

Отчёт по лабораторной работе №2

Дисциплина: Администрирование локальных сетей

Мишина Анастасия Алексеевна

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	8
3.1	Конфигурация маршрутизатора	9
3.2	Конфигурация коммутатора	15
4	Контрольные вопросы	20
5	Выводы	22
	Список литературы	23

Список иллюстраций

3.1	Схема подключения оборудования для проведения его предварительной настройки	8
3.2	Настройка статического ip-адреса PC0	9
3.3	Настройка статического ip-адреса PC1	9
3.4	Установка имени хоста и задание интерфейсу Fast Ethernet с номером 0 ip-адреса	10
3.5	Проверка соединения с помощью команды ping	11
3.6	Установка паролей	12
3.7	Просмотр паролей	13
3.8	Шифрование паролей	13
3.9	Просмотр зашифрованных паролей	14
3.10	Настройка доступа через telnet и ssh	14
3.11	Проверка работы доступа через telnet и ssh	15
3.12	Сохранение конфигурации маршрутизатора	15
3.13	Установка имени хоста и задание интерфейсу Fast Ethernet vlan2 ip-адреса	16
3.14	Привязка интерфейса Fast Ethernet с номером 1 к vlan2	16
3.15	Задание в качестве адреса шлюза адрес 192.168.2.254	16
3.16	Проверка соединения с помощью команды ping	17
3.17	Установка паролей и их шифрование	17
3.18	Задание доступа 1-ого уровня по паролю	18
3.19	Настройка доступа через telnet и ssh	18
3.20	Проверка работы доступа через telnet и ssh	18
3.21	Сохранение конфигурации коммутатора	19

Список таблиц

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.

2. 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. 3.1).

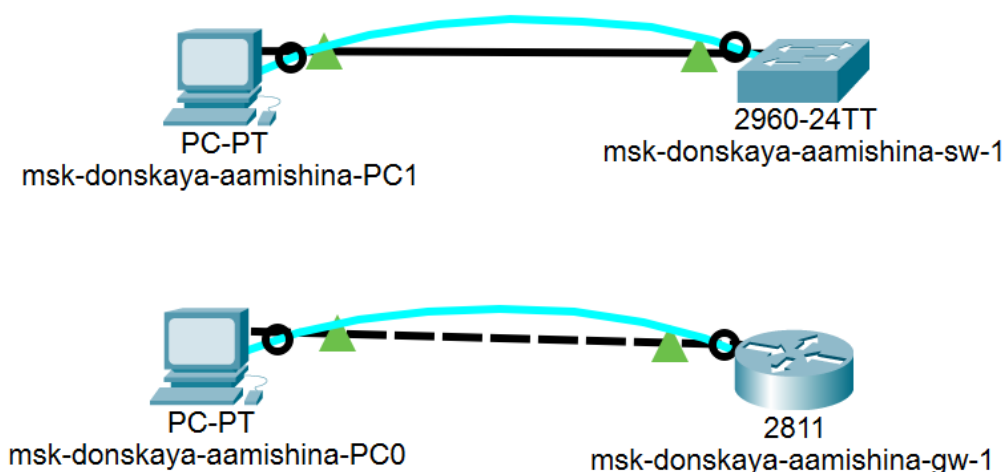


Рис. 3.1: Схема подключения оборудования для проведения его предварительной настройки

Для начала настроим статические ip-адреса PC0 - 192.168.1.10 (рис. 3.2) и PC1 - 192.168.2.10 (рис. 3.3) и маски подсети 255.255.255.0.

