

Лабораторная работа № 2. Предварительная настройка оборудования Cisco

Абакумова Олеся Максимовна, НФИбд-02-22

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	8
4	Контрольные вопросы	18
5	Выводы	20

Список иллюстраций

3.1	Схема подключения оборудования для проведения его предварительной настройки	8
3.2	Заданный ip-адрес	9
3.3	Раздел конфигурации в маршрутизаторе	10
3.4	Задание интерфейса	11
3.5	Задание двух типов паролей и настройка доступа	12
3.6	Сохранение конфигурации	13
3.7	Правильное именование коммутатора	14
3.8	Задание ip-адреса интерфейсу	14
3.9	Привязка интерфейса и задание адреса шлюза	15
3.10	Задание пароля в двух видах	15
3.11	Настройка доступа	15
3.12	Сохранение конфигурации коммутатора	16
3.13	Пингование 192.168.2.1	16
3.14	Пингование 192.168.1.254	16
3.15	Неудача	17

Список таблиц

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_запись-тип_оборудования-номер», 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 donsкаya.rudn.edu);
- сохранить и экспортировать конфигурацию в отдельный файл.

2. Сделать предварительную настройку коммутатора:

- задать имя в виде «город-территория-учётная_запись-тип_оборудования-номер», 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 donsкаya.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 разместите коммутатор, маршрутизатор и 2 оконечных устройства типа PC, соедините один PC с маршрутизатором, другой PC — с коммутатором (рис. 3.1):

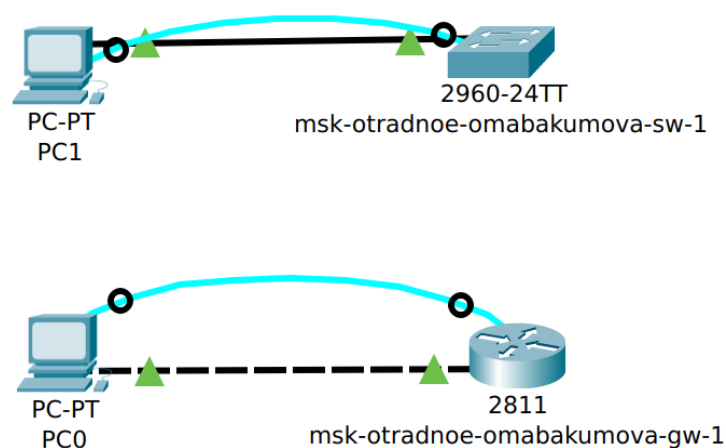


Рис. 3.1: Схема подключения оборудования для проведения его предварительной настройки

Проведем настройку маршрутизатора в соответствии с заданием. Для начала зададим ему ip-адрес, после того как правильно именовали его (рис. 3.2):

