Отчёт по лабораторной работе №2

Дисциплина: Администрирование локальных сетей

Мишина Анастасия Алексеевна

Содержание

# 1 Цель работы

Получить основные навыки по начальному конфигурированию оборудования Cisco [1].

# 2 Задание

1. Сделать предварительную настройку маршрутизатора:

* задать имя в виде «город-территория-учётная\_записьтип\_оборудования-номер»;
* 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\_записьтип\_оборудования-номер»
* 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 логической рабочей области Packet Tracer разместим коммутатор, маршрутизатор и 2 оконечных устройства типа PC, соедините один PC с маршрутизатором, другой PC — с коммутатором (рис. 1).

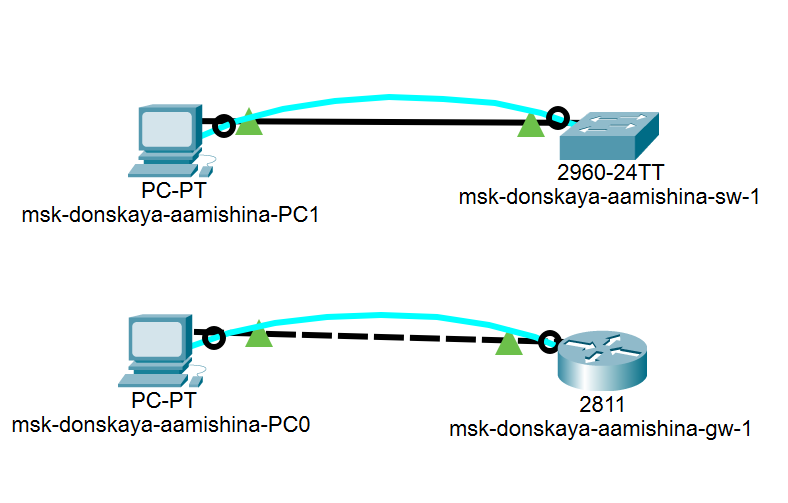


Рис. 1: Схема подключения оборудования для проведения его предварительной настройки

Для начала настроим статические ip-адреса PC0 - 192.168.1.10 (рис. 2) и PC1 - 192.168.2.10 (рис. 3) и маски подсети 255.255.255.0.

