Отчёт по лабораторной работе №2

дисциплина: Администрирование локальных сетей

Студент: Кузнецова София Вадимовна

Содержание

Список иллюстраций

Список таблиц

Цель работы

Получить основные навыки по начальному конфигурированию оборудования Cisco.

Выполнение лабораторной работы

Создание нового проекта lab_PT-02.pkt.

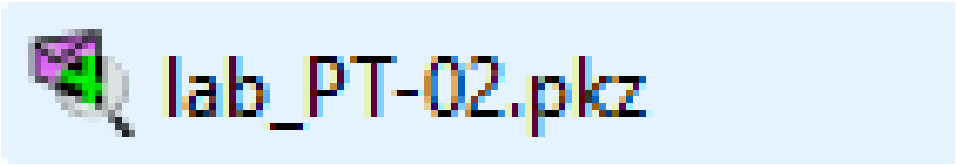

Рис. 0.1: Создание нового проекта

В логической рабочей области Packet Tracer разместим коммутатор, маршрутизатор и 2 оконечных устройства типа PC, соединим один PC с маршрутизатором, другой PC — с коммутатором.

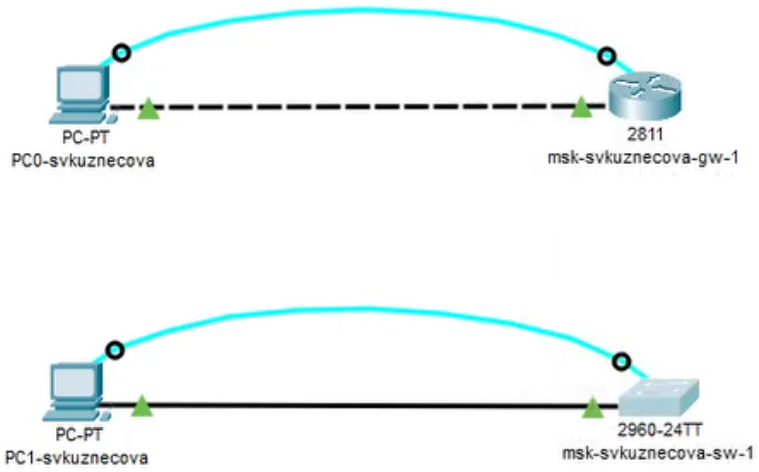

Рис. 0.2: Размещение концентратора, маршрутизатора и двух оконечных устройств. Последующее соединение

После чего, щёлкнув последовательно на каждом оконечном устройстве, зададим статические IP-адреса: 192.168.1.10 192.168.2.10 с маской подсети 255.255.255.0

