**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

**ОТЧЕТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ № 2**

***дисциплина: Администрирование локальных сетей***

Студент: Каримов Зуфар

Группа: НПИ-01-18

Москва 2021

**Оглавление**

1. Цель работы………………………………………………………………………..3

2. Порядок выполнения работы..................................................................................4

3. Выводы ...................................................................................................................35

4. Контрольные вопросы…………………………………………………………...36

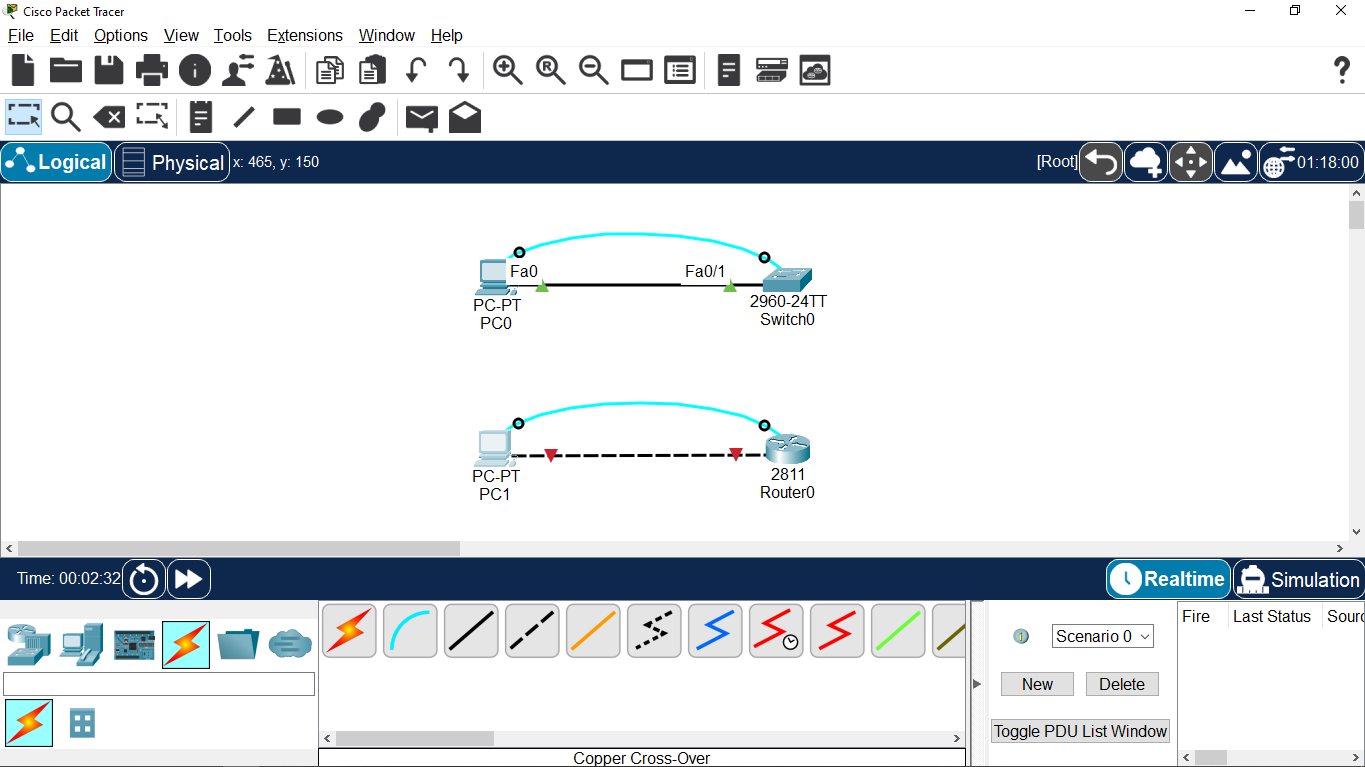
1. **Цель работы**

Получить основные навыки по начальному конфигурированию оборудования Cisco.

1. **Последовательность выполнения работы**

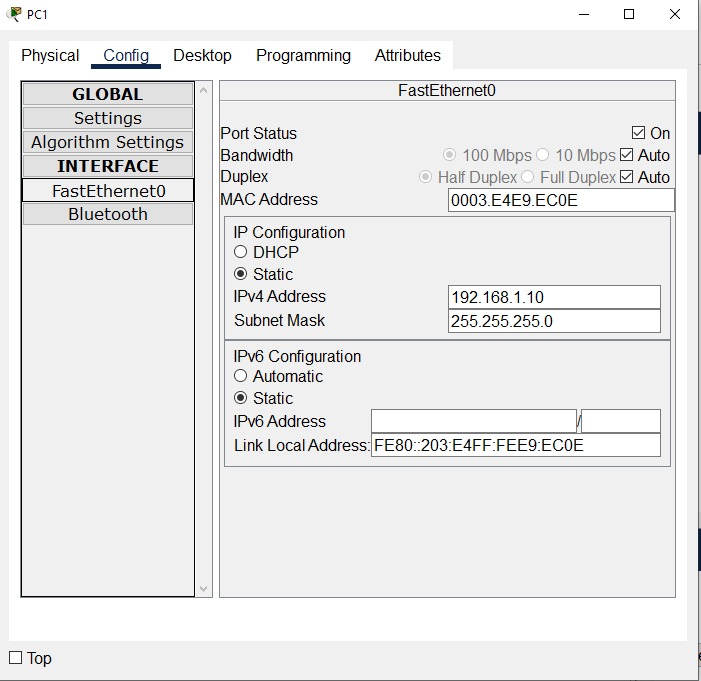
**Конфигурация маршрутизатора**

1. В логической рабочей области Packet Tracer разместите коммутатор, маршрутизатор и 2 оконечных устройства типа PC, соедините один PC с маршрутизатором, другой PC — с коммутатором (рис. 2.1).