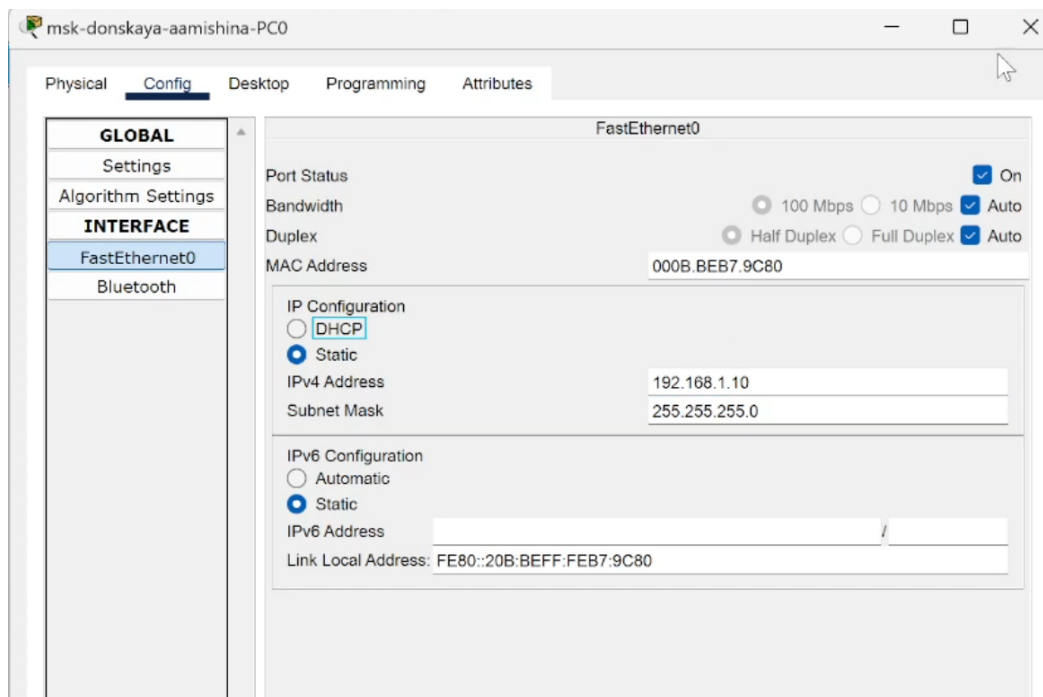


Рис. 3.2: Настройка статического ip-адреса PC0

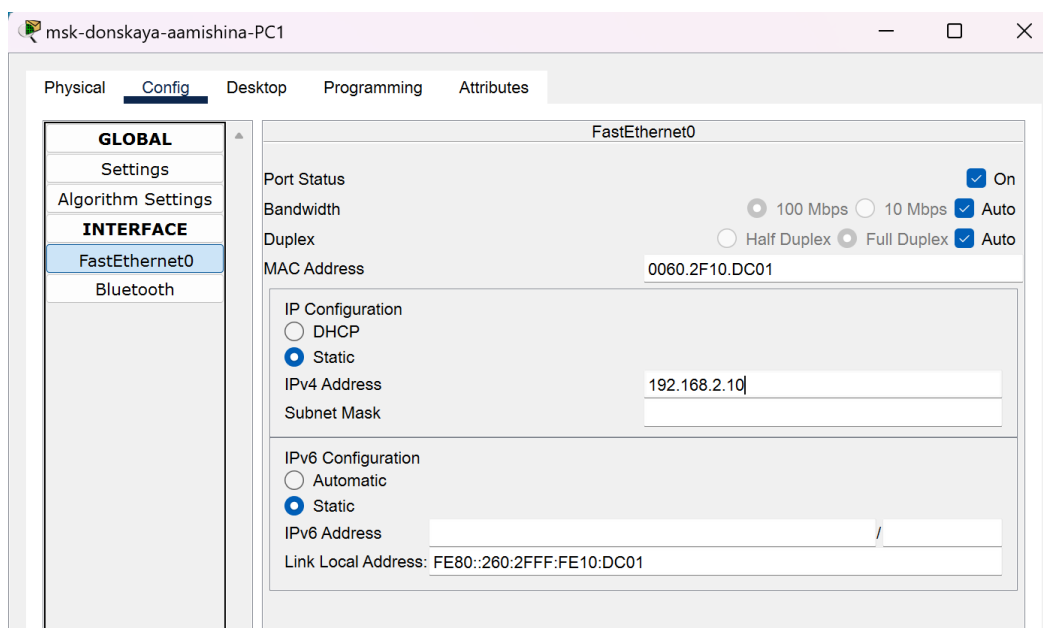


Рис. 3.3: Настройка статического ip-адреса PC1

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. 3.4).

