

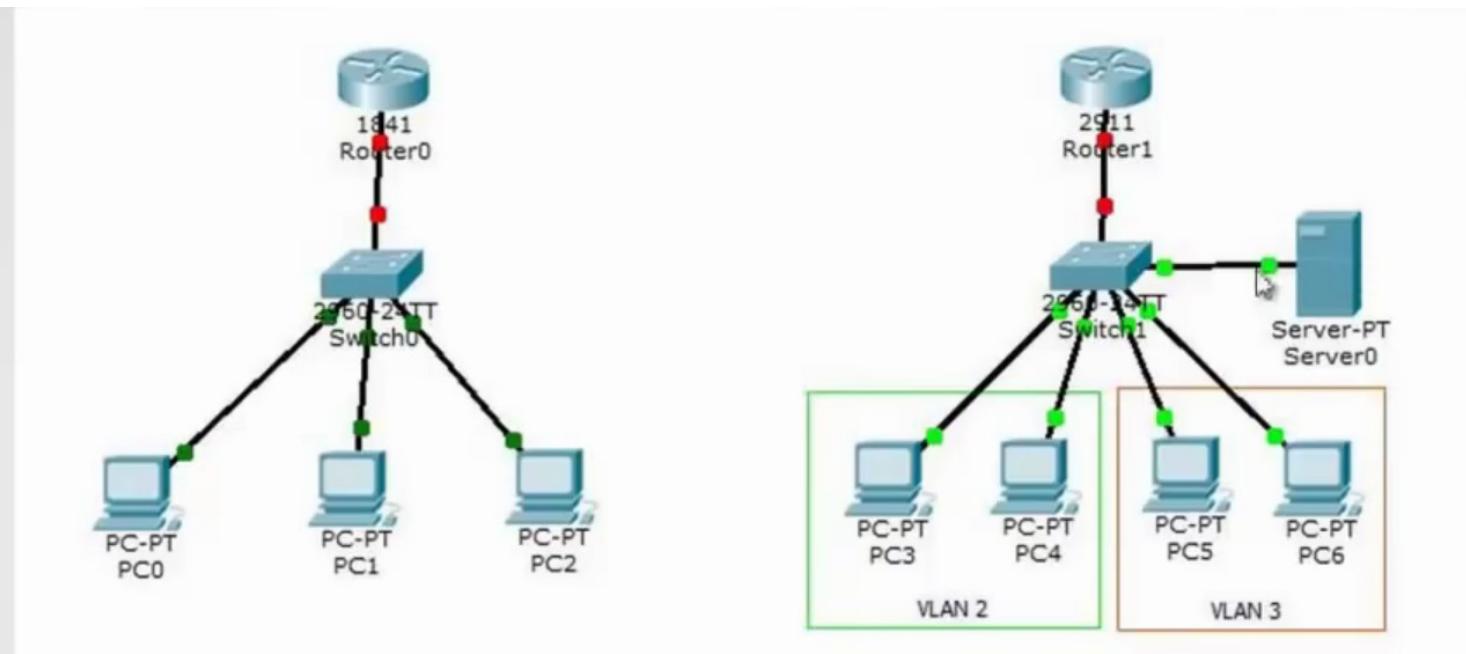
DHCP



Курс Cisco Packet Tracer <https://habrahabr.ru/post/252085/>

11. Видео уроки Cisco Packet Tracer. Курс молодого бойца. DHCP <https://www.youtube.com/watch?v=MoElaNJn-9w>

DHCP



```

conf t
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
exit
ip dhcp pool DHCP
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 8.8.8.8
exit

```

```

ip dhcp excluded-address 192.168.1.100
ip dhcp excluded-address 192.168.1.1
exit
show ip dhcp binding

```

```

interface GigabitEthernet0/1.2
encapsulation dot1Q 2
ip address 192.168.2.1 255.255.255.0
ip helper-address 192.168.4.2
exit
interface GigabitEthernet0/1.3
encapsulation dot1Q 3
ip address 192.168.3.1 255.255.255.0
ip helper-address 192.168.4.2

```

```

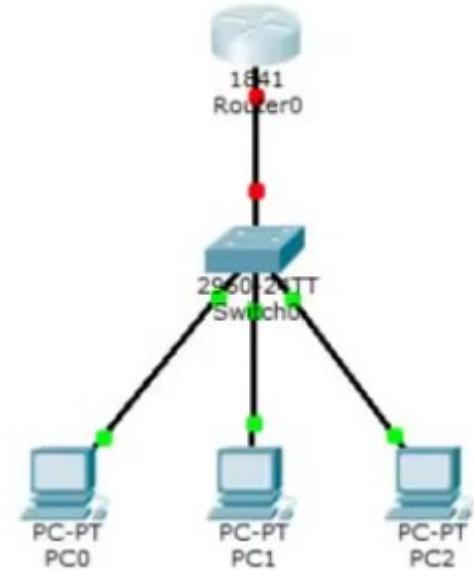
exit
interface GigabitEthernet0/1.4
encapsulation dot1Q 4
ip address 192.168.4.1 255.255.255.0