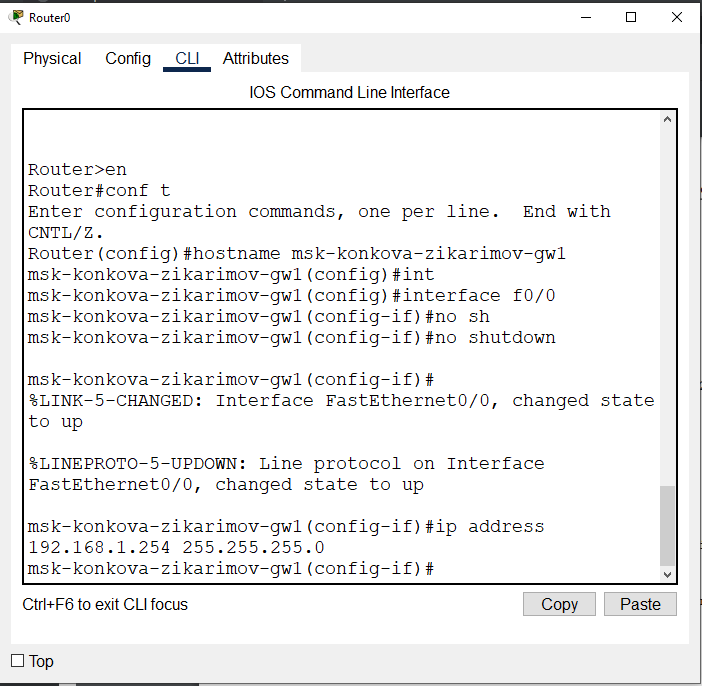


В логической рабочей среде разместил коммутатор, маршрутизатор и 2 устройства PC и соединил их. PC и коммутатор соединил витой парой, а PC и маршрутизатор соединил кроссовером.

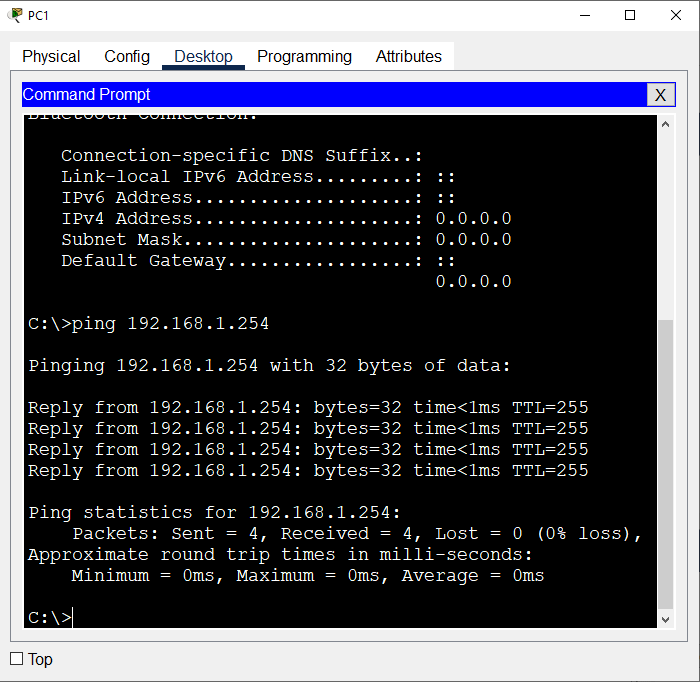
1. Проведите настройку маршрутизатора в соответствии с заданием, ориентируясь на приведённую ниже часть конфигурации маршрутизатора (см. раздел 2.4.1).
2. Проведите настройку коммутатора в соответствии с заданием, ориентируясь на приведённую ниже часть конфигурации коммутатора (см. раздел 2.4.2).
3. Проверьте работоспособность соединений с помощью команды ping.
4. Попробуйте подключиться к коммутатору и маршрутизатору разными способами: с помощью консольного кабеля, по протоколу удалённого доступа (telnet, ssh).



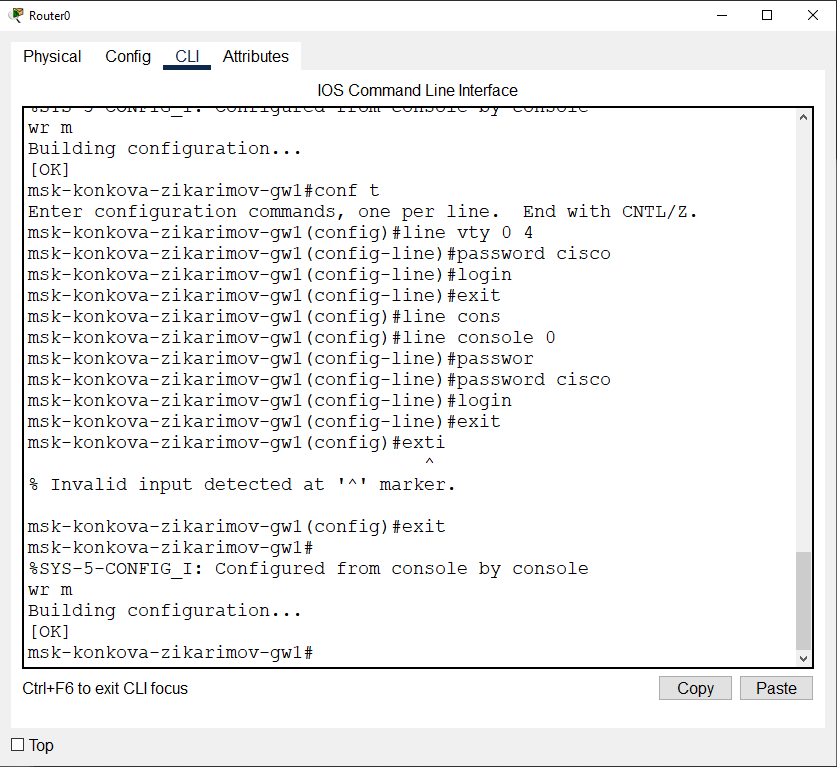
Для начала я задал ip-address для PC1 и уже потом перешел к конфигурации маршрутизатора.



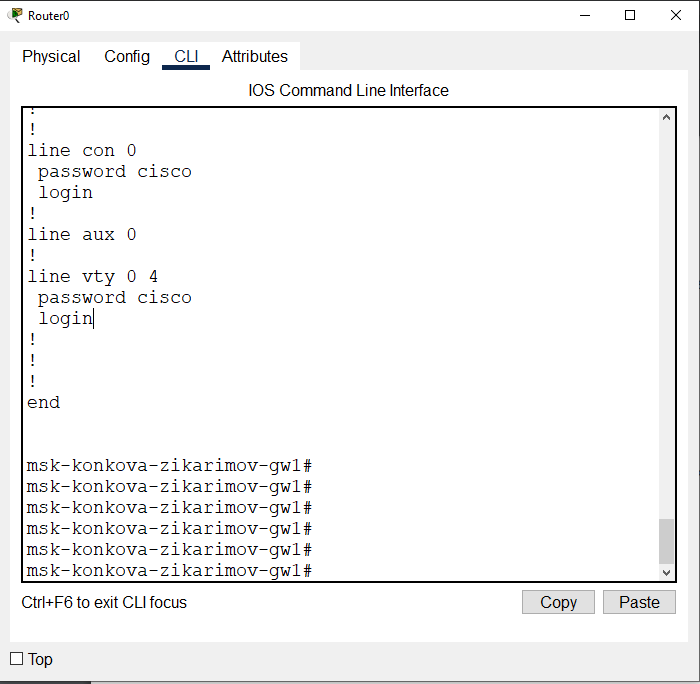
Нам надо было перейти к режиму глобальной конфигурации, чтобы задать имя hostname. Далее с помощью команды interface я перешел к специфической конфигурации, где можно задать ip-address и поднять интерфейс. Я поднял интерфейс и задал ip-address.