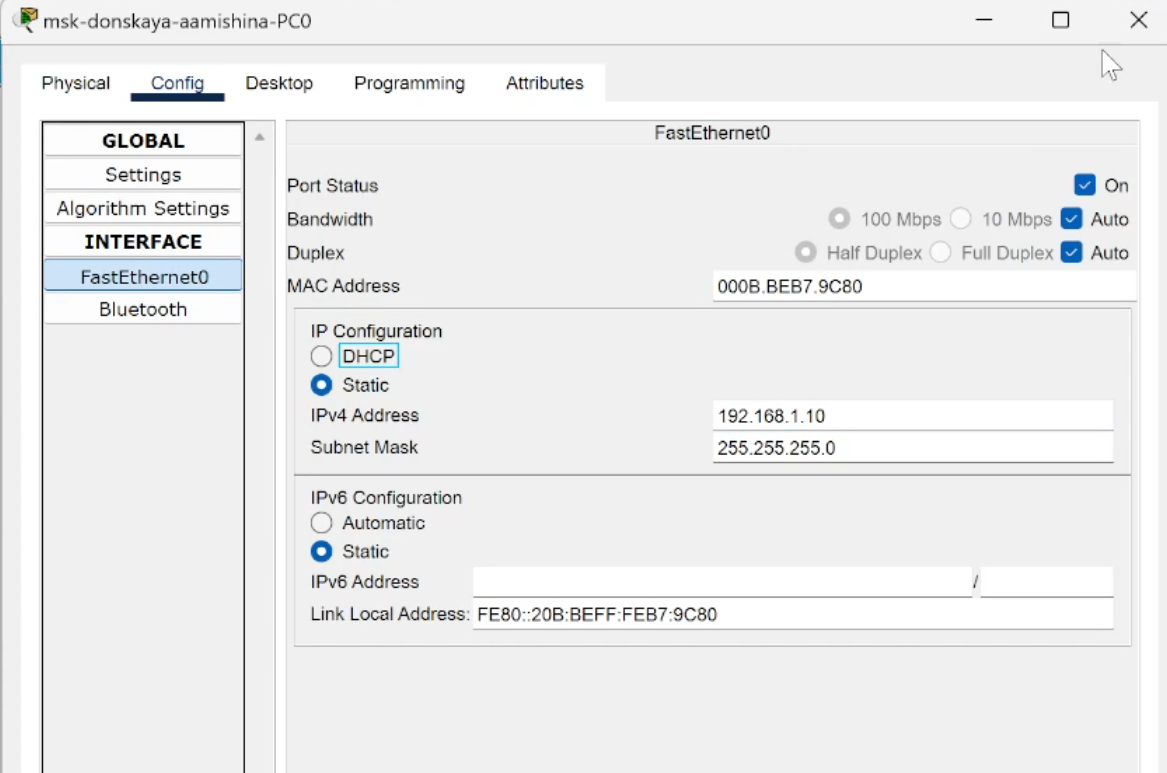


Рис. 2: Настройка статическего ip-адреса PC0

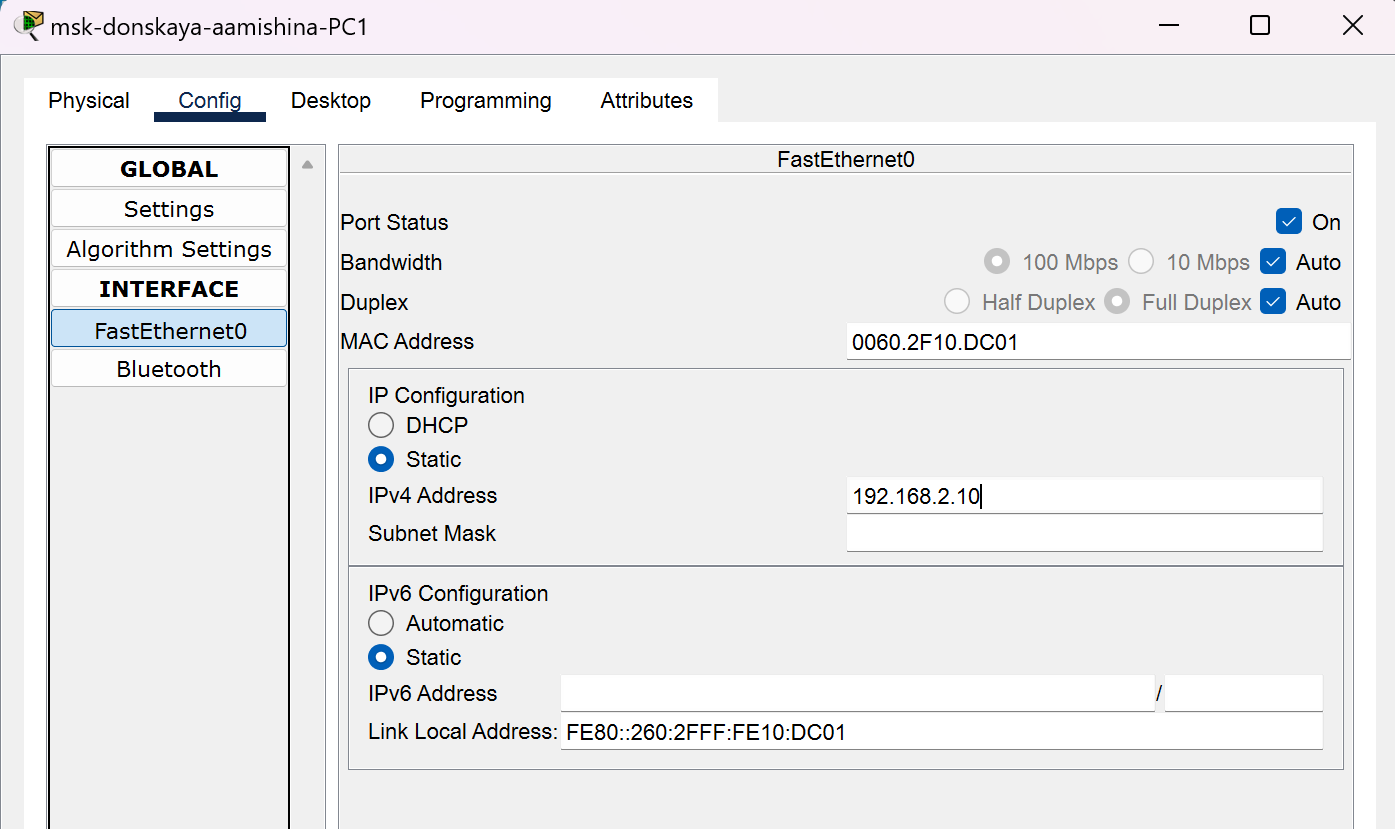


Рис. 3: Настройка статическего ip-адреса PC1

## 3.1 Конфигурация маршрутизатора

Проведем настройку маршрутизатора в соответствии с заданием. Откроем Command Line Interface (CLI) у маршрутизатора, который идентичен терминалу ПК. Перейдем в привилегированный режим с помощью команды enable. Перейдем в режим глобальной конфигурации с помощью команды configure terminal. Зададим имя хоста: hostname msk-donskaya-aamishina-gw-1. Зададим интерфейсу Fast Ethernet с номером 0 ip-адрес 192.168.1.254 с маской 255.255.255.0, поднимем интерфейс командой no shutdown (рис. 4).

