

Отчёт по лабораторной работе 2

Предварительная настройка оборудования Cisco

Седохин Даниил Алексеевич

Содержание

1 Цель работы	5
2 Задание	6
3 Выполнение лабораторной работы	8
4 Контрольные вопросы	15
5 Выводы	17

Список иллюстраций

3.1	Воспроизведение топологии сети с двумя оконечными устройствами, маршрутизатором и коммутатором	8
3.2	Настройка маршрутизатора	10
3.3	Настройка коммутатора	12
3.4	Проверка работоспособности соединений с помощью команды ping .	12
3.5	Подключение к маршрутизатору по протоколу удаленного доступа telnet и ssh	13
3.6	Подключение к коммутатору по протоколу удаленного доступа telnet и ssh	14

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_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.

2. Сделать предварительную настройку коммутатора:

задать имя в виде «город-территория-учётная_записьтип_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 экспорттировать 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).

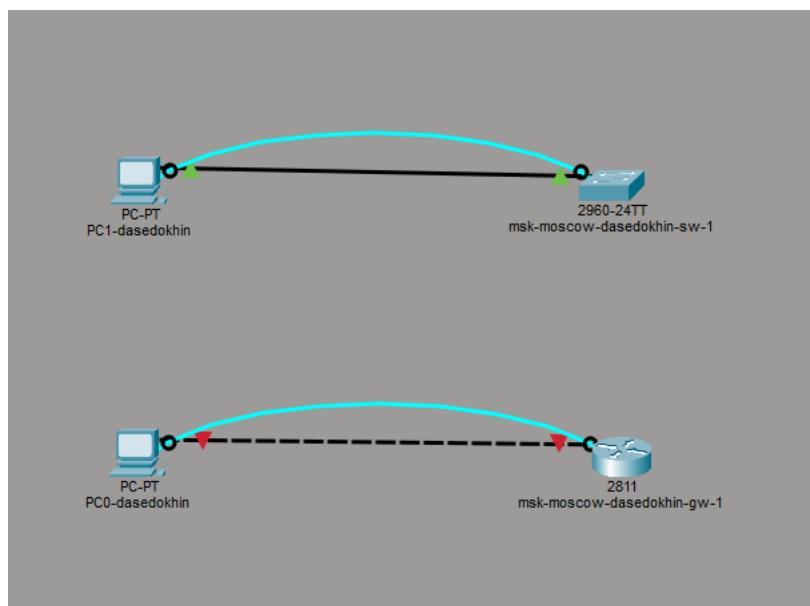


Рисунок 3.1: Воспроизведение топологии сети с двумя оконечными устройствами, маршрутизатором и коммутатором

Проведите настройку маршрутизатора в соответствии с заданием, ориентируясь на приведённую ниже часть конфигурации маршрутизатора.

Ниже приведены команды, для первичной настройки маршрутизатора:

Router >enable

Router#configure terminal

```
Router(config)#hostname msk-donskaya -gw-1
msk-donskaya -gw -1(config)#interface f0/0
msk-donskaya -gw -1(config -if)#no shutdown
msk-donskaya -gw -1(config -if)#ip address 192.168.1.254 255.255.255.0
msk-donskaya -gw -1(config)#line vty 0 4
msk-donskaya -gw -1(config -line)#password cisco
msk-donskaya -gw -1(config -line)#login
msk-donskaya -gw -1(config)#line console 0
msk-donskaya -gw -1(config -line)#password cisco
msk-donskaya -gw -1(config -line)#login
msk-donskaya -gw -1(config)#enable secret cisco
msk-donskaya -gw -1(config)#service password -encryption
msk-donskaya -gw -1(config)#username admin privilege 1 secret cisco
msk-donskaya -gw -1(config)#ip domain -name donskaya.rudn.edu
msk-donskaya -gw -1(config)#crypto key generate rsa
msk-donskaya -gw -1(config)#line vty 0 4
msk-donskaya -gw -1(config -line)#transport input ssh (рис. 3.2).
```

```

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

msk-moscow-dasedokhin-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-moscow-dasedokhin-gw-1(config-if)#ip address 192.168.1.254 255.255.255.0
msk-moscow-dasedokhin-gw-1(config-if)#line vty 0 4
msk-moscow-dasedokhin-gw-1(config-line)#password cisco
msk-moscow-dasedokhin-gw-1(config-line)#login
msk-moscow-dasedokhin-gw-1(config-line)#
*SYS-5-CONFIG_I: Configured from console by console

msk-moscow-dasedokhin-gw-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
msk-moscow-dasedokhin-gw-1(config)#line console 0
msk-moscow-dasedokhin-gw-1(config)#password cisco
msk-moscow-dasedokhin-gw-1(config)#login
msk-moscow-dasedokhin-gw-1(config-line)#
*SYS-5-CONFIG_I: Configured from console by console

msk-moscow-dasedokhin-gw-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
msk-moscow-dasedokhin-gw-1(config)#enable secret cisco
msk-moscow-dasedokhin-gw-1(config)#service password-encryption
msk-moscow-dasedokhin-gw-1(config)#username admin privilege 1 secret cisco
msk-moscow-dasedokhin-gw-1(config)#ip domain-name moscow.rudn.edu
msk-moscow-dasedokhin-gw-1(config)#crypto key generate rsa
The name for the keys will be: msk-moscow-dasedokhin-gw-1.moscow.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-moscow-dasedokhin-gw-1(config)#line vty 0 4
*Mar 1 0:8:45.973: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:8:45.973: SSH-5-ENABLED: SSH 1.5 has been enabled
msk-moscow-dasedokhin-gw-1(config-line)#transport input ssh
msk-moscow-dasedokhin-gw-1(config-line)#

