Failure Request as described in Section 2.5, if the error is non-retryable (e.g. R=0), or if the maximum number of retries has been exhausted, then the Authenticator MAY terminate the authentication conversation. Where EAP MS-CHAP-V2 is running standalone (e.g. without PEAP), this will result in transmission of an EAP Failure message to the authenticator. Since EAP Failure packets do not carry additional data, no error message may be transmitted to the peer.

2.9. Known bugs

In Windows XP SP1, Failure Request packets are only sent where the error is retryable (R=1). Rather than sending a Failure Request with a non-retryable error (R=0), a Windows XP SP1 authenticator will terminate authentication. This is undesirable, because it prevents non-retryable error messages from being received by the peer. A Windows XP SP1 host, on receiving a Failure Request packet with a non-retryable error (R=0), will silently discard the packet.

Since a Windows XP SP1 peer will respond to a retryable (R=1) Failure Request by retrying authentication (such as by sending a Response or Change-Password packet), and non-retryable (R=0) Failure Requests are silently discarded, Windows XP SP1 peers do not send Failure Response packets. If a Windows XP SP1 authenticator receives a Failure Response packet, it will be silently discarded.

3. Security Claims

EAP security claims are defined in [RFC3748] Section 7.2.1. Using the terms defined there, the security properties of the Microsoft EAP MS-CHAP-v2 protocol are as follows:

Auth. mechanism:	Password
Ciphersuite negotiation:	No
Mutual authentication:	Yes
Integrity protection:	Yes
Replay protection:	Yes
Confidentiality:	No
Key derivation:	Yes
Key strength:	Depends on password policy
Dictionary attack prot.:	No
Fast reconnect:	No
Crypt. binding:	N/A
Session independence:	Depends on password policy
Fragmentation:	No
Channel binding:	No

The Microsoft EAP MS-CHAP-v2 protocol is based on MS-CHAP-v2 as defined in [RFC2759]. MS-CHAP-v2 is a password-based authentication method that supports mutual authentication. While backward compatibility with MS-CHAP-v1 is supported, this does not really constitute a protected ciphersuite negotiation, since the cryptographic algorithms are largely fixed.

Integrity and replay protection are supported. As described in Section 2.2, the NT-Response field is an encoded function of the password, the Name field of the Response packet, the contents of the

Peer-Challenge field and the received Challenge. The inclusion of both the Peer-Challenge and received challenge provides replay protection. Fields within the EAP header (Code, Identifier, Length, Type) are not protected.

Confidentiality is not supported; the Name field in both the Challenge and Response packets are sent in the clear.

While Key Derivation is supported, the key strength is limited by the password policy. As noted in Section 2.2, in practice the password may be limited to 14 octets. If these octets are randomly chosen from the ASCII character set, then an effective key strength of 98 bits can be obtained. However, if the octets are only chosen from an English language dictionary, then an effective key strength of 2.2 bits per octet or 31 bits will obtain.

Session independence also depends on password policy. Where the password is weak, it may be obtained via dictionary attack, in which case future and past keys can be calculated. However, if the password is strong then the inclusion of nonces in both directions provides for session independence, absent invalidation of a cryptographic assumption.

As noted in [PPTPv1] and [PPTPv2], the MS-CHAP-v2 protocol is subject to dictionary attack. It is advised that this method only be used when protected from snooping by a tunnel method such as [PEAP]; this will also mask potential key strength issues.

As the protocol exchanges fit within the minimum EAP MTU size defined in [RFC3748], there is no need for fragmentation support. Fast reconnect and Channel binding are not supported.

4. References

4.1. Normative references

[RFC1320] Rivest, R., "MD4 Message Digest Algorithm", RFC 1320, April 1992.

[RFC1994] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[RFC1750] Eastlake, D., Crocker, S. and J. Schiller, "Randomness Recommendations for Security", RFC 1750, December 1994.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2433] Zorn, G. and Cobb, S., "Microsoft PPP CHAP Extensions", RFC 2433, October 1998.

[RFC2484] Zorn, G., "PPP LCP Internationalization Configuration Option", RFC 2484, January 1999.

[RFC2759] Zorn, G., "Microsoft PPP CHAP Extensions, Version 2", RFC 2759, January 2000.

[RFC3748] Blunk, L., "Extensible Authentication Protocol (EAP)", RFC 3748, April 2004.

[RC4] RC4 is a proprietary encryption algorithm available under license from RSA Data Security Inc. For licensing information, contact:

RSA Data Security, Inc.
100 Marine Parkway
Redwood City, CA 94065-1031

[IEEE8021X] IEEE Standards for Local and Metropolitan Area Networks: Port Based Network Access Control, IEEE Std 802.1X-2001, June 2001.

[SHA1] "Secure Hash Standard", Federal Information Processing Standards Publication 180-1, National Institute of Standards and Technology, April 1995.

[UNICODE] "The Unicode Standard, Version 2.0", The Unicode Consortium, Addison-Wesley, 1996. ISBN 0-201-48345-9.

4.2. Informative references

[RFC1570] Simpson, W., Editor, "PPP LCP Extensions", RFC 1570, January 1994.

[RFC1661] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[DES] "Data Encryption Standard (DES)", Federal Information Processing Standard Publication 46-2, National Institute of Standards and Technology, December 1993.

[DESMODES] "DES Modes of Operation", Federal Information Processing Standards Publication 81, National Institute of Standards and Technology, December 1980.

[RFC3079] Zorn, G., "Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)", RFC 3079, March 2001.

[PEAP] Palekar, A., et al., "Protected EAP Protocol (PEAP) Version 2", draft-josefsson-pppext-eap-tls-eap-08.txt, Internet draft (work in progress), April 2004.