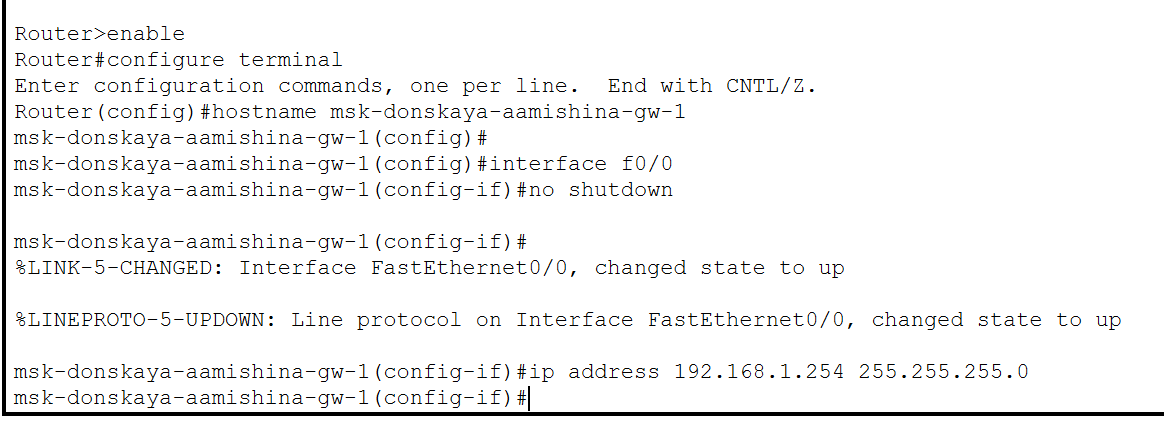


Рис. 4: Установка имени хоста и задание интерфейсу Fast Ethernet с номером 0 ip-адреса

Проверим работоспособность соединений с помощью команды ping. Видим, что было послано 4 пакета и получено тоже 4 пакета, потерь нет, соединение работает успешно (рис. 5).