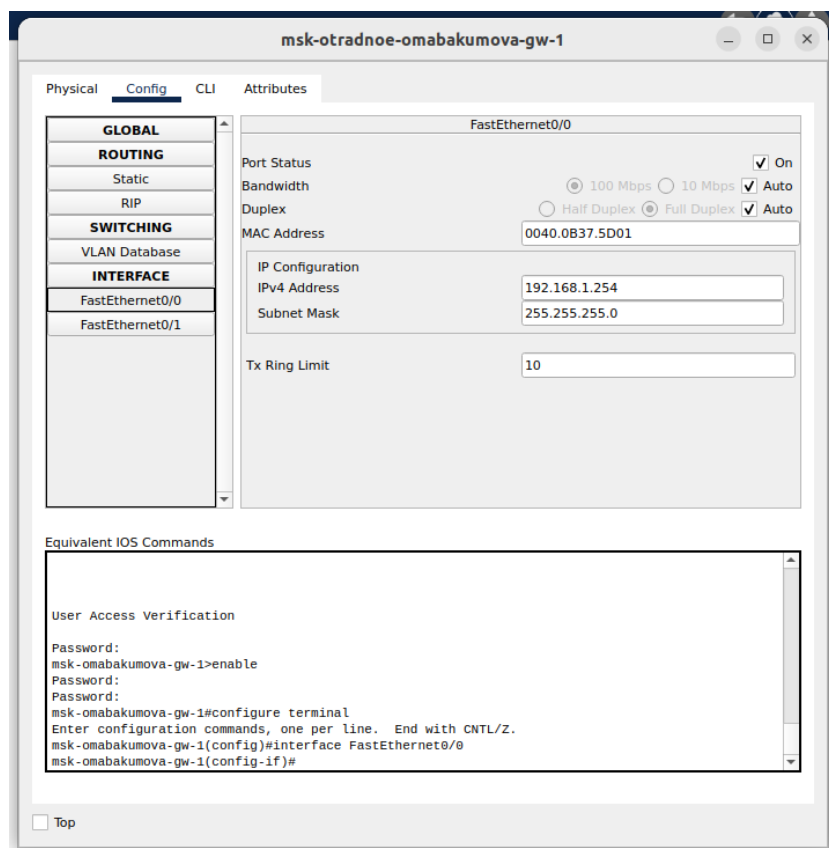


Рис. 3.2: Заданный ip-адрес

Затем зададим для него hostname в его консоли (рис. 3.3):

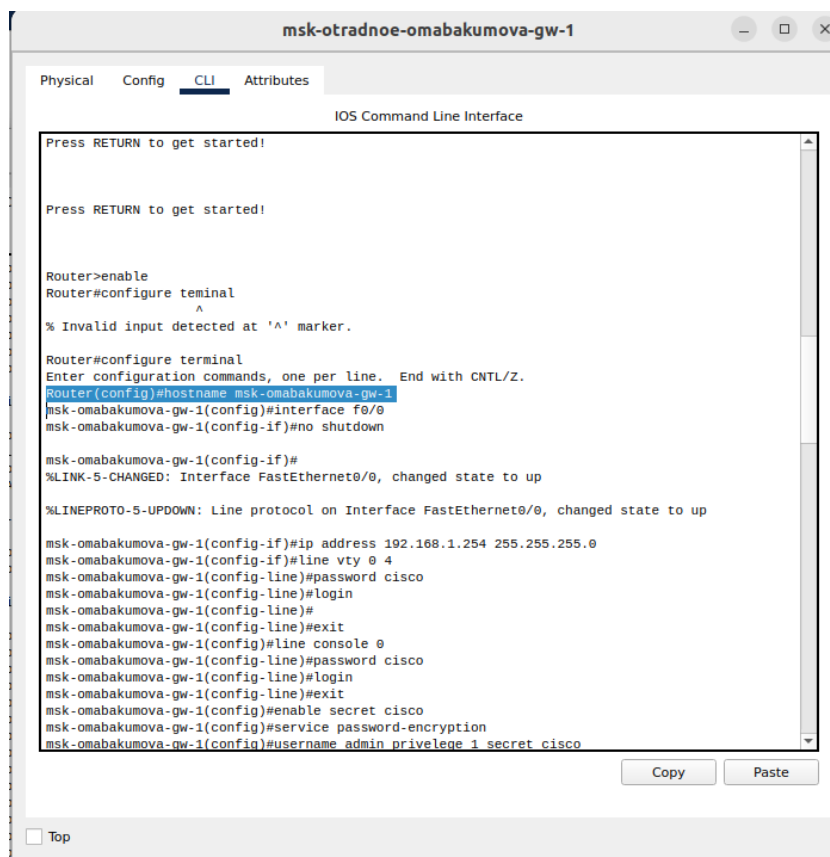


Рис. 3.3: Раздел конфигурации в маршрутизаторе

Зададим интерфейсу Fast Ethernet с номером 0 ip-адрес 192.168.1.254 и маску 255.255.255.0, затем поднимем его (рис. 3.4):

