Лабораторная работа № 2

Предварительная настройка оборудования Cisco

Абд эль хай Мохамад

Содержание

# 1 Цель работы

Получить основные навыки по начальному конфигурированию оборудования Cisco.

# 2 Задание

1. Сделать предварительную настройку маршрутизатора:

* задать имя в виде «город-территория-учётная\_записьтип\_оборудования-номер» (см. пункт 2.5), например msk-donskaya-osbender-gw-1;
* задать интерфейсу Fast Ethernet с номером 0 ip-адрес 192.168.1.254 и маску 255.255.255.0, затем поднять интерфейс;
* задать пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном);
* настроить доступ к оборудованию сначала через telnet, затем — через ssh (используя в качестве имени домена donskaya.rudn.edu);
* сохранить и экспортировать конфигурацию в отдельный файл.

1. Сделать предварительную настройку коммутатора:

* задать имя в виде «город-территория-учётная\_запись-тип\_оборудования-номер» (см. пункт 2.5), например msk-donskaya-osbender-sw-1;
* задать интерфейсу vlan 2 ip-адрес 192.168.2.1 и маску 255.255.255.0, затем поднять интерфейс;
* привязать интерфейс Fast Ethernet с номером 1 к vlan 2;
* задать в качестве адреса шлюза по умолчанию адрес 192.168.2.254;
* задать пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном);
* настроить доступ к оборудованию сначала через telnet, затем — через ssh (используя в качестве имени домена donskaya.rudn.edu);
* для пользователя admin задать доступ 1-го уровня по паролю;
* сохранить и экспортировать конфигурацию в отдельный файл.

# 3 Выполнение лабораторной работы

В логическом рабочем пространстве Packet Tracer я разместил коммутатор, маршрутизатор и 2 конечных точки ПК, подключил один ПК к маршрутизатору, другой ПК к коммутатору.

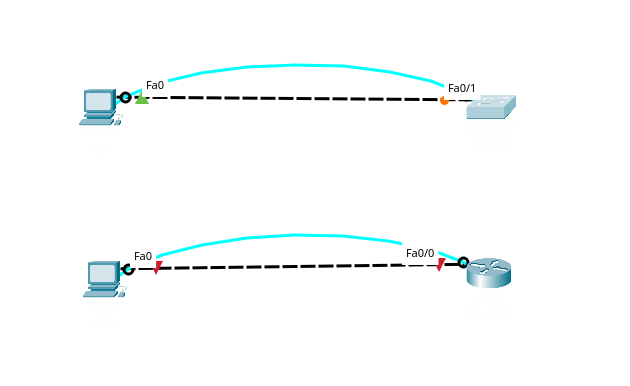


Рис. 1: Схема подключения оборудования для проведения его предварительной настройки

## 3.1 Конфигурация маршрутизатора

Установка имени хоста Команда: имя хоста msk-donnaya-gw-1 Эта команда устанавливает имя хоста маршрутизатора «msk-obruchevsky-gw-1».