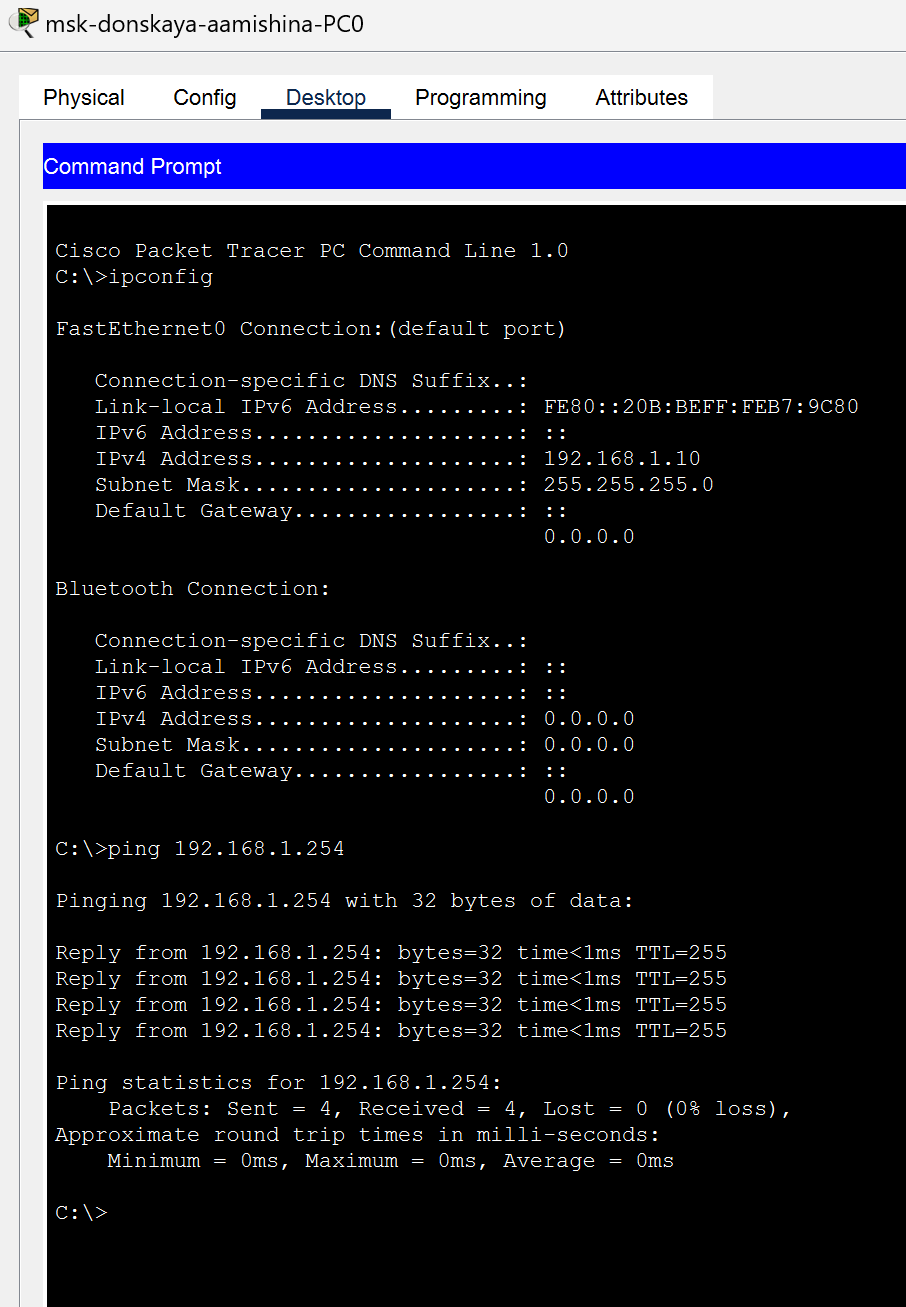


Рис. 5: Проверка соединения с помощью команды ping

Задаем пароль для доступа к привилегированному режиму (сначала в открытом, потом в зашифрованном виде). Зададим пароль для доступа к терминалу, к консоли и поставим пароль на enable (привилегированный режим) (рис. 6).

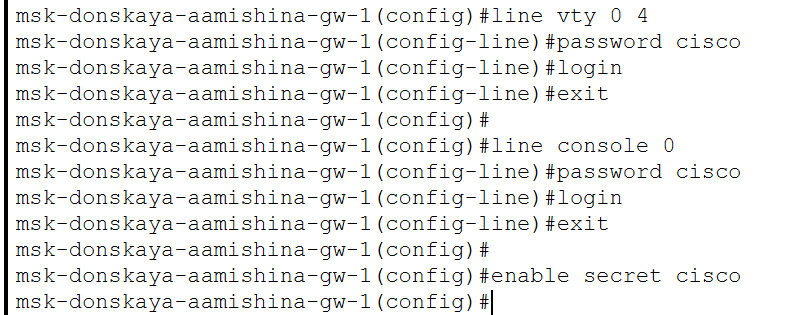


Рис. 6: Установка паролей

Если мы используем команду secret, то пароль сразу будет зашифрован. Но там, где мы использовали команду password пароль не скрыт, и его можно посмотреть (рис. 7).

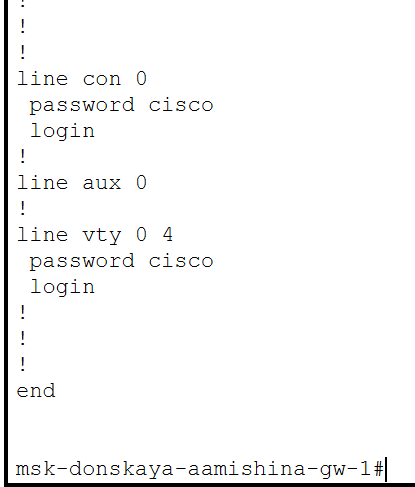


Рис. 7: Просмотр паролей

Исправим это, зашифруем пароли с помощью команды service password−encryption (рис. 8).

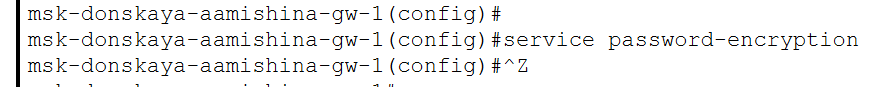


Рис. 8: Шифрование паролей

Просмотрим пароли еще раз, теперь они зашифрованы (рис. 9).

