

# Отчёт по лабораторной работе 2

## Предварительная настройка оборудования Cisco

Авдадаев Джамал

### Содержание

1	Введение.....	1
1.1	Цель работы.....	1
2	Ход выполнения .....	1
3	Вывод.....	9
3.1	Контрольные вопросы .....	10
3.1.1	1. Укажите возможные способы подключения к сетевому оборудованию.	10
3.1.2	2. Каким типом сетевого кабеля следует подключать оконечное оборудование пользователя к маршрутизатору и почему? .....	10
3.1.3	3. Каким типом сетевого кабеля следует подключать оконечное оборудование пользователя к коммутатору и почему? .....	10
3.1.4	4. Каким типом сетевого кабеля следует подключать коммутатор к коммутатору и почему? .....	10
3.1.5	5. Укажите возможные способы настройки доступа к сетевому оборудованию по паролю. ....	10
3.1.6	6. Укажите возможные способы настройки удалённого доступа к сетевому оборудованию. Какой из способов предпочтительнее и почему? .....	11

### 1 Введение

#### 1.1 Цель работы

Получить основные навыки по начальному конфигурированию оборудования Cisco.

### 2 Ход выполнения

В логической рабочей области Packet Tracer был создан новый проект. В рабочее поле размещены маршрутизатор **2811**, коммутатор **2960-24ТТ** и два оконечных устройства типа **PC-PT**. Один компьютер подключён напрямую к маршрутизатору, второй — к коммутатору. Соединения выполнены медным прямым кабелем (Copper Straight-Through), как показано на схеме.

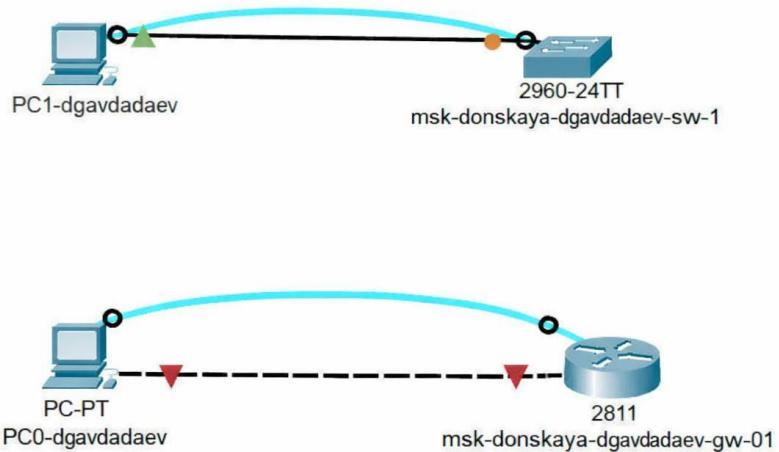


Рис. 1: Топология сети: ПК — коммутатор и ПК — маршрутизатор

На первом ПК (подключённом к коммутатору) был задан статический IP-адрес в сети 192.168.2.0/24:  
- PC1 — **192.168.2.10**

