

Лабораторная работа № 2

Предварительная настройка оборудования Cisco

Абд эль хай Мохамад

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	7
3.1	Конфигурация маршрутизатора	7
3.2	Конфигурация коммутатора	11
4	Выводы	15
5	Контрольные вопросы	16

Список иллюстраций

3.1	Схема подключения оборудования для проведения его предварительной настройки	7
3.2	router	8
3.3	ssh key router	9
3.4	Ping router	10
3.5	shh router	10
3.6	telnet router	11
3.7	switch conf	12
3.8	ping switch	13
3.9	ssh switch	13
3.10	telnet ssh	14
3.11	ping ssh	14

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» (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 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» (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 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 логическом рабочем пространстве Packet Tracer я разместил коммутатор, маршрутизатор и 2 конечных точки ПК, подключил один ПК к маршрутизатору, другой ПК к коммутатору.

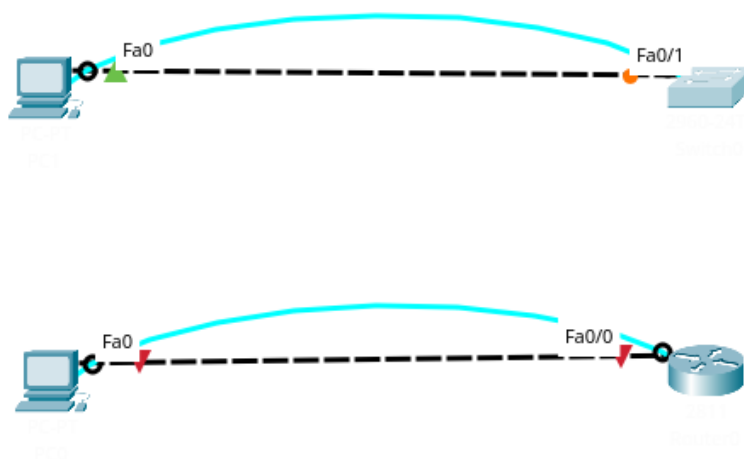


Рис. 3.1: Схема подключения оборудования для проведения его предварительной настройки

3.1 Конфигурация маршрутизатора

Установка имени хоста Команда: имя хоста msk-donnaya-gw-1 Эта команда устанавливает имя хоста маршрутизатора «msk-obruchevsky-gw-1».