```

Рисунок 3.2: Настройка маршрутизатора

Проведите настройку коммутатора в соответствии с заданием, ориентируясь на приведённую ниже часть конфигурации коммутатора.

Ниже приведены команды, для первичной настройки коммутатора:

Switch >enable

Switch#configure terminal

Switch(config)#hostname msk-donskaya -sw-1

msk-donskaya -sw -1(config)#interface vlan2

msk-donskaya -sw -1(config -if)#no shutdown

msk-donskaya -sw -1(config -if)#ip address 192.168.2.1 255.255.255.0

msk-donskaya -sw -1(config)#interface f0/1

```
msk-donskaya -sw -1(config-if)#switchport mode access
msk-donskaya -sw -1(config-if)#switchport access vlan 2
msk-donskaya -sw -1(config)#ip default-gateway 192.168.2.254
msk-donskaya -sw -1(config)#line vty 0 4
msk-donskaya -sw -1(config-line)#password cisco
msk-donskaya -sw -1(config-line)#login
msk-donskaya -sw -1(config)#line console 0
msk-donskaya -sw -1(config-line)#password cisco
msk-donskaya -sw -1(config-line)#login
msk-donskaya -sw -1(config)#enable secret cisco
msk-donskaya -sw -1(config)#service password-encryption
msk-donskaya -sw -1(config)#username admin privilege 1 secret cisco
msk-donskaya -sw -1(config)#ip domain-name donskaya.rudn.edu
msk-donskaya -sw -1(config)#crypto key generate rsa
msk-donskaya -sw -1(config)#line vty 0 4
msk-donskaya -sw -1(config-line)#transport input ssh (рис. 3.3).
```

```
msk-moscow-dasedokhin-sw1

Physical Config CLI Attributes

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname msk-moscow-dasedokhin-sw1
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.2.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch#configure terminal
Switch#interface Vlan1
Switch(config-if)#ip address 192.168.2.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch#LINK-0-CHANGED: Interface Vlan1, changed state to up

msk-moscow-dasedokhin-sw1(config)#no shutdown
msk-moscow-dasedokhin-sw1(config)#ip address 192.168.2.1 255.255.255.0
msk-moscow-dasedokhin-sw1(config)#exit
Switch#configure terminal
Switch#interface Vlan1
Switch(config-if)#ip address 192.168.2.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch#LINK-0-CHANGED: Interface Vlan1, changed state to up

*SYS-6-CONFIG_I: Configured from console by console

msk-moscow-dasedokhin-sw1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
msk-moscow-dasedokhin-sw1(config)#interface F0/1
msk-moscow-dasedokhin-sw1(config-if)#switchport mode access
msk-moscow-dasedokhin-sw1(config-if)#switchport access vlan 2
msk-moscow-dasedokhin-sw1(config-if)#exit
*LINEPROTO-0-UPDOWN: Line protocol on Interface Vlan2, changed state to up

msk-moscow-dasedokhin-sw1(config)#no shutdown
msk-moscow-dasedokhin-sw1#exit
*SYS-6-CONFIG_I: Configured from console by console

msk-moscow-dasedokhin-sw1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
msk-moscow-dasedokhin-sw1(config)#ip default-gateway 192.168.2.254
^
* Invalid input detected at '^' marker.

msk-moscow-dasedokhin-sw1(config)#ip default-gateway 192.168.2.254
msk-moscow-dasedokhin-sw1(config)#line vty 0 4
msk-moscow-dasedokhin-sw1(config-line)#password cisco
msk-moscow-dasedokhin-sw1(config-line)#login
msk-moscow-dasedokhin-sw1(config-line)#secret
msk-moscow-dasedokhin-sw1#exit
*SYS-6-CONFIG_I: Configured from console by console

msk-moscow-dasedokhin-sw1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
msk-moscow-dasedokhin-sw1(config)#line console 0
msk-moscow-dasedokhin-sw1(config-line)#password cisco
msk-moscow-dasedokhin-sw1(config-line)#login
msk-moscow-dasedokhin-sw1(config-line)#secret
msk-moscow-dasedokhin-sw1#exit
*SYS-6-CONFIG_I: Configured from console by console

configure terminal
Configure terminal#2

msk-moscow-dasedokhin-sw1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
msk-moscow-dasedokhin-sw1(config)#enable secret cisco
msk-moscow-dasedokhin-sw1(config)#service password-encryption
msk-moscow-dasedokhin-sw1(config)#username admin privilege 1 secret cisco
msk-moscow-dasedokhin-sw1(config)#domainname mskov.rudn.edu
msk-moscow-dasedokhin-sw1(config)#key-size 1024
The name for the keys will be: msk-moscow-dasedokhin-sw1.mskov.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-moscow-dasedokhin-sw1(config)#line vty 0 4
```