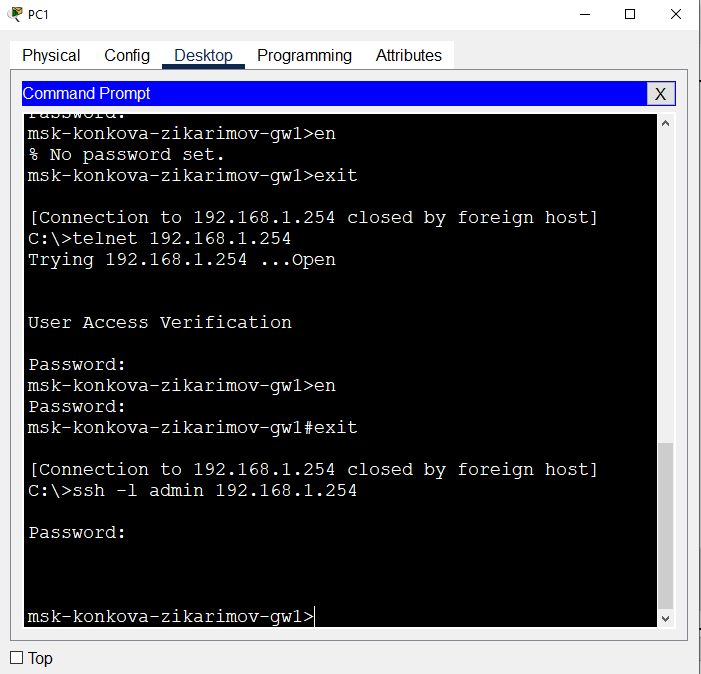
Далее я проверил доступность данного узла пропинговав ip-address.



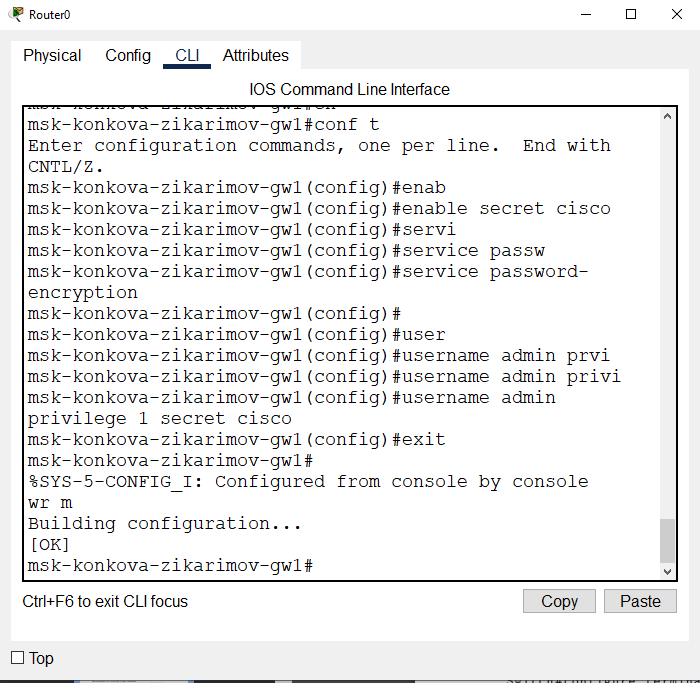
Теперь нам нужно было подключиться по telnet виртуальным терминалом vt. Что дает мне попасть в пользовательский режим. С помощью команды line vty 0 4, я к telnet сессиям, чтобы попасть в пользовательский режим и задаю пароль cisco. Далее я задаю пароль для консоли. И сохраняю изменения.



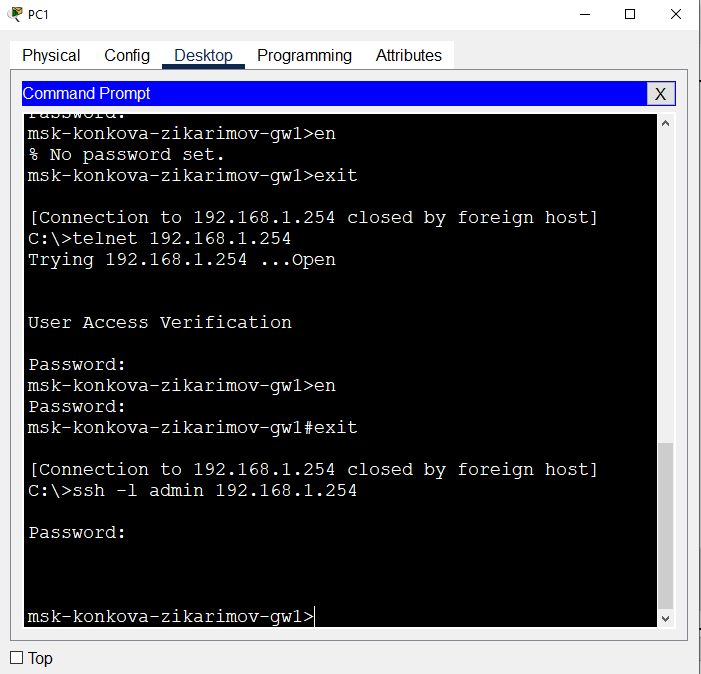
Вот мы видим наши пароли, но они в открытом виде.



