

Лабораторная работа № 2

Предварительная настройка оборудования Cisco

Замбалова Дина Владимировна

Содержание

Цель работы	2
Задание.....	2
Выполнение лабораторной работы.....	2
Настройка маршрутизатора	3
Настройка коммутатора	6
Выводы.....	8
Контрольные вопросы	8

Список иллюстраций

Схема подключения оборудования для проведения его предварительной настройки	3
Задание статического ip-адреса PC0.....	3
Задание имени оборудованию	4
Задание интерфейсу Fast Ethernet с номером 0 ip-адреса	4
Проверка соединения с помощью команды ping	4
Задание паролей	4
Шифрование паролей.....	4
Просмотр зашифрованных паролей	5
Задание доступа 1-го уровня по паролю пользователю admin.....	5
Настройка доступа через telnet и ssh	5
Проверка работы доступа через telnet и ssh	6
Задание статического ip-адреса PC2.....	6
Задание имени оборудованию	6
Привязка интерфейса Fast Ethernet с номером 1 к vlan 2	7
Задание в качестве адреса шлюза адрес 192.168.2.254	7
Проверка соединения с помощью команды ping	7
Задание и шифрование паролей	7
Задание доступа 1-го уровня по паролю пользователю admin.....	7
Настройка доступа через telnet и ssh	8
Проверка работы доступа через telnet и ssh	8

Цель работы

Получить основные навыки по начальному конфигурированию оборудования Cisco.

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.

Выполнение лабораторной работы

В логической рабочей области Packet Tracer разместим коммутатор, маршрутизатор и 2 конечных устройства типа PC, соединим один PC с маршрутизатором консольным и кроссовым кабелем, другой PC — с коммутатором консольным и прямым кабелем (рис. [-@fig:001]).

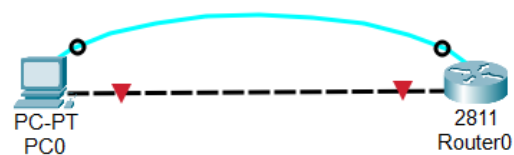
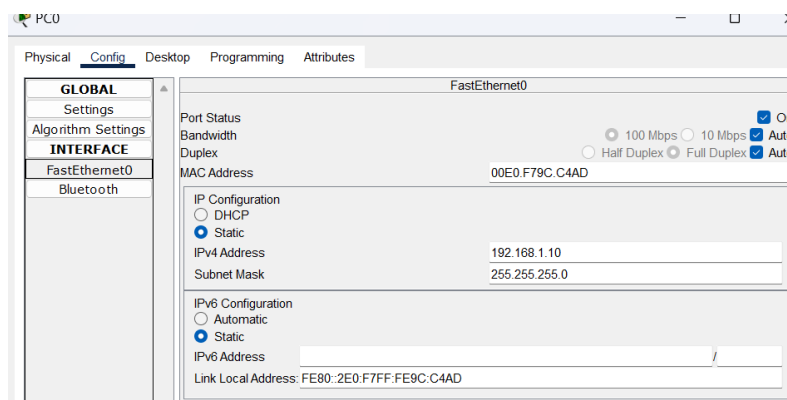


Схема подключения оборудования для проведения его предварительной настройки

Для начала зададим статический ip-адрес PC0 192.168.1.10 с соответствующей маской подсети 255.255.255.0 (рис. [-@fig:002]).



Задание статического ip-адреса PC0

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`. И в этом режиме зададим имя хоста, введя команду `hostname msk-donskaya-dvzambalova-gw-1` (рис. [-@fig:003]).

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

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. [-@fig:004]).

```
msk-donskaya-dvzambalova-gw-1(config)#interface f0/0
msk-donskaya-dvzambalova-gw-1(config-if)#no shutdown

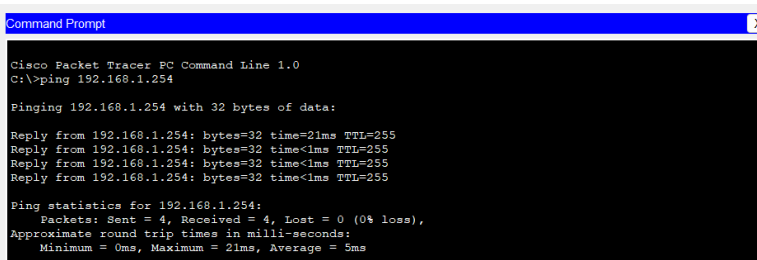
msk-donskaya-dvzambalova-gw-1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

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

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. [-@fig:005]).



```
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
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=21ms 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 = 21ms, Average = 5ms
```

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. [-@fig:006]).

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

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.

Чтобы это исправить, надо зашифровать наши пароли с помощью команды `service password-encryption` (рис. [-@fig:008]).

```
msk-donskaya-dvzambalova-gw-1(config)#service password-encryption
```

Шифрование паролей

Проверим, что пароли зашифрованы (рис. [-@fig:009]):

```

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

```

Просмотр зашифрованных паролей

В качестве дополнительного уровня защиты для пользователя admin зададим доступ 1-го уровня по паролю (рис. [-@fig:010]).

```

msk-donskaya-dvzambalova-gw-1(config)#username admin privilege 1 secret cisco
msk-donskaya-dvzambalova-gw-1(config)#end

```

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. [-@fig:011]).