Рисунок 3.3: Настройка коммутатора

Проверьте работоспособность соединений с помощью команды ping. (рис. 3.4).

```
PC0-daseddohin
rassword:
mak-moccor-daseddohin-rv-1ping 192.168.1.254
Type escape sequence to abort.
Sending 8, 100-byte ICMP Echos to 192.168.1.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (6/6), round-trip min/avg/max = 0/1.8 ms
mak-moccor-daseddohin-rv-1

PC1-daseddohin
rassword:
mak-moccor-daseddohin-rv-1ping 192.168.2.1
Type escape sequence to abort.
Sending 8, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4.7 ms
mak-moccor-daseddohin-rv-1


```

Рисунок 3.4: Проверка работоспособности соединений с помощью команды ping

Попробуем подключиться к коммутатору и маршрутизатору по протоколу удалённого доступа (telnet, ssh). Для подключения по протоколу удаленного доступа telnet предварительно изменили конфигурацию и добавили этот протокол помимо ранее добавленного протокола ssh. (рис. 3.5).

The screenshot shows a terminal window titled "Terminal" within a software interface titled "PC0-dasedokhin". The window displays the following text:

```
Enter configuration commands, one per line. End with CNTL/Z.  
mask-moscow-dasedokhin-gw-1(config)#line vty 0 4  
mask-moscow-dasedokhin-gw-1(config-line)#transport input all  
mask-moscow-dasedokhin-gw-1(config-line)#password cisco  
mask-moscow-dasedokhin-gw-1(config-line)#login  
mask-moscow-dasedokhin-gw-1(config-line)#end  
mask-moscow-dasedokhin-gw-1#  
*SYS-5-CONNIG_1: Configured from console by console  
  
mask-moscow-dasedokhin-gw-1#show running-config | section line vty  
line vty 0 4  
  password 7 0822455D0A16  
  login  
mask-moscow-dasedokhin-gw-1#telnet 192.168.1.254  
Trying 192.168.1.254 ...Open  
  
User Access Verification  
  
Password:  
Password:  
mask-moscow-dasedokhin-gw-1>exit  
  
[Connection to 192.168.1.254 closed by foreign host]  
mask-moscow-dasedokhin-gw-1#ssh -l admin 192.168.1.254  
  
Password:  
  
Password:  
  
mask-moscow-dasedokhin-gw-1>exit  
  
[Connection to 192.168.1.254 closed by foreign host]  
mask-moscow-dasedokhin-gw-1#
```

Рисунок 3.5: Подключение к маршрутизатору по протоколу удаленного доступа telnet и ssh

Аналогичные действия для подключения по протоколам удаленного доступа telnet и ssh, добавив протокол telnet в разделе конфигураций на коммутаторе. (рис. 3.6).