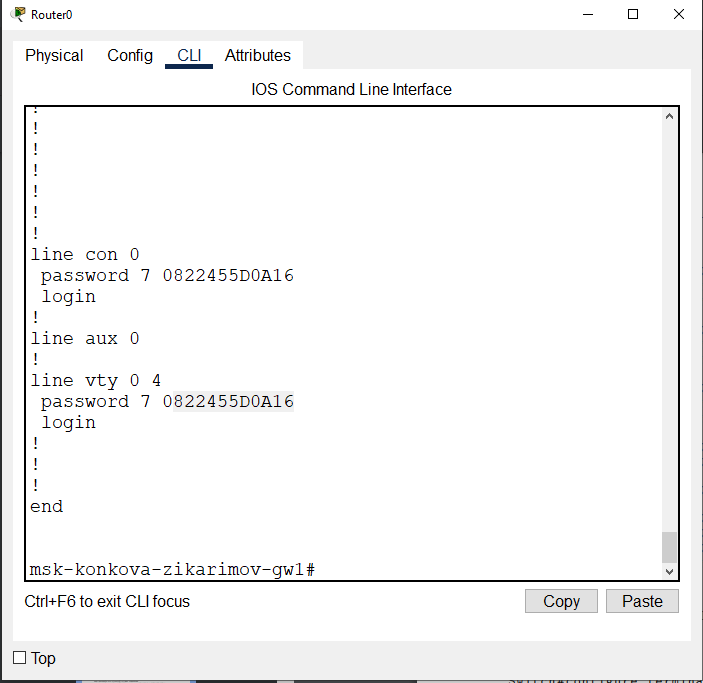
Здесь мы видим, что telnet работает. Но сверху можно заметить, что он работает только в пользовательском режиме, а в привилегированном режиме не работает.



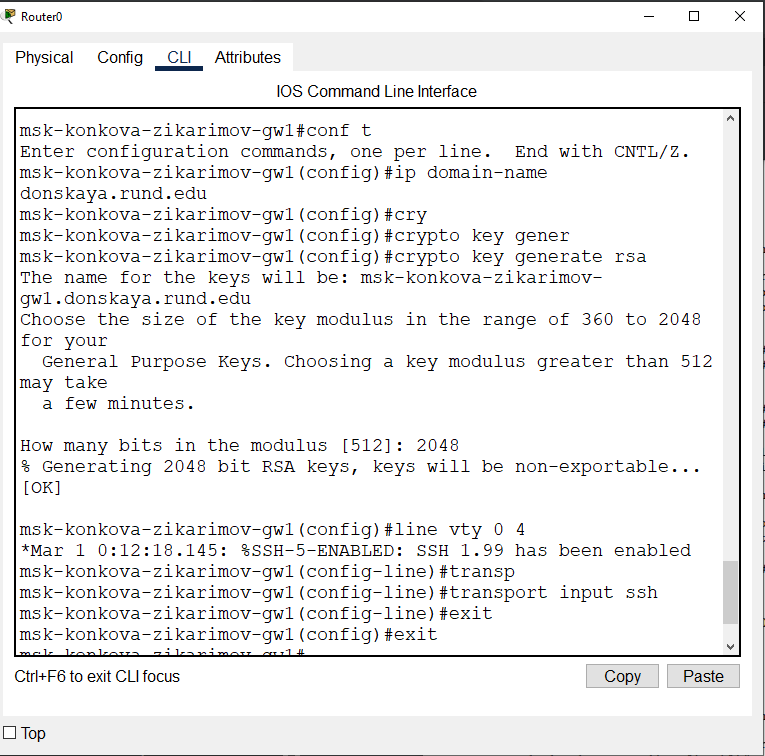
Здесь я настроил пароль для enable-режима с помощью команды enable secret cisco. Но так как у нас наши пароли находятся в открытом виде, надо их зашифровать и с помощью команды service password-encryption мы это сделаем. Далее мы задаем уровень прав пользователя 1. Это команды disable, enable, exit, help и logout, которые работают во всех режимах.



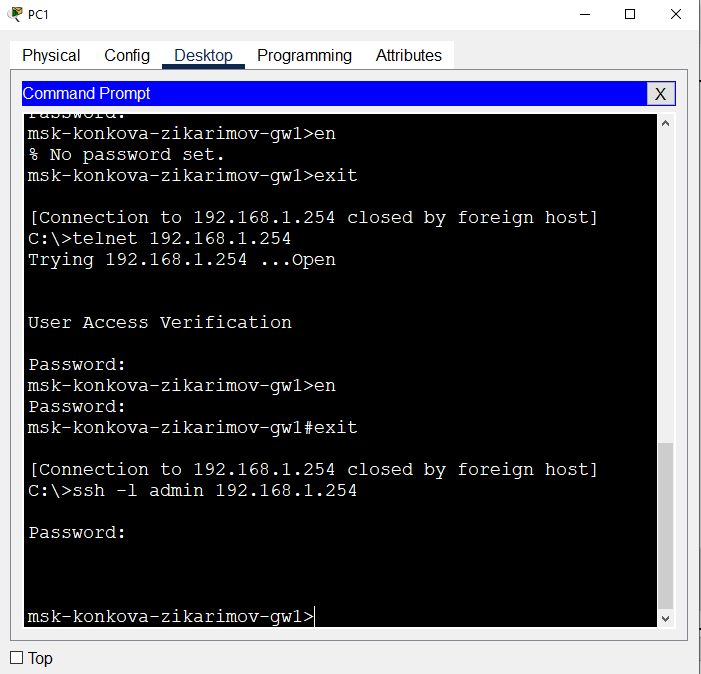
А здесь можно увидеть, что enable-режим работает. Задав пароль, мы можем в войти в привилегированный режим.



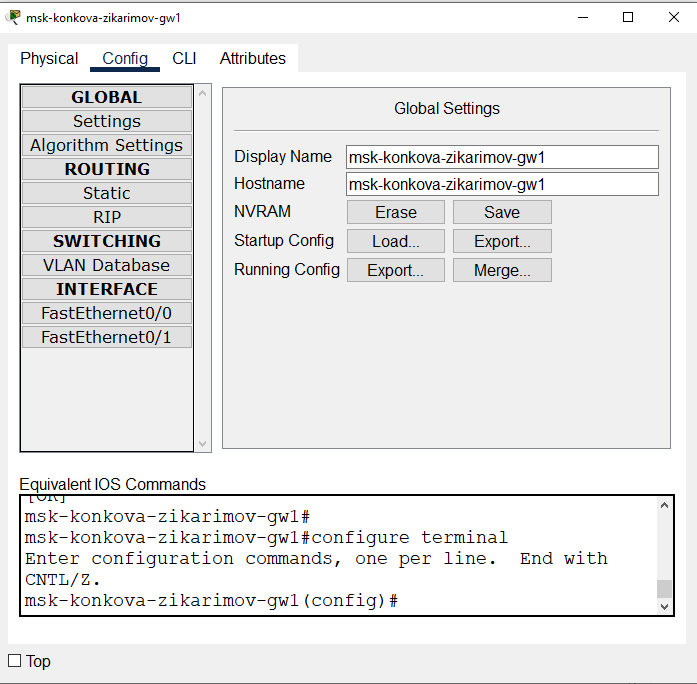
Можно увидеть, что наши пароли зашифрованы.