```

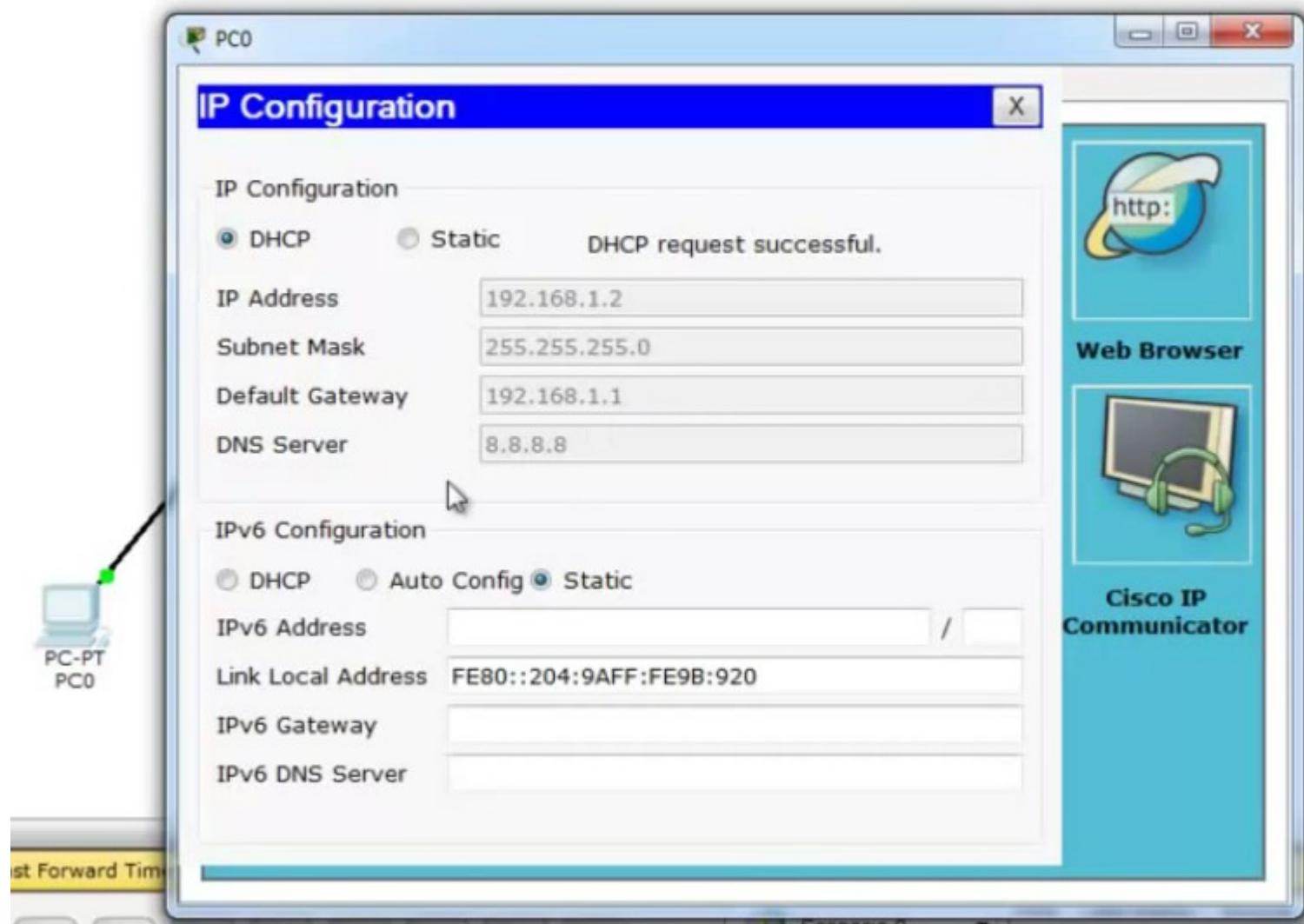
Настраиваем DHCP-сервер на Router0

Router0

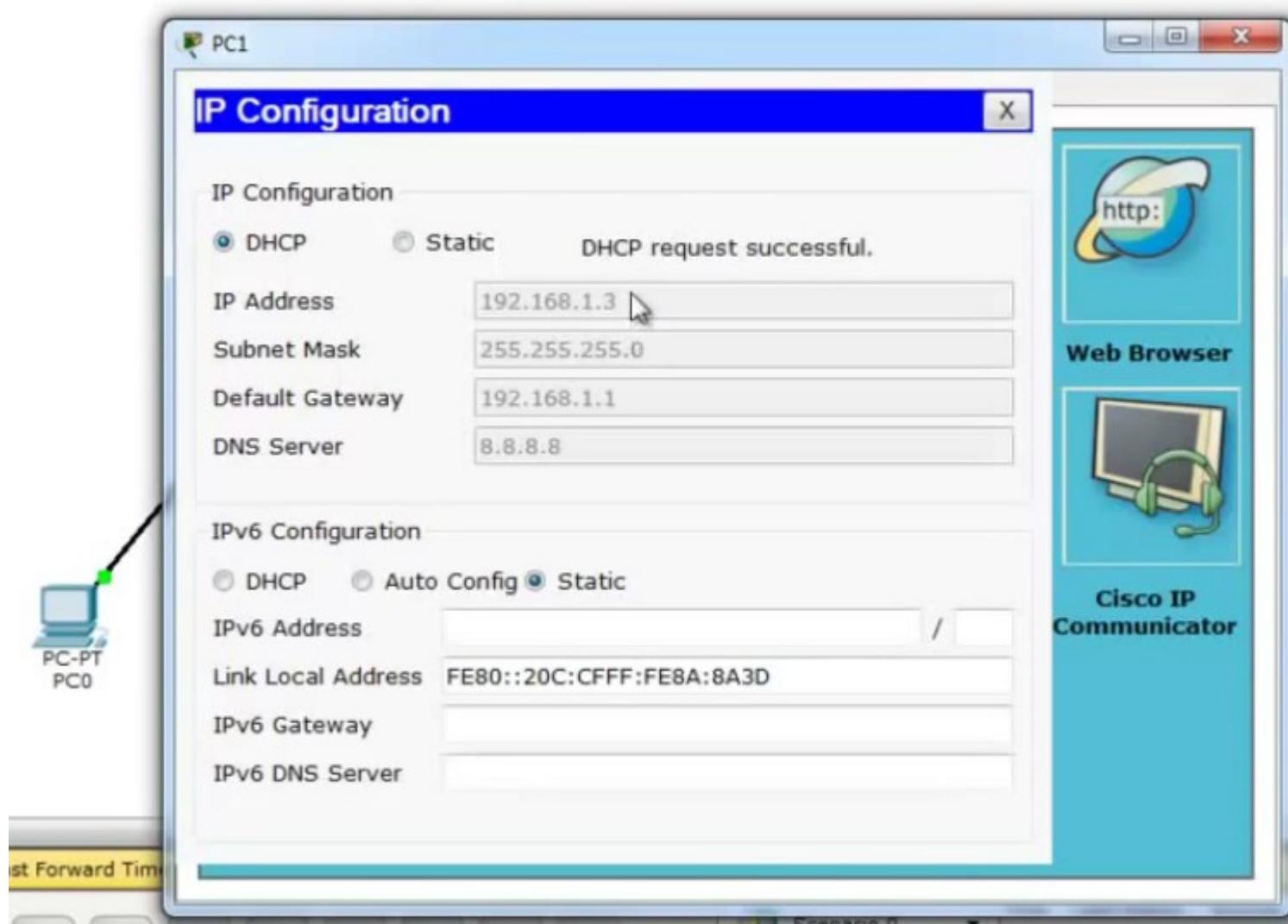
```
> no  
> en  
# conf t  
(config)# int fa0/0  
(config-if)# no shutdown  
(config-if)# ip address 192.168.1.1 255.255.255.0  
(config-if)# exit  
(config)# ip dhcp pool DHCP  
(dhcp-config)# network 192.168.1.0 255.255.255.0  
(dhcp-config)# default-router 192.168.1.1  
(dhcp-config)# dns-server 8.8.8.8  
(dhcp-config)# exit  
(config)# ip dhcp excluded-address 192.168.1.100  
(config)# ip dhcp excluded-address 192.168.1.1  
(config)#exit  
# wr mem
```