The screenshot shows a terminal window titled "Terminal" with the following content:

```
msk-moscow-dasedokhin-sw-1#show running-config | section line vty
line vty 0 4
password 7 0822455D0A16
login
transport input ssh
line vty 5 15
login
msk-moscow-dasedokhin-sw-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
msk-moscow-dasedokhin-sw-1(config)#line vty 0 4
msk-moscow-dasedokhin-sw-1(config-line)#transport input all
msk-moscow-dasedokhin-sw-1(config-line)#password cisco
msk-moscow-dasedokhin-sw-1(config-line)#login
msk-moscow-dasedokhin-sw-1(config-line)#end
msk-moscow-dasedokhin-sw-1#
SYS-5-CONFIG_I: Configured from console by console

msk-moscow-dasedokhin-sw-1#show running-config | section line vty
line vty 0 4
password 7 0822455D0A16
login
line vty 5 15
login
msk-moscow-dasedokhin-sw-1#telnet 192.168.2.1
Trying 192.168.2.1 ...Open

User Access Verification

Password:
msk-moscow-dasedokhin-sw-1>exit
[Connection to 192.168.2.1 closed by foreign host]
msk-moscow-dasedokhin-sw-1#ssh -l admin 192.168.2.1
Password:

msk-moscow-dasedokhin-sw-1>exit
[Connection to 192.168.2.1 closed by foreign host]
msk-moscow-dasedokhin-sw-1#
```

Рисунок 3.6: Подключение к коммутатору по протоколу удаленного доступа telnet и ssh

4 Контрольные вопросы

1. Возможные способы подключения к сетевому оборудованию: Консольное подключение (console) — через консольный порт с использованием консольного кабеля (обычно RS-232 к RJ-45) для первоначальной настройки

Удалённое подключение через сеть:

Telnet — нешифрованное подключение (порт 23)

SSH — защищённое шифрованное подключение (порт 22)

HTTP/HTTPS — через веб-интерфейс (если поддерживается)

2. Подключение оконечного оборудования к маршрутизатору: Прямой кабель (Straight-through)

Почему: Маршрутизатор (как DTE-устройство) и PC (как DTE) соединяются через промежуточное устройство, но в данном случае маршрутизатор выступает в роли концентратора сети, и его порт настроен как MDI-X (или используется автоопределение). Прямой кабель используется при соединении разнотипных устройств (DTE к DCE).

3. Подключение оконечного оборудования к коммутатору: Прямой кабель (Straight-through)

Почему: Коммутатор имеет порты MDI-X (Auto-MDIX), а PC имеет порт MDI. Прямой кабель используется для соединения разнотипных интерфейсов (MDI к MDI-X).

4. Подключение коммутатора к коммутатору: Перекрёстный кабель (Crossover)

Почему: При соединении однотипных устройств (коммутатор-коммутатор) используются порты одного типа (MDI-X к MDI-X), поэтому требуется перекрёстный кабель. Однако в современном оборудовании с поддержкой Auto-MDIX можно использовать и прямой кабель, так как устройства автоматически определяют тип соединения.

5. Способы настройки доступа к сетевому оборудованию по паролю: Пароль на консоль (line console 0): для доступа через консольный порт

Пароль на виртуальные терминалы (line vty): для удалённого доступа (Telnet/SSH)

Пароль на привилегированный режим (enable password/enable secret): для доступа к режиму глобальной конфигурации

Локальная база пользователей (username/password): для аутентификации при удалённом доступе (особенно для SSH)

Шифрование паролей (service password-encryption): для защиты паролей в конфигурационном файле

6. Способы настройки удалённого доступа и предпочтительный вариант:

Способы удалённого доступа:

Telnet: передача данных и паролей в открытом (незашифрованном) виде

SSH (Secure Shell): все данные шифруются, включая пароли

Предпочтительный способ: SSH

Почему:

Безопасность: все данные шифруются, включая пароли (в Telnet пароли передаются в открытом виде)

Аутентификация: поддерживает как парольную, так и ключевую аутентификацию

Целостность данных: гарантирует, что данные не были изменены во время передачи

Конфиденциальность: защищает от перехвата трафика

5 Выводы

Я получил основные навыки по начальному конфигурированию оборудования Cisco.