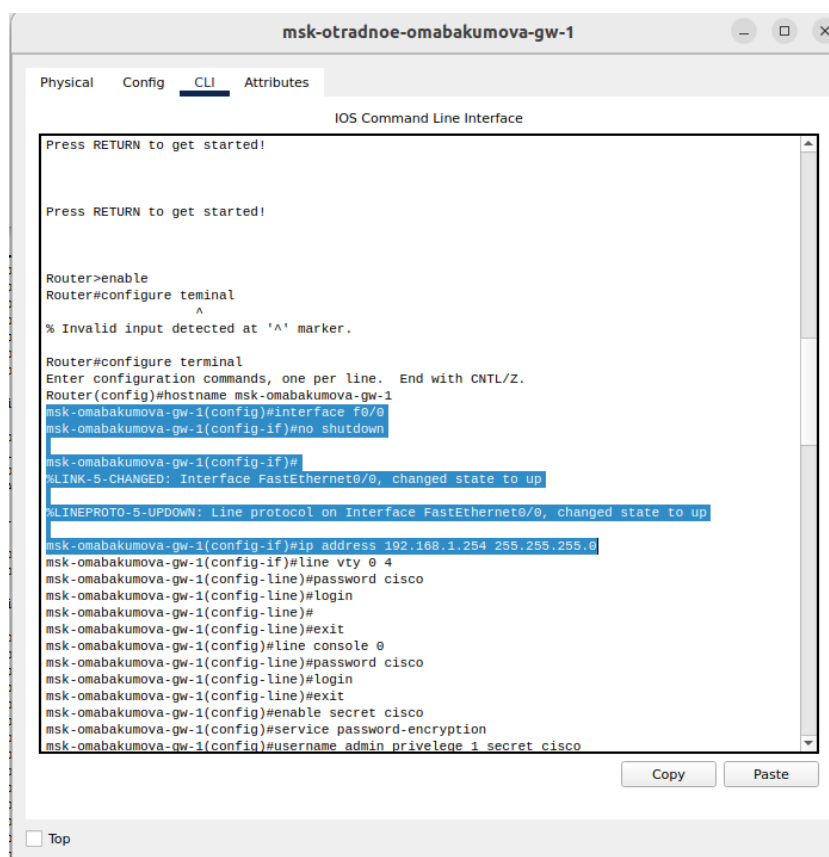


Рис. 3.4: Задание интерфейса

Теперь требуется задать пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном) и настроить доступ к оборудованию через ssh (используя в качестве имени домена `donskaya.rudn.edu`) (рис. 3.5):

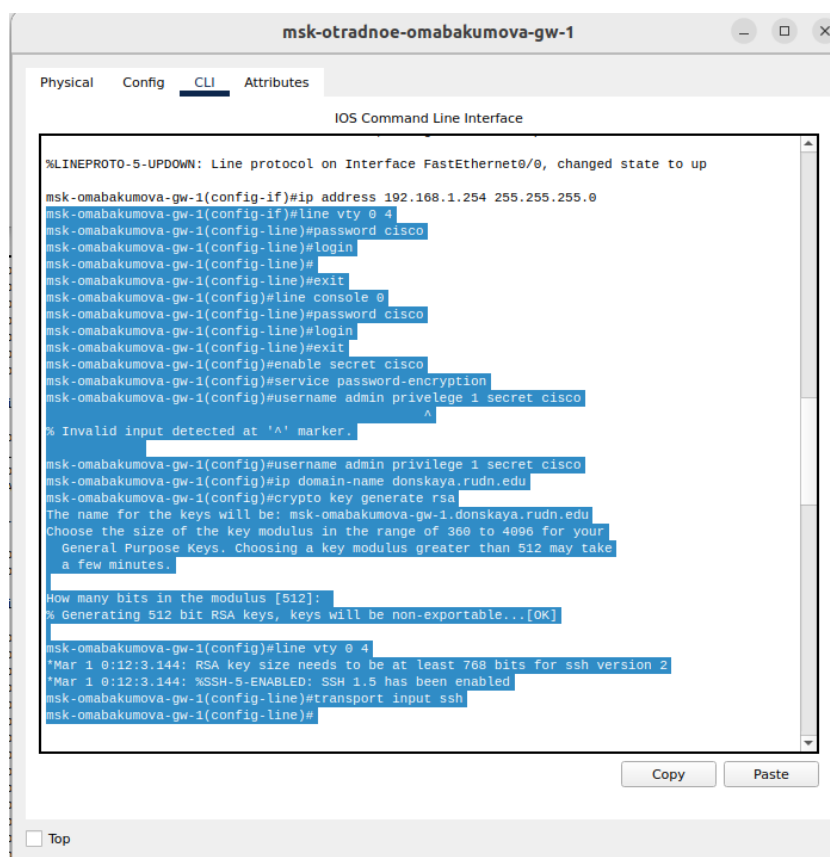


Рис. 3.5: Задание двух типов паролей и настройка доступа

После настройки маршрутизатора, сохраним и экспортируем конфигурацию в отдельный файл (рис. 3.6):