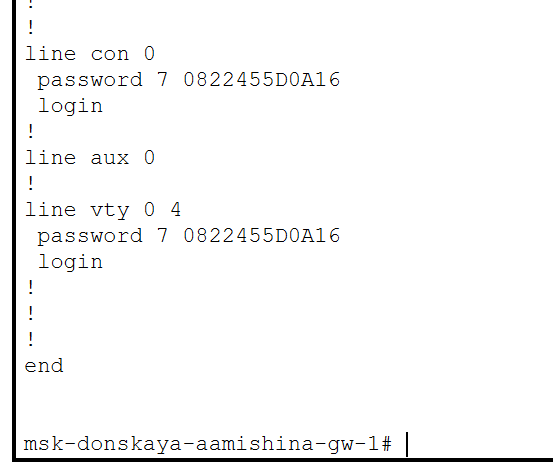


Рис. 9: Просмотр зашифрованных паролей

В качестве дополнительного уровня защиты для пользователя admin зададим доступ 1-ого уровня по паролю. Настроим доступ к оборудованию сначала через telnet, потом через ssh (в качестве доменного имени используем donskaya.rudn.edu) (рис. 10).

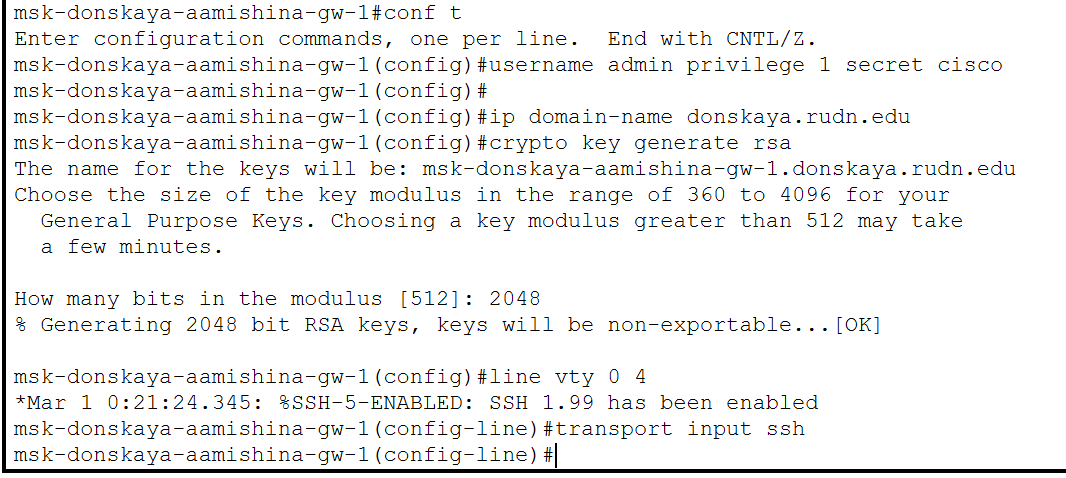


Рис. 10: Настройка доступа через telnet и ssh

Так как мы оставили возможным доступ только через ssh, то при попытке доступа через telnet нам отказано. При доступе через ssh запрашивается пароль (cisco), доступ предоставляется (рис. 11).

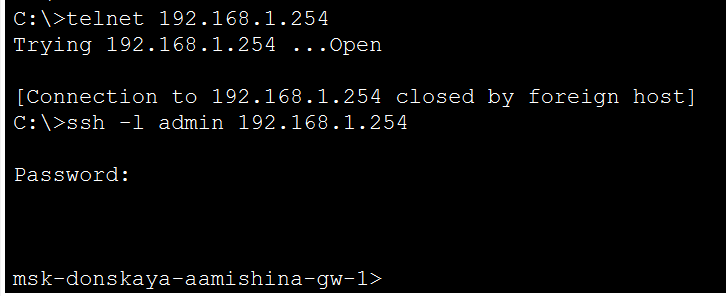


Рис. 11: Проверка работы доступап через telnet и ssh

Сохраним конфигурацию маршрутизатора (рис. 12).