Здесь мы указываем имя домена (необходимо для генерации ключа), генерируем rsa ключ (необходимо будет выбрать размер ключа). Размер ключа я выбрал 2048. И далее разрешается только ssh.



SSH работает.



Далее нам нужно было сохранить и экспортировать. Предоставляю экспортируемый файл.

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

!

hostname msk-konkova-zikarimov-gw1

!

!

!

enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0

!

!

!

!

!

!

ip cef

no ipv6 cef

!

!

!

username admin secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0

!

!

license udi pid CISCO2811/K9 sn FTX1017326M-

!

!

!

!

!

!

!

!

!

ip domain-name donskaya.rund.edu

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface FastEthernet0/0

ip address 192.168.1.254 255.255.255.0

duplex auto

speed auto

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Vlan1

no ip address

shutdown

!

ip classless

!

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

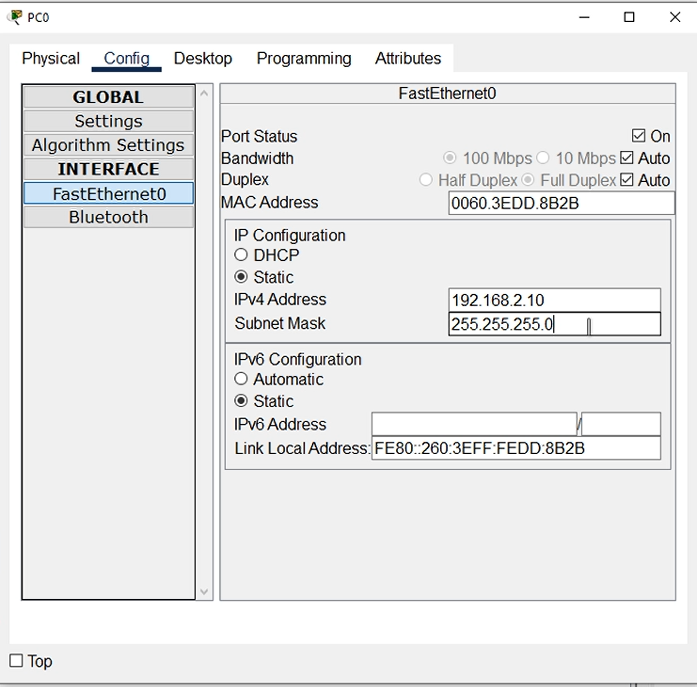
!

!

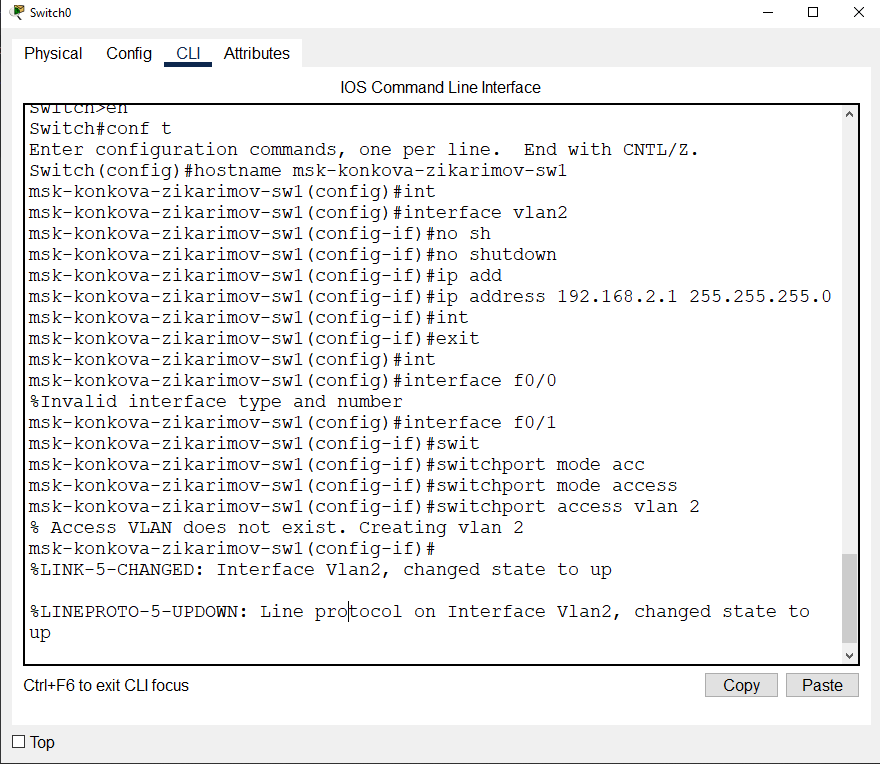
!