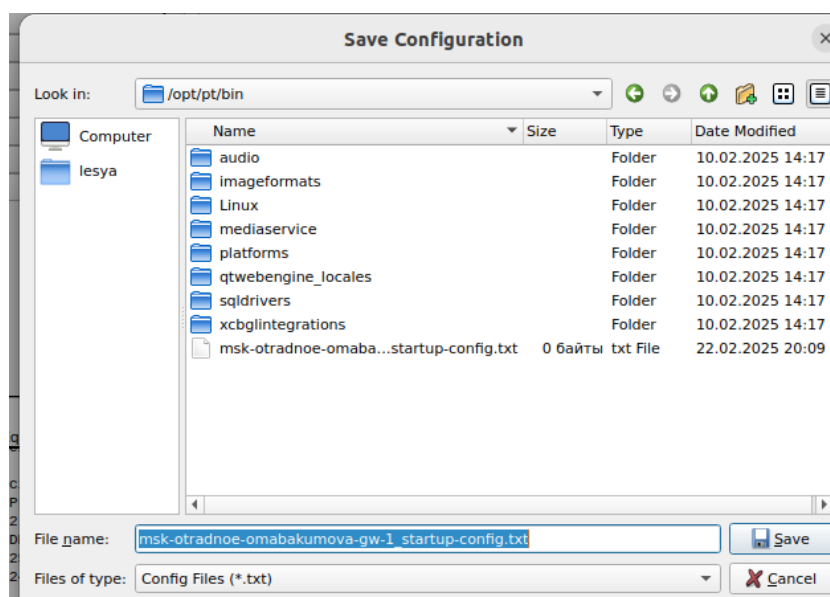


Рис. 3.6: Сохранение конфигурации

Теперь настроим коммутатор аналогичным методом. Для начала зададим ему правильное именование (рис. 3.7):

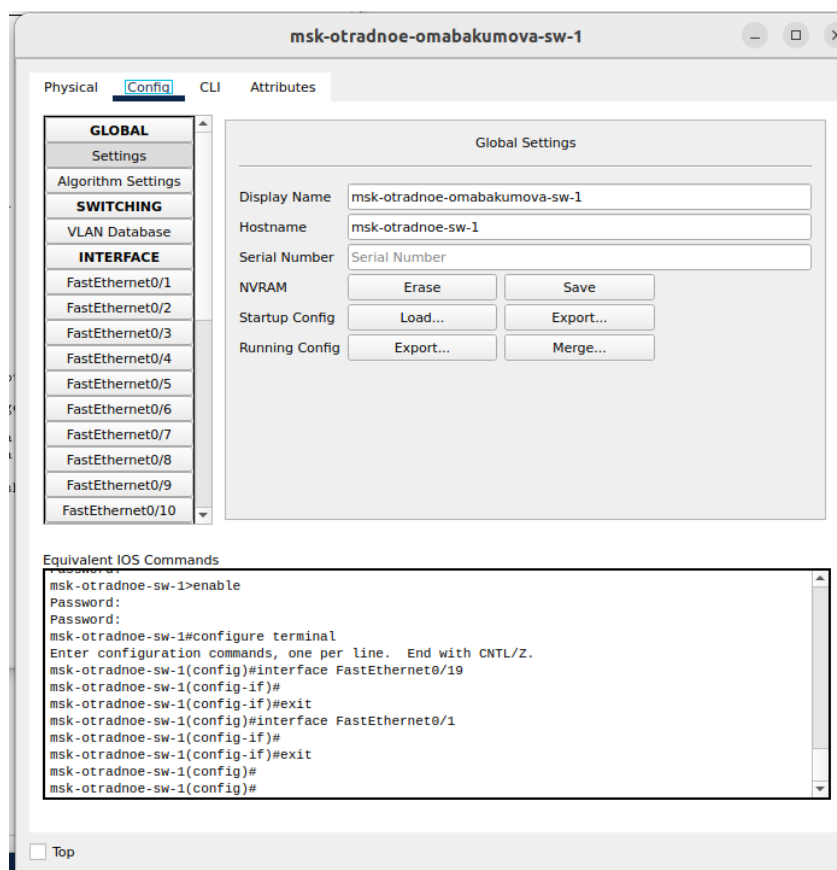


Рис. 3.7: Правильное именование коммутатора

После именованя и задачи hostname для коммутатора, зададим интерфейсу vlan 2 ip-адрес 192.168.2.1 и маску 255.255.255.0 и поднимем его (рис. 3.8):