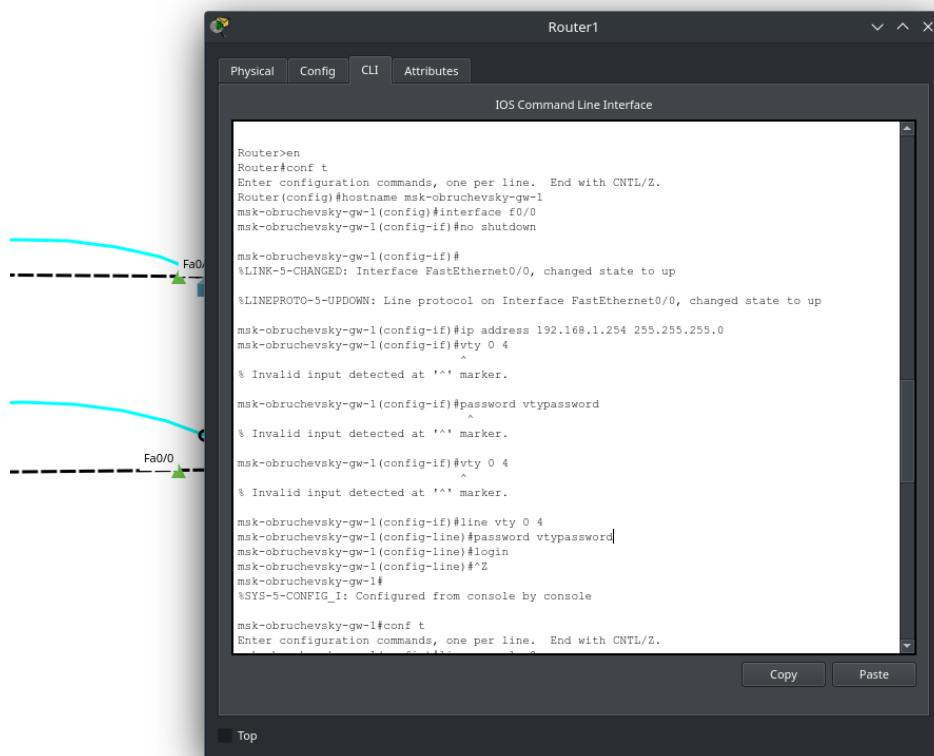


Рис. 3.2: router

Настройка интерфейса f0/0 Команды: `interface f0/0 no shutdown ip address 192.168.1.254 255.255.255.0` Эти команды включают интерфейс f0/0 и назначают этому интерфейсу IP-адрес 192.168.1.254 с маской подсети 255.255.255.0.

Эти команды устанавливают пароли для виртуального терминала (VTY) и линий консоли, включают секрет для привилегированного режима, шифруют пароли и создают пользователя «admin» с уровнем привилегий 1 и паролем «adminpassword».

