|  |
| --- |
| *Министерство образование и науки*  *Российской федерации*  Федеральное агентство по образованию  Курганский государственный университет |
| Кафедра «Безопасность информационных и автоматизированных систем» |
| Лабораторная работа № 11:  **«WAN: Настройка HDLC, PPP. Протоколы аутентификации PPP (PAP, CHAP).»** |
| Выполнил \_\_\_\_ Бутенко А.Ю.  Принял \_\_\_\_\_\_ Дубровских В.А. |
|  |
| Курган 2016 |

Цель работы:

* ознакомиться с принципами работы HDLC, PPP.
* Ознакомиться с протоколами аутентификации PAP, CHAP.

**Ход работы:**

**Топология сети**

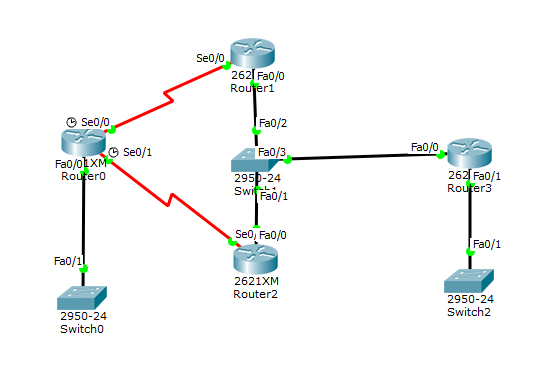


Рисунок 1 – Топология сети

Скорость канала определяется устройством, которое выступает в роли [DCE](http://ciscotips.ru/dce-term) (Data Communication Equipment) – то есть тем самым провайдерским устройством. Нам достаточно подключить к нему маршрутизатор, который, в данном случае выступает в роли [DTE](http://ciscotips.ru/dte-term)(Data Terminal Equipment) и про скорость канала узнаёт от DCE. На маршрутизаторе надо прописать нужную инкапсуляцию, настроить ip адрес на интерфейсе и включить.

**PAP и CHAP** – протоколы аутентификации, использующиеся в протоколе PPP. PAP расшифровывается банально – Password Authentication Protocol. Возможно такая простая расшифровка связана с тем, что протокол был одним из первых. CHAP расшифровывается как Challenge Handshake Authentication Protocol. В курсе CCNA затрагиваются оба этих протокола.

**Как работает PAP?**

Клиент хочет подключиться к серверу, он отправляет серверу пароль, сервер отвечает либо «Да», либо «Нет». Казалось бы, всё просто – зачем добавлять что-то ещё? Однако, всё становится сложнее, в случае если мы в силу каких-то обстоятельств обратились не к серверу, к, которому собирались, а к устройству злоумышленника. В этом случае получается, что спрашивая его, нравится ли ему наш пароль, мы по сути просто передаём ему пароль, с которым он в дальнейшем может делать всё что угодно. Чтобы избежать такой ситуации был придуман CHAP.

**Как работает CHAP?**

Клиент хочет обратиться к серверу, сервер передаёт клиенту случайную строку, клиент берёт пароль и эту строку и вычисляет от неё MD5 хеш, который возвращает серверу. Сервер проделывает те же операции (если он сам, конечно, знает правильный пароль). Если хеши слвпадают – клиент авторизован. Что мы получаем? Если клиент не знает пароль – хеши не совпадут, если вместо сервера злоумышленник – он получит только хеш, из которого ничего не выудить.

Таким образом, в реальных ситуациях лучше использовать протокол CHAP.

**Вывод:** В ходе проделанной работы, я разобрался в принципах работы протоколов HDLC и PPP. Научился конфигурировать сети на основе полученных знаний.