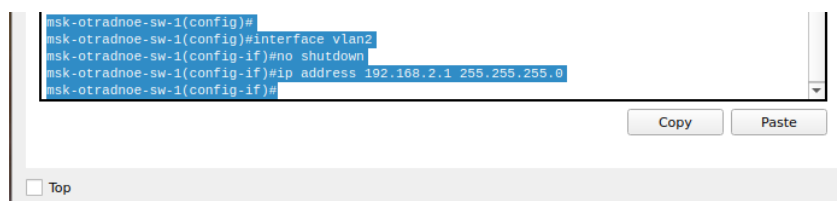


Рис. 3.8: Задание ip-адреса интерфейсу

Привяжем интерфейс Fast Ethernet с номером 1 к vlan 2 и зададим в качестве адреса шлюза по умолчанию адрес 192.168.2.254 (рис. 3.9):

```

msk-otradnoe-sw-1(config)#interface f0/1
msk-otradnoe-sw-1(config-if)#switchport mode access
msk-otradnoe-sw-1(config-if)#switchport access access vlan 2
                                     ^
% Invalid input detected at '^' marker.

msk-otradnoe-sw-1(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
msk-otradnoe-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

msk-otradnoe-sw-1(config-if)#exit
msk-otradnoe-sw-1(config)#ip default-gateway 192.168.2.254
                                     ^
% Invalid input detected at '^' marker.

msk-otradnoe-sw-1(config)#ip default-gateway 192.168.2.254
msk-otradnoe-sw-1(config)#line vty 0 4

```

Рис. 3.9: Привязка интерфейса и задание адреса шлюза

Также зададим пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном), для пользователя admin задать доступ 1-го уровня по паролю (рис. 3.10):

```

msk-otradnoe-sw-1(config)#line console 0
msk-otradnoe-sw-1(config-line)#password cisco
msk-otradnoe-sw-1(config-line)#login
msk-otradnoe-sw-1(config-line)#exit
msk-otradnoe-sw-1(config)#enable secret cisco
msk-otradnoe-sw-1(config)#service password-encryption
msk-otradnoe-sw-1(config)#username admin privilege 1 secret cisco

```

Рис. 3.10: Задание пароля в двух видах

Настроим доступ к оборудованию через ssh (используя в качестве имени домена donskaya.rudn.edu) (рис. 3.11):

```

msk-otradnoe-sw-1(config)#ip domain-name donskaya.rudn.edu
msk-otradnoe-sw-1(config)#crypto key generate rsa
The name for the keys will be: msk-otradnoe-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]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

msk-otradnoe-sw-1(config)#line vty 0 4
*Mar 1 0:19:36.336: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:19:36.336: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-otradnoe-sw-1(config-line)#transport input ssh
msk-otradnoe-sw-1(config-line)#

```

Рис. 3.11: Настройка доступа

Сохраним и экспортируем конфигурацию коммутатора (рис. 3.12):