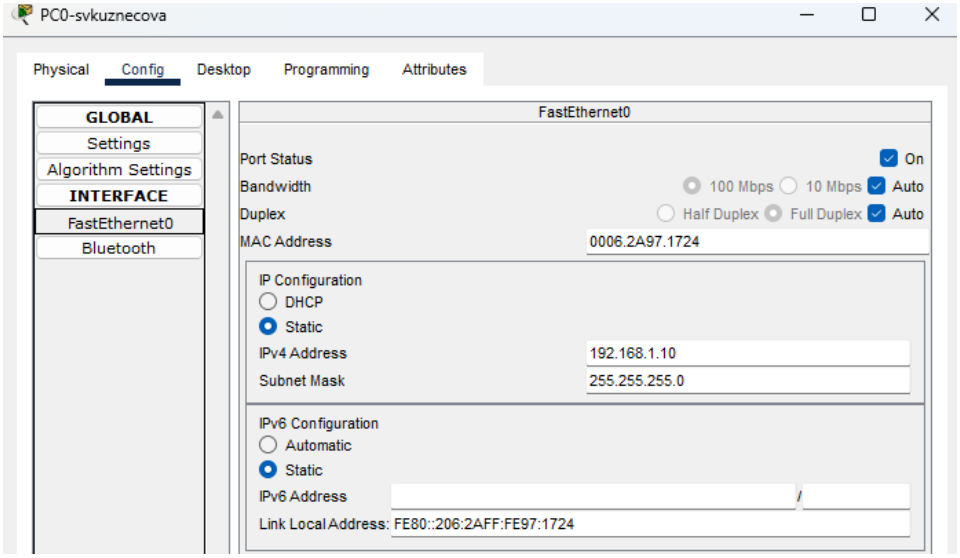

Рис. 0.3: Присвоение статического IP-адреса и маски подсети

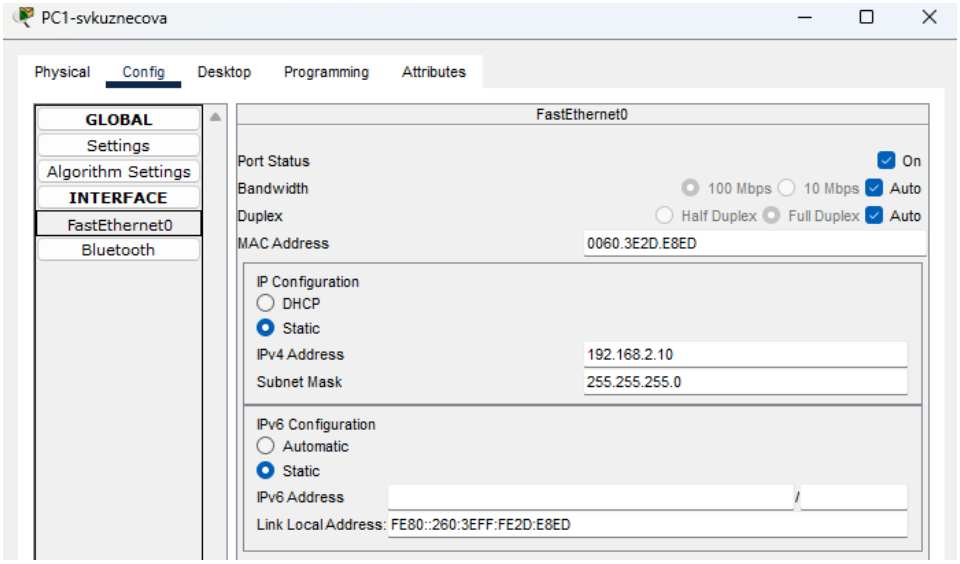

Рис. 0.4: Присвоение статического IP-адреса и маски подсети

Проведём настройку маршрутизатора в соответствии с заданием.

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

msk-svkuznecova-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-svkuznecova-gw-1(config-if)#ip address 192.168.1.254 255.255.255.0
msk-svkuznecova-gw-1(config-if)#exit
msk-svkuznecova-gw-1(config)#line vty 0 4
msk-svkuznecova-gw-1(config-line)#password cisco
msk-svkuznecova-gw-1(config-line)#login
msk-svkuznecova-gw-1(config-line)#exit
msk-svkuznecova-gw-1(config)#line console 0
msk-svkuznecova-gw-1(config-line)#password cisco
msk-svkuznecova-gw-1(config-line)#login
msk-svkuznecova-gw-1(config-line)#exit
msk-svkuznecova-gw-1(config)#enable secret cisco
msk-svkuznecova-gw-1(config)#service password-encryption
msk-svkuznecova-gw-1(config)#username admin privilege 1 secret cisco
msk-svkuznecova-gw-1(config)#ip domain name donskaya.rudn.edu
msk-svkuznecova-gw-1(config)#crypto key generate rsa
The name for the keys will be: msk-svkuznecova-gw-1.donskaya.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-svkuznecova-gw-1(config)#line vty 0 4
*Mar 1 0:7:24.791: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:7:24.791: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-svkuznecova-gw-1(config-line)#transport input ssh
```

Рис. 0.5: Проведение настройки маршрутизатора

Также проведём настройку коммутатора в соответствии с заданием.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname mskdonskaya sw1
                                   ^
% Invalid input detected at '^' marker.

Switch(config)#hostname mskdonskaya sw1
                                   ^
% Invalid input detected at '^' marker.

Switch(config)#hostname mskdonskaya sw1
                                   ^
% Invalid input detected at '^' marker.

Switch(config)#hostname msk-svkuznecova-sw-1
msk-svkuznecova-sw-1(config)#no shutdown
                                 ^
% Invalid input detected at '^' marker.

msk-svkuznecova-sw-1(config)#interface vlan2
msk-svkuznecova-sw-1(config-if)#no shutdown
msk-svkuznecova-sw-1(config-if)#ip address 192.168.2.1 255.255.255.0
msk-svkuznecova-sw-1(config-if)#exit
msk-svkuznecova-sw-1(config)#interface f0/1
msk-svkuznecova-sw-1(config-if)#switchport mode access
msk-svkuznecova-sw-1(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
msk-svkuznecova-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-svkuznecova-sw-1(config-if)#exit
msk-svkuznecova-sw-1(config)#ip default-gateway 192.168.2.254
msk-svkuznecova-sw-1(config)#line vty 0 4
msk-svkuznecova-sw-1(config-line)#password cisco
msk-svkuznecova-sw-1(config-line)#login
msk-svkuznecova-sw-1(config-line)#exit
msk-svkuznecova-sw-1(config)#line console 0
msk-svkuznecova-sw-1(config-line)#password cisco
msk-svkuznecova-sw-1(config-line)#login
msk-svkuznecova-sw-1(config-line)#exit
msk-svkuznecova-sw-1(config)#enable secret cisco
msk-svkuznecova-sw-1(config)#service password-encryption
msk-svkuznecova-sw-1(config)#username admin privilege 1 secret cisco
msk-svkuznecova-sw-1(config)#ip domain-name donskaya.rudn.edu
msk-svkuznecova-sw-1(config)#crypto key generate rsa
The name for the keys will be: msk-svkuznecova-sw-1.donskaya.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-svkuznecova-sw-1(config)#line vty 0 4
*Mar 1 0:9:14.101: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:9:14.101: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-svkuznecova-sw-1(config-line)#transport input ssh
```