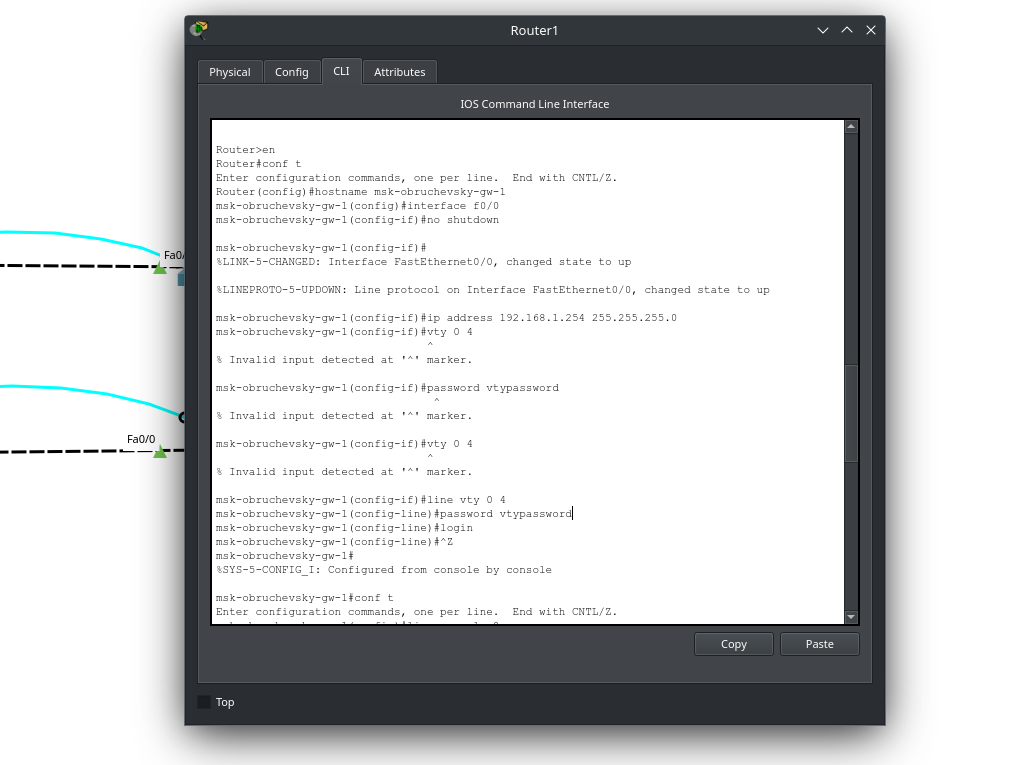


Рис. 2: router

Настройка интерфейса f0/0 Команды: interface f0/0 no shutdown ip address 192.168.1.254 255.255.255.0 Эти команды включают интерфейс f0/0 и назначают этому интерфейсу IP-адрес 192.168.1.254 с маской подсети 255.255.255.0.

Эти команды устанавливают пароли для виртуального терминала (VTY) и линий консоли, включают секрет для привилегированного режима, шифруют пароли и создают пользователя «admin» с уровнем привилегий 1 и паролем «adminpassword».

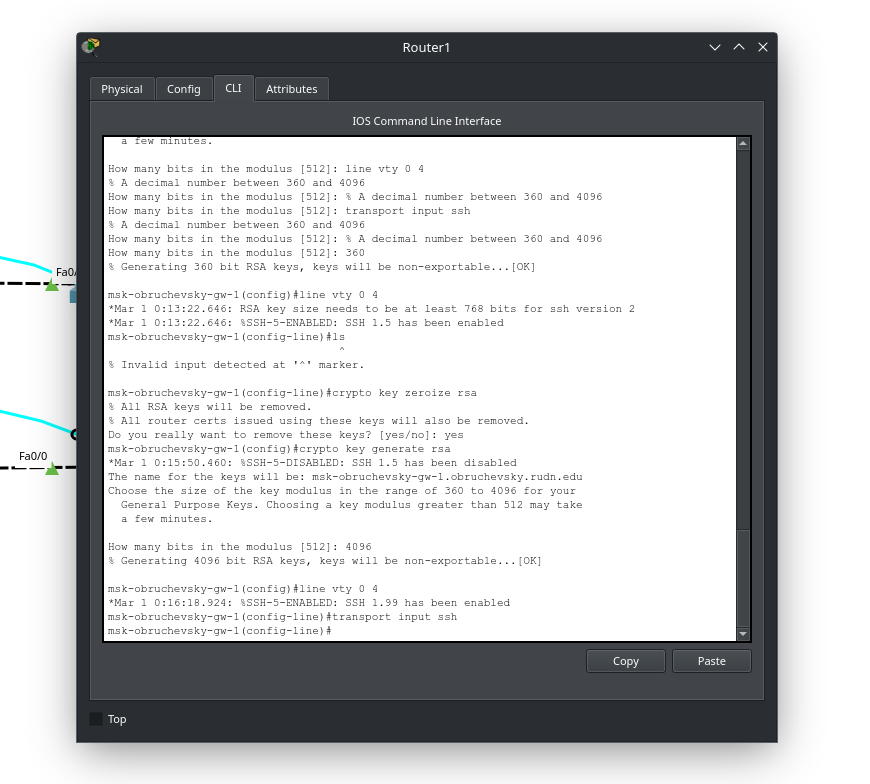


Рис. 3: ssh key router

Эти команды задают имя домена, генерируют пару ключей RSA для шифрования и настраивают SSH в качестве транспортного входа для линий VTY.