- Маска: **255.255.255.0**
- Основной шлюз: **192.168.2.1**

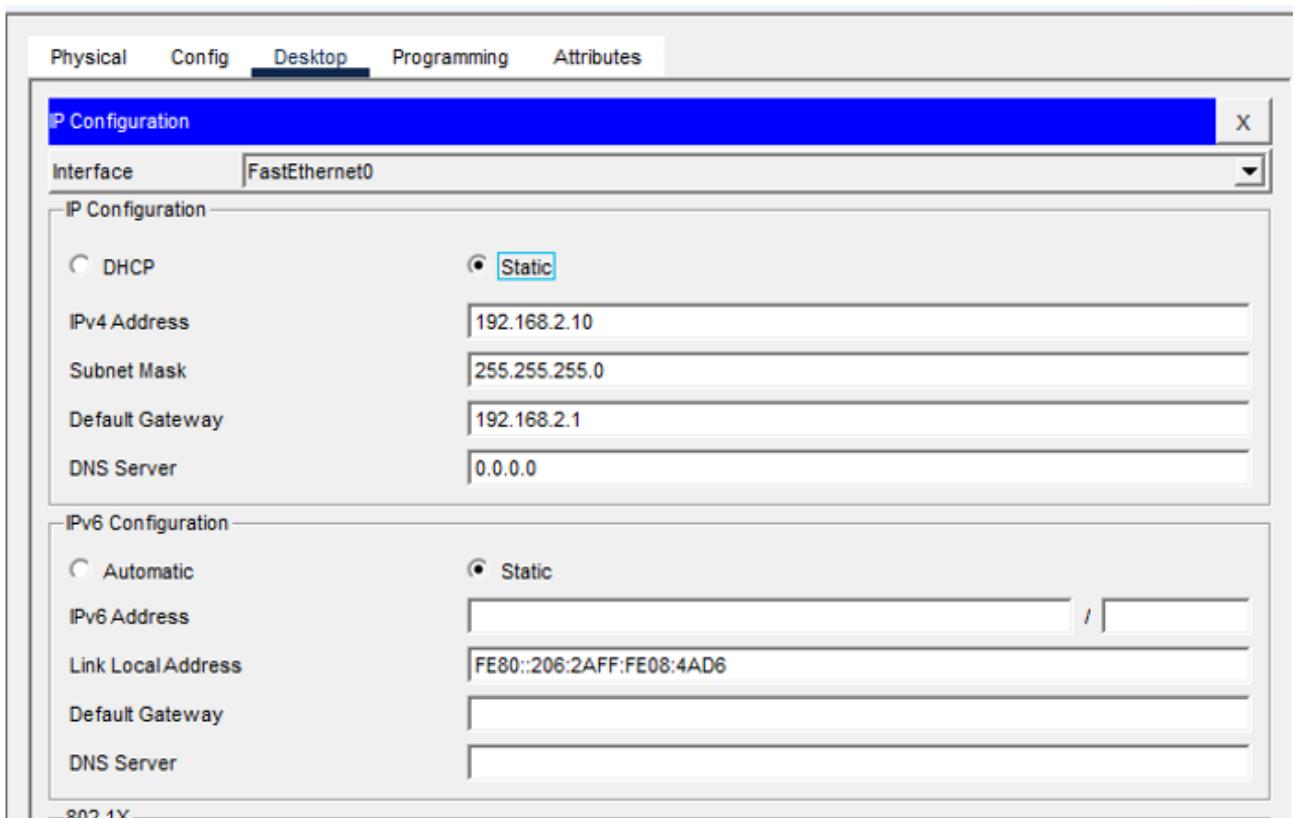


Рис. 2: Настройка IP на PC1

На втором ПК (подключённом к маршрутизатору) была настроена адресация сети 192.168.1.0/24: - PC0 — **192.168.1.1**  
- Маска: **255.255.255.0**  
- Основной шлюз: **192.168.1.254**