Рис. 0.6: Проведение настройки коммутатора

Далее проверим работоспособность соединений с помощью команды ping.

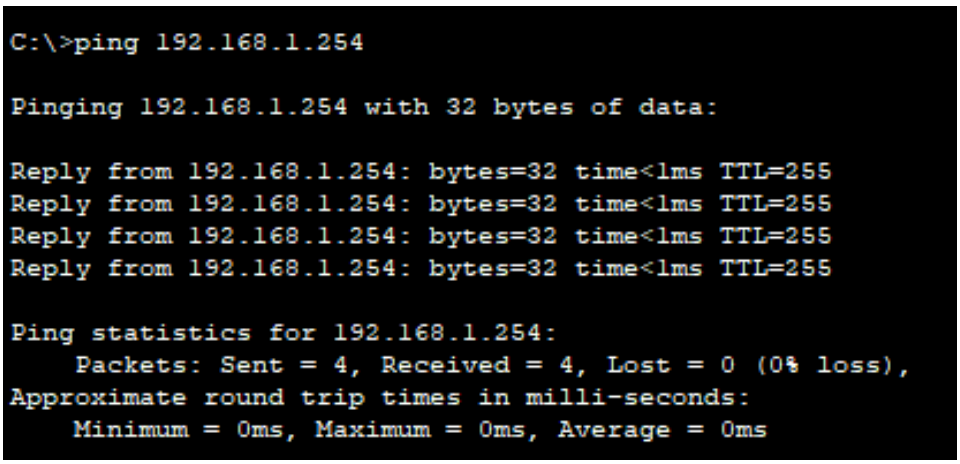

Рис. 0.7: Проверка работоспособности соединения PC0-svkuznecova -> msk-svkuznecova-gw-1

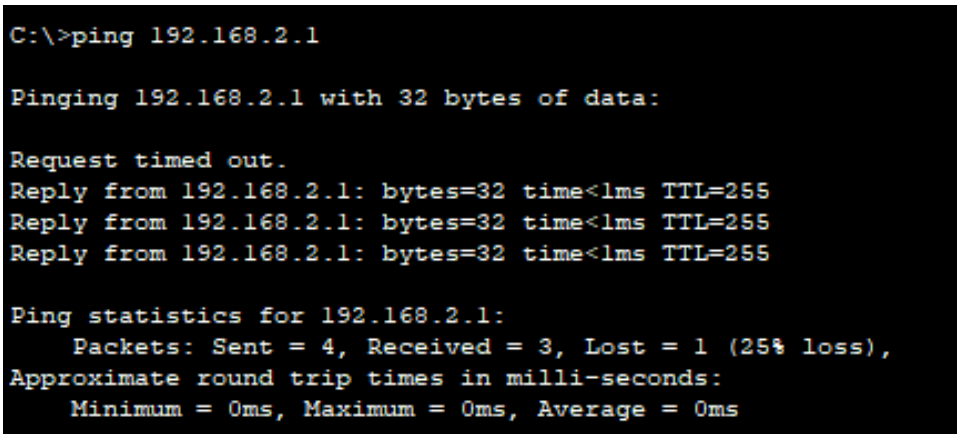

Рис. 0.8: Проверка работоспособности соединения PC1-svkuznecova -> msk-svkuznecova-sw-1

Попробуем подключиться к коммутатору и маршрутизатору разными способами: с помощью консольного кабеля, по протоколу удалённого доступа (telnet, ssh).

