**Лабораторная работа 11.**

**Работа с протоколом SSH в Cisco Packet Tracer**

**Цель работы:** научиться работать с протоколом SSH в Cisco Packet Tracer

**Теоретическая часть**

SSH — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений.

Схож по функциональности с протоколами Telnet и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли.

SSH позволяет безопасно передавать в незащищённой среде практически любой другой сетевой протокол. Таким образом, можно не только удалённо работать на компьютере через командную оболочку, но и передавать по шифрованному каналу звуковой поток или видео (например, с веб-камеры). Также SSH может использовать сжатие передаваемых данных для последующего их шифрования.

SSH предоставляет все те функциональные возможности, которые представлялись в Telnet, с добавлением эффектного кодирования с целью предотвращения перехвата таких данных, как логины и пароли. Введенная в протоколе SSH система аутентификации с использованием публичного ключа гарантирует, что удаленный компьютер действительно является тем, за кого себя выдает.

Главной функцией протоколов TELNET и SSH является предоставление возможности входа в удаленную систему. Эта функция предоставляет практически неограниченные возможности использования этих протоколов:

- Они могут использоваться системными администраторами для удаленной настройки компьютеров некоторой сети, что позволит им выполнять свои непосредственные обязанности, не вставая со своего рабочего места.

- Они могут использоваться для настройки различного рода сетевых служб, таких как сервер исходящей почты SMTP или сервер доменных имен DNS.

- Они могут использоваться для обмена файлами между компьютерами подключенными, например через модем.

- Они могут предложить пользователю возможность общения с сетевыми сервисами «вручную», что иногда бывает полезно для системных администраторов для отправки различных команд сетевым службам и последующего анализа полученных ответов.

SSH — это протокол прикладного уровня.

SSH-сервер обычно прослушивает соединения на TCP-порту 22. Спецификация протокола SSH-2 содержится в RFC 4251.

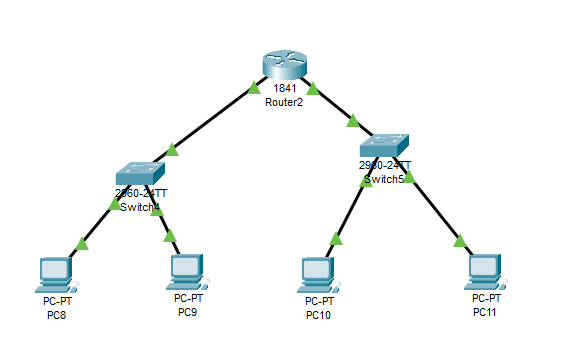
Для аутентификации сервера в SSH используется протокол аутентификации сторон на основе алгоритмов электронно-цифровой подписи RSA или DSA, но допускается также аутентификация при помощи пароля (режим обратной совместимости с Telnet) и даже IP-адреса хоста (режим обратной совместимости с rlogin).

В 1996 году была разработана более безопасная версия протокола, SSH-2, несовместимая с SSH-1. Протокол приобрел ещё большую популярность, и к 2000 году у него было около двух миллионов пользователей.

В настоящее время под термином SSH обычно подразумевается именно SSH-2, так как первая версия протокола ввиду существенных недостатков сейчас практически не применяется.

Спроектируем и настроим сеть.

Используем 4 компьютера, 2 коммутатора и маршрутизатор.



Настройки аналогичные лабораторной работе 10.

Присвоим IP-адреса компьютерам:

PC8 – 192.168.12.10/24

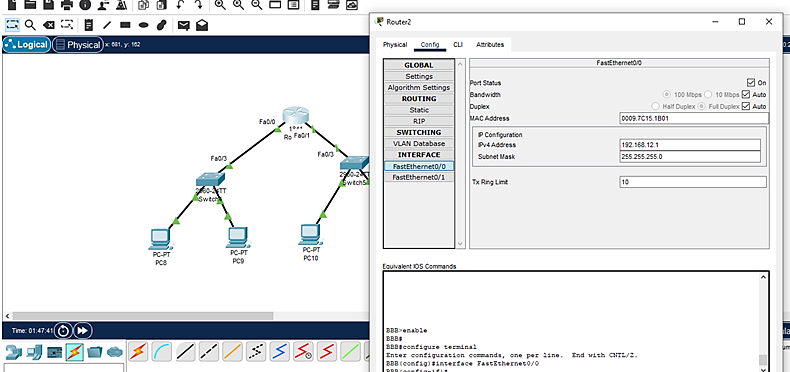
PC9 – 192.168.12.11/24

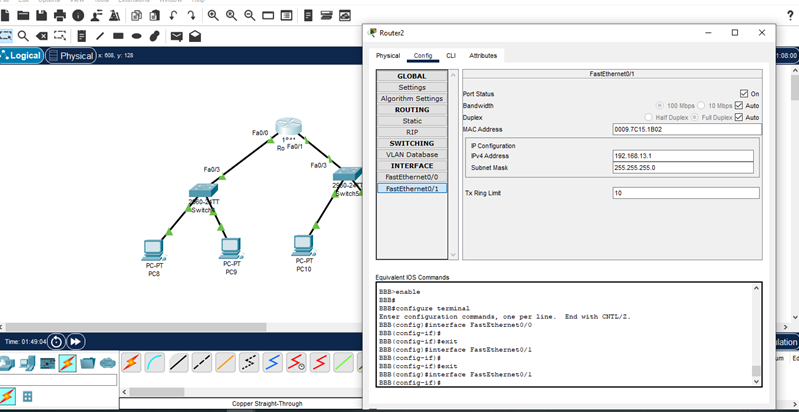
PC10 – 192.168.13.10/24

PC3 – 192.168.13.11/24

Необходимо пропинговать компьютеры между собой.

Настройка роутера:





Необходимо пропинговать сети до роутера.

Добавить в конфигурацию компьютеров адрес шлюзов:

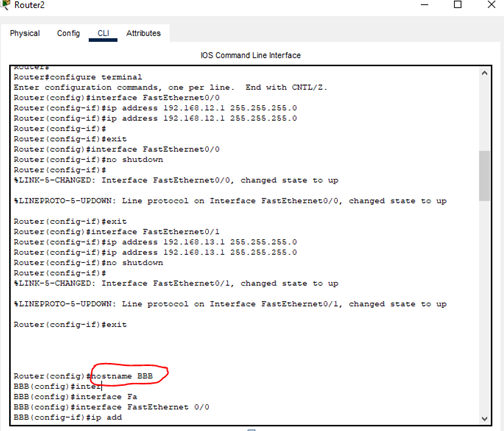
Для PC8 и PC9 - 192.168.12.1

Для PC10 и PC11 - 192.168.13.1

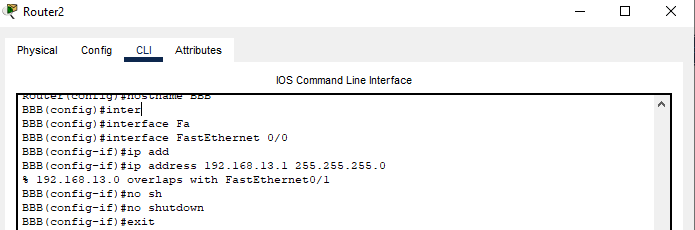
Пропинговать все компьютеры между собой.

Настроим протокол SSH.

На роутере войти в привилегированный режим. Войти в режим конфигурации. Настроить имя маршрутизатора (ВВВ – можно любое).



Можно и так провести настройку физического интерфейса роутера FastEthernet 0/1. Настроить IP адрес и маску сети и включить интерфейс.

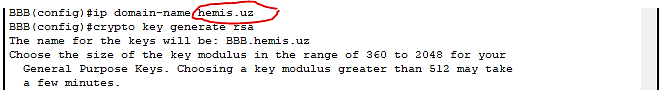


Выйти из режима настройки интерфейса.

Настроить имя домена (может быть любым) и сгенерировать ключ для SSH. Ключ представляет собой объект, который фактически используется для шифрования и расшифровки данных. (Примечание, RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел).

***ip domain-name hemis.uz***

***crypto key generate rsa***



Требуется выбрать длину ключа. Ключ можно настроить в диапазоне от 512 до 2048 бит. Чем он больше, тем выше уровень безопасности ключа, но тем больше времени занимает шифрование и расшифровка данных. Минимальная рекомендуемая длина — 1024 бит.



Создать локальную запись имени пользователя базы данных (создать по своему имени).

***username hemis password пароль***



Создали пользователя (marina) в локальной базе маршрутизатора.