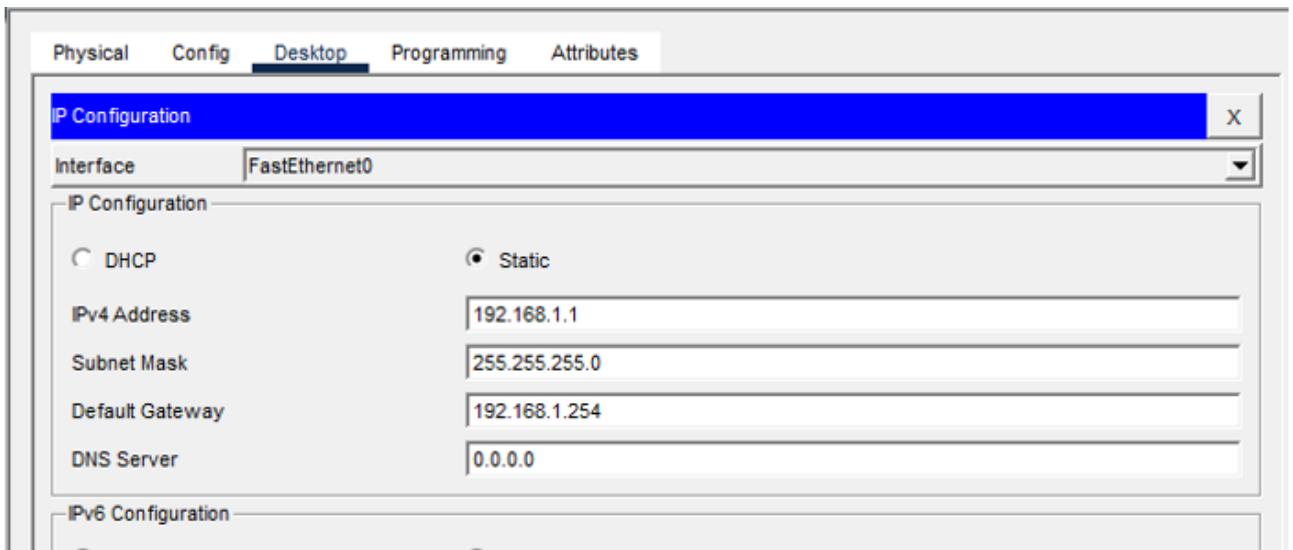


Рис. 3: Настройка IP на PC0

На коммутаторе выполнена базовая конфигурация. Установлено имя устройства, создан интерфейс управления VLAN 2 и назначен IP-адрес **192.168.2.1/24**, который используется для удалённого администрирования. Порт FastEthernet0/1 переведён в режим access и привязан к VLAN 2. Также задан шлюз по умолчанию **192.168.2.254**.

Дополнительно настроены параметры доступа: - пароль на консоль и VTY-линии — **cisco**; - включено шифрование паролей; - создан пользователь **admin**; - задан домен; - сгенерированы RSA-ключи; - разрешён доступ по протоколу **SSH**.

Sical Config CLI Attributes

IOS Command Line Interface

```
user@conf term
ter configuration commands, one per line. End with CNTL/Z.
user(config)#hostname mk-donskaya-gw-dgavdadaev-01
c-donskaya-gw-dgavdadaev-01(config)#int f0/0
c-donskaya-gw-dgavdadaev-01(config-if)no shut

c-donskaya-gw-dgavdadaev-01(config-if)#
LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

c-donskaya-gw-dgavdadaev-01(config-if)#ip address 192.168.1.254 255.255.255.0
c-donskaya-gw-dgavdadaev-01(config)#line vty 0 4
c-donskaya-gw-dgavdadaev-01(config)##password cisco
c-donskaya-gw-dgavdadaev-01(config)##login
c-donskaya-gw-dgavdadaev-01(config)#linee console 0
c-donskaya-gw-dgavdadaev-01(config)##password cisco
c-donskaya-gw-dgavdadaev-01(config)#ttrrrpt
c-donskaya-gw-dgavdadaev-01(config)#service secret cisco
c-donskaya-gw-dgavdadaev-01(config)#encripto passw
c-donskaya-gw-dgavdadaev-01(config)#service passworrd-encrption
c-donskaya-gw-dgavdadaev-01(config)#ip domain-name donskaya.rud.edu
c-donskaya-gw-dgavdadaev-01(config)#ip ssh version 2
c-donskaya-gw-dgavdadaev-01(config)#encrypt key gen rsa
c-donskaya-gw-dgavdadaev-01(config)#domain donskaya.songde.gem.aedu
c-donskaya-gw-dgavdadaev-01(config)#'Unauthorized access is prohibited
+ name for the keys will be at least 768 bits for ssh version 2 If= t=#
ose the Security Service may wage of 360 to 400$ for your act.^C      Service

Generated RSA keys [1024 b: [OK]
Now generate a 512 bit RSA key, keys will be non-exportable...[OK]

How many bits in the modulus [512]:
Generating 512 bit RSA keys, keys will avty 0 4
c-Olnasmya-gw-dgavdadaev-01(config)#line vty 0 least 768 bits for sh version 2
ar 1 0:12.593: #SSH-5-ENABLED: SSH 1.5 has been enabled to
ar 1 0:12:31.599: #SSH-5-ENABLED: SSH 1.5 has been enabled
c-donskaya-gw-dgavdadaev-01(config-line)#transport in ssh
SE-5-CONFIG_1: Configured from console by console
```