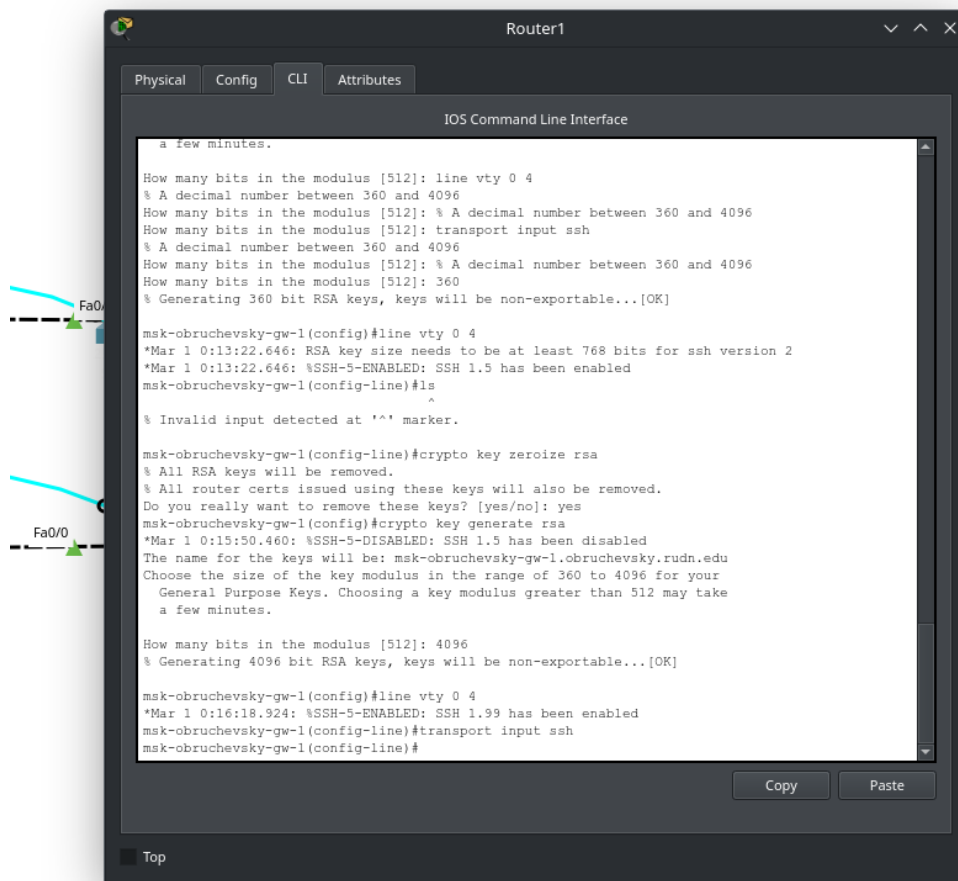


Рис. 3.3: ssh key router

Эти команды задают имя домена, генерируют пару ключей RSA для шифрования и настраивают SSH в качестве транспортного входа для линий VTY.

```
msk-obruchevsky-maabedelhay-sw-1>exit

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

Рис. 3.4: Ping router

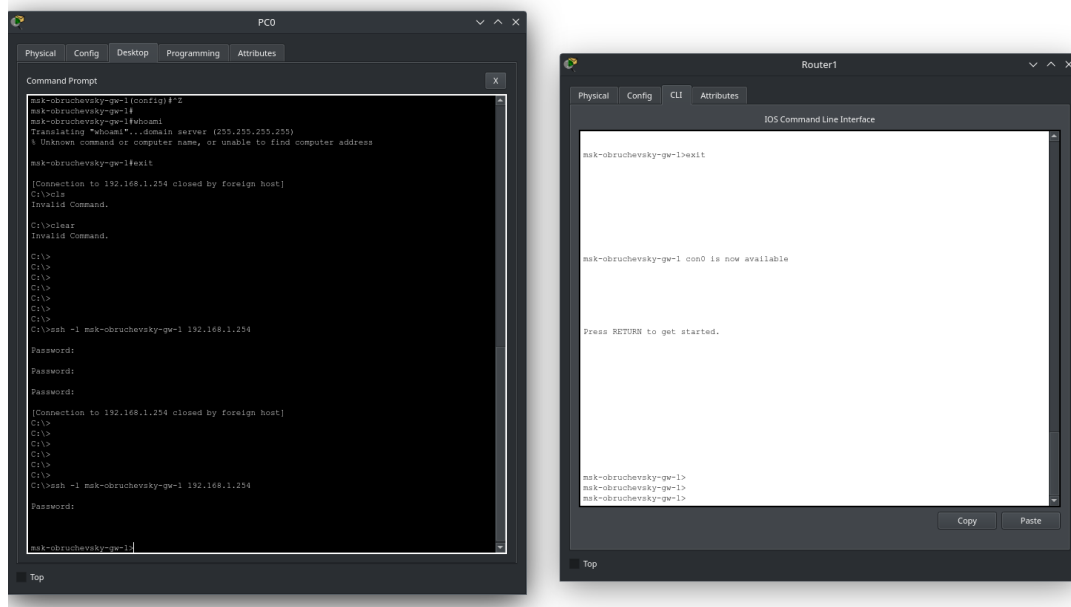


Рис. 3.5: ssh router

я подключился к роутеру через SSH

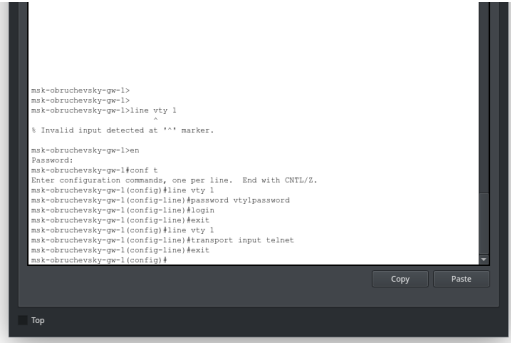
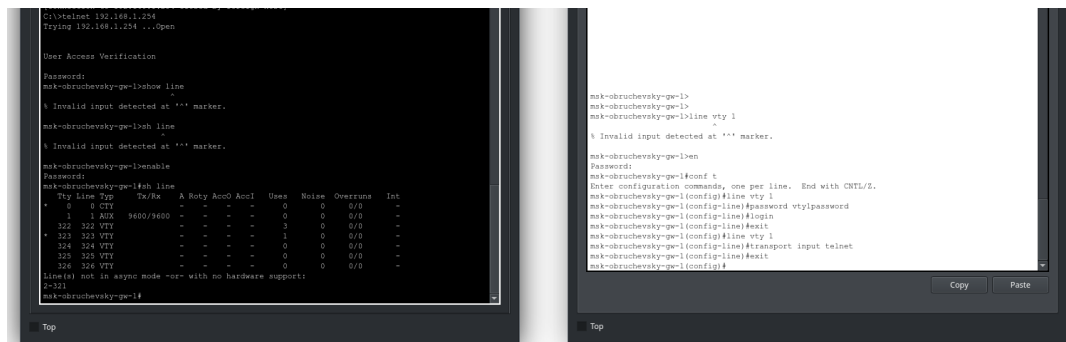


Рис. 3.6: telnet router

Затем я настроил vty 1 на использование telnet и подключился от PC0 к маршрутизатору с помощью telnet.

3.2 Конфигурация коммутатора

Установка имени хоста

Команда `hostname msk-obruchievsky-sw-1` устанавливает имя хоста коммутатора на «msk-obruchevich-sw-1».

Настройка интерфейса VLAN

Команды в интерфейсе `vlan2` и интерфейсе `f0/1` настраивают интерфейс VLAN и режим порт

Настройка IP-адреса и шлюза по умолчанию

Команды ip адрес 192.168.2.1 255.255.255.0 и ip default-gateway 192.168.2.254 назначают адреса интерфейсам и устанавливают шлюз по умолчанию для коммутатора.

Настройка линий доступа и шифрования

Команды, относящиеся к строке `vtu 0 4`, строке консоли `0`, включению секрета, шифрован