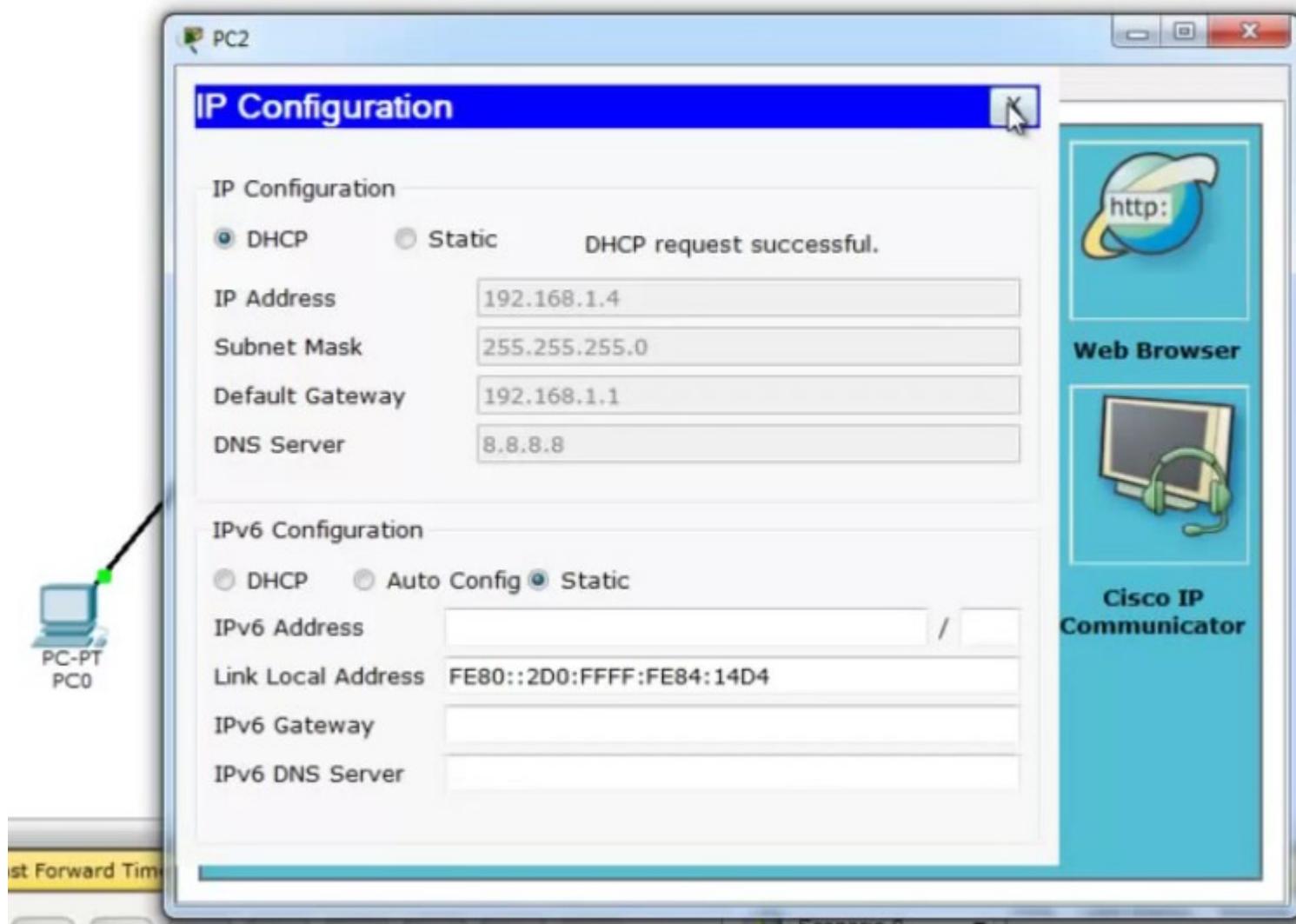
Включаем динамическое получение IP - DHCP на клиенте - PC0