Рис. 4: Конфигурация коммутатора через CLI

The screenshot shows a software interface for managing network devices. At the top, there's a navigation bar with tabs: 'Physical', 'Config', 'Desktop' (which is selected), 'Programming', and 'Attributes'. Below the navigation bar is a blue header bar with the text 'Terminal' and a right-pointing arrow. The main area is a black terminal window displaying configuration commands. The commands include setting the hostname to 'mak-f0/0', activating interface FastEthernet0/0, setting IP address 192.168.1.254, defining VTY line 0 with password 'cisco', enabling SSH version 2, generating RSA keys, and configuring a banner. The configuration concludes with a warning about site monitoring and a success message indicating the configuration was saved.

```
Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
mak-donskaya-dv-dgavdadaev-01(config)#hostname mak-f0/0
mak-donskaya-dv-dgavdadaev-01(config-if)no shut

mak-donskaya-dv-dgavdadaev-01(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

mak-donskaya-dv-dgavdadaev-01(config)##ip address 192.168.1.254 255.255.255.0
mak-donskaya-dv-dgavdadaev-01(config)#line vty 0 4
mak-donskaya-dv-dgavdadaev-01(config)#password cisco
mak-donskaya-dv-dgavdadaev-01(config)#login
mak-donskaya-dv-dgavdadaev-01(config)#line console 0
mak-donskaya-dv-dgavdadaev-01(config)#password ciscoses
mak-donskaya-dv-dgavdadaev-01(config)#con 0
mak-donskaya-dv-dgavdadaev-01(config)#enable secref cisco
mak-donskaya-dv-dgavdadaev-01(config)#service password-encryption
mak-donskaya-dv-dgavdadaev-01(config)#ip domain-name
mak-donskaya-dv-dgavdadaev-01(config)#ip enheya.rudn.edu
mak-donskaya-dv-dgavdadaev-01(config)#ip ash version 2
mak-donskaya-dv-dgavdadaev-01(config)#banner [logun -f=]
    Whastousite morder in protadived, some of this system it ba6ed. traced.
    Extstensect 5#MEDIATCY or You Will be Logged. Computer Security Service may :"
# Generated RSA keys/1024 b: [OK]

Now generate a 512 bit RSA key, keys will be non-exportable..[OK]
* mk-donskaya-dv-dgavdadaev-01(config)#line vty # 4
* Werning. VRF key bits megn to be at least 768 bits for ssh verst version 2
  #SSH-S-ENARLED: SSH 1.5 has been enabled
mak-donskaya-dv-dgavdadaev-01(config)#lseeI:axport in ash
mak-donskaya-dv-dgavdadaev-01(config)#Banner [logun con.woma:cn
mak-donskaya-dv-dgavdadaev-01(config)#lineI::ransport im skh

*578-5-CONFIC_I: Configured from conacle by console

mak-donskaya-dv-dgavdadaev-01(config-line)#[
```

Рис. 5: Завершение настройки SSH на коммутаторе

На маршрутизаторе настроен интерфейс FastEthernet0/0 с адресом **192.168.1.254/24**, который используется в качестве шлюза для подключённого ПК. Интерфейс активирован командой **no shutdown**.

Также выполнены настройки удалённого доступа: - заданы пароли на консоль и VTY-линиях; - включено шифрование паролей; - создан пользователь **admin**; - указан домен; - сгенерированы RSA-ключи; - разрешено подключение по **SSH**.

IOS Command Line Interface

Physical Config Attributes

```
Switch(config) term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname mk-donskaya-dgavdadaev-sw-1
mk-donskaya-dgavdadaev-sw-1(config)#int vlan2
mk-donskaya-dgavdadaev-sw-1(config-if)#no shut
$LINK-5-CHANGED: Interface Vlan2, changed state to up

mk-donskaya-dgavdadaev-sw-1(config)#ino shut
mk-donskaya-dgavdadaev-sw-1(config-if) ip addr 192.168.2.1 255.255.255.0
mk-donskaya-dgavdadaev-sw-1(config-if)#shut
mk-donskaya-dgavdadaev-sw-1(config-if)#ip addr 192.168.2.1 255.255.2.0
mk-donskaya-dgavdadaev-sw-1(config-if)#switchport access vlan2
$LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2*, changed state to up

mk-donskaya-dgavdadaev-sw-1(config)#ip default-gateway 192.168.2.254
mk-donskaya-dgavdadaev-sw-1(config-if) line vty 0 4
mk-donskaya-dgavdadaev-sw-1(config-line)#password cisco
mk-donskaya-dgavdadaev-sw-1(config-line)#login
mk-donskaya-dgavdadaev-sw-1(config-line)#line con 0
mk-donskaya-dgavdadaev-sw-1(config-line)#password cisco
mk-donskaya-dgavdadaev-sw-1(config-line)#service
mk-donskaya-dgavdadaev-sw-1(config-line)#service password-encryption
mk-donskaya-dgavdadaev-sw-1(config-line)#ip domain-name donskaya.rudn.edu
mk-donskaya-dgavdadaev-sw-1(config-line)#crypto key gen rsa
mk-donskaya-dgavdadaev-sw-1(config)#banner ya domsoc us.mnn.key
mk-donskaya-dgavdadaev-sw-1(config) #service password-encryption paswarme8m=0
General Purpose time. Choosing a key modulus greater than 512 may take
General Purpose time.

How many bits in the modulus [512]:
* Generating 512 bit RSA keys, keys will be non-exportable...[OK]

mk-donskaya-dgavdadaev-sw-1(config)#line vty 0 4
* Warning: VME key size needs to be at least 768 bits for ssh versh version 2
* Mar 1 0:6:6.65: %SSH-5-ENABLED: SSH 1.5 has been enabled
mk-donskaya-dgavdadaev-sw-1(config-line)#transport ssh
$SYS-5-CONFIG_3: Configured from console by console
```