[PPTPv1] Schneier, B. and Mudge, "Cryptanalysis of Microsoft's Point-to- Point Tunneling Protocol", Proceedings of the 5th ACM Conference on Communications and Computer Security, ACM Press, November 1998.

[PPTPv2] Schneier, B. and Mudge, "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)", CQRE '99, Springer-Verlag, 1999, pp. 192-203.

Appendix A - Examples

In the case where the EAP-MS-CHAP-V2 authentication is successful, the conversation will appear as follows:

```
Peer                    Authenticator
----                    -------------
                        <- EAP-Request/Identity
EAP-Response/
Identity (MyID) ->
                        <- EAP-Request/
                           EAP-Type=EAP MS-CHAP-V2
                           (Challenge)
EAP-Response/
EAP-Type=EAP-MS-CHAP-V2
(Response)->
                        <- EAP-Request/
                           EAP-Type=EAP-MS-CHAP-V2
                           (Success)
EAP-Response/
EAP-Type=EAP-MS-CHAP-V2
(Success) ->
                        <- EAP-Success
```

In the case where the EAP MS-CHAP-V2 authentication is unsuccessful, due to a retryable error, the conversation will appear as follows (assuming a maximum of two retries):

```
Peer                    Authenticator
----                    -------------
                        <- EAP-Request/Identity
EAP-Response/
Identity (MyID) ->
                        <- EAP-Request/
                           EAP-Type=EAP MS-CHAP-V2
                           (Challenge)
EAP-Response/
EAP-Type=EAP-MS-CHAP-V2
(Response)->
                        <- EAP-Request/
                           EAP-Type=EAP-MS-CHAP-V2
                          (Failure, R=1)
EAP-Response/
EAP-Type=EAP-MS-CHAP-V2
(Response) ->
                        <- EAP-Request/
                           EAP-Type=EAP-MS-CHAP-V2
                          (Failure, R=1)
```

```
   EAP-Response/
   EAP-Type=EAP-MS-CHAP-V2
   (Response) ->

                         <- EAP-Failure
```

In the case where the EAP MS-CHAP-V2 authentication is unsuccessful, due to a non-retryable error, the conversation will appear as follows (Windows XP SP1):

```
   Peer                  Authenticator
   ----                  -------------
                         <- EAP-Request/Identity
   EAP-Response/
   Identity (MyID) ->
                         <- EAP-Request/
                            EAP-Type=EAP MS-CHAP-V2
                            (Challenge)
   EAP-Response/
   EAP-Type=EAP-MS-CHAP-V2
   (Response)->
                         <- EAP-Failure
```

In the case where the EAP MS-CHAP-V2 authentication is unsuccessful, due to a non-retryable error, and a Failure Request packet is sent, the conversation will appear as follows (behavior not exhibited by Windows XP SP1):

```
   Peer                  Authenticator
   ----                  -------------
                         <- EAP-Request/Identity
   EAP-Response/
   Identity (MyID) ->
                         <- EAP-Request/
                            EAP-Type=EAP MS-CHAP-V2
                            (Challenge)
   EAP-Response/
   EAP-Type=EAP-MS-CHAP-V2
   (Response)->
                         <- EAP-Request/
                            EAP-Type=EAP MS-CHAP-V2
                            (Failure, R=0)
   EAP-Response/
   EAP-Type=EAP-MS-CHAP-V2
   (Failure)->
                         <- EAP-Failure
```

In the case where the EAP MS-CHAP-V2 authentication is initially

unsuccessful due to password expiration, but the subsequent Change Password operation succeeds, the conversation will appear as follows:

```
Peer                    Authenticator
----                    -------------
                        <- EAP-Request/Identity
EAP-Response/
Identity (MyID) ->
                        <- EAP-Request/
                           EAP-Type=EAP MS-CHAP-V2
                           (Challenge)
EAP-Response/
EAP-Type=EAP-MS-CHAP-V2
(Response)->
                        <- EAP-Request/
                           EAP-Type=MS-CHAP-V2
                           (Failure, R=1,
                            Message=ERROR_PASSWD_EXPIRED (E=648))
EAP-Response/
EAP-Type=EAP-MS-CHAP-V2
(Change-Password) ->
                        <- EAP-Request/
                           EAP-Type=MS-CHAP-V2
                           (Success)
EAP-Response/
EAP-Type=EAP-MS-CHAP-V2
(Success) ->
                         <- EAP-Success
```

In the case where the EAP MS-CHAP-V2 authentication is unnsuccessful due to password failure and a successful retry occurs, the conversation appears as follows:

```
Peer                    Authenticator
----                    -------------
                        <- EAP-Request/Identity
EAP-Response/
Identity (MyID) ->
                        <- EAP-Request/
                           EAP-Type=EAP MS-CHAP-V2
                           (Challenge)
EAP-Response/
EAP-Type=EAP-MS-CHAP-V2
(Response)->
                        <- EAP-Request/
                           EAP-Type=MS-CHAP-V2
                          (Failure, R=1,
                           Message=ERROR_AUTHENTICATION_FAILURE (E=691)
```

```
   EAP-Response/
   EAP-Type=EAP-MS-CHAP-V2
   (Response)->
                          <- EAP-Request/
                             EAP-Type=MS-CHAP-V2
                             (Success)
   EAP-Response/
   EAP-Type=EAP-MS-CHAP-V2
   (Success) ->
                          <- EAP-Success
```

Acknowledgments

Thanks to Vivek Kamath, Mark Wodrich and Narendra Gidwani for discussions, comments and text relating to this document.

Authors' Addresses

Vivek Kamath
Ashwin Palekar
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

EMail: {vivek, ashwinp}@microsoft.com
Phone: +1 425 882 8080
Fax: +1 425 936 7329

Full Copyright Statement

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).