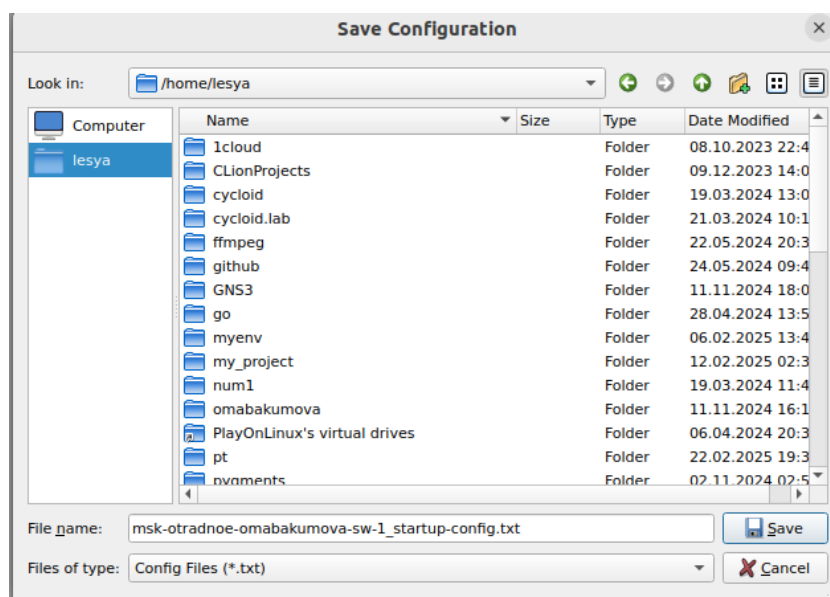


Рис. 3.12: Сохранение конфигурации коммутатора

Проверим работоспособность соединений с помощью команды **ping** (рис. 3.13):

```
lesya@lesya-Aspire-A115-32:~$ ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
 64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=2.64 ms
 64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=1.19 ms
 64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=3.06 ms
 64 bytes from 192.168.2.1: icmp_seq=4 ttl=64 time=5.92 ms
 64 bytes from 192.168.2.1: icmp_seq=5 ttl=64 time=2.54 ms
^C
--- 192.168.2.1 ping statistics ---
 5 packets transmitted, 5 received, 0% packet loss, time 4005ms
 rtt min/avg/max/mdev = 1.190/3.069/5.920/1.557 ms
```

Рис. 3.13: Пингование 192.168.2.1

```
lesya@lesya-Aspire-A115-32:~$ ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
 64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=4.70 ms
 64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=2.76 ms
 64 bytes from 192.168.1.254: icmp_seq=3 ttl=64 time=2.67 ms
 64 bytes from 192.168.1.254: icmp_seq=4 ttl=64 time=6.51 ms
 64 bytes from 192.168.1.254: icmp_seq=5 ttl=64 time=2.54 ms
```

Рис. 3.14: Пингование 192.168.1.254

Попробуем подключиться к коммутатору и маршрутизатору через ssh 3.15):


```
net offer: ssh-rsa,ssh-dss
lesya@lesya-Aspire-A115-32:~$ ssh -l admin 192.168.2.1
Unable to negotiate with 192.168.2.1 port 22: no matching host key type found. T
heir offer: ssh-rsa,ssh-dss
lesya@lesya-Aspire-A115-32:~$ ssh -l admin 192.168.1.254
Unable to negotiate with 192.168.1.254 port 22: no matching host key type found.
Their offer: ssh-rsa,ssh-dss
```

Рис. 3.15: Неудача

К сожалению, у меня не получилось подключиться по ssh к коммутатору и маршрутизатору ;(.

4 Контрольные вопросы

1. Укажите возможные способы подключения к сетевому оборудованию.

Возможные способы подключения к сетевому оборудованию включают: использование консольного кабеля (обычно RJ-45 к DB-9), подключение через Telnet, подключение через SSH, а также использование веб-интерфейса (если он поддерживается устройством).

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

Для подключения оконечного оборудования пользователя к маршрутизатору следует использовать кабель категории 5е или выше (например, Cat 6). Это связано с тем, что такие кабели обеспечивают достаточную скорость передачи данных и поддержку современных сетевых стандартов, таких как Ethernet.

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

Для подключения оконечного оборудования пользователя к коммутатору также рекомендуется использовать кабель категории 5е или выше (например, Cat 6). Это необходимо для обеспечения высокой скорости передачи данных и надежной работы в локальной сети.

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

Для подключения коммутатора к коммутатору лучше использовать опто-

волоконные кабели или медные кабели категории 6 и выше (например, Cat 6a), особенно если нужно обеспечить высокую пропускную способность на больших расстояниях. Оптоволоконные кабели обеспечивают большую дальность и пропускную способность, что делает их предпочтительными для межкоммутаторных соединений.

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

Возможные способы настройки доступа к сетевому оборудованию по паролю включают установку пароля на консольный доступ, настройку пароля для VTY-линий (для Telnet/SSH) и использование аутентификации через протоколы, такие как RADIUS или TACACS+.

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

Возможные способы настройки удалённого доступа к сетевому оборудованию включают Telnet и SSH. SSH является предпочтительным способом, так как он обеспечивает шифрование данных, что делает соединение более безопасным по сравнению с Telnet, который передает данные в открытом виде и подвержен перехвату.

5 Выводы

Во время выполнения данной лабораторной работы я получила основные навыки по начальному конфигурированию оборудования Cisco.