

Лабораторная работа №2

Предварительная настройка оборудования Cisco

Беличева Дарья Михайловна

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	7
3.1	Настройка маршрутизатора	8
3.2	Настройка коммутатора	14
4	Выводы	18
5	Контрольные вопросы	19

Список иллюстраций

3.1	Схема подключения оборудования для проведения его предвари- тельной настройки	7
3.2	Задание статического ip-адреса PC0	8
3.3	Задание имени оборудованию	8
3.4	Задание интерфейсу Fast Ethernet с номером 0 ip-адреса	9
3.5	Проверка соединения с помощью команды ping	9
3.6	Задание паролей	10
3.7	Просмотр паролей	11
3.8	Шифрование паролей	11
3.9	Просмотр зашифрованных паролей	12
3.10	Задание доступа 1-го уровня по паролю пользователю admin . . .	12
3.11	Настройка доступа через telnet и ssh	13
3.12	Проверка работы доступа через telnet и ssh	13
3.13	Сохранение конфигурации	14
3.14	Задание статического ip-адреса PC2	14
3.15	Задание имени оборудованию	15
3.16	Привязка интерфейса Fast Ethernet с номером 1 к vlan 2	15
3.17	Задание в качестве адреса шлюза адрес 192.168.2.254	15
3.18	Проверка соединения с помощью команды ping	16
3.19	Задание и шифрование паролей	16
3.20	Задание доступа 1-го уровня по паролю пользователю admin . . .	16
3.21	Настройка доступа через telnet и ssh	17
3.22	Проверка работы доступа через telnet и ssh	17
3.23	Сохранение конфигурации	17

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»;
- 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, соединим один PC с маршрутизатором консольным и кроссовым кабелем, другой PC — с коммутатором консольным и прямым кабелем (рис. [3.1]).

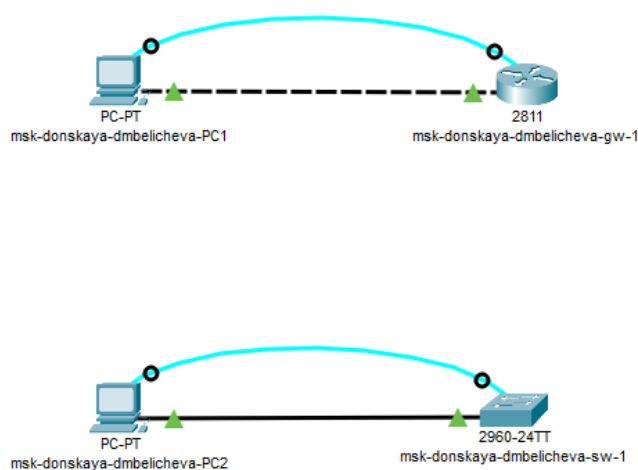


Рис. 3.1: Схема подключения оборудования для проведения его предварительной настройки

Для начала зададим статический ip-адрес PC0 192.168.1.10 с соответствующей маской подсети 255.255.255.0 (рис. [3.2]).

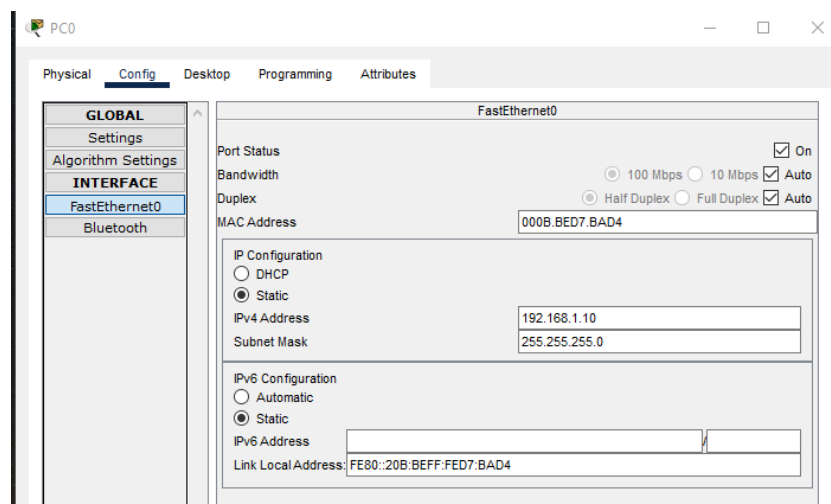


Рис. 3.2: Задание статического ip-адреса PC0

3.1 Настройка маршрутизатора

Теперь проведем настройку маршрутизатора в соответствии с заданием. Откроем Command Line Interface (CLI) у маршрутизатора, который идентичен терминалу ПК. Для перехода в привилегированный режим из пользовательского режима воспользуемся командой `enable`. А для перехода в режим глобальной конфигурации из привилегированного режима используем команду `configure terminal` или её сокращённый аналог `conf t`. И в этом режиме зададим имя хоста, введя команду `hostname msk-donskaya -gw-1` (рис. [3.3]).