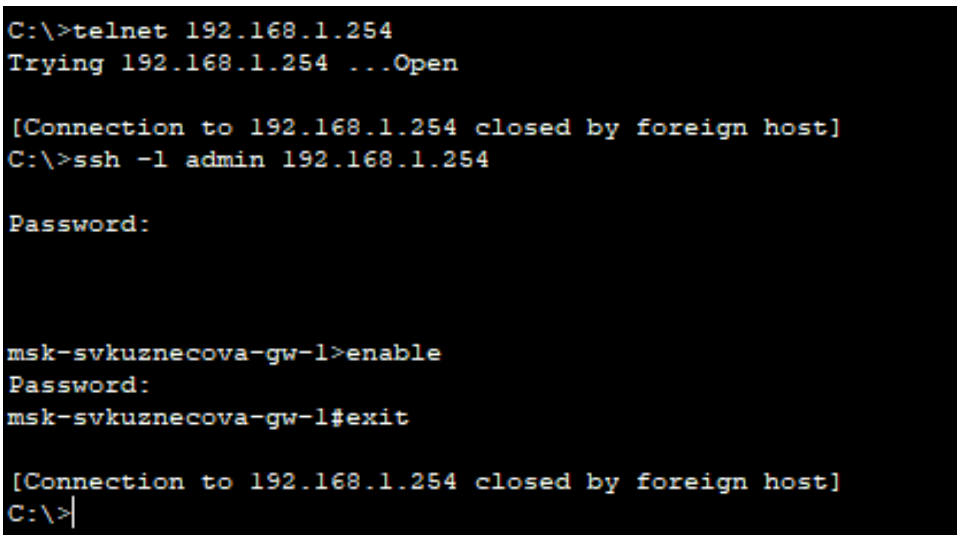

Рис. 0.9: Попытка подключения к маршрутизатору разными способами: с помощью консольного кабеля, по протоколу удалённого доступа (telnet, ssh)

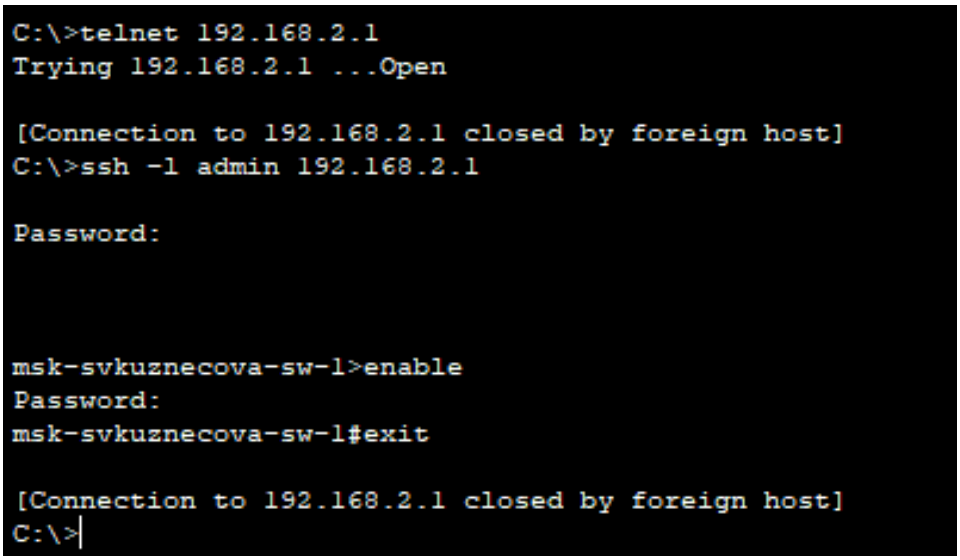

Рис. 0.10: Попытка подключения к коммутатору разными способами: с помощью консольного кабеля, по протоколу удалённого доступа (telnet, ssh)

Выводы

В ходе выполнения лабораторной работы были приобретены практические навыки по начальному конфигурированию оборудования Cisco.

Ответы на контрольные вопросы:

1. Укажите возможные способы подключения к сетевому оборудованию.

    - Проводное подключение (Ethernet): наиболее распространенный метод подключения, который использует сетевой кабель (обычно категории Ethernet) для соединения компьютера, маршрутизатора, коммутатора или другого сетевого устройства.
    - Беспроводное подключение (Wi-Fi): используют радиоволновые соединения для передачи данных между устройствами. Wi-Fi обычно используется для подключения мобильных устройств, но также может использоваться для подключения компьютеров и другого сетевого оборудования.