Войти в режим настройки терминальных линий:

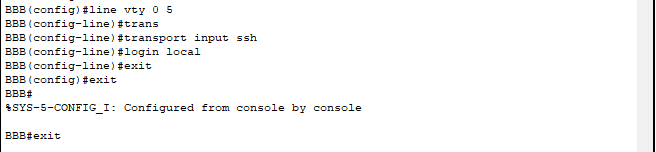
***line vty 0 15***

Указать протокола SSH для подключения к линиям:

***transport input ssh***

Разрешить использование входящих сеансов SSH для VTY. Указать использовать локальную базу для аутентификации пользователей по SSH:

***login local***



Доступ к службе протокола SSH на маршрутизаторе теперь можно осуществлять посредством программного обеспечения клиента SSH.

Конфигурация маршрутизатора (BBB) завершена. Теперь можно подключиться к маршрутизатору удаленно при помощи протокола SSH используя имя пользователя (hemis) и пароль (marina).

Если настройка произведена правильно, то можно подключиться к маршрутизатору (ВВВ) по протоколу SSH.

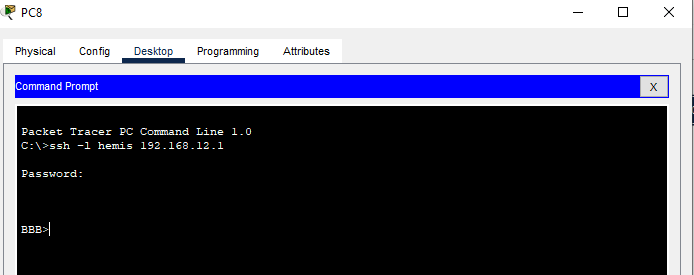
Это базовая настройка устройства, которая позволяет получить к нему доступ удаленно через сеть.

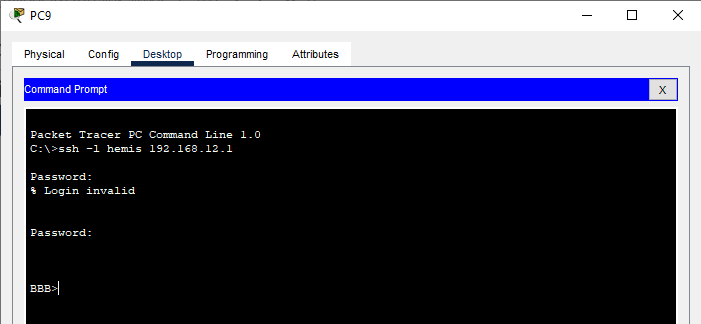
Протокол SSH является стандартным протоколом доступа к сетевым устройствам всевозможных производителей в виду своей защищенности.

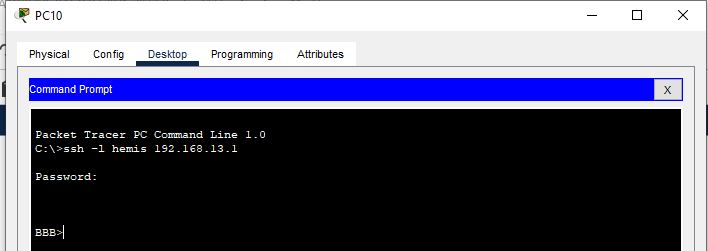
*Проверка подключения к SSH*

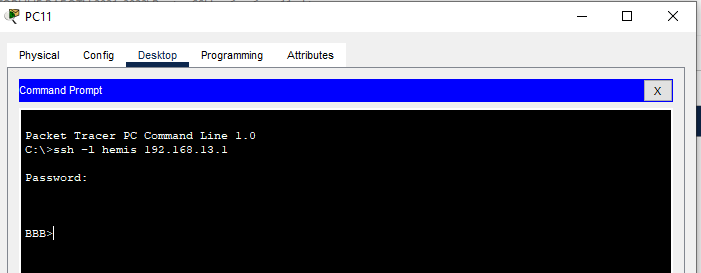
Самый простой способ проверить работоспособность конфигурации, не используя дополнительное оборудование, — подключиться с устройства на свой IP адрес.

Проверим доступ по SSH к маршрутизатору BBB с компьютеров сети.









**Задание на лабораторную работу:**

1. Настроить протокол SSH в Cisco Packet Tracer. Имя маршрутизатора и имя пользователя настроить по своему имени и фамилии. Имя домена должно быть индивидуальным. Скриншоты всех действий поместить в отчет.
2. Ответить письменно на контрольные вопросы к лекциям 21 и 22.