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host
Router(config)#hostname msk-donskaya-dmbelicheva-gw-1
```

Рис. 3.3: Задание имени оборудованию

Зададим интерфейсу Fast Ethernet с номером 0 ip-адрес 192.168.1.254 и маску 255.255.255.0, затем поднимем интерфейс командой `no shutdown` (рис. [3.4]).


```

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

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

```

Рис. 3.4: Задание интерфейсу Fast Ethernet с номером 0 ip-адреса

Проверим работоспособность соединения с помощью команды ping. Увидим, что было послано 4 пакета и принято тоже 4, потерь нет. Так что соединение успешно работает (рис. [3.5]).

```

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=13ms 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 = 13ms, Average = 3ms

```

Рис. 3.5: Проверка соединения с помощью команды ping

Зададим пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном). Зададим пароль для доступа к терминалу, к консоли, и поставим пароль на enable (привилегированным режим) (рис. [3.6]).

```

msk-donskaya-dmbelicheva-gw-1(config)#line vty 0 4
msk-donskaya-dmbelicheva-gw-1(config-line)#password cisco
msk-donskaya-dmbelicheva-gw-1(config-line)#login
msk-donskaya-dmbelicheva-gw-1(config-line)#^Z
msk-donskaya-dmbelicheva-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-dmbelicheva-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-dmbelicheva-gw-1(config)#line console 0
msk-donskaya-dmbelicheva-gw-1(config-line)#password cisco
msk-donskaya-dmbelicheva-gw-1(config-line)#login
msk-donskaya-dmbelicheva-gw-1(config-line)#^Z
msk-donskaya-dmbelicheva-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-dmbelicheva-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-dmbelicheva-gw-1(config)#enable secret cisco

```

Рис. 3.6: Задание паролей

Если использовать команду `secret`, то пароль сразу будет зашифрованным. Но там, где мы использовали команду `password` пароль не скрыт, и любой может его посмотреть (рис. [3.7]).

```

interface Vlan1
  no ip address
  shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
  password cisco
  login
!
line aux 0
!
line vty 0 4
  password cisco
  login
!
!
!

```

Рис. 3.7: Просмотр паролей

Чтобы это исправить, надо зашифровать наши пароли с помощью команды `service password -encryption` (рис. [3.8]).

```

msk-donskaya-dmbelicheva-gw-1#
msk-donskaya-dmbelicheva-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-dmbelicheva-gw-1(config)#service password-encryption
msk-donskaya-dmbelicheva-gw-1(config)#ur m

```

Рис. 3.8: Шифрование паролей

Проверим, что пароли зашифрованы (рис. [3.9]):

```

.
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
  password 7 0822455D0A16
  login
!
line aux 0
!
line vty 0 4
  password 7 0822455D0A16
  login
  transport input ssh
!
!
!
end

```

Рис. 3.9: Просмотр зашифрованных паролей

В качестве дополнительного уровня защиты для пользователя admin зададим доступ 1-го уровня по паролю (рис. [3.10]).

```
msk-donskaya-dmbelicheva-gw-1(config)#username admin privilege 1 secret cisco
```

Рис. 3.10: Задание доступа 1-го уровня по паролю пользователю admin

Теперь настроим доступ к оборудованию сначала через telnet, затем — через ssh (используя в качестве имени домена donsкаya.rudn.edu) (рис. [3.11]).