```

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname msk-obruchevsky-maabedelhay-sw-1
msk-obruchevsky-maabedelhay-sw-1(config)#interface vlan2
msk-obruchevsky-maabedelhay-sw-1(config-if)#no shutdown
msk-obruchevsky-maabedelhay-sw-1(config-if)#ip address 192.168.2.1 255.255.255.0
msk-obruchevsky-maabedelhay-sw-1(config-if)#exit
msk-obruchevsky-maabedelhay-sw-1(config)#interface f0/1
msk-obruchevsky-maabedelhay-sw-1(config-if)#switchport mode access
msk-obruchevsky-maabedelhay-sw-1(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
msk-obruchevsky-maabedelhay-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-obruchevsky-maabedelhay-sw-1(config-if)#exit
msk-obruchevsky-maabedelhay-sw-1(config)#ip default-gateway 192.168.2.254
msk-obruchevsky-maabedelhay-sw-1(config)#line vty 0 4
msk-obruchevsky-maabedelhay-sw-1(config-line)#password vtypassword
msk-obruchevsky-maabedelhay-sw-1(config-line)#login
msk-obruchevsky-maabedelhay-sw-1(config-line)#exit
msk-obruchevsky-maabedelhay-sw-1(config)#line console 0
msk-obruchevsky-maabedelhay-sw-1(config-line)#password vty0password
^
% Invalid input detected at '^' marker.

msk-obruchevsky-maabedelhay-sw-1(config-line)#password vty0password
msk-obruchevsky-maabedelhay-sw-1(config-line)#login
msk-obruchevsky-maabedelhay-sw-1(config-line)#exit
msk-obruchevsky-maabedelhay-sw-1(config)#enable secret enablepassword
msk-obruchevsky-maabedelhay-sw-1(config)#service password-encryption
msk-obruchevsky-maabedelhay-sw-1(config)#username admin privilege 1 secret adminpassword
msk-obruchevsky-maabedelhay-sw-1(config)#ip domain-name obruchevsky.rudn.ru
msk-obruchevsky-maabedelhay-sw-1(config)#crypto key generate rsa
The name for the keys will be: msk-obruchevsky-maabedelhay-sw-1.obruchevsky.rudn.ru
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]: 4096
% Generating 4096 bit RSA keys, keys will be non-exportable...[OK]

msk-obruchevsky-maabedelhay-sw-1(config)#line vty 0 4
*Mar 1 0:58:1.200: %SSH-5-ENABLED: SSH 1.99 has been enabled
msk-obruchevsky-maabedelhay-sw-1(config-line)#transport input ssh
msk-obruchevsky-maabedelhay-sw-1(config-line)#

```

Copy

Paste

Рис. 3.7: switch conf