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname msk-donskaya-aamishina-gw-1
msk-donskaya-aamishina-gw-1(config)#
msk-donskaya-aamishina-gw-1(config)#interface f0/0
msk-donskaya-aamishina-gw-1(config-if)#no shutdown

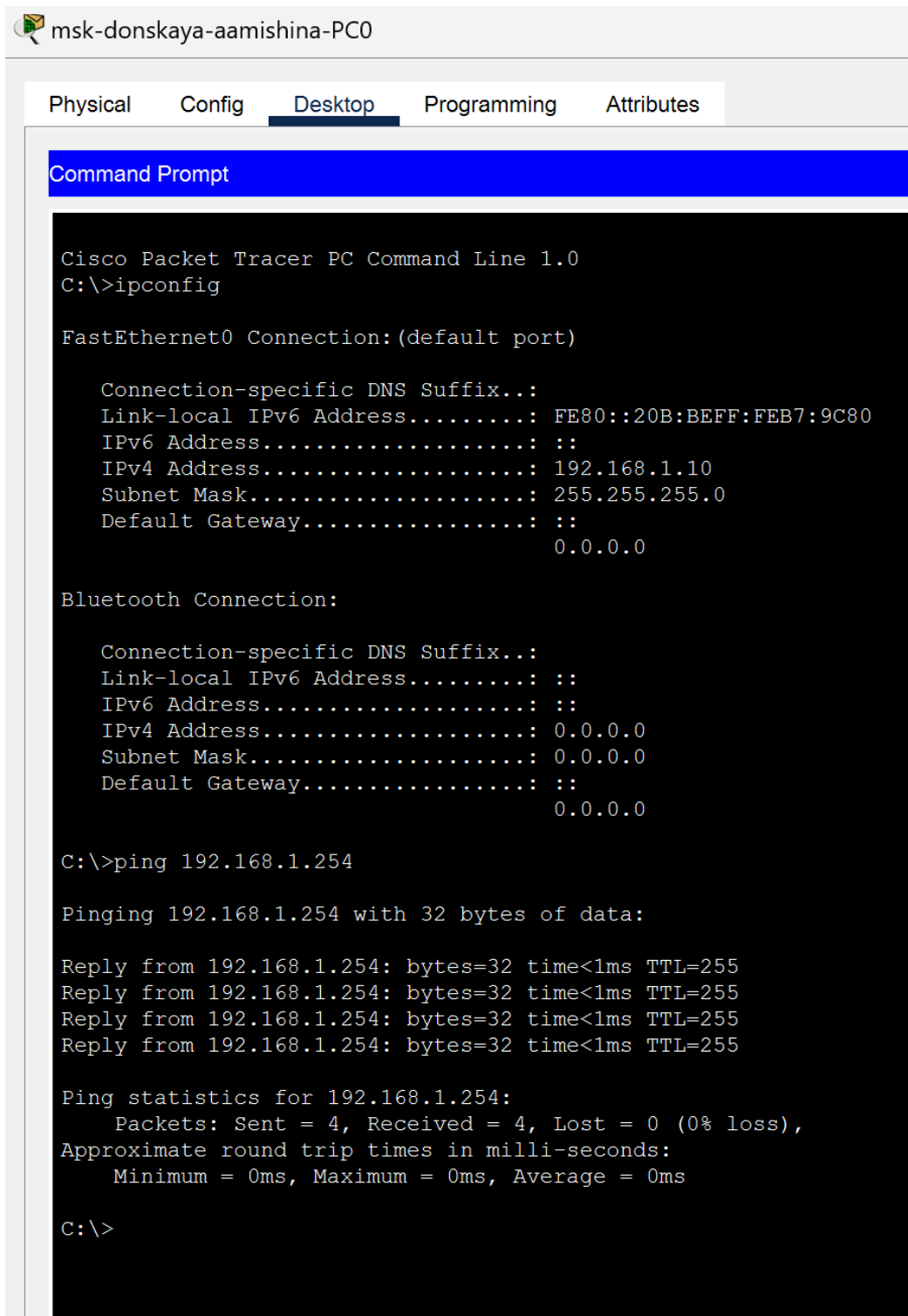
msk-donskaya-aamishina-gw-1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