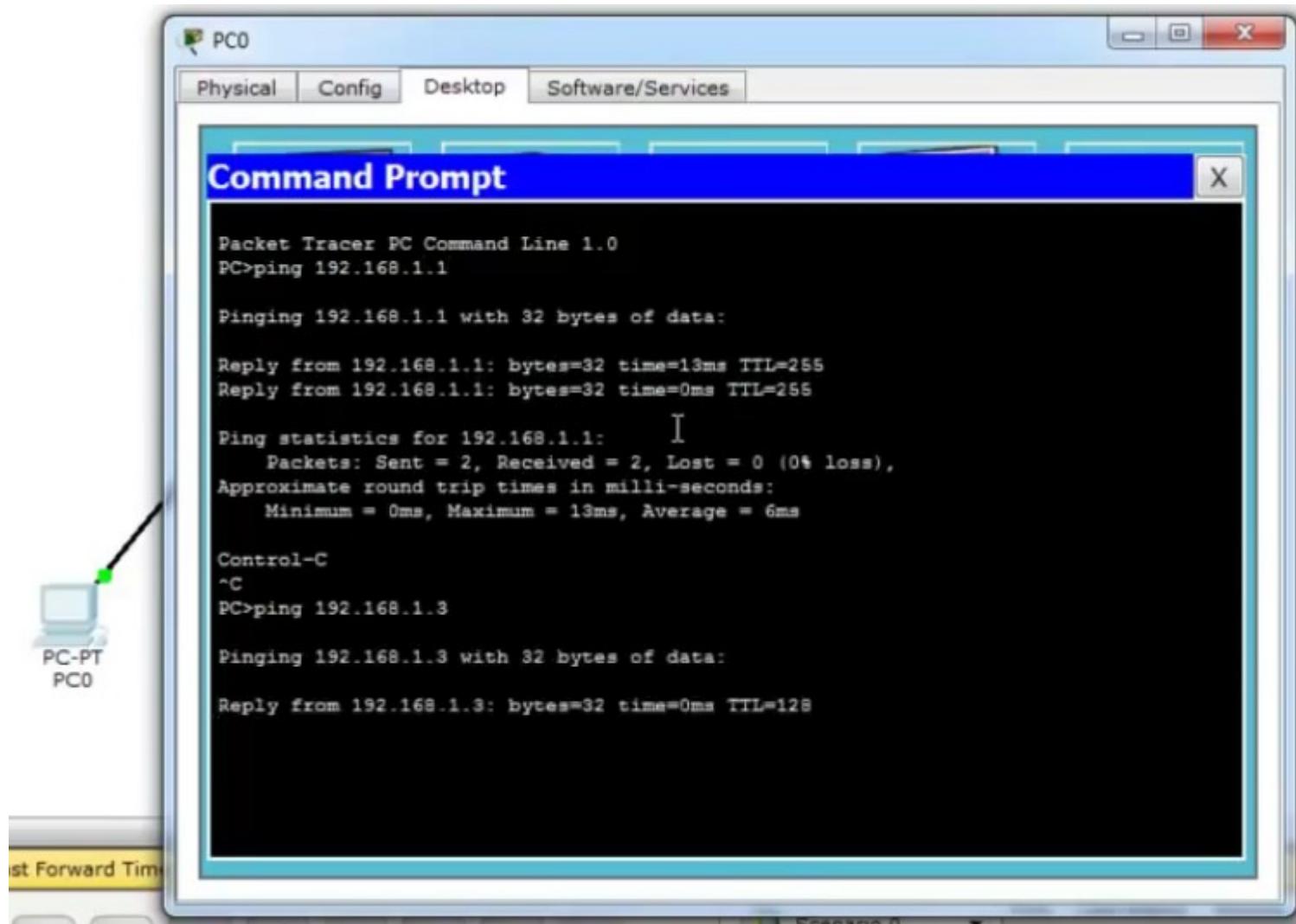
Аналогично поступаем на PC1



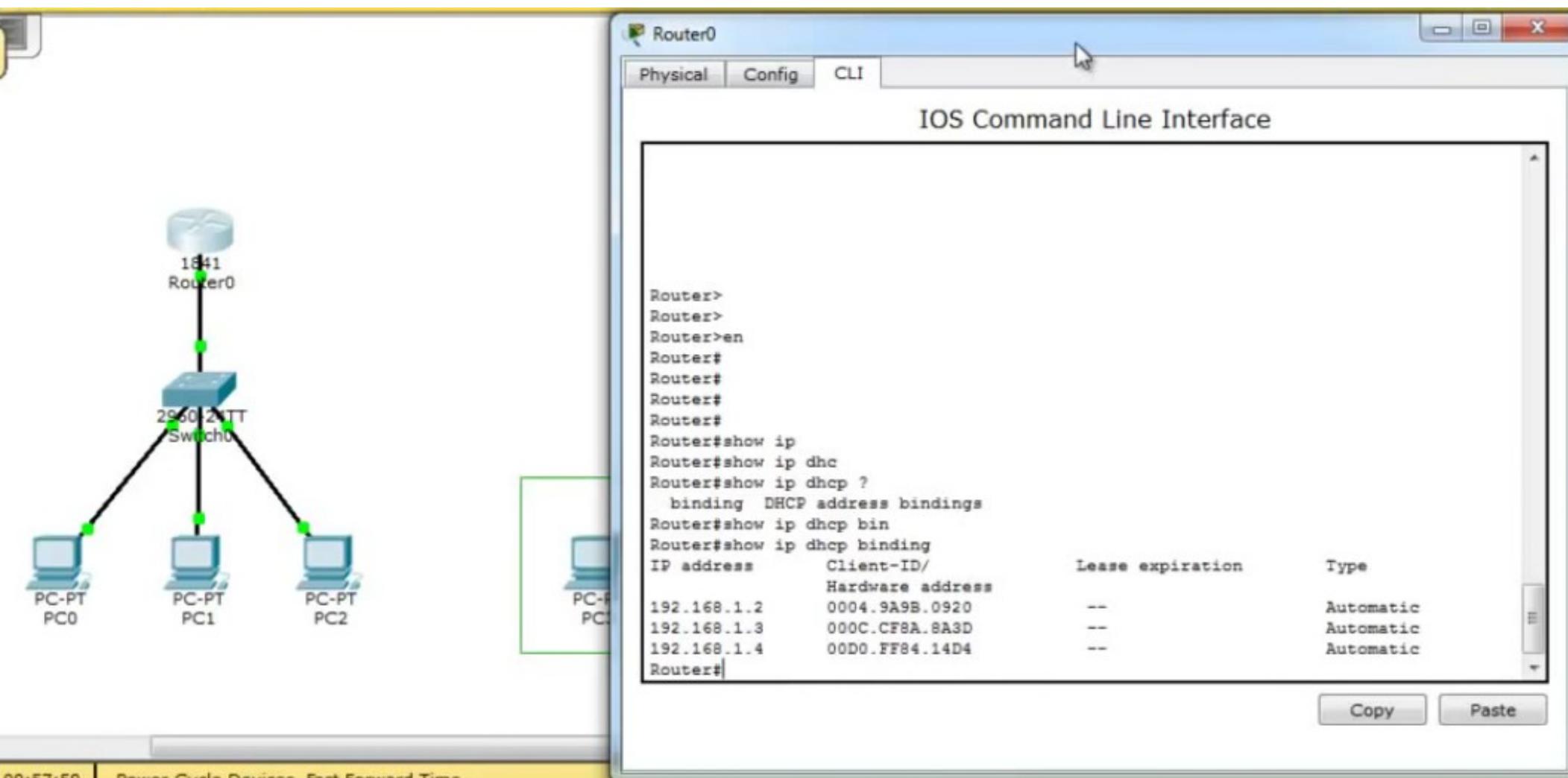
... и на PC2



Проверяем взаимодействие. Готово.