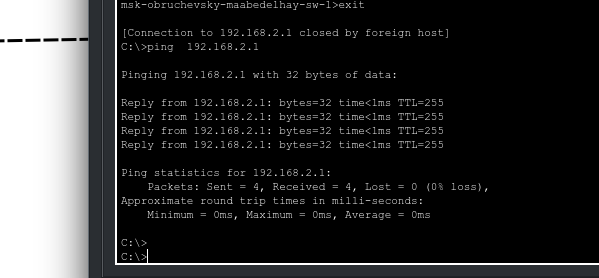


Рис. 4: Ping router

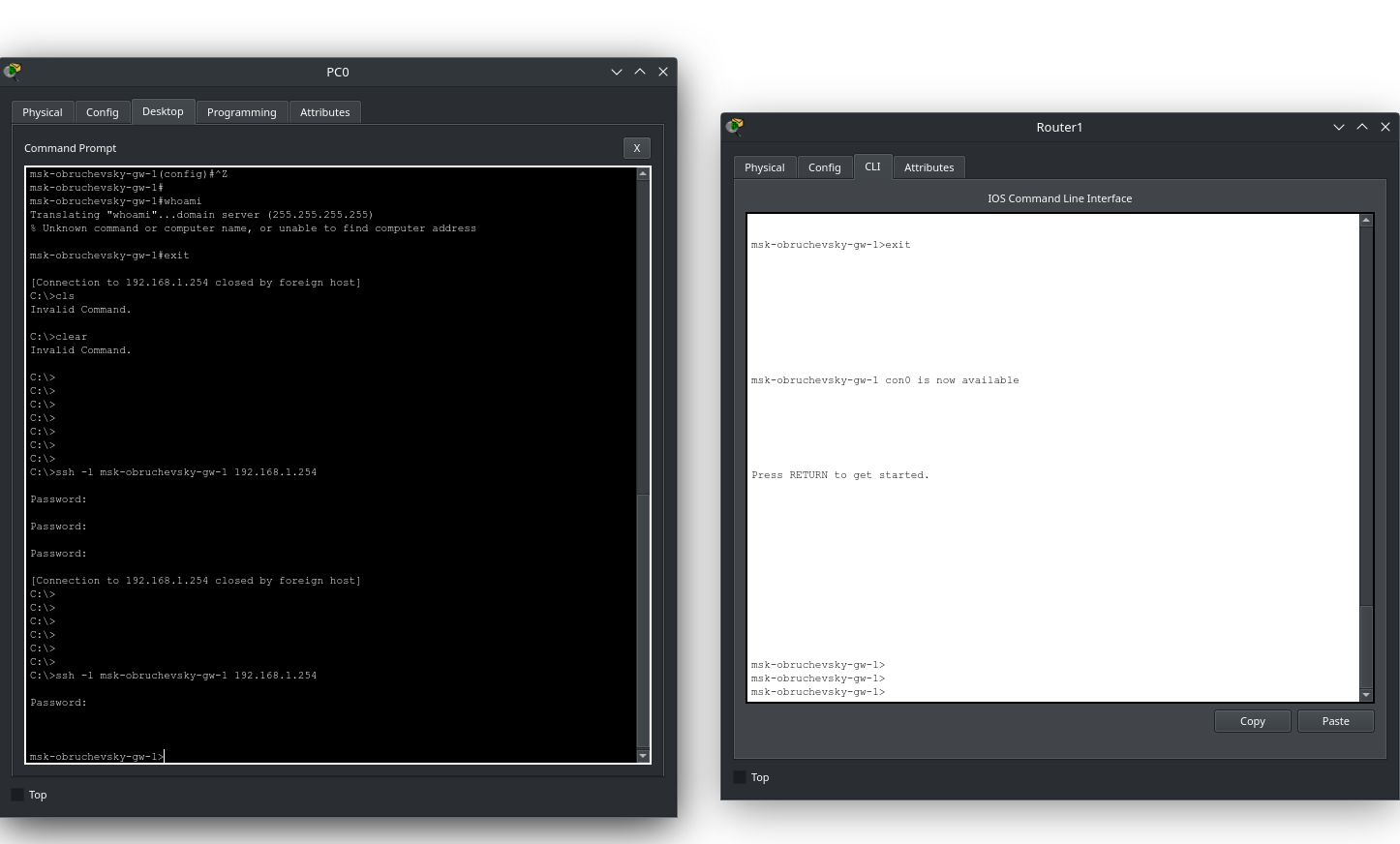


Рис. 5: shh router

я подключился к роутеру через SSH



Рис. 6: telnet router

Затем я настроил vty 1 на использование telnet и подключился от PC0 к маршрутизатору с помощью telnet.

## 3.2 Конфигурация коммутатора

Установка имени хоста

Команда hostname msk-obruchievsky-sw-1 устанавливает имя хоста коммутатора на «msk-obruchevich-sw-1».

Настройка интерфейса VLAN

Команды в интерфейсе vlan2 и интерфейсе f0/1 настраивают интерфейс VLAN и режим порта коммутатора для доступа.

Настройка IP-адреса и шлюза по умолчанию

Команды ip адрес 192.168.2.1 255.255.255.0 и ip default-gateway 192.168.2.254 назначают IP-адреса интерфейсам и устанавливают шлюз по умолчанию для коммутатора.

Настройка линий доступа и шифрования

Команды, относящиеся к строке vty 0 4, строке консоли 0, включению секрета, шифрованию паролей службы, имени пользователя, имени домена IP, генерации криптографического ключа rsa и входному транспортному протоколу ssh, настраивают линии доступа, включают шифрование паролей, создают пользователя. с определенными привилегиями, настройкой доменного имени, созданием пары ключей RSA для шифрования и указанием SSH в качестве входного транспортного сигнала для безопасного доступа.

