1 Terminology

This document frequently uses the following terms:

- authenticator: The end of the communication link requiring the authentication.
- peer: The other end of the communication link; the end which is being authenticated by the authenticator.
- silently discard: This means discarding the packet without further processing.

Also, several words are used to signify the requirements of the specification. These words are often capitalized.

- **MUST**: This word, or the adjective "required", means that the definition is an absolute requirement of the specification.
- **MUST NOT**: This phrase means that the definition is an absolute prohibition of the specification.
- **SHOULD** :This word, or the adjective "recommended", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighed before choosing a different course.
- **MAY**: This word, or the adjective "optional", means that this item is one of an allowed set of alternatives. An implementation which does not include this option **MUST** be prepared to interoperate with another implementation which does include the option.

2 Challenge-Handshake Authentication Protocol

The Challenge-Handshake Authentication Protocol (CHAP) is used to verify the identity of the peer using a 3-way handshake. This is done upon initial request by the peer. These are the steps used to carry on the authentication protocol:

1. The peer sends an authentication request message to the authenticator, specifying the identity the peer wants to authenticate with.
2. The authenticator sends a "challenge" message to the peer.
3. The peer responds with a value calculated using a “one-way hash” function. In our case, we will use the SHA-256 one-way hash function.
4. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged and the connection can go on; otherwise the authentication is not acknowleged and the connection **MUST** be terminated by the authenticator.

Each challenge value **MUST** be unique, since repetition of a challenge value in conjunction with the same secret would permit an attacker to reply with a previously intercepted response. Each challenge value **MUST** also be unpredictable, least an attacker trick a peer into responding to a predicted future challenge, and then use the response to masquerade as that peer to an authenticator.

3 Packet Format

3.1 General packet format

A summary of the CHAP packet format is shown below. The fields are transmitted from left to right. All the values **MUST** be transmitted in network byte order (that is, big endian format: see RFC-1700, section “Data Notations”, and http://en.wikipedia.org/wiki/Endianness#Endianness_in_networking):

Code	Identifier	Length	Data

Where:

- Code: The Code field is one octet long and identifies the type of CHAP packet. CHAP Codes are assigned as follows:
    0. Authentication Request.
    1. Challenge.
    2. Response.
    3. Success.
    4. Failure.
- Identifier: The Identifier field is one octet long and aids in matching authentication requests, challenges, responses and replies.
- Length: The Length field is two octets long and indicates the length of the CHAP packet including the Code, Identifier, Length and Data fields.
- Data: The Data field is zero or more octets long. The format of the Data field is determined by the Code field.

3.2 Authentication Request packet format

The peer wanting to be authenticated **MUST** transmit a CHAP packet with the Code field set to 0 (Authentication Request) to start the authentication protocol with the authenticator.

A summary of the Authentication Request packet format is shown below. The fields are transmitted from left to right.

Code	Identifier	Length	Identity

Where:

- Code is:
    0. for Authentication Request.
- Identifier: The Identifier field is one octet long and **MUST** be the zero value for an authentication request.
- Length: The Length field is two octets long and indicates the length of the CHAP packet including the Code, Identifier, Length and Identity fields.
- Identity: The Identity field is one or more octets long, and it contains the identity the peer wants to authenticate with. It is intended to be human readable and it is recommended that the Identity contain displayable ASCII characters from 32 to 126 decimal. The size is determined from the Length field.

3.3 Challenge and Response packet format

When receiving an Authentication Request packet the authenticator **MUST** transmit a CHAP packet with the Code field set to 1 (Challenge).

If the peer receives a Challenge packet after it has sent an Authentication Request packet, the peer **MUST** transmit a CHAP packet with the Code field set to 2 (Response). If the peer has not sent an Authentication Request packet yet, it **MUST** ignore the Challenge packet.

If the authenticator receives a Response packet after it has sent a Challenge packet, the authenticator compares the Response Value with its own calculation of the expected value. Based on this comparison, the authenticator **MUST** send a Success or Failure packet (described below). If the authenticator has not sent a Challenge packet yet, or if the Identifier value in the Response packet does not match the Identifier value it has sent in the Challenge packet, it **MUST** ingnore the Response packet.

A summary of the Challenge and Response packet format is shown below. The fields are transmitted from left to right.

Code	Identifier	Length	Value-Size	Value	Name

Where:

- Code is:
    1. for Challenge.
    2. for Response.
- Identifier: The Identifier field is one octet long. The Identifier field **MUST** be changed each time a Challenge is sent. The Response Identifier **MUST** be copied from the Identifier field of the Challenge which caused the Response.
- Length: The Length field is two octets long and indicates the length of the CHAP packet including the Code, Identifier, Length, Value-Size, Value and Name fields.
- Value-Size: This field is one octet long and indicates the length of the Value field.
- Value: The Value field is one or more octets long. The most significant octet is transmitted first.

  The Challenge Value is a variable stream of octets. The importance of the uniqueness of the Challenge Value and its relationship to the secret is described above. The Challenge Value **MUST** be changed each time a Challenge is sent. The length of the Challenge Value depends upon the method used to generate the octets, and is independent of the hashing algorithm used.

  The Response Value is the one-way hash calculated over a stream of octets consisting of the Identifier, followed by (concatenated with) the "secret", followed by (concatenated with) the Challenge Value. The length of the Response Value depends upon the hash algorithm used (32 octets for SHA-256).
- Name: The Name field is one or more octets long representing the identification of the system transmitting the packet (either the authenticator or the peer). There are no limitations on the content of this field. For example, it **MAY** contain ASCII character strings or globally unique identifiers in ASN.1 syntax. The size is determined from the Length field.

3.3.1 Success and Failure

If the Value received in a Response is equal to the expected value, then the implementation **MUST** transmit a CHAP packet with the Code field set to 3 (Success).

If the Value received in a Response is not equal to the expected value, then the implementation **MUST** transmit a CHAP packet with the Code field set to 4 (Failure), and **SHOULD** take action to terminate the communication link.

A summary of the Success and Failure packet format is shown below. The fields are transmitted from left to right.

Code	Identifier	Length	Message

Where:

- Code is:
    3. for Success.
    4. for Failure.
- Identifier: The Identifier field is one octet long and aids in matching requests and replies. The Identifier field **MUST** be copied from the Identifier field of the Response which caused this reply.
- Length: The Length field is two octets long and indicates the length of the CHAP packet including the Code, Identifier, Length and Message fields.
- Message: The Message field is zero or more octets long, and its contents are implementation dependent. It is intended to be human readable, and **MUST NOT** affect operation of the protocol. It is recommended that the message contain displayable ASCII characters from 32 to 126 decimal. The size is determined from the Length field.