Можно посмотреть какие ip адреса каким узлам выданы.
Командой #show ip dhcp binding



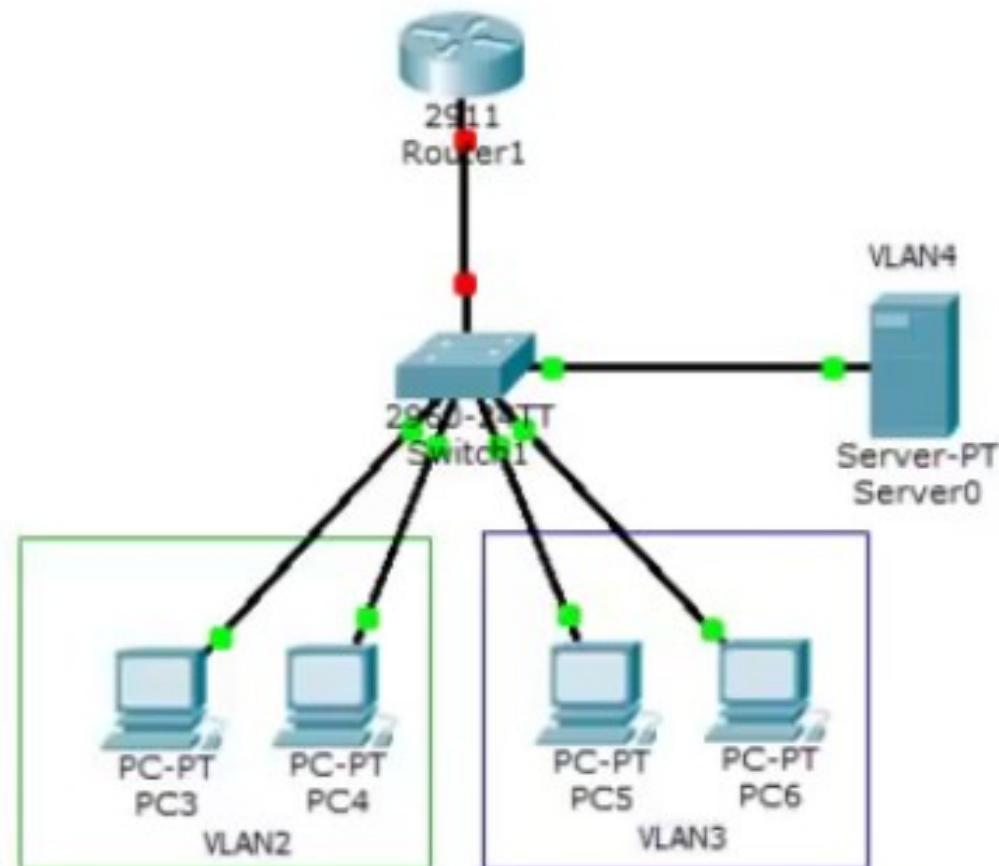
Второй пример.
Уже есть 2 VLAN'a.
(На самом деле Server-PT находится в 3-ем VLAN'e). Настраиваем
коммутатор Switch1

```
> en
# conf t
(config)# vlan 2
(config-vlan)# name VLAN2
(config-vlan)# exit
(config)# vlan 3
(config-vlan)# name VLAN3
(config-vlan)# exit
(config)# vlan 4
(config-vlan)# name DHCP
(config-vlan)# exit

(config)# int range fastEthernet 0/2-3
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 2
(config-if-range)# exit

(config)# int range fastEthernet 0/4-5
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 3
(config-if-range)# exit

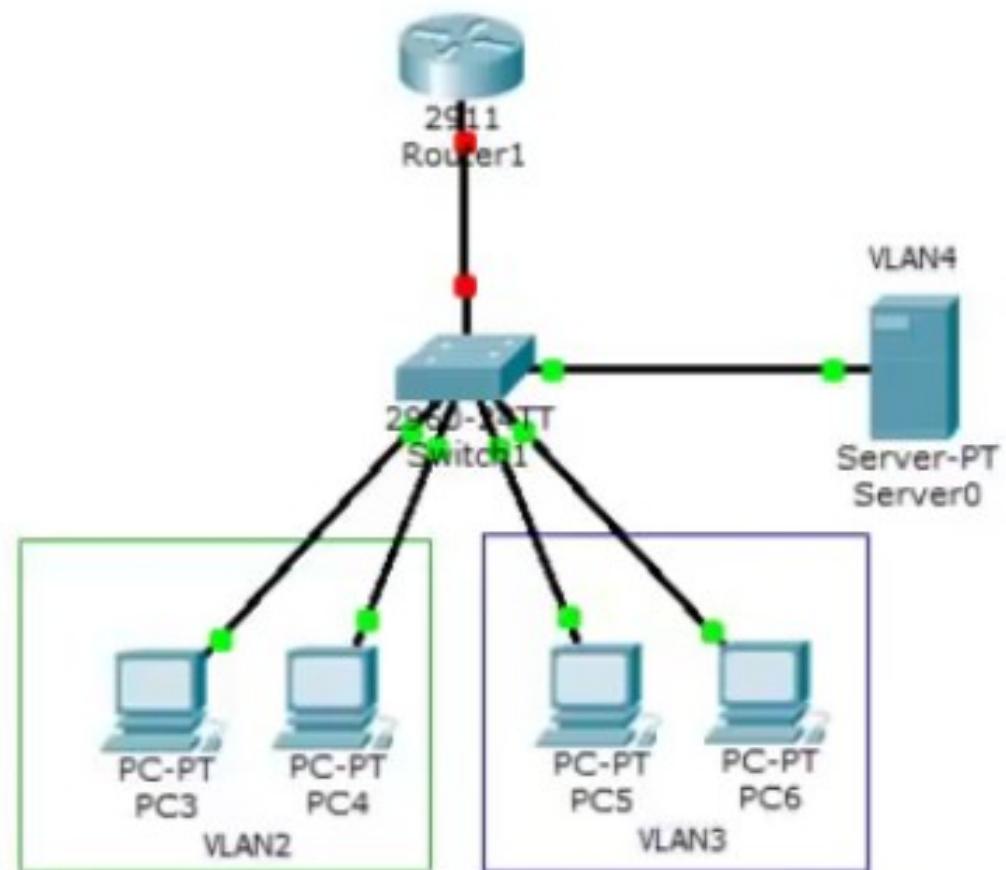
(config)# int range fastEthernet 0/6
(config-if)# switchport mode access
(config-if)# switchport access vlan 4
(config-if)# exit
```