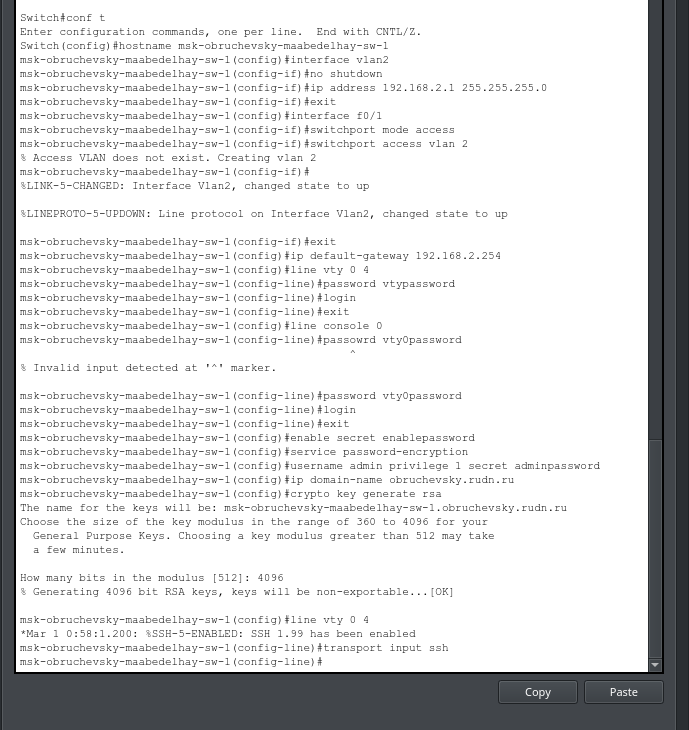


Рис. 7: switch conf

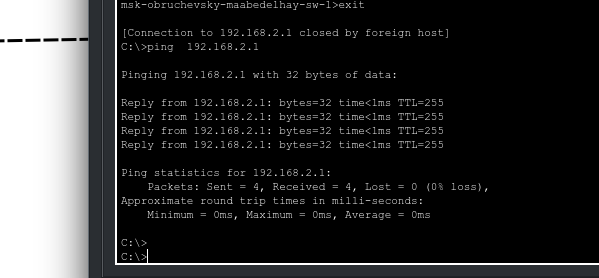


Рис. 8: ping switch

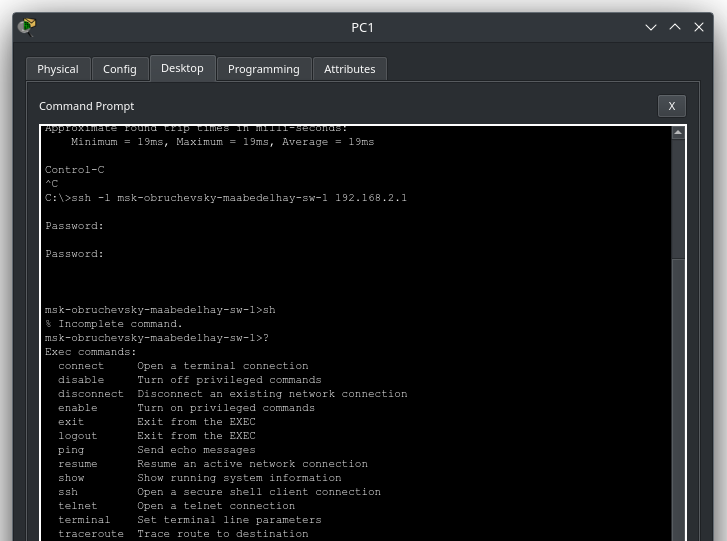


Рис. 9: ssh switch



Рис. 10: telnet ssh

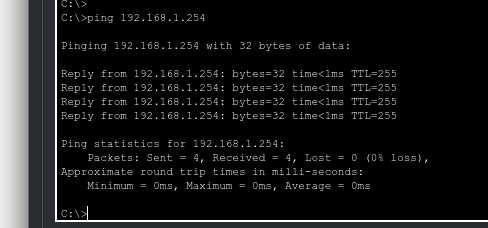


Рис. 11: ping ssh

# 4 Выводы

Я научился настраивать коммутатор и маршрутизатор и получать удаленный доступ через SSH/Telnet.

# 5 Контрольные вопросы

1. Укажите возможные способы подключения к сетевому оборудованию.
   * SSH (Secure Shell)
   * Telnet
   * Консольный кабель
   * Удаленное управление через веб-интерфейс (HTTP/HTTPS)
   * Удаленное управление через SNMP (Simple Network Management Protocol)
2. Каким типом сетевого кабеля следует подключать оконечное оборудование пользователя к маршрутизатору и почему?
   * Тип кабеля: Ethernet-кабель (обычно используется кабель категории 5e или 6) Этот т кабеля обеспечивает соответствующую пропускную способность и поддерживает передачу данных на дальние расстояния, что важно для соединения с маршрутизатором.
3. Каким типом сетевого кабеля следует подключать оконечное оборудование пользователя к коммутатору и почему?
   * Тип кабеля: Тот же Ethernet-кабель, также категории 5e или 6 Для соединения с коммутатором также требуется обеспечить соответствующую пропускную способность и поддержку передачи данных на короткие и средние расстояния
4. Каким типом сетевого кабеля следует подключать коммутатор к коммута- тору и почему?
   * Тип кабеля: Обычно используется витая пара категории 5e или 6 Почему: Этот тип кабеля обеспечивает соединение между коммутаторами в локальной сети, поддерживая передачу данных на короткие расстояния и обеспечивая необходимую пропускную способность
5. Укажите возможные способы настройки доступа к сетевому оборудованию по паролю.
   * Локальные учетные записи на устройстве
   * Аутентификация через сервер AAA (Authentication, Authorization, and Accounting)
   * Использование привилегированных паролей для доступа к привилегированному режиму конфигурации
6. Укажите возможные способы настройки удалённого доступа к сетевому оборудованию. Какой из способов предпочтительнее и почему?
   * SSH (Secure Shell) - предпочтительнее из-за шифрования трафика и повышенной безопасности по сравнению с Telnet
   * Telnet - менее безопасный, поскольку передает данные в незашифрованном виде
   * Удаленное управление через веб-интерфейс (HTTP/HTTPS) - удобно, но требует наличия веб-сервера на устройстве
   * Удаленное управление через SNMP - используется для мониторинга и сбора информации, но не для настройки устройств