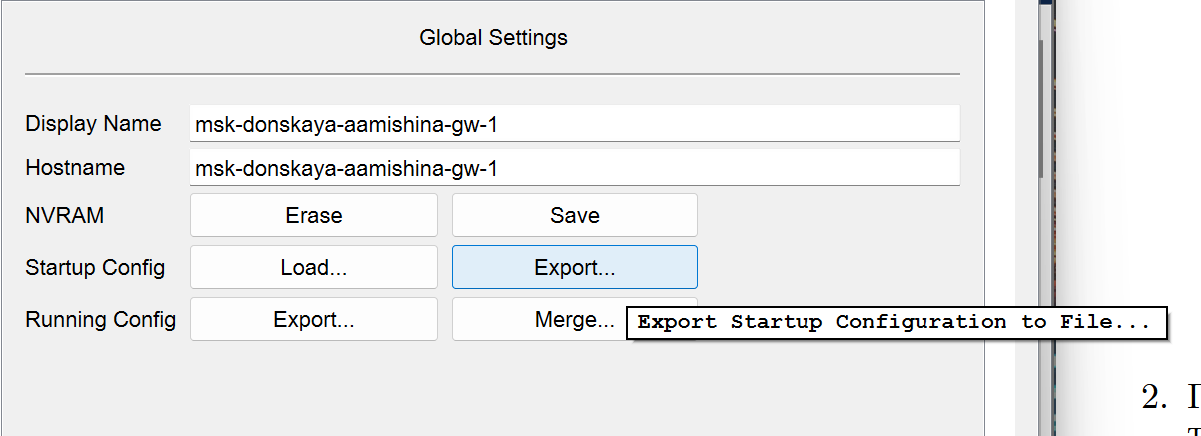


Рис. 12: Сохранение конфигурации маршрутизатора

## 3.2 Конфигурация коммутатора

Проведем настройку коммутатора в соответствии с заданием. Откроем Command Line Interface (CLI) у коммутатора, который идентичен терминалу ПК. Перейдем в привилегированный режим с помощью команды enable. Перейдем в режим глобальной конфигурации с помощью команды configure terminal. Зададим имя хоста: hostname msk-donskaya-aamishina-sw-1. Зададим интерфейсу Fast Ethernet vlan2 ip-адрес 192.168.2.1 с маской 255.255.255.0, поднимем интерфейс командой no shutdown (рис. 13).

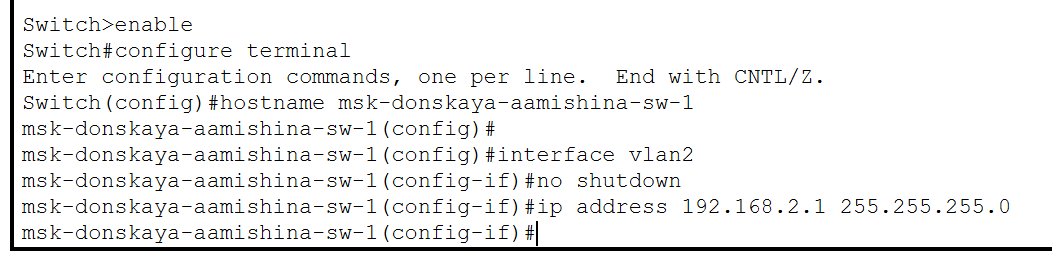


Рис. 13: Установка имени хоста и задание интерфейсу Fast Ethernet vlan2 ip-адреса

Привяжем интерфейс Fast Ethernet с номером 1 к vlan2 (рис. 14).

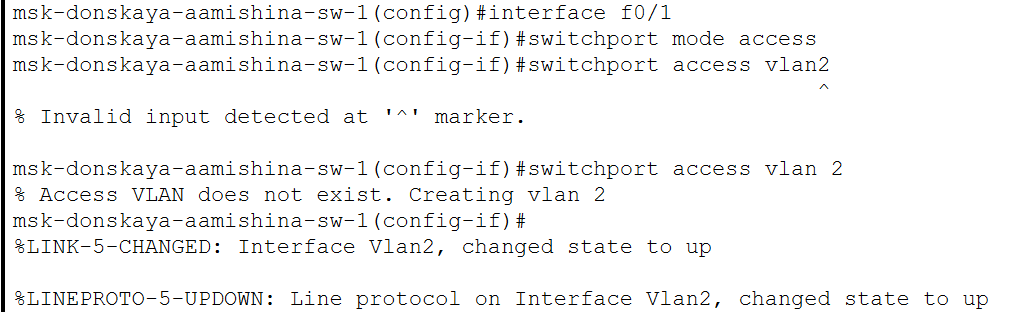


Рис. 14: Привязка интерфейса Fast Ethernet с номером 1 к vlan2

Зададим в качестве адреса шлюза по умолчанию адрес 192.168.2.254 (рис. 15).

Задание в качестве адреса шлюза адрес 192.168.2.254

Рис. 15: Задание в качестве адреса шлюза адрес 192.168.2.254

Проверим работоспособность соединений с помощью команды ping. Видим, что было послано 4 пакета и получено тоже 4 пакета, потерь нет, соединение работает успешно (рис. 16).