msk-donskaya-aamishina-gw-1(config-if)#ip address 192.168.1.254 255.255.255.0
msk-donskaya-aamishina-gw-1(config-if)#
```

Рис. 3.4: 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. 3.5).



```
msk-donskaya-aamishina-PC0

Physical  Config  Desktop  Programming  Attributes

Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: FE80::20B:BEFF:FEB7:9C80
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.1.10
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: ::
                                0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: ::
    IPv6 Address.....: ::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: ::
                                0.0.0.0

C:\>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Рис. 3.5: 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. 3.6).

```
msk-donskaya-aamishina-gw-1(config)#line vty 0 4
msk-donskaya-aamishina-gw-1(config-line)#password cisco
msk-donskaya-aamishina-gw-1(config-line)#login
msk-donskaya-aamishina-gw-1(config-line)#exit
msk-donskaya-aamishina-gw-1(config)#
msk-donskaya-aamishina-gw-1(config)#line console 0
msk-donskaya-aamishina-gw-1(config-line)#password cisco
msk-donskaya-aamishina-gw-1(config-line)#login
msk-donskaya-aamishina-gw-1(config-line)#exit
msk-donskaya-aamishina-gw-1(config)#
msk-donskaya-aamishina-gw-1(config)#enable secret cisco
msk-donskaya-aamishina-gw-1(config)#|
```

Рис. 3.6: 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. 3.7).

```
:
!  
!  
line con 0  
  password cisco  
  login  
!  
line aux 0  
!  
line vty 0 4  
  password cisco  
  login  
!  
!  
!  
end  
  
msk-donskaya-aamishina-gw-1#
```

Рис. 3.7: Просмотр паролей

Исправим это, зашифруем пароли с помощью команды `service password-encryption` (рис. 3.8).

```
msk-donskaya-aamishina-gw-1(config)#  
msk-donskaya-aamishina-gw-1(config)#service password-encryption  
msk-donskaya-aamishina-gw-1(config)#^Z
```

Рис. 3.8: Шифрование паролей

Посмотрим пароли еще раз, теперь они зашифрованы (рис. 3.9).

```

:
!
line con 0
  password 7 0822455D0A16
  login
!
line aux 0
!
line vty 0 4
  password 7 0822455D0A16
  login
!
!
!
end

msk-donskaya-aamishina-gw-1#

```

Рис. 3.9: 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. 3.10).

```

msk-donskaya-aamishina-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-aamishina-gw-1(config)#username admin privilege 1 secret cisco
msk-donskaya-aamishina-gw-1(config)#
msk-donskaya-aamishina-gw-1(config)#ip domain-name donsкаya.rudn.edu
msk-donskaya-aamishina-gw-1(config)#crypto key generate rsa
The name for the keys will be: msk-donskaya-aamishina-gw-1.donsкаya.rudn.edu
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

msk-donskaya-aamishina-gw-1(config)#line vty 0 4
*Mar 1 0:21:24.345: %SSH-5-ENABLED: SSH 1.99 has been enabled
msk-donskaya-aamishina-gw-1(config-line)#transport input ssh
msk-donskaya-aamishina-gw-1(config-line)#

```

Рис. 3.10: 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. 3.11).

```
C:\>telnet 192.168.1.254
Trying 192.168.1.254 ...Open

[Connection to 192.168.1.254 closed by foreign host]
C:\>ssh -l admin 192.168.1.254

Password:

msk-donskaya-aamishina-gw-1>
```

Рис. 3.11: Проверка работы доступа через telnet и ssh

Сохраним конфигурацию маршрутизатора (рис. 3.12).