```

msk-donskaya-dmbelicheva-gw-1(config)#ip domain name donsкаya.rudn.edu
msk-donskaya-dmbelicheva-gw-1(config)#crypto key generate rsa
The name for the keys will be: msk-donskaya-dmbelicheva-gw-1.donsкаya.rudn.edu
Choose the size of the key modulus in the range of 360 to 2048 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-dmbelicheva-gw-1(config)#line vty 0 4
*Mar 1 1:5:20.11: %SSH-5-ENABLED: SSH 1.99 has been enabled
msk-donskaya-dmbelicheva-gw-1(config-line)#transport input ?
% Unrecognized command
msk-donskaya-dmbelicheva-gw-1(config-line)#transport input ?
all      All protocols
none     No protocols
ssh      TCP/IP SSH protocol
telnet   TCP/IP Telnet protocol
msk-donskaya-dmbelicheva-gw-1(config-line)#transport input ssh

```

Рис. 3.11: Настройка доступа через telnet и ssh

Так как мы оставили возможным доступ только через ssh, то при попытке доступа через telnet нам будет отказано. А при доступе через ssh запрашивается пароль, как и должен, и доступ успешно предоставляется (рис. [3.12]).

```

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

[Connection to 192.168.1.254 closed by foreign host]
C:\>ssh 192.168.1.254
Invalid Command.

C:\>ssh -l admin 192.168.1.254

Password:

msk-donskaya-dmbelicheva-gw-1>en
Password:
msk-donskaya-dmbelicheva-gw-1#

```

Рис. 3.12: Проверка работы доступа через telnet и ssh

Наконец сохраним нашу конфигурацию маршрутизатора (рис. [3.13]).

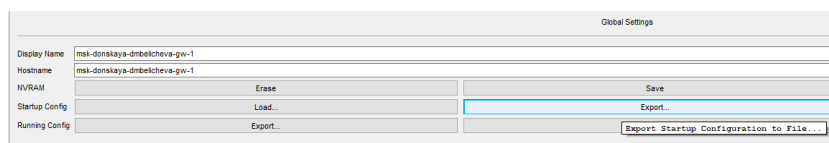


Рис. 3.13: Сохранение конфигурации

3.2 Настройка коммутатора

Для начала зададим статический IP-адрес PC0 192.168.2.10 с соответствующей маской подсети 255.255.255.0 (рис. [3.14]).

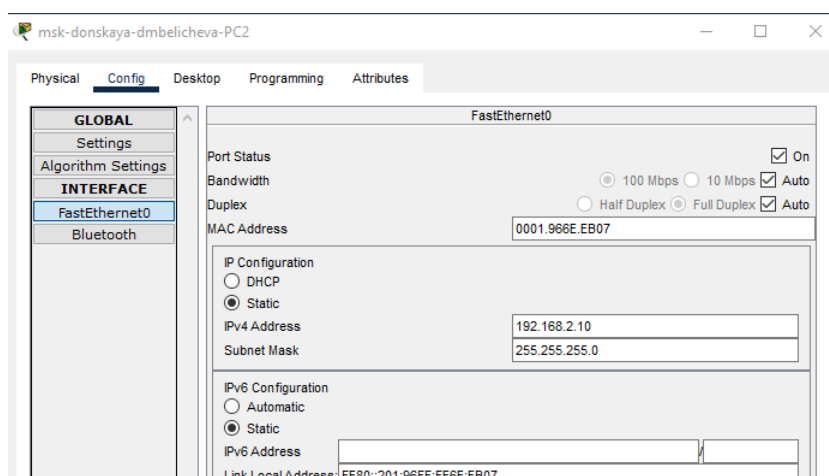


Рис. 3.14: Задание статического IP-адреса PC2

Теперь проведем настройку коммутатора в соответствии с заданием. Откроем Command Line Interface (CLI) у маршрутизатора, который идентичен терминалу ПК. Для перехода в привилегированный режим из пользовательского режима воспользуемся командой `enable`. А для перехода в режим глобальной конфигурации из привилегированного режима используем команду `configure terminal` или её сокращённый аналог `conf t`. И в этом режиме зададим имя хоста, введя команду `hostname msk-donskaya-gw-1`. Также зададим интерфейсу Fast Ethernet с номером 0 IP-адрес 192.168.1.254 и маску 255.255.255.0, затем поднимем интерфейс командой `no shutdown` (рис. [3.15]).

```

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

```

Рис. 3.15: Задание имени оборудованию

Привяжем интерфейс Fast Ethernet с номером 1 к vlan 2 (рис. [3.18]).