```
msk-obruchevsky-maabedelhay-sw-1>exit

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

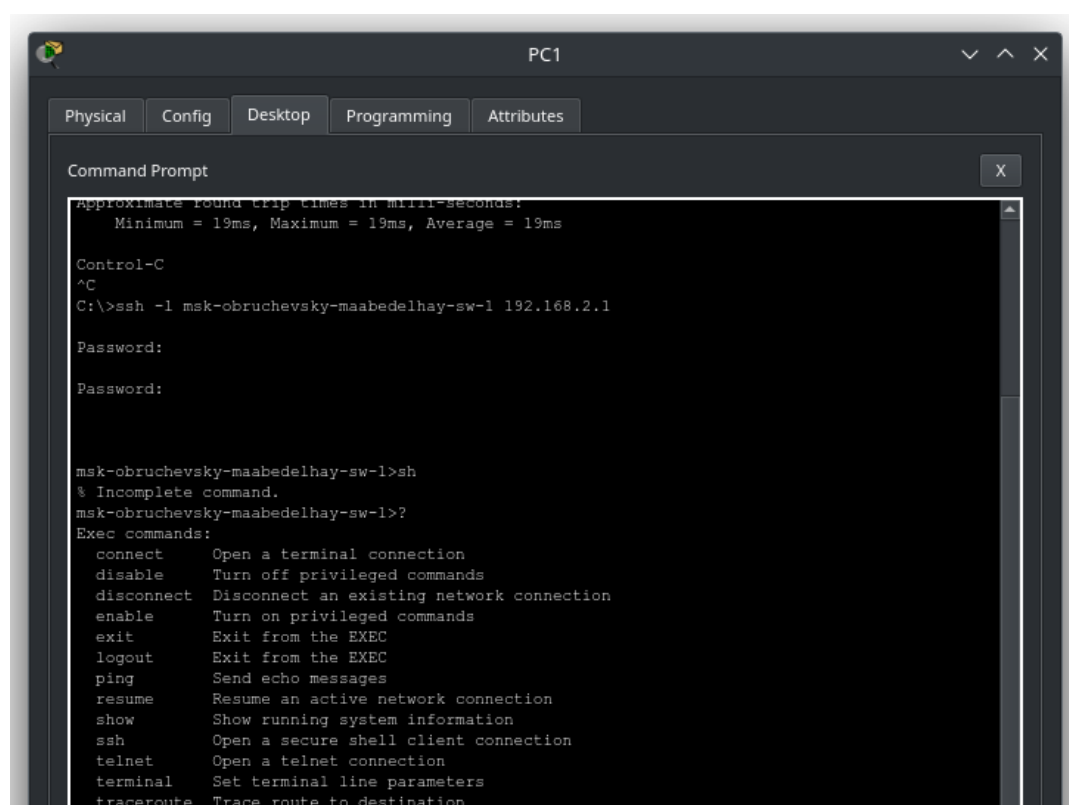
Pinging 192.168.2.1 with 32 bytes of data:

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:\>
C:\>
```

Рис. 3.8: ping switch



PC1

Physical Config Desktop Programming Attributes

Command Prompt

```
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 19ms, Average = 19ms

Control-C
^C
C:\>ssh -l msk-obruchevsky-maabedelhay-sw-1 192.168.2.1

Password:

Password:

msk-obruchevsky-maabedelhay-sw-1>sh
% Incomplete command.
msk-obruchevsky-maabedelhay-sw-1>?
Exec commands:
  connect      Open a terminal connection
  disable      Turn off privileged commands
  disconnect   Disconnect an existing network connection
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  logout       Exit from the EXEC
  ping         Send echo messages
  resume       Resume an active network connection
  show         Show running system information
  ssh          Open a secure shell client connection
  telnet       Open a telnet connection
  terminal     Set terminal line parameters
  traceroute   Trace route to destination
```

Рис. 3.9: ssh switch



Рис. 3.10: telnet ssh

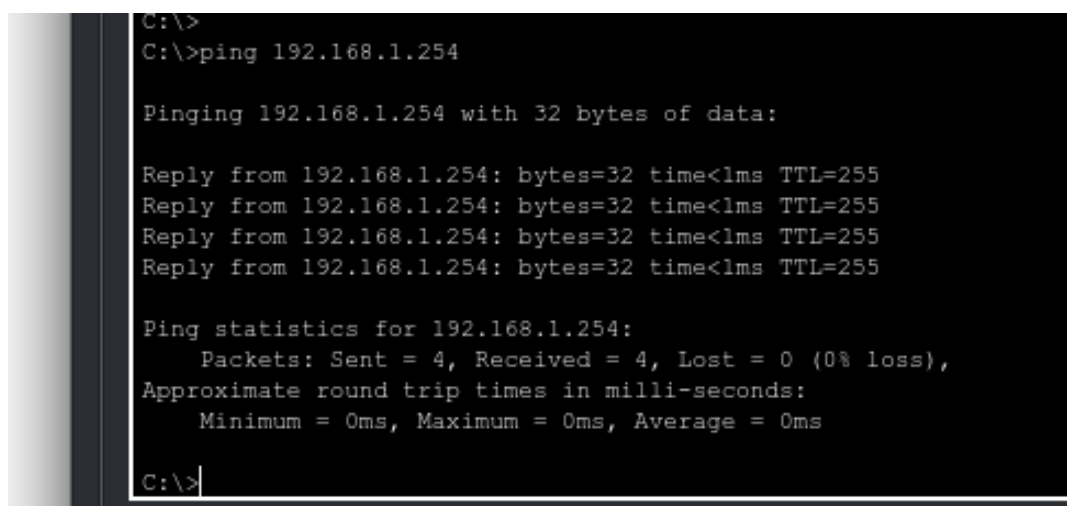


Рис. 3.11: ping ssh

4 Выводы

Я научился настраивать коммутатор и маршрутизатор и получать удаленный доступ через SSH/Telnet.

5 Контрольные вопросы

1. Укажите возможные способы подключения к сетевому оборудованию.

- SSH (Secure Shell)
- Telnet
- Консольный кабель
- Удаленное управление через веб-интерфейс (HTTP/HTTPS)
- Удаленное управление через SNMP (Simple Network Management Protocol)

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

- Тип кабеля: Ethernet-кабель (обычно используется кабель категории 5е или 6) Этот т кабеля обеспечивает соответствующую пропускную способность и поддерживает передачу данных на дальние расстояния, что важно для соединения с маршрутизатором.

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

- Тип кабеля: Тот же Ethernet-кабель, также категории 5е или 6
Для соединения с коммутатором также требуется обеспечить соответствующую пропускную способность и поддержку передачи данных на короткие и средние расстояния

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

- Тип кабеля: Обычно используется витая пара категории 5е или 6
- Почему: Этот тип кабеля обеспечивает соединение между коммутаторами в локальной сети, поддерживая передачу данных на короткие расстояния и обеспечивая необходимую пропускную способность

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

- Локальные учетные записи на устройстве
- Аутентификация через сервер AAA (Authentication, Authorization, and Accounting)
- Использование привилегированных паролей для доступа к привилегированному режиму конфигурации

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

- SSH (Secure Shell) - предпочтительнее из-за шифрования трафика и повышенной безопасности по сравнению с Telnet
- Telnet - менее безопасный, поскольку передает данные в незашифрованном виде
- Удаленное управление через веб-интерфейс (HTTP/HTTPS) - удобно, но требует наличия веб-сервера на устройстве
- Удаленное управление через SNMP - используется для мониторинга и сбора информации, но не для настройки устройств