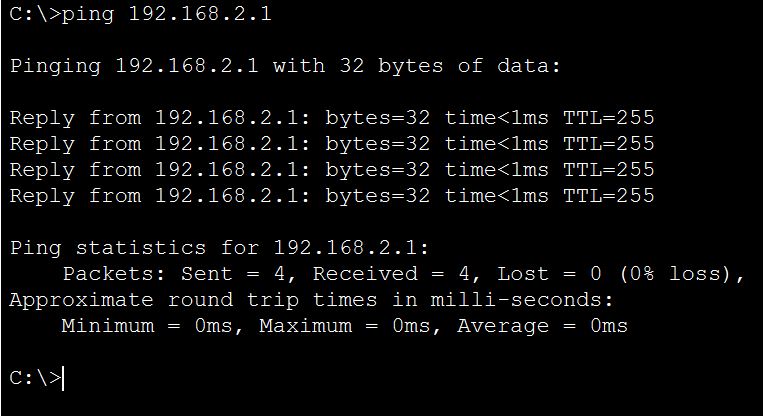


Рис. 16: Проверка соединения с помощью команды ping

Задаем пароль для доступа к привилегированному режиму (сначала в открытом, потом в зашифрованном виде). Зададим пароль для доступа к терминалу, к консоли и поставим пароль на enable (привилегированный режим). Зашифруем пароли с помощью команды service password−encryption (рис. 17).

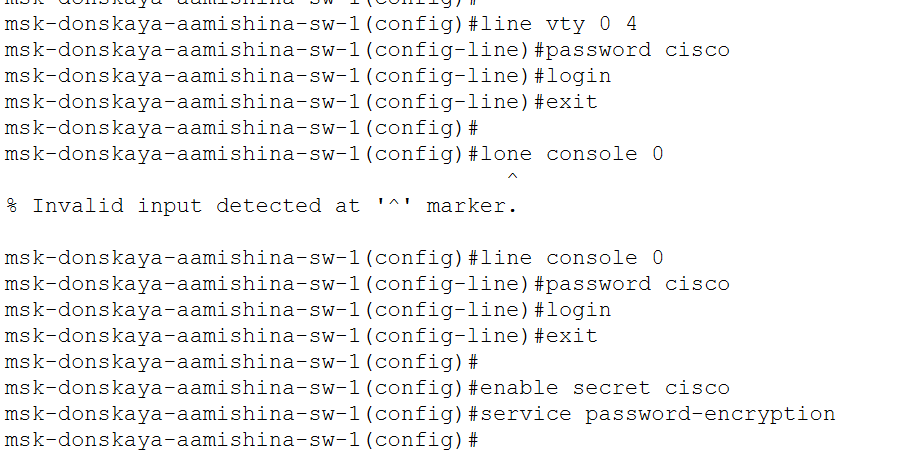


Рис. 17: Установка паролей и их шифрование

В качестве дополнительного уровня защиты для пользователя admin зададим доступ 1-ого уровня по паролю (рис. 18).

Задание доступа 1-ого уровня по паролю

Рис. 18: Задание доступа 1-ого уровня по паролю

Настроим доступ к оборудованию сначала через telnet, потом через ssh (в качестве доменного имени используем donskaya.rudn.edu) (рис. 19).

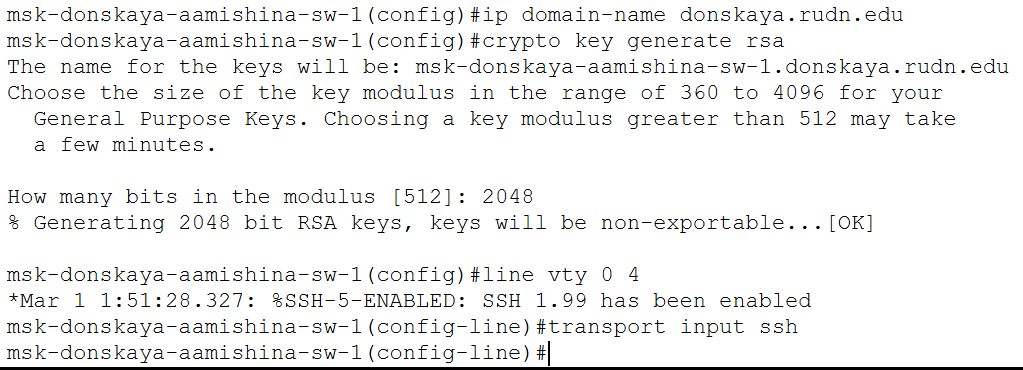


Рис. 19: Настройка доступа через telnet и ssh

Так как мы оставили возможным доступ только через ssh, то при попытке доступа через telnet нам отказано. При доступе через ssh запрашивается пароль (cisco), доступ предоставляется (рис. 20).