```

msk-donskaya-dmbelicheva-sw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-dmbelicheva-sw-1(config)#interface f0/1
msk-donskaya-dmbelicheva-sw-1(config-if)#switchport mode access
msk-donskaya-dmbelicheva-sw-1(config-if)#switchport access vlan2
^
% Invalid input detected at '^' marker.

msk-donskaya-dmbelicheva-sw-1(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
msk-donskaya-dmbelicheva-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. 3.16: Привязка интерфейса Fast Ethernet с номером 1 к vlan 2

И зададим в качестве адреса шлюза по умолчанию адрес 192.168.2.254 (рис. [3.17]).

```

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

```

Рис. 3.17: Задание в качестве адреса шлюза адрес 192.168.2.254

Проверим работоспособность соединения с помощью команды ping. Увидим, что было послано 4 пакета и принято тоже 4, потерь нет. Так что соединение успешно работает (рис. [??]).

```

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 = 1ms, Average = 0ms
C:\>

```

Рис. 3.18: Проверка соединения с помощью команды ping

Зададим пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном). Зададим пароль для доступа к терминалу, к консоли, и поставим пароль на enable (привилегированным режим). Зашифруем наши пароли с помощью команды `service password -encryption` (рис. [3.19]).

```

msk-donskaya-dmbelicheva-sw-1(config)#line vty 0 4
msk-donskaya-dmbelicheva-sw-1(config-line)#password cisco
msk-donskaya-dmbelicheva-sw-1(config-line)#login
msk-donskaya-dmbelicheva-sw-1(config-line)#^Z
msk-donskaya-dmbelicheva-sw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-dmbelicheva-sw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-dmbelicheva-sw-1(config)#line console 0\
^
% Invalid input detected at '^' marker.

msk-donskaya-dmbelicheva-sw-1(config)#line console 0
msk-donskaya-dmbelicheva-sw-1(config-line)#password cisco
msk-donskaya-dmbelicheva-sw-1(config-line)#login
msk-donskaya-dmbelicheva-sw-1(config-line)#^Z
msk-donskaya-dmbelicheva-sw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-dmbelicheva-sw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-dmbelicheva-sw-1(config)#enable secret cisco
msk-donskaya-dmbelicheva-sw-1(config)#service password-encryption

```

Рис. 3.19: Задание и шифрование паролей

В качестве дополнительного уровня защиты для пользователя admin зададим доступ 1-го уровня по паролю (рис. [3.20]).

```

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

```

Рис. 3.20: Задание доступа 1-го уровня по паролю пользователю admin

Теперь настроим доступ к оборудованию сначала через telnet, затем — через ssh (используя в качестве имени домена `donskaya.rudn.edu`) (рис. [3.21]).

```
msk-donskaya-dmbelicheva-sw-1(config)#ip domain name donsкаya.rudn.edu
msk-donskaya-dmbelicheva-sw-1(config)#crypto key generate rsa
The name for the keys will be: msk-donskaya-dmbelicheva-sw-1.donskaya.rudn.edu
Choose the size of the key modulus in the range of 360 to 2048 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-dmbelicheva-sw-1(config)#line vty 0 4
*Mar 1 1:56:55.667: %SSH-5-ENABLED: SSH 1.99 has been enabled
msk-donskaya-dmbelicheva-sw-1(config-line)#transport input ?
all      All protocols
none     No protocols
ssh      TCP/IP SSH protocol
telnet   TCP/IP Telnet protocol
msk-donskaya-dmbelicheva-sw-1(config-line)#transport input ssh
msk-donskaya-dmbelicheva-sw-1(config-line)#
```

Рис. 3.21: Настройка доступа через telnet и ssh

Так как мы оставили возможным доступ только через ssh, то при попытке доступа через telnet нам будет отказано. А при доступе через ssh запрашивается пароль, как и должен, и доступ успешно предоставляется (рис. [3.22]).

```
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-dmbelicheva-sw-1>enable
Password:
msk-donskaya-dmbelicheva-sw-1#
```

Рис. 3.22: Проверка работы доступа через telnet и ssh

Наконец сохраним нашу конфигурацию маршрутизатора (рис. [3.23]).

Global Settings		
Display Name	msk-donskaya-dmbelicheva-sw-1	
Hostname	msk-donskaya-dmbelicheva-sw-1	
Serial Number	Serial Number	
NVRAM	Erase	Save
Startup Config	Load...	Export...
Running Config	Export...	Export Startup Configuration to File...

Рис. 3.23: Сохранение конфигурации

4 Выводы

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

5 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 одиночного 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.