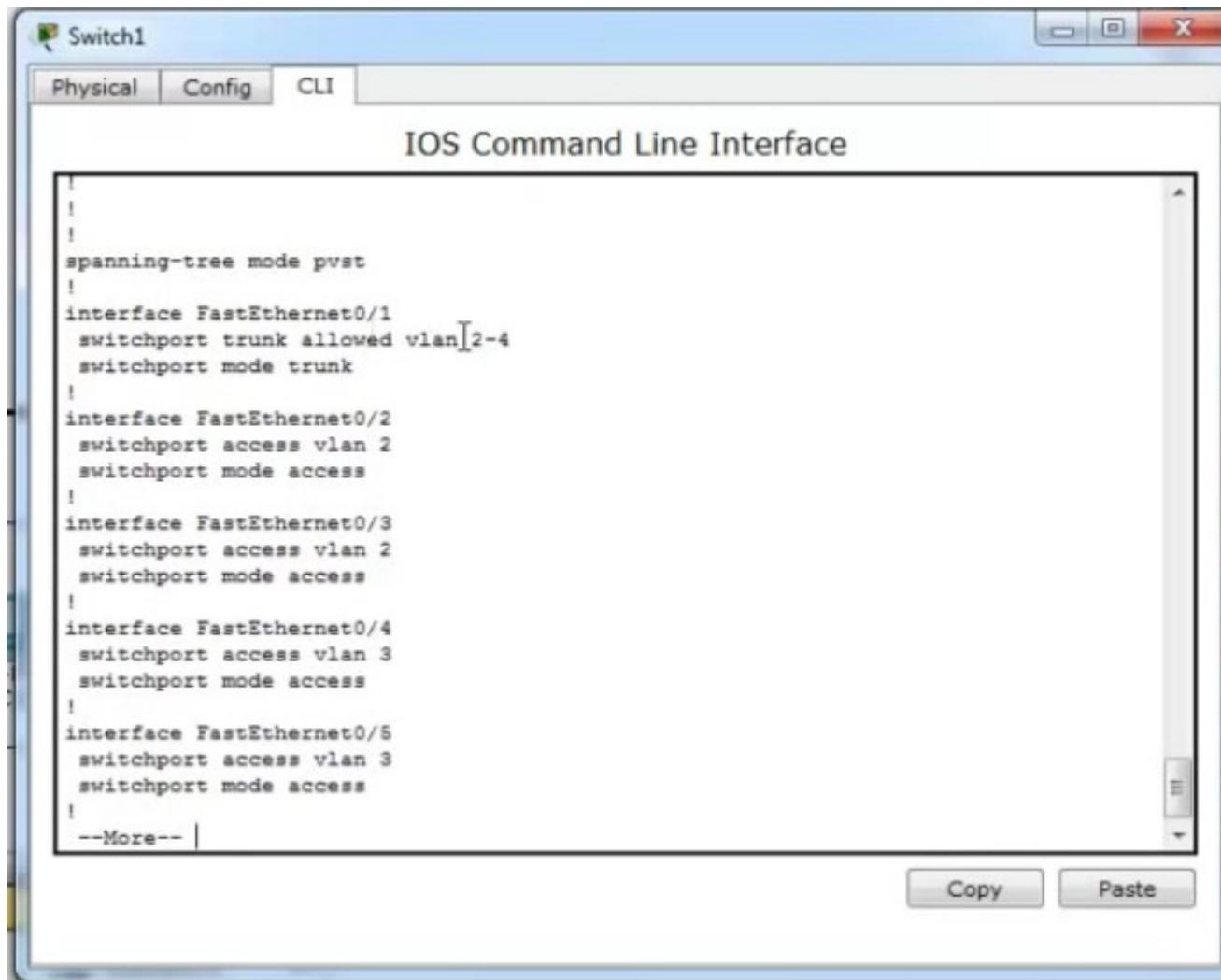
Настраиваем коммутатор Switch1

```
(config)# int fastEthernet 0/1  
(config-if)# switchport mode trunk  
(config-if)# switchport trunk allowed vlan 2,3,4  
(config)# exit
```

```
# wr mem  
# show run
```



Проверяем конфигурацию Switch1



Switch1

Physical Config CLI

IOS Command Line Interface

```
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport trunk allowed vlan[2-4
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 3
switchport mode access
!
--More--
```

Copy Paste

Настраиваем маршрутизатор Router1

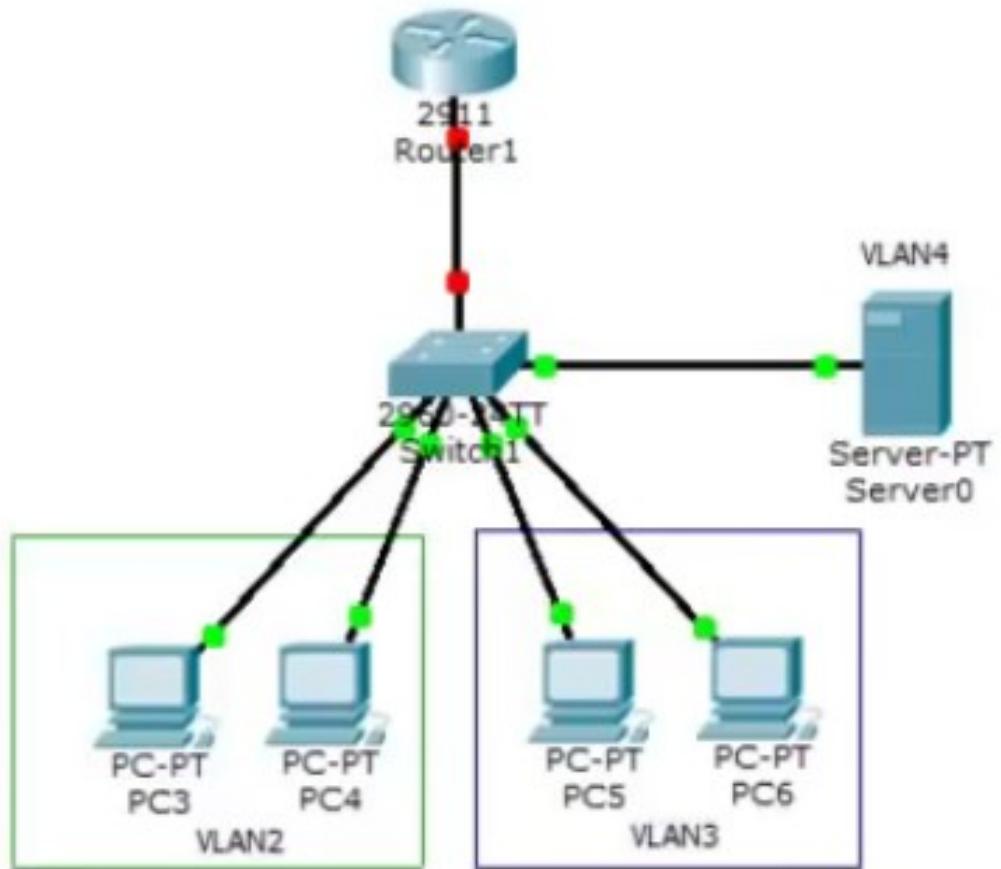
```
> en
# config t
(config)# int gi0/0.2
(config-subif)# encapsulation dot1Q 2
(config-subif)# ip address 192.168.2.1 255.255.255.0
(config-subif)# no shutdown
(config)# exit

(config)# int gi0/0
(config-if)# no shutdown
(config)# exit

(config)# int gi0/0.3
(config-subif)# encapsulation dot1Q 3
(config-subif)# ip address 192.168.3.1 255.255.255.0
(config-subif)# no shutdown
(config)# exit

(config)# int gi0/0.4
(config-subif)# encapsulation dot1Q 4
(config-subif)# ip address 192.168.4.1 255.255.255.0
(config-subif)# no shutdown
(config)# end

# wr mem
```