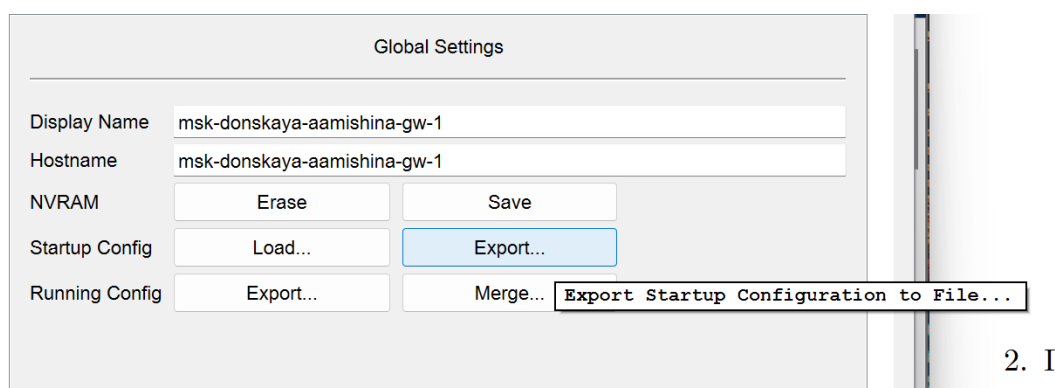


Рис. 3.12: Сохранение конфигурации маршрутизатора

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. 3.13).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname msk-donskaya-aamishina-sw-1
msk-donskaya-aamishina-sw-1(config)#
msk-donskaya-aamishina-sw-1(config)#interface vlan2
msk-donskaya-aamishina-sw-1(config-if)#no shutdown
msk-donskaya-aamishina-sw-1(config-if)#ip address 192.168.2.1 255.255.255.0
msk-donskaya-aamishina-sw-1(config-if)#
```

Рис. 3.13: Установка имени хоста и задание интерфейсу Fast Ethernet vlan2 ip-адреса

Привяжем интерфейс Fast Ethernet с номером 1 к vlan2 (рис. 3.14).

```
msk-donskaya-aamishina-sw-1(config)#interface f0/1
msk-donskaya-aamishina-sw-1(config-if)#switchport mode access
msk-donskaya-aamishina-sw-1(config-if)#switchport access vlan2
^
% Invalid input detected at '^' marker.

msk-donskaya-aamishina-sw-1(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
msk-donskaya-aamishina-sw-1(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
```

Рис. 3.14: Привязка интерфейса Fast Ethernet с номером 1 к vlan2

Зададим в качестве адреса шлюза по умолчанию адрес 192.168.2.254 (рис. 3.15).

```
msk-donskaya-aamishina-sw-1(config)#ip default-gateway 192.168.2.254
msk-donskaya-aamishina-sw-1(config)#
```

Рис. 3.15: 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. 3.16).


```

C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>|

```

Рис. 3.16: 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. 3.17).

