**Лабораторная работа 8**

Сетевая безопасность

**Задача:**

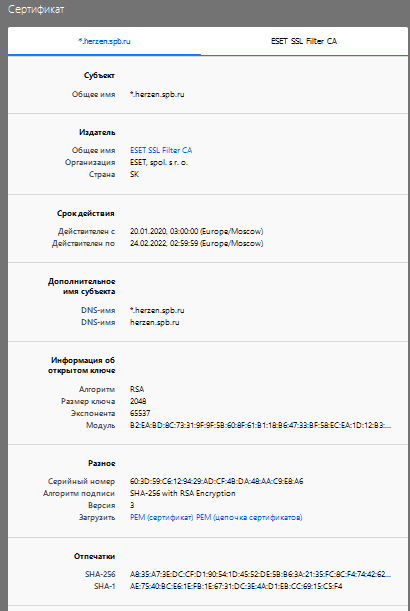
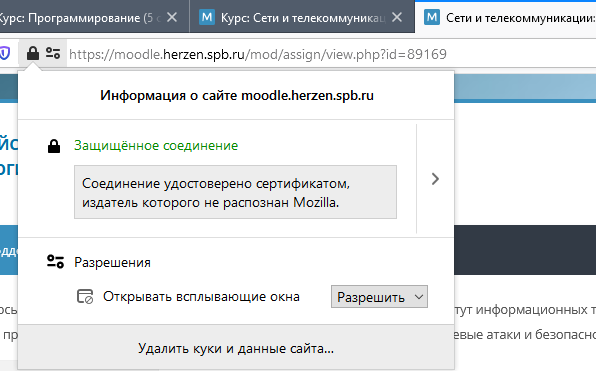
Продемонстрировать и объяснить поля цифрового сертификата на SSL-соединении. Продемонстрировать отправку сообщения по электронной почте через telnet. Настроить сетевую трансляцию адресов (SNAT) для общего доступа в интернет

**Оборудование:**

браузер Mozilla Firefox, Mailtrap, Cisco packet tracer.

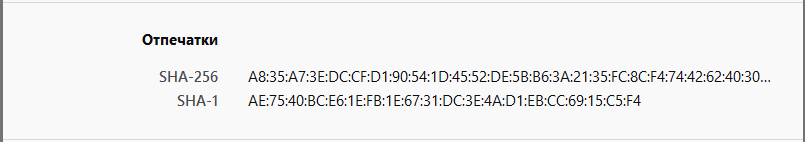
**Ход выполнения работы:**

1. Сейчас везде используется TLS - открытое расширение SSL. Для исследования сертификата в Mozilla Firefox нужно обратиться к серверу, утверждающему, что он - подлинный и работает по протоколу TLS. Браузер отправляет запрос на установление TLS-соединения, посылая поддерживаемые методы шифрования.



Информация о SSL-сертификате в Mozilla Firefox

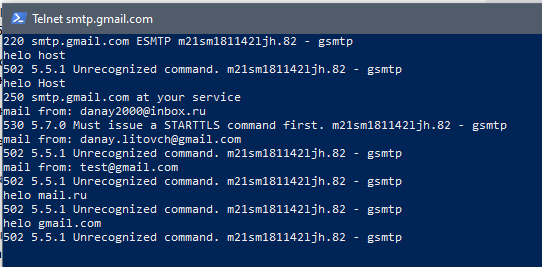
В ответ браузер посылает свой сертификат, “промежуточный” сертификат, выданный одной из корневых служб и открытый ключ



Публичный ключ

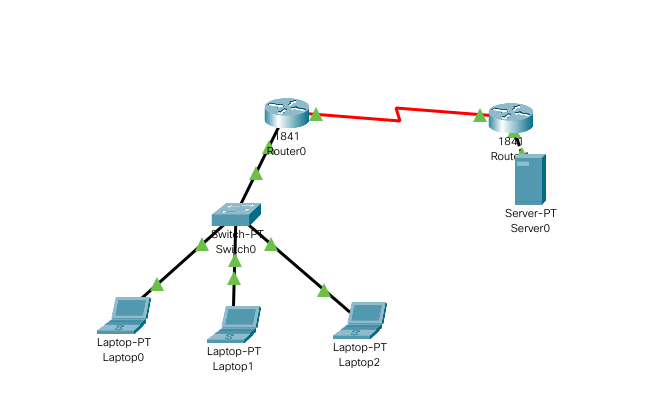
Далее, используя подписи сертификатов, браузер проверяет их подлинность, генерирует pre-master password, шифрует его, используя публичный ключ и посылает серверу. Этот ключ восстанавливается с помощью закрытого ключа на стороне сервера и на его основе генерируется ключ для симметричного шифрования.

1. Для отлавливания письма, отправленного через протокол SMTP используется сервис gmail.



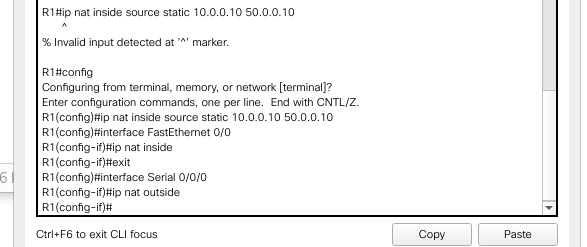
Так как gmail защищен, как и остальные почтовые сервисы, отправка письма через telnet не увенчалась успехом.

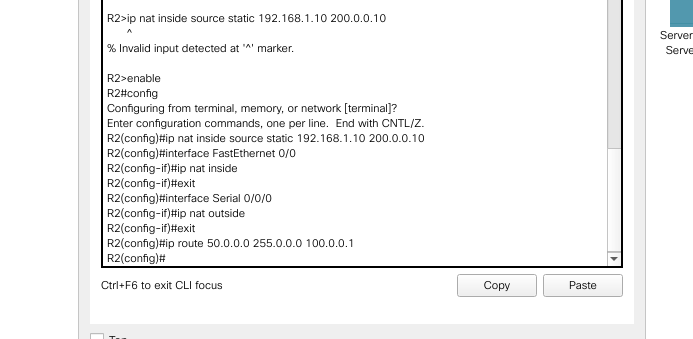
1. Для демонстрации работы NAT (статического) собрана следующая схема



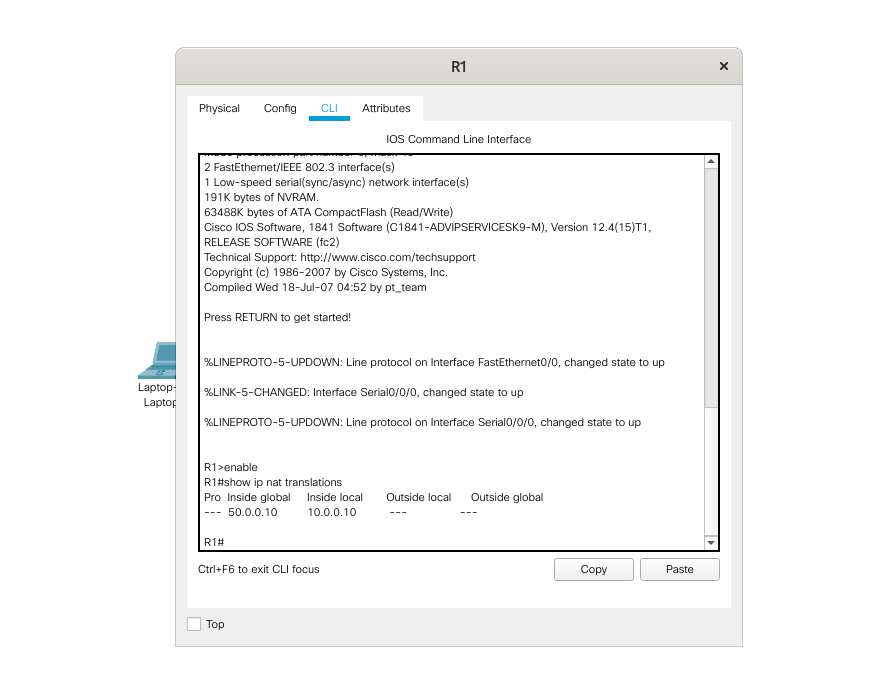
|  |  |  |
| --- | --- | --- |
| Устройство | Адрес/маска | Интерфейс |
| Laotop0 | 10.0.0.10/8 | Fa0/0 of R0 |
| Laptop1 | 10.0.0.20/8 | Fa0/0 of R0 |
| Laptop2 | 10.0.0.30/8 | Fa0/0 of R0 |
| Server0 | 192.168.1.10/24 | Fa0/0 of R1 |
| Serial 0/0/0 of R1 | 100.0.0.1/8 | Serial 0/0/0 of R2 |
| Serial 0/0/0 of R2 | 100.0.0.2/8 | Serial 0/0/0 of R2 |

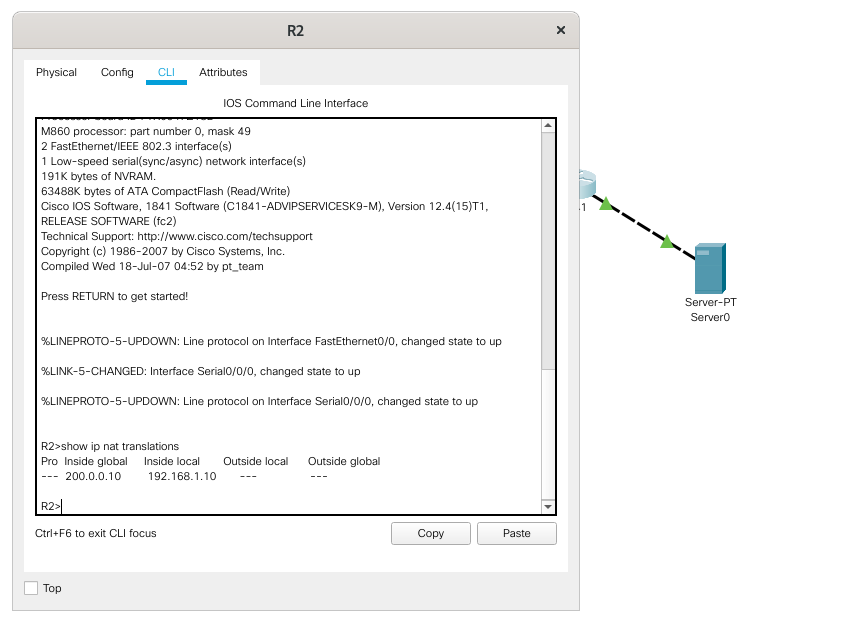
Настройка роутеров



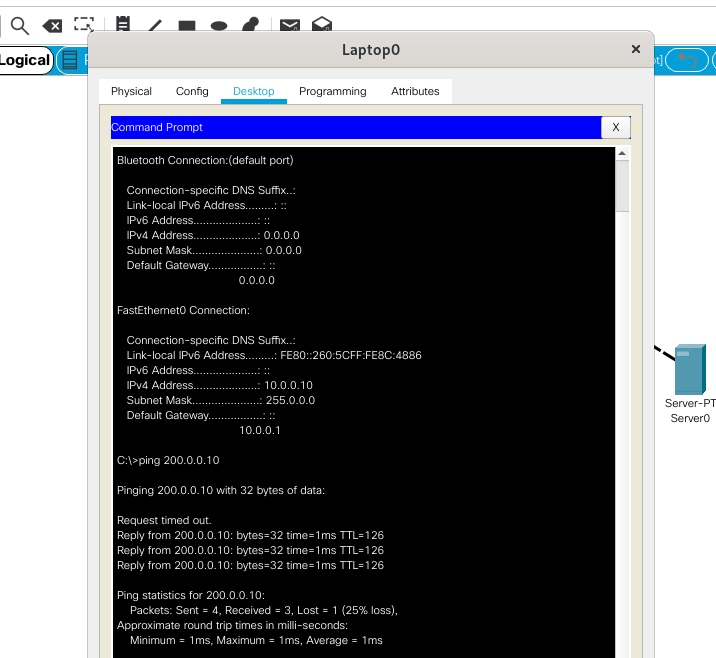


Таблицы NAT





Проверка работы



**Выводы:**

При выполнении данной лабораторной работы был изучен протокол SSL(TSL), были продемонстрированы и объяснены поля сертификата SSL. Был изучен протокол SMTP и утилита Telnet. Был изучен метод NAT (со статически задаваемой таблицей).