end

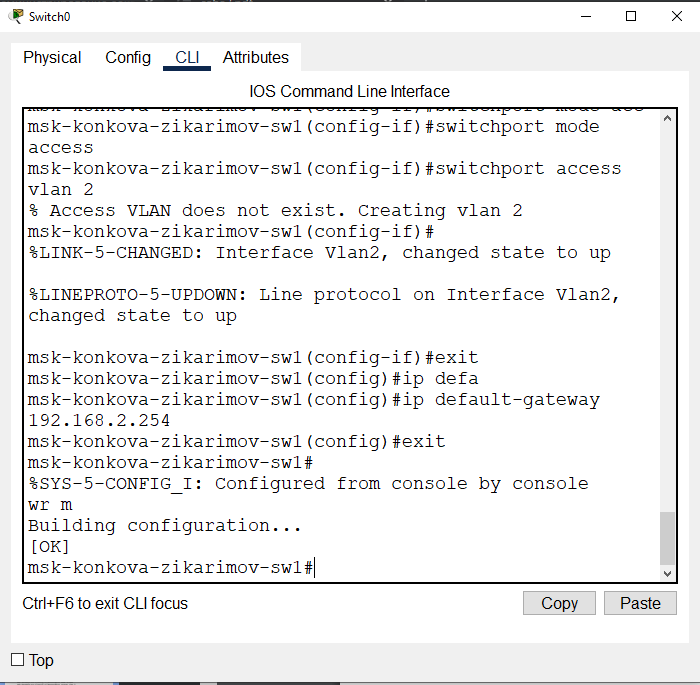
**Конфигурация коммутатора**

****

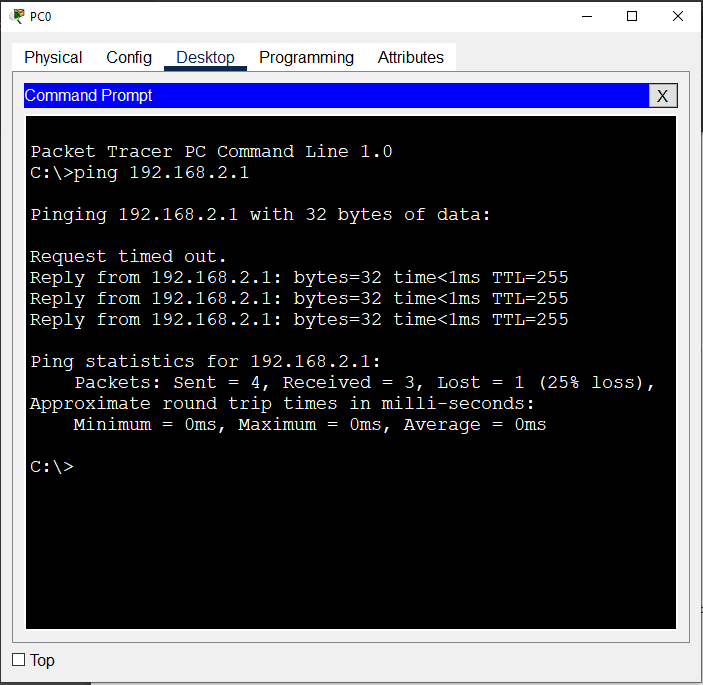
Задаю ip-address PC0 и сетевую маску.

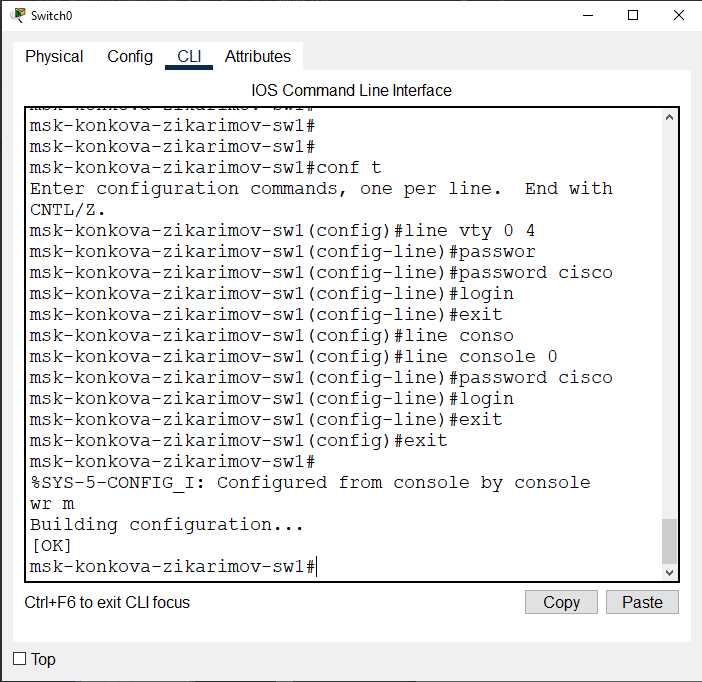


Здесь я поднимал интерфейс для виртуальной локальной компьютерной сети и задавал ip-адресс. Здесь мы задаем интерфейсу access port, который передает нетегированный трафик.

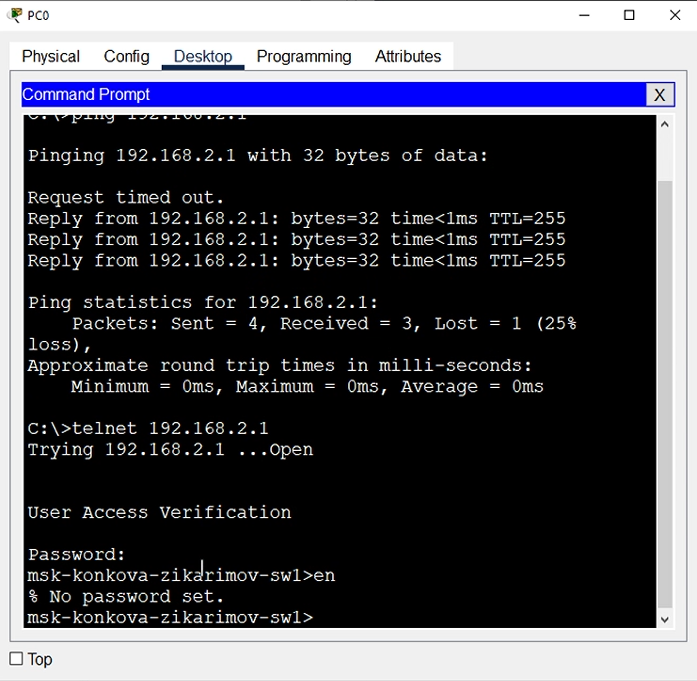


И также задаем шлюз по умолчанию.