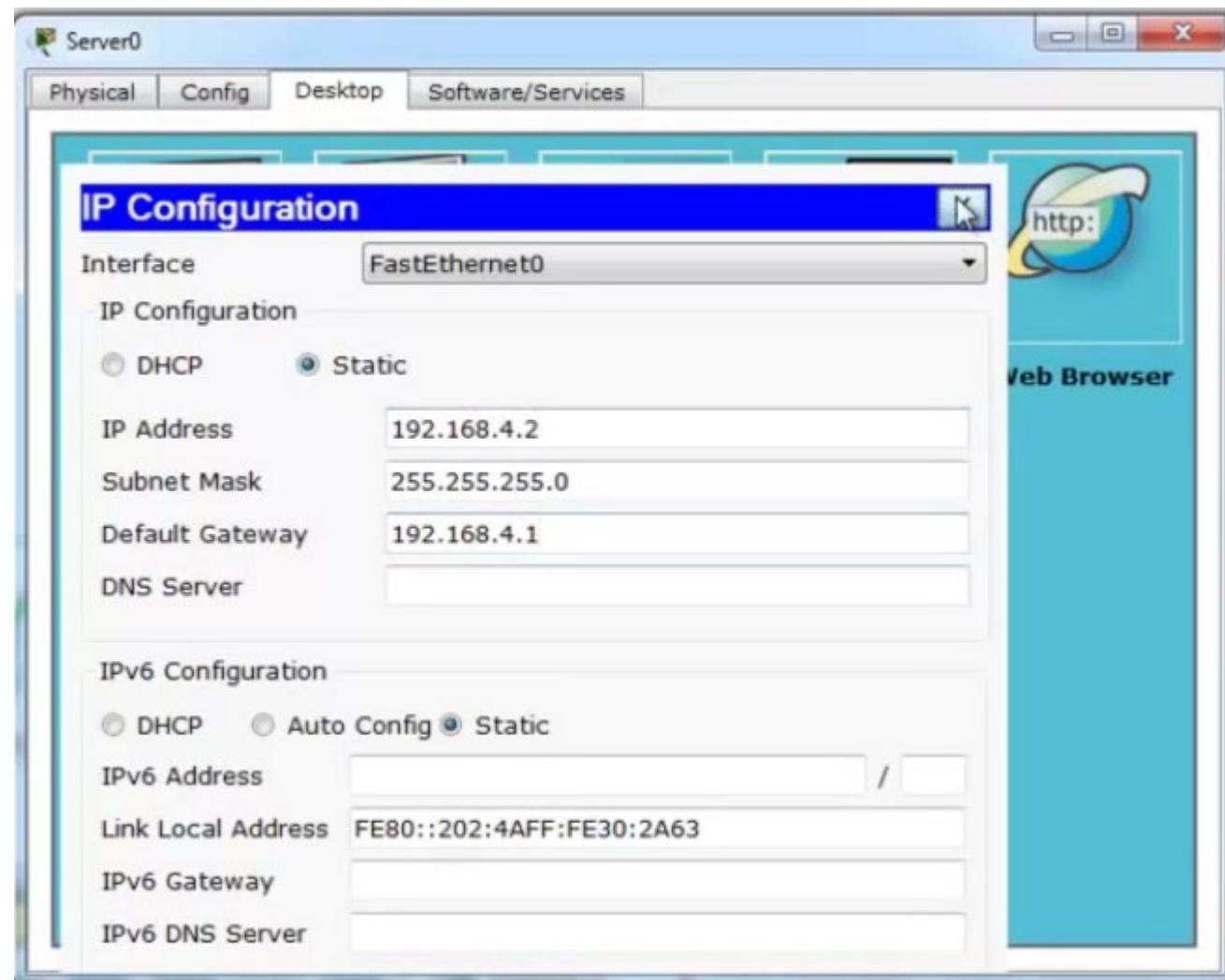
Проверяем настройки маршрутизатора Router1

