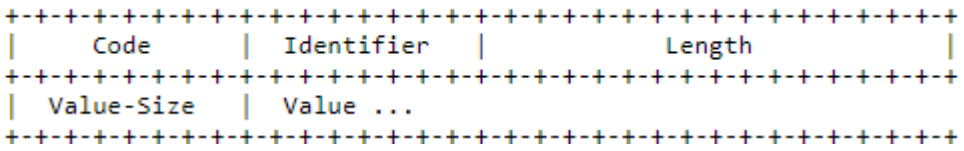
Отчёт по лабораторной работе “CHAP”.

Реализация протокола.

Согласно описанию протокола “CHAP”- широко поддерживаемый метод аутентификации, в котором используется передача косвенных сведений о пароле, вместо передачи его самого.

Формат пакета:



Для того, чтобы осуществить аутентификацию на стороне сервера и клиента должен быть установлен общий secret. При этом сервер через определенные промежутки времени просит пользователя пройти аутентификацию ещё раз.

Дадим некоторые пояснения.

Code: 1 - для challenge, 2 - ответ на challenge, 3 - успех аутентификации, 4 - неудача. Length - длина всего сообщения, Value-Size - длина Value, Value - значение challenge или хэша, вычисленного на стороне клиента.

Этапы аутентификации:

1. Клиент отправляет любое сообщение на сервер;
2. Сервер вычисляет случайную строку (Value) и идентификатор пользователя (Identifier) и отправляет на клиент сообщение следующего вида: 1|Identifier|Length|Value-Size|Value;
3. После этого клиент конкатенирует Identifier,secret,Value и вычисляет хэш md5 от этого значения, отправляет на сервер: 2|Identifier|Length|Value-Size|Value, где Value - хэш md5
4. Сервер сравнивает значение полученное от клиента, с вычисленным на своей стороне, если они равны, то сервер отправляет клиенту: 3|Identifier|Length и разрешает соединение, если нет то: 4|Identifier|Length и прекращает соединение.
5. После некоторого промежутка времени сервер повторно отправляет challenge (возвращается на пункт 2).