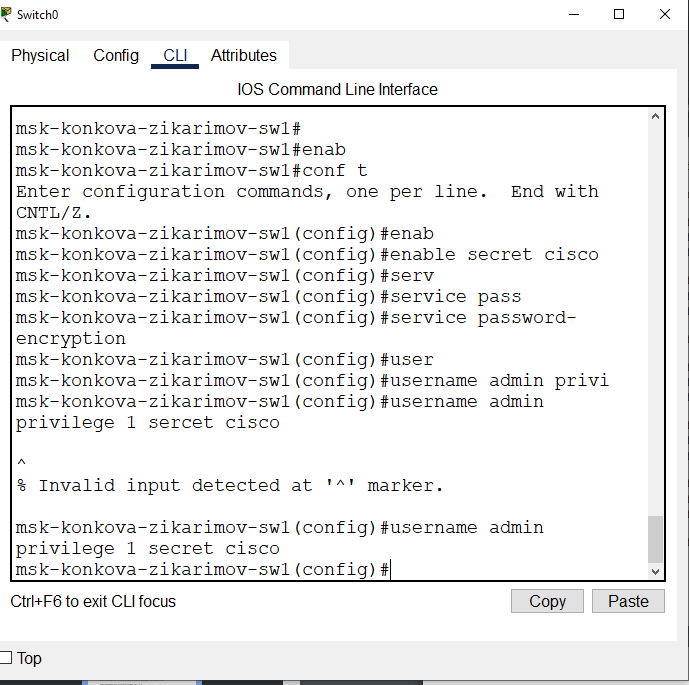




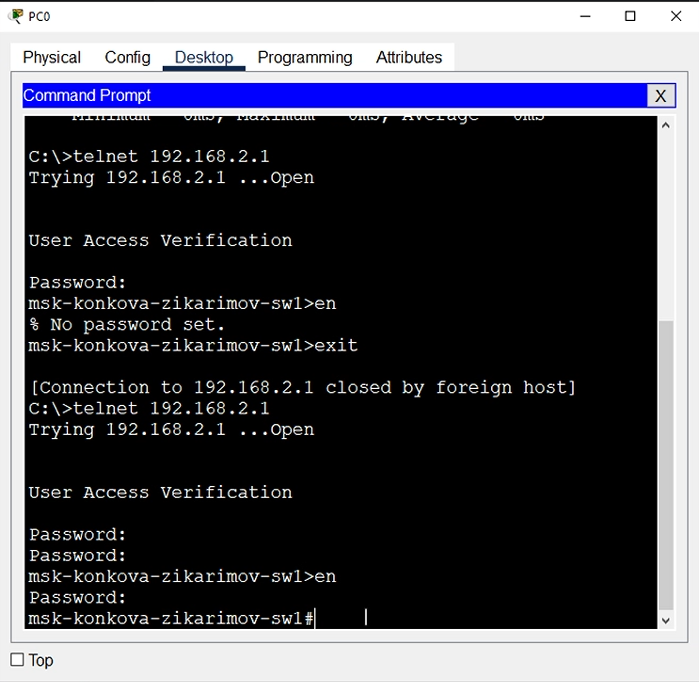
Теперь нам нужно было подключиться по telnet виртуальным терминалом vt. Что дает мне попасть в пользовательский режим. С помощью команды line vty 0 4, я к telnet сессиям, чтобы попасть в пользовательский режим и задаю пароль cisco. Далее я задаю пароль для консоли. И сохраняю изменения.



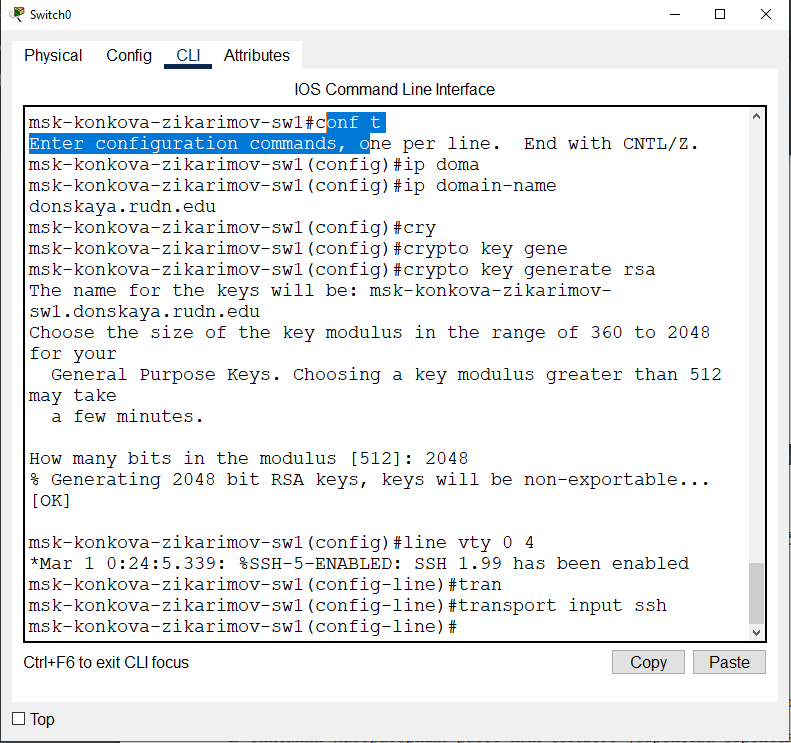
Здесь мы видим, что telnet работает. Но только в пользовательском режиме.



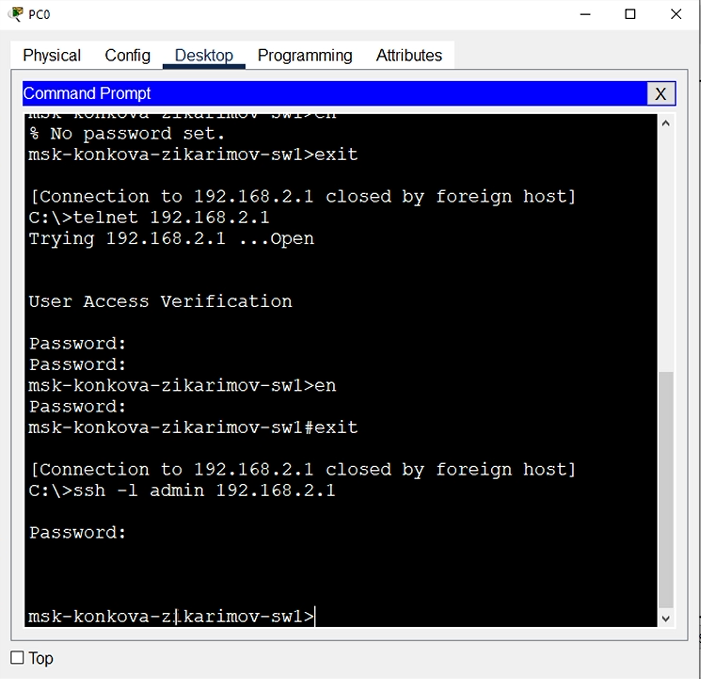
Здесь я настроил пароль для enable-режима с помощью команды enable secret cisco. Но так как у нас наши пароли находятся в открытом виде, надо их зашифровать и с помощью команды service password-encryption мы это сделаем. Далее мы задаем уровень прав пользователя 1. Это команды disable, enable, exit, help и logout, которые работают во всех режимах.



А здесь уже можно попасть на привилегированный режим.



Здесь мы указываем имя домена (необходимо для генерации ключа), генерируем rsa ключ (необходимо будет выбрать размер ключа). Размер ключа я выбрал 2048. И далее разрешается только ssh.



SSH работает.

Далее нам нужно было сохранить и экспортировать конфигурация коммутатора. Ниже предоставлю экспортируемый файл.

!

version 15.0

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

!

hostname msk-konkova-zikarimov-sw1

!

enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0

!

!

!

ip domain-name donskaya.rudn.edu

!

username admin secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0

!