```

msk-donskaya-aamishina-sw-1(config)#
msk-donskaya-aamishina-sw-1(config)#line vty 0 4
msk-donskaya-aamishina-sw-1(config-line)#password cisco
msk-donskaya-aamishina-sw-1(config-line)#login
msk-donskaya-aamishina-sw-1(config-line)#exit
msk-donskaya-aamishina-sw-1(config)#
msk-donskaya-aamishina-sw-1(config)#lone console 0
msk-donskaya-aamishina-sw-1(config)#^
% Invalid input detected at '^' marker.

msk-donskaya-aamishina-sw-1(config)#line console 0
msk-donskaya-aamishina-sw-1(config-line)#password cisco
msk-donskaya-aamishina-sw-1(config-line)#login
msk-donskaya-aamishina-sw-1(config-line)#exit
msk-donskaya-aamishina-sw-1(config)#
msk-donskaya-aamishina-sw-1(config)#enable secret cisco
msk-donskaya-aamishina-sw-1(config)#service password-encryption
msk-donskaya-aamishina-sw-1(config)#

```

Рис. 3.17: Установка паролей и их шифрование

В качестве дополнительного уровня защиты для пользователя admin зададим доступ 1-ого уровня по паролю (рис. 3.18).

```
msk-donskaya-aamishina-sw-1(config)#
msk-donskaya-aamishina-sw-1(config)#username admin privilege 1 secret cisco
msk-donskaya-aamishina-sw-1(config)#
```

Рис. 3.18: 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. 3.19).

```
msk-donskaya-aamishina-sw-1(config)#ip domain-name donskaya.rudn.edu
msk-donskaya-aamishina-sw-1(config)#crypto key generate rsa
The name for the keys will be: msk-donskaya-aamishina-sw-1.donskaya.rudn.edu
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

msk-donskaya-aamishina-sw-1(config)#line vty 0 4
*Mar 1 1:51:28.327: %SSH-5-ENABLED: SSH 1.99 has been enabled
msk-donskaya-aamishina-sw-1(config-line)#transport input ssh
msk-donskaya-aamishina-sw-1(config-line)#
```

Рис. 3.19: 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. 3.20).

```
C:\>
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open

[Connection to 192.168.2.1 closed by foreign host]
C:\>ssh -l admin 192.168.2.1

Password:

msk-donskaya-aamishina-sw-1>
```

Рис. 3.20: Проверка работы доступа через telnet и ssh

Сохраним конфигурацию коммутатора (рис. 3.21).

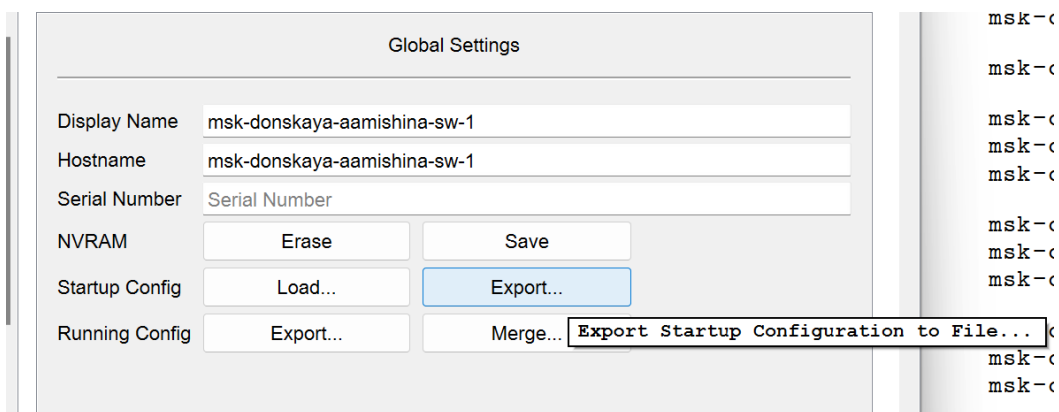


Рис. 3.21: Сохранение конфигурации коммутатора

4 Контрольные вопросы

1. Укажите возможные способы подключения к сетевому оборудованию.

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

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

Кроссовым кабелем

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

Прямым кабелем (витой парой).

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

Кроссовым кабелем (для соединения одинокого оборудования используют кроссовый кабель)

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

С помощью команды `password` или с помощью команды `secret`

6. 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.