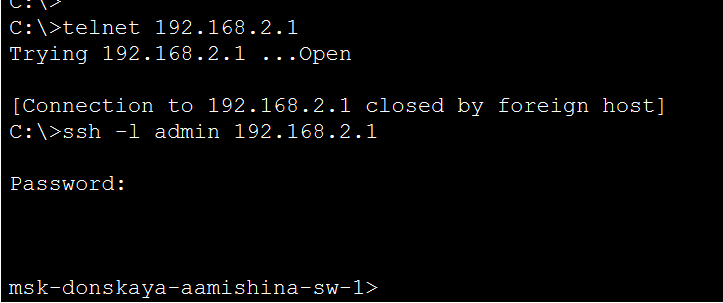


Рис. 20: Проверка работы доступап через telnet и ssh

Сохраним конфигурацию коммутатора (рис. 21).

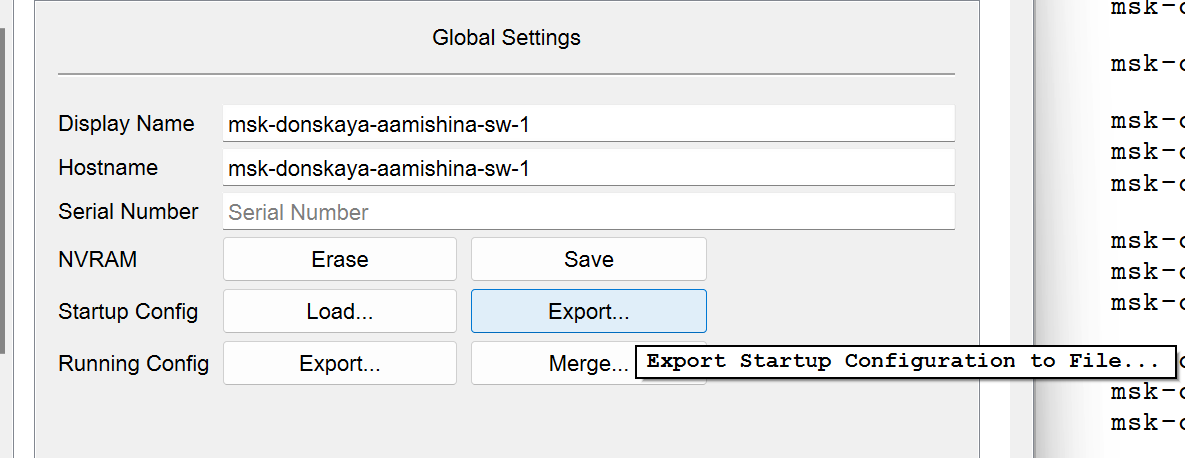


Рис. 21: Сохранение конфигурации коммутатора

# 4 Контрольные вопросы

1. Укажите возможные способы подключения к сетевому оборудованию.

Можно подключиться с помощью консольного кабеля или удаленно по ssh или telnet.

1. Каким типом сетевого кабеля следует подключать оконечное оборудование пользователя к маршрутизатору и почему?

Кроссовым кабелем

1. Каким типом сетевого кабеля следует подключать оконечное оборудование пользователя к коммутатору и почему?

Прямым кабелем (витой парой).

1. Каким типом сетевого кабеля следует подключать коммутатор к коммутатору и почему?

Кроссовым кабелем (для соединения одинокого оборудования используют кроссовый кабель)

1. Укажите возможные способы настройки доступа к сетевому оборудованию по паролю.

С помощью команды password или с помощью команды secret

1. Укажите возможные способы настройки удалённого доступа к сетевому оборудованию. Какой из способов предпочтительнее и почему?

Через telnet или ssh. SSH обеспечивает шифрование и аутентификацию по умолчанию, в отличие от Telnet, который не предоставляет эти функции, поэтому он лучше.

# 5 Выводы

В процессе выполнения данной лабораторной работы я получила основные навыки по начальному конфигурированию оборудования Cisco.

# Список литературы

1. Кулябов Д.С., Королькова А.В. Администрирование локальных систем: лабораторные работы : учебное пособие. Москва: РУДН, 2017. 119 с.