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

interface FastEthernet0/1

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/2

!

interface FastEthernet0/3

!

interface FastEthernet0/4

!

interface FastEthernet0/5

!

interface FastEthernet0/6

!

interface FastEthernet0/7

!

interface FastEthernet0/8

!

interface FastEthernet0/9

!

interface FastEthernet0/10

!

interface FastEthernet0/11

!

interface FastEthernet0/12

!

interface FastEthernet0/13

!

interface FastEthernet0/14

!

interface FastEthernet0/15

!

interface FastEthernet0/16

!

interface FastEthernet0/17

!

interface FastEthernet0/18

!

interface FastEthernet0/19

!

interface FastEthernet0/20

!

interface FastEthernet0/21

!

interface FastEthernet0/22

!

interface FastEthernet0/23

!

interface FastEthernet0/24

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/2

!

interface Vlan1

no ip address

shutdown

!

interface Vlan2

ip address 192.168.2.1 255.255.255.0

!

ip default-gateway 192.168.2.254

!

!

!

!

line con 0

password 7 0822455D0A16

login

!

line vty 0 4

password 7 0822455D0A16

login

transport input ssh

line vty 5 15

login

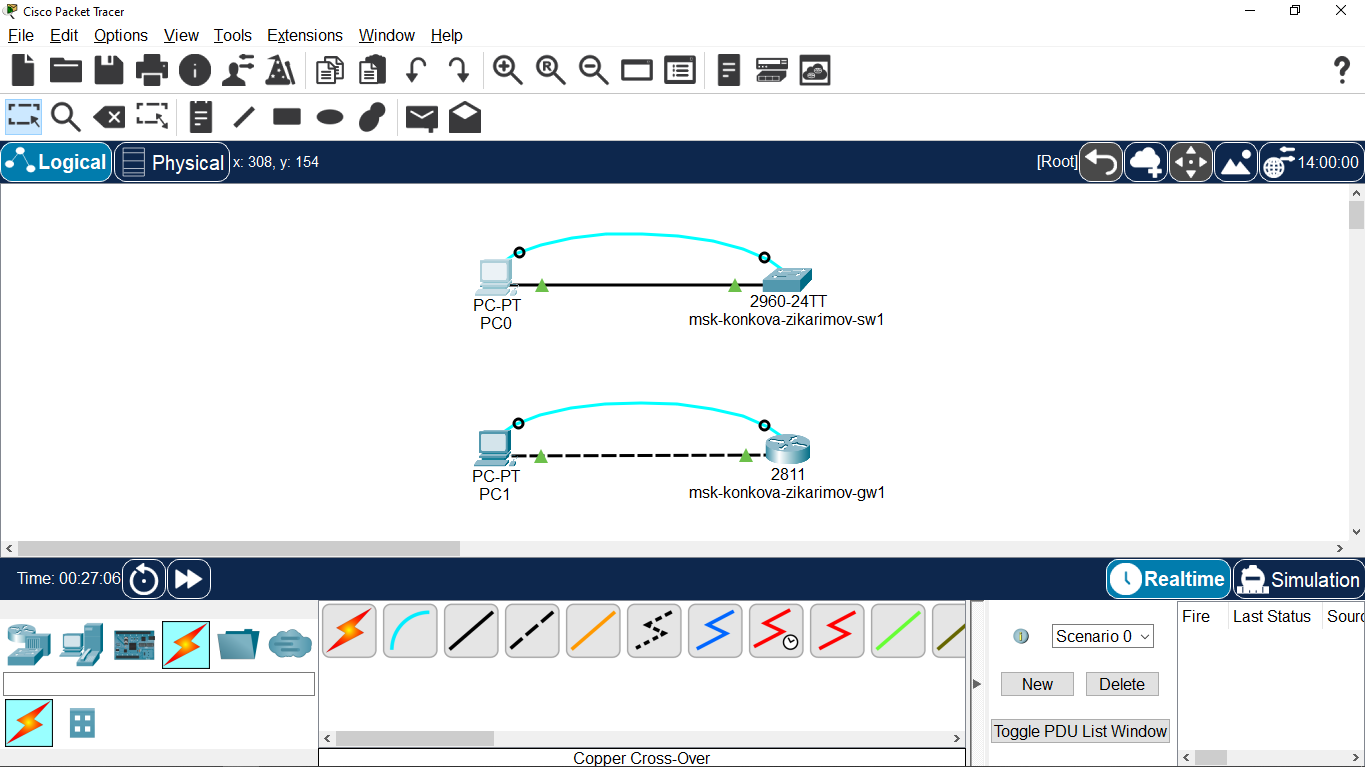
!

!

!

!

end



1. **Выводы**

Получил основные навыки по начальному конфигурированию оборудования Cisco.

1. **Контрольные вопросы**

1. Укажите возможные способы подключения к сетевому оборудованию.

Стандарты CCITT серии V и EIA серии RS описывают интерфейсы DTE-DCE. Две линии стандартов дублируют друг друга во многих отношениях. Самые распространённые стандарты: HSSI, RS-232, V.35, RS530.

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

Маршрутизатор DTE - терминальное оборудование, которое преобразует информацию пользователя в данные для передачи по линии связи и выполняет обратное преобразования (оконечное оборудование обработки). Для соединения оконечное оборудование обработки и пользователя используется перекрестный кабель, так как он используется для соединения устройств одного типа друг с другом.

3. Каким типом сетевого кабеля следует подключать оконечное оборудование

пользователя к коммутатору и почему?

Коммутатор DCE - оконечное оборудование для передачи данных (линии связи) (оборудование канала связи или оборудование канала данных). Оборудование преобразует данные, сгенерированные DTE, в сигнал для передачи по линии связи и выполняя обратное преобразование. Тип этого оборудования отличается от

абонентского оборудования. Для их соединения используется прямой кабель.

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

Для подключения двух устройства одного типа необходимо использовать перекрестный кабель, соединяющий сигналы приема/ передачи.

5. Укажите возможные способы настройки доступа к сетевому оборудованию

по паролю.

- настроить IP-адрес на терминале устройства и сетевом оборудовании;

- ограничить доступ к консольному порту;

- настроить линии VTY для коммутатора для разрешения удаленного доступа через Telnet или SSH.

6. Укажите возможные способы настройки удалённого доступа к сетевому

оборудованию. Какой из способов предпочтительнее и почему?

Telnet в первую очередь предназначен для операционной системы Unix. С его помощью можно зарегистрировать удаленного пользователя через логин. Удаленный вход в систему допускается, когда имя пользователя и пароль уже введены в системе. После регистрации пользователю даётся доступ к управлению компьютером (установка системных команды, запуск программ). SSH – лучше Telnet. Отличие в кодировании передаваемой информации. Это необходимо при работе с паролями или файлами конфигурации на удалённом компьютере.