Copy Paste

Рис. 6: Конфигурация маршрутизатора через CLI

```
Physical Config Desktop Programming Attributes

Terminal >

Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
mk-donskaya-dv-dgavdadaev-01(config)#hostname mx-f0/0
mk-donskaya-dv-dgavdadaev-01(config-if)no shut

mak-donskaya-dv-dgavdadaev-01(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

mak-donskaya-dv-dgavdadaev-01(config)##ip address 192.168.1.254 255.255.255.0
mak-donskaya-dv-dgavdadaev-01(config)#line vty 0 4
mak-donskaya-dv-dgavdadaev-01(config)#password cisco
mak-donskaya-dv-dgavdadaev-01(config)#login
mak-donskaya-dv-dgavdadaev-01(config)#line console 0
mak-donskaya-dv-dgavdadaev-01(config)#password ciscoses
mak-donskaya-dv-dgavdadaev-01(config)#con 0
mak-donskaya-dv-dgavdadaev-01(config)#enable secref cisco
mak-donskaya-dv-dgavdadaev-01(config)#service password-encryption
mak-donskaya-dv-dgavdadaev-01(config)#ip domain-name
mak-donskaya-dv-dgavdadaev-01(config)#ip enheya.rudn.edu
mak-donskaya-dv-dgavdadaev-01(config)#ip ash version 2
mak-donskaya-dv-dgavdadaev-01(config)#banner [logun -f=]
    Whastousite morder in protadived, some of this system it ba6ed. traced.
    Extstensect 5#MEDIATCY or You Will be Logged. Computer Security Service may :"
# Generated RSA keys/1024 b: [OK]

Now generate a 512 bit RSA key, keys will be non-exportable..[OK]
* mk-donskaya-dv-dgavdadaev-01(config)#line vty # 4
* Werning. VRF key bits megn to be at least 768 bits for ssh verst version 2
  #SSH-S-ENARLED: SSH 1.5 has been enabled
mak-donskaya-dv-dgavdadaev-01(config)#lseeI:axport in ash
mak-donskaya-dv-dgavdadaev-01(config)#Banner [logun con.woma:cn
mak-donskaya-dv-dgavdadaev-01(config)#lineI::ransport im skh

*578-5-CONFIC_I: Configured from conacle by console

mak-donskaya-dv-dgavdadaev-01(config-line)#[
```

Рис. 7: Настройка параметров удалённого доступа на маршрутизаторе

После завершения настройки была выполнена проверка доступности устройств с помощью команды **ping**.

С ПК, подключённого к коммутатору, была проверена доступность IP-адреса коммутатора **192.168.2.1**. Ответы получены, что подтверждает корректную настройку сети.

Далее была выполнена попытка удалённого подключения: - по **telnet** — соединение устанавливается, но закрывается; - по **SSH** — выполнен успешный вход под пользователем **admin**.

The screenshot shows a Cisco Packet Tracer interface with a 'Command Prompt' window open. The window title is 'Command Prompt'. The menu bar at the top includes 'Physical', 'Config', 'Desktop' (which is selected), 'Programming', and 'Attributes'. The command line output is as follows:

```
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

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:
```

Рис. 8: Проверка ping и подключение по SSH к коммутатору

Аналогичная проверка была выполнена с ПК, подключённого к маршрутизатору. Выполнен ping до адреса **192.168.1.254**, получены ответы без потерь пакетов. Затем выполнено подключение по SSH, подтверждающее корректную настройку удалённого администрирования.