```

msk-donskaya-dvzambalova-gw-1(config)#ip domain-name donsкаya.rudn.edu
msk-donskaya-dvzambalova-gw-1(config)#crypto key generate rsa
The name for the keys will be: msk-donskaya-dvzambalova-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]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
msk-donskaya-dvzambalova-gw-1(config)#line vty 0 4
*Mar 1 0:11:11.49: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:11:11.49: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-donskaya-dvzambalova-gw-1(config-line)#transport input ssh

```

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. [-@fig:012]).

```
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
Invalid Command.

C:\>ssh -l admin 192.168.1.254

Password:

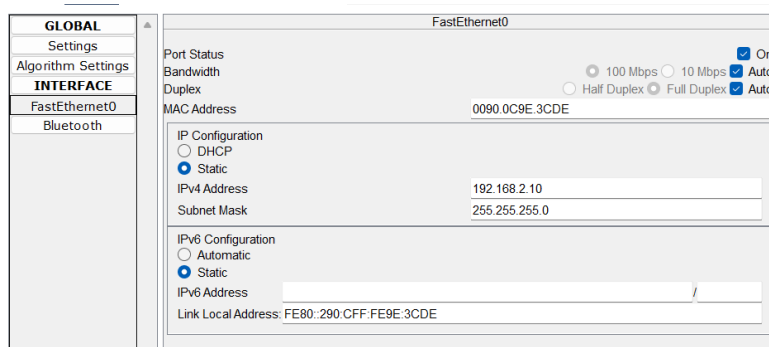
msk-donskaya-dvzambalova-gw-1>enable
Password:
msk-donskaya-dvzambalova-gw-1#exit

[Connection to 192.168.1.254 closed by foreign host]
C:\>
```

Проверка работы доступа через telnet и ssh

Настройка коммутатора

Для начала зададим статический ip-адрес PC1 192.168.2.10 с соответствующей маской подсети 255.255.255.0 (рис. [-@fig:014]).



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-dvzambalova-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. [-@fig:015]).

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

Задание имени оборудованию

Привяжем интерфейс Fast Ethernet с номером 1 к vlan 2 (рис. [-@fig:016]).

```

msk-donskaya-dvzambalova-sw-1(config)#interface f0/1
msk-donskaya-dvzambalova-sw-1(config-if)#switchport mode access
% Invalid input detected at '^' marker.
msk-donskaya-dvzambalova-sw-1(config-if)#switchport mode access
msk-donskaya-dvzambalova-sw-1(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
msk-donskaya-dvzambalova-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

```

Привязка интерфейса Fast Ethernet с номером 1 к vlan 2

И зададим в качестве адреса шлюза по умолчанию адрес 192.168.2.254 (рис. [-@fig:017]).

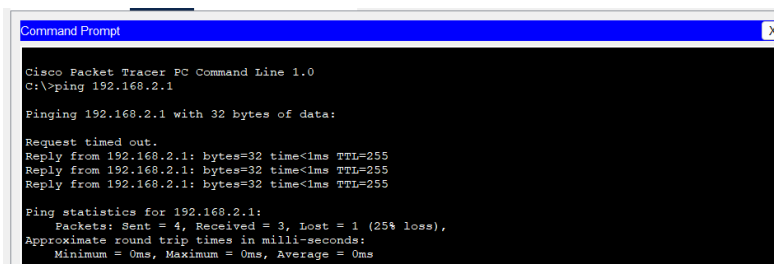
```

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

```

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. [-@fig:018]).



```

Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

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. [-@fig:019]).

```

msk-donskaya-dvzambalova-sw-1(config)#line vty 0 4
msk-donskaya-dvzambalova-sw-1(config-line)#password cisco
msk-donskaya-dvzambalova-sw-1(config-line)#login
msk-donskaya-dvzambalova-sw-1(config-line)#exit
msk-donskaya-dvzambalova-sw-1(config)#line console 0
msk-donskaya-dvzambalova-sw-1(config-line)#password cisco
msk-donskaya-dvzambalova-sw-1(config-line)#login
msk-donskaya-dvzambalova-sw-1(config-line)#exit
msk-donskaya-dvzambalova-sw-1(config)#enable secret cisco
msk-donskaya-dvzambalova-sw-1(config)#service password-encryption

```

Задание и шифрование паролей

В качестве дополнительного уровня защиты для пользователя admin зададим доступ 1-го уровня по паролю (рис. [-@fig:020]).

```

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

```

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. [-@fig:021]).

```

msk-donskaya-dvzambalova-sw-1(config)#ip domain-name donsкаya.rudn.edu
msk-donskaya-dvzambalova-sw-1(config)#crypto key generate rsa
The name for the keys will be: msk-donskaya-dvzambalova-sw-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]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
msk-donskaya-dvzambalova-sw-1(config)#line vty 0 4
*Mar 1 0:21:38.7: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:21:38.7: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-donskaya-dvzambalova-sw-1(config-line)#transport input ssh

```

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. [-@fig:022]).

```

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-dvzambalova-sw-1>enable
Password:
msk-donskaya-dvzambalova-sw-1#exit

[Connection to 192.168.2.1 closed by foreign host]
C:\>

```

Проверка работы доступа через telnet и ssh

Выводы

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

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.