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

    - Для подключения оконечного оборудования пользователя обычно используется кабель маршрутизатору к Ethernet. Существует несколько видов Ethernet-кабелей, но наиболее распространенным и рекомендуемым для этой цели является кабель категории 5e (Cat5e) или категории 6 (Cat6). Кабели Cat5e и Cat6 имеют несколько преимуществ, делающих их предпочтительными для подключения оконечного оборудования к маршрутизатору: • Скорость и пропускная способность. • Поддержка Gigabit Ethernet. • Устойчивость к помехам. • Будущая совместимость.

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

- Для подключения оконечного оборудования пользователя к коммутатору также рекомендуется использовать кабель Ethernet. В зависимости от требований сети и возможностей коммутатора, можно использовать кабели различных категорий, но обычно предпочтительными являются кабели категории 5e (Cat5e) или категории 6 (Cat6) по тем же причинам, что и при подключении к маршрутизатору: • Скорость и пропускная способность. • Поддержка Gigabit Ethernet. • Устойчивость к помехам. • Будущая совместимость.

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

   - Для подключения коммутатора к коммутатору также используются сетевые кабели Ethernet. Однако здесь обычно используются кабели определенной категории в зависимости от требований к сети и пропускной способности, а также от расстояния между коммутаторами. Наиболее распространенными кабелями для соединения коммутаторов являются кабели категории 5e (Cat5e), категории 6 (Cat6) и категории 6a (Cat6a).

Выбор кабеля зависит от нескольких факторов: • Пропускная способность и расстояние. • Будущие потребности. • Бюджет. • Совместимость с имеющейся инфраструктурой.

Таким образом, для подключения коммутатора к коммутатору наиболее подходящими кабелями являются Cat5e, Cat6 или Cat6a, в зависимости от требований к пропускной способности, расстоянию и бюджету.

5. Укажите возможные способы настройки доступа к сетевому оборудованию по паролю. • Пароли на уровне устройства. • AAA (Authentication, Authorization, Accounting. • SSH (Secure Shell) или Telnet: SSH и Telnet - это протоколы удаленного управления, которые позволяют администраторам подключаться к сетевому оборудованию через сеть и вводить команды для настройки и управления устройством. Часто они могут быть защищены паролем для обеспечения

безопасного доступа. • Web-based интерфейс управления. • Локальные аккаунты. • Протокол SNMP (Simple Network Management Protocol). • Все эти методы позволяют администраторам обеспечить безопасный доступ к сетевому оборудованию по паролю, минимизируя риски несанкционированного доступа и обеспечивая конфиденциальность и целостность сетевых данных.

6. Укажите возможные способы настройки удалённого доступа к сетевому оборудованию. Какой из способов предпочтительнее и почему? • SSH (Secure Shell): SSH предоставляет защищенное соединение с удаленным сетевым оборудованием через шифрование данных. Этот метод обеспечивает безопасность и конфиденциальность при передаче команд и данных по сети. • Telnet: Telnet также предоставляет удаленный доступ к сетевому оборудованию, но не обеспечивает защиту данных,так как информация передается в открытом виде. Использование Telnet не рекомендуется из-за небезопасности этого протокола. • VPN (Virtual Private Network): VPN создает защищенное соединение через общую сеть, такую как интернет, что позволяет удаленным пользователям безопасно подключаться к сетевому оборудованию, как если бы они были внутри локальной сети. • SSL VPN (Secure Socket Layer Virtual Private Network): SSL VPN предоставляет удаленным пользователям защищенный доступ к сетевому оборудованию через веб-браузер, используя SSL-шифрование для защиты данных. • Модемный доступ: Многие сетевые устройства могут быть настроены для доступа через модемы, обеспечивая резервное подключение в случае проблем с основной сетью. • Удаленное управление через веб-интерфейс: Некоторые удаленного предоставляют веб-интерфейс для управления, который позволяет администраторам настроить и управлять устройством через веб-браузер.

Предпочтительным методом для настройки удаленного доступа к сетевому оборудованию является использование SSH или VPN. Оба эти метода обеспечивают защищенноесоединение и шифрование данных, что обеспечивает конфиденциальность и безопасность при удаленном доступе. SSH особенно удобен для доступа к

командной строке устройства, в то время как VPN Таким образом, использование SSH VPN является предпочтительным для обеспечения безопасного удаленного доступа к сетевому оборудованию.