show run

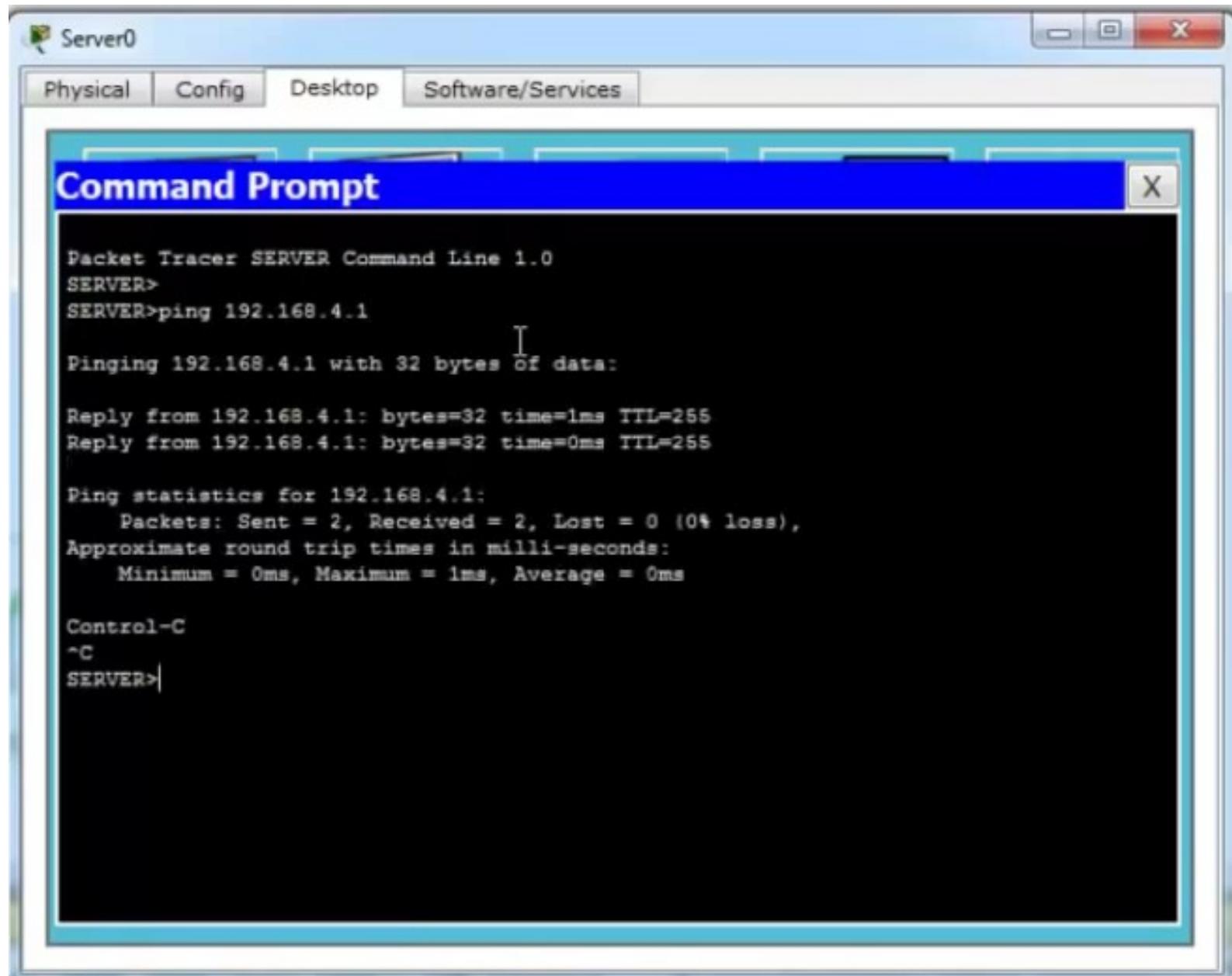
```
Router1
Physical | Config | CLI
IOS Command Line Interface
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/0.2
encapsulation dot1Q 2
ip address 192.168.2.1 255.255.255.0
!
interface GigabitEthernet0/0.3
encapsulation dot1Q 3
ip address 192.168.3.1 255.255.255.0
!
interface GigabitEthernet0/0.4
encapsulation dot1Q 4
ip address 192.168.4.1 255.255.255.0
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/2
no ip address
duplex auto
--More--
```

Copy Paste

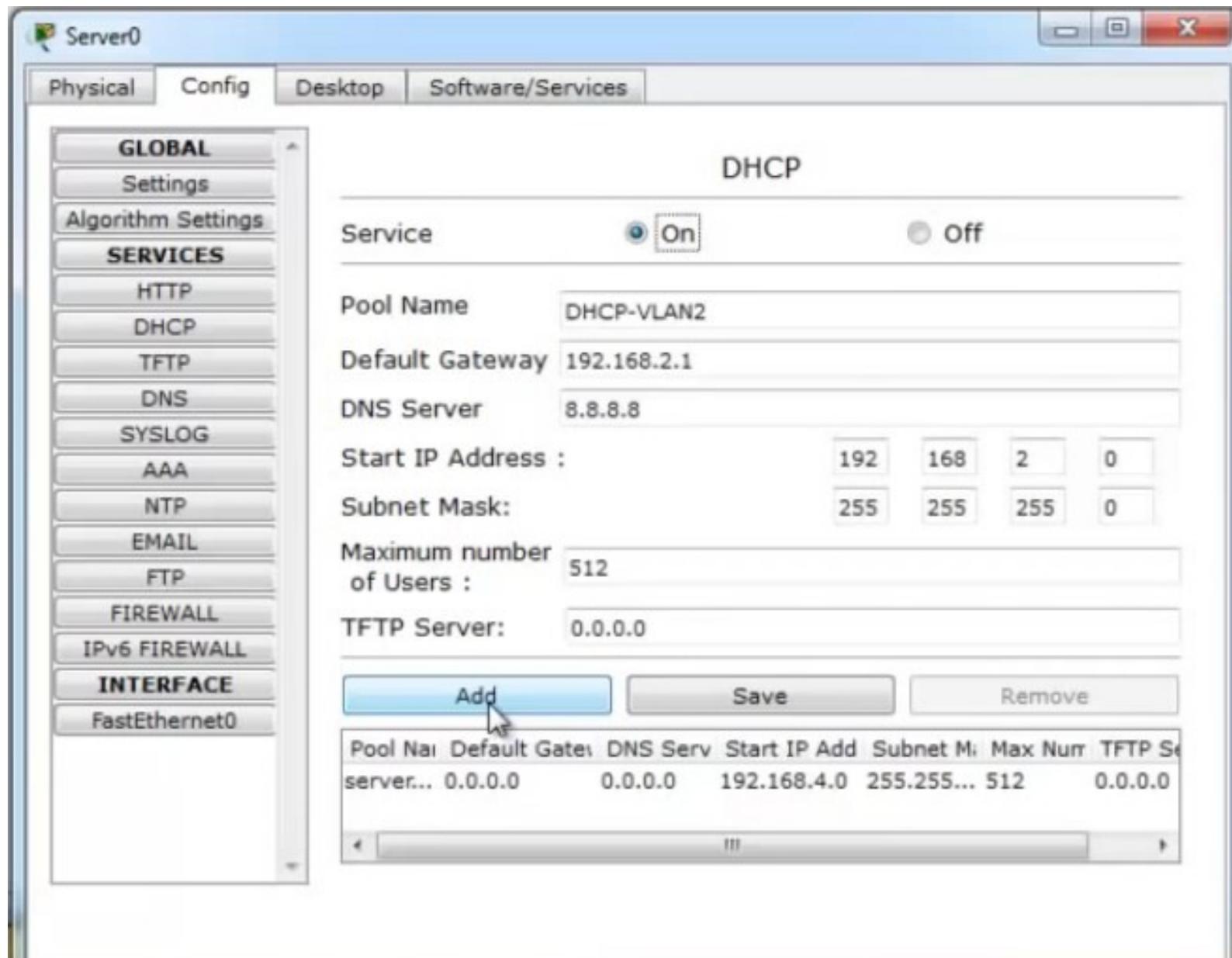
Зададим статический IP для сервера Server0