The screenshot shows a Cisco Packet Tracer interface with a 'Command Prompt' window. The window title is 'Command Prompt'. The command line shows the following output:

```
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<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 = 0ms, Average = 0ms

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

Password:
```

Рис. 9: Проверка связи и подключение по SSH к маршрутизатору

В результате выполнения работы была создана и настроена простая сеть с использованием маршрутизатора и коммутатора. Проведена базовая конфигурация устройств, назначены IP-адреса, настроены параметры удалённого доступа и выполнена проверка связности с помощью ICMP-пакетов и протокола SSH.

### 3 Вывод

В ходе выполнения работы была создана и настроена простая сеть в Cisco Packet Tracer с использованием маршрутизатора, коммутатора и двух оконечных устройств. Выполнена базовая конфигурация сетевого оборудования: назначены IP-адреса интерфейсам, настроены параметры управления коммутатором через VLAN, задан шлюз по умолчанию и активированы интерфейсы. Были отработаны навыки настройки удалённого доступа к сетевым устройствам. Настроены линии console и VTY, включено шифрование паролей, создан локальный пользователь, сгенерированы RSA-ключи и выполнена настройка подключения по протоколу SSH. Проведена проверка доступности устройств с помощью команды ping, что подтвердило корректность выполненной адресации и соединений. Также была выполнена попытка подключения к маршрутизатору и коммутатору различными способами: через консольный кабель, а также по протоколам удалённого доступа telnet и SSH. Установлено, что защищённое подключение по SSH обеспечивает успешный удалённый вход на устройства и позволяет управлять ими по сети.

### **3.1 Контрольные вопросы**

#### **3.1.1 1. Укажите возможные способы подключения к сетевому оборудованию.**

Существует несколько способов подключения к сетевым устройствам для их настройки и администрирования:

- **Консольное подключение** — прямое соединение компьютера с устройством через консольный кабель. Используется для первоначальной настройки.
- **Telnet** — удалённое подключение по сети с передачей данных в открытом виде.
- **SSH** — удалённое защищённое подключение с шифрованием данных.
- **Web-интерфейс** — доступ через браузер (если поддерживается устройством).
- **Через вспомогательный (AUX) порт** — используется реже, обычно для удалённого доступа через модем.

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

Оконечное оборудование подключается к маршрутизатору с помощью **прямого медного кабеля (Copper Straight-Through)**.

Это связано с тем, что соединяются устройства разного типа: - компьютер (оконечное устройство); - маршрутизатор (сетевое устройство).

У таких устройств используются разные схемы передачи и приёма сигналов, поэтому прямой кабель обеспечивает корректное соединение.

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

Для подключения ПК к коммутатору также используется **прямой медный кабель (Copper Straight-Through)**.

Коммутатор является промежуточным сетевым устройством, а компьютер — оконечным. Поскольку соединяются разные типы устройств, применяется прямой кабель, обеспечивающий правильное соответствие контактов передачи и приёма.

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

Для соединения двух коммутаторов традиционно используется **перекрёстный кабель (Copper Cross-Over)**.

Это объясняется тем, что соединяются однотипные устройства. У них одинаковое расположение линий передачи и приёма, поэтому требуется перекрёстное соединение контактов для корректной передачи данных. В современных устройствах часто применяется технология Auto-MDIX, которая позволяет использовать и прямой кабель.

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

Доступ к сетевому оборудованию можно защитить несколькими способами:

- установка пароля на **console line** — для локального доступа через консоль;
- установка пароля на **VTY-линии** — для удалённых подключений;
- использование команды **enable secret** — для защиты привилегированного режима;
- создание локального пользователя с именем и паролем;
- включение шифрования паролей с помощью service password-encryption.

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

Удалённый доступ можно настроить следующими способами:

- **Telnet** — простой способ удалённого подключения по сети;
- **SSH** — защищённое подключение с использованием шифрования.

Предпочтительным является **SSH**, так как он шифрует передаваемые данные, включая логины и пароли. В отличие от Telnet, который передаёт информацию в открытом виде, SSH обеспечивает более высокий уровень безопасности и защиты от перехвата данных.