**Лабораторная работа №3**

**Удаленный доступ по протоколу SSH к оборудованию Cisco**

**Что такое SSH?**

В настоящее время для получения удаленного доступа к сетевому оборудованию часто используют протокол **SSH**. И это не случайно, ведь данный протокол имеет важное преимущество, которое заключается в его способности шифровать весь трафик и передаваемые пароли. Перед тем, как приступить к настройке оборудования, кратко рассмотрим принципы работы SSH.

**SSH (Secure Shell)** — сетевой протокол, позволяющий производить удаленное управление сетевым оборудованием и туннелировать TCP-соединения. Для своей работы SSH использует 22 порт.

Перед тем, как установить соединение происходит аутентификация.

**Аутентификация** — это процедура установления подлинности. При аутентификации предварительно генерируется пара открытого и закрытого ключа для определенного пользователя. Оба файла хранятся как на удаленной машине, так и на машине, к которой производится подключение.

Эти файлы не передаются при аутентификации, система лишь проверяет, что пользователь открытого ключа также владеет и закрытым.

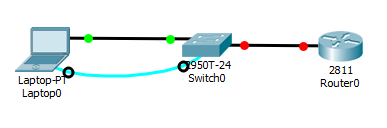
Открытый ключ используется для проверки электронной цифровой подписи и шифрования сообщений.

Закрытый ключ используется для генерации электронной цифровой подписи и расшифрования сообщений. Электронная цифровая подпись позволяет проверить отсутствие искажений информации, а также подтвердить владельца сертификата.

Для шифрования данных и создания ЭЦП используется криптографический алгоритм RSA. Работа RSA основывается на вычислительной сложности задачи факторизации больших целых чисел.

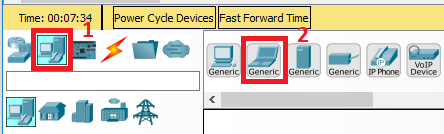
**Создание схемы сети в Packet Tracer**

1. Открываем Packet Tracer и создаем вот такую схему сети (Рис. 1), которая состоит из:
2. Ноутбука **Laptop-PT**
3. Коммутатора (Switch) **2950T**
4. Маршрутизатора (Router) **2811**
5. Консольного (**голубой**) и двух Ethernet проводов (**черный**)



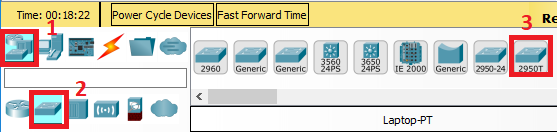
**Рис. 1.** Схема сети

1. Для этого, в нижней части Packet Tracer находим панель с оборудованием, именно через нее добавляются все устройства для эмулирования. Выбираем **End Devices,** в правой части находим ноутбук и перетаскиваем его на рабочую поверхность (Рис. 2).



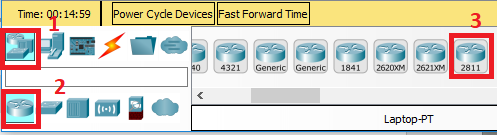
**Рис. 2.** Добавление ноутбука

1. Теперь добавим коммутатор. Жмем на иконку **Network Devices**, ниже выбираем **Switches**, находим коммутатор **2950T** и перетаскиваем его (Рис. 3).



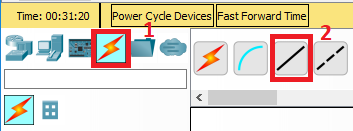
**Рис. 3.** Добавление коммутатора

1. Далее жмем на иконку на иконку **Routers**, находим роутер **2811** и так же перетаскиваем его (Рис. 4).



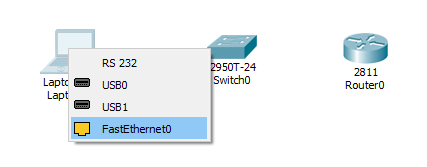
**Рис. 4.** Добавление ноутбука

1. Соединим наши устройства при помощи кабелей. Находим значок молнии **Connections** и кликаем на черную витую пару **Copper Straight-Through** (Рис. 5).

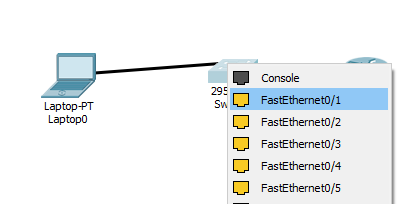


**Рис. 5**. Добавление, витой пары

1. Затем кликаем на ноутбук и выбираем порт **FastEthernet0** (Рис. 6), ведем мышку к коммутатору (провод будет тянуться за вашим курсором), нажимаем на него и выбираем порт **FastEthernet0/1** (Рис. 7).



**Рис. 6.** Подключение витой пары к ноутбуку

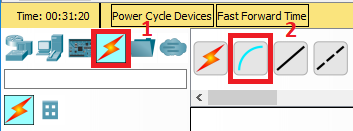


**Рис. 7.** Подключение витой пары к коммутатору

Таким образом вы физически объединили ноутбук и коммутатор в сеть при помощи медного провода.

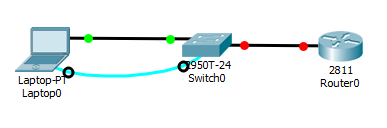
1. Аналогичным способом соедините порт коммутатора **FastEthernet0/2** с портом маршрутизатора **FastEthernet0/0.**
2. Для того чтобы настроить коммутатор, необходимо воспользоваться его консольным портом и подключить его к ноутбуку.

Выбираем **голубой** консольный кабель (Рис. 8), на ноутбуке подключаем его в разъем **RS232,** а на коммутаторе выбираем консольный интерфейс **Console.**



**Рис. 8.** Добавление консольного кабеля

У нас получилась вот такая схема (Рис. 9):



**Рис. 9.** Схема подключения

**Настройка IP адреса ноутбука**

1. Задайте адреса для ноутбука:

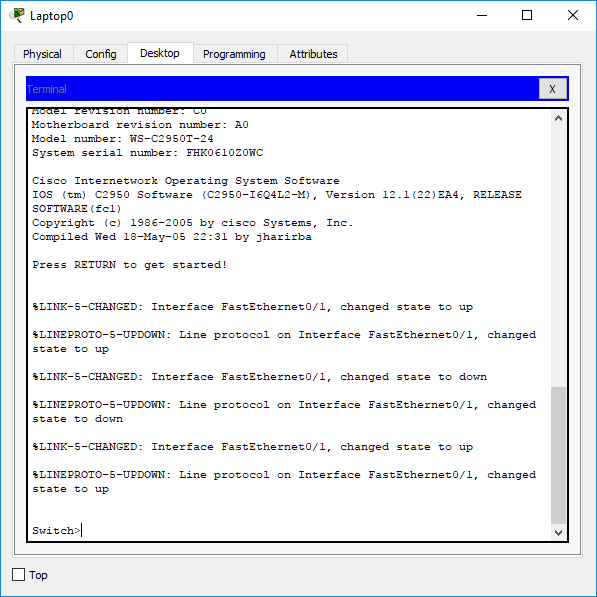
* IP адрес **192.168.0.5**
* Маска подсети (Subnet Mask) **255.255.255.0**
* Шлюз по-умолчанию (Default Gateway) **192.168.0.1**

В предыдущей лабораторной работе вы уже задавали адреса для компьютера. Если забыли, открываем работу 2.3.2.5 и смотрим.

Шлюз по-умолчанию это и есть адрес маршрутизатора, который мы настроим далее.

**Настройка коммутатора через терминал ноутбука**

1. Два раза кликаем по ноутбуку, выбираем вкладку **Desktop**, нажимаем на иконку **Terminal**, соглашаемся со стандартными параметрами и жмем **Ок** и попав на белый экран терминала жмем клавишу **Enter**. Мы подключились к командной строке операционной системы IOS нашего коммутатора (Рис. 1).



**Рис. 1.** Терминал коммутатора

1. В данный момент мы находимся в **пользовательском** режиме (обратите внимание на символ **>** ). **Перейдем в привилегированный режим**, для этого вводим команду:

**enable**

1. Далее перейдем в **режим конфигурации** командой:

**config terminal**

1. Для доступа к коммутатору по SSH нам необходимо настроить виртуальный интерфейс vlan. Переходим в режим настройки интерфейса:

**interface vlan 1**

Задаем IP адрес и маску подсети:

**ip address 192.168.0.100 255.255.255.0**

Включаем интерфейс:

**no shutdown**

Выходим из режима конфигурации vlan интерфейса:

**exit**

Задаем шлюз по умолчанию:

**ip default-gateway 192.168.0.1**

1. В пункте 4 мы настроили виртуальный интерфейс коммутатора, теперь необходимо сконфигурировать его физический порт. Переходим в настройку физического интерфейса fastEthernet 0/1:

**interface fastEthernet 0/1**

Добавим описание для этого интерфейса о том, что это порт для администратора:

**description admin**

Переведем порт в режим доступа:

**switch mode access**

Связываем физический порт с виртуальным:

**switch access vlan 1**

Выходим:

**exit**

1. Теперь все готово для настройки SSH. Добавим нового пользователя **user** c паролем **pass** для удаленного доступа:

**username user secret pass**

Защищаем привилегированный режим паролем pass:

**enable secret pass**

Переходим в настройки виртуальной линии:

**line vty 0 4**

Добавляем авторизацию по имени и паролю из локальной базы коммутатора:

**login local**

Разрешаем доступ только по SSH:

**transport input ssh**

Добавляем настройку при бездеятельности и отключении ее через 60 секунд:

**exec-timeout 0 60**

Убираем всплывающие уведомления:

**logging synchronous**

Выходим:

**exit**

Устанавливаем последнюю версию SSH:

**ip ssh version 2**

Указываем доменное имя:

**ip domain-name Switch1**

Переименовываем коммутатор:

**hostname Sw**

Генерируем SSH ключи (на вопрос о количестве бит вводим цифру 1024):

**crypto key generate rsa**

Разрешим коммутатору пропускал vlan 1 через свой порт fastEthernet 0/2, к которому подключен маршрутизатор:

**interface fastEthernet 0/2**

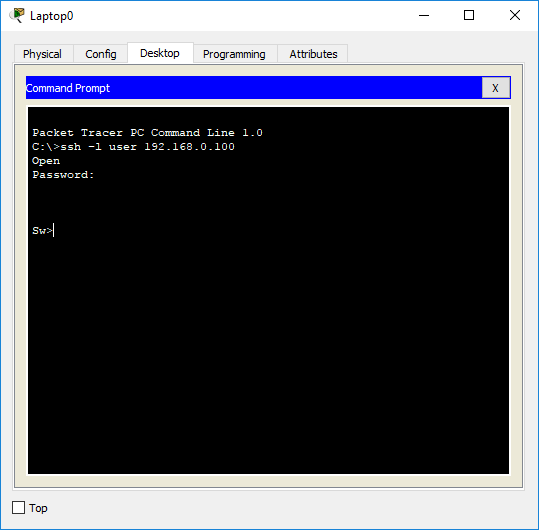
**switchport mode trunk**

**switchport trunk allowed vlan 1**

**exit**

1. Проверим удаленное подключение. Убираем консольный провод от ноутбука к коммутатору. Для этого нажимаем на красный крест (**х**) в правой панели инструментов Packet Tracer и кликаем по голубому проводу.

Заходим в ноутбук, переходим во вкладку Desktop, кликаем на иконку Command Prompt и вводим команду **ssh –l user 192.168.0.100**, (**l - это маленькая буква L**) пароль pass (Рис. 2):



**Рис. 2**. Проверка SSH доступа

1. Если появилась строчка приветствия коммутатора **Sw>**, то все настроено верно. Теперь у нас есть удаленный доступ до коммутатора и консольный провод нам больше не нужен.

**Настройка маршрутизатора через терминал ноутбука**

1. Теперь настроим маршрутизатор. Соединяем ноутбук голубым консольным кабелем к маршрутизатору и подключаемся к нему через терминал лэптопа. Терминал задаст вопрос о запуске мастера настроек маршрутизатора. Вписываем слово **no** и нажимаем **Enter**.
2. Проведем первоначальную настройку маршрутизатора:

**enable**

**config terminal**

**hostname Rt**

**interface fastEthernet 0/0**

**description Swith**

**no shutdown**

**exit**

Создаем виртуальный сабинтерфейс:

**interface fastEthernet 0/0.2**

Тегируем vlan 1. Это означает что все кадры, которые попадают на интерфейс fastEthernet 0/0 с тегом vlan 1 будут отправляться на сабинтерфейс fastEthernet 0/0.2:

**encapsulation dot1Q 1**

Задаем IP адрес (это и есть шлюз по умолчанию для коммутатора и ноутбука) и маску подсети маршрутизатору:

**ip address 192.168.0.1 255.255.255.0**

**exit**

1. Настроим SSH на маршрутизаторе. Все аналогично тому, что было на коммутаторе.

Вводим нового пользователя и пароль:

**username user secret pass**

Защищаем привилегированный режим:

**enable secret pass**

Переходим в настройки виртуальной линии:

**line vty 0 4**

Добавляем авторизацию по имени и паролю:

**login local**

Разрешаем доступ только по SSH:

**transport input ssh**

Добавляем отключение при бездеятельности через 60 секунд:

**exec-timeout 0 60**

Убираем всплывающие сообщения:

**logging synchronous**

**exit**

Ставим последнюю версию SSH:

**ip ssh version 2**

Указываем доменное имя:

**ip domain-name Router1**

Генерируем SSH ключи (вводим 1024):

**crypto key generate rsa**

1. Проверим удаленное подключение. Убираем консольный провод от ноутбука к маршрутизатору.

Заходим в ноутбук, переходим во вкладку Desktop, кликаем на иконку Command Prompt и вводим команду **ssh –l user 192.168.0.1**, пароль pass. Если видим приветствие от маршрутизатора **Rt>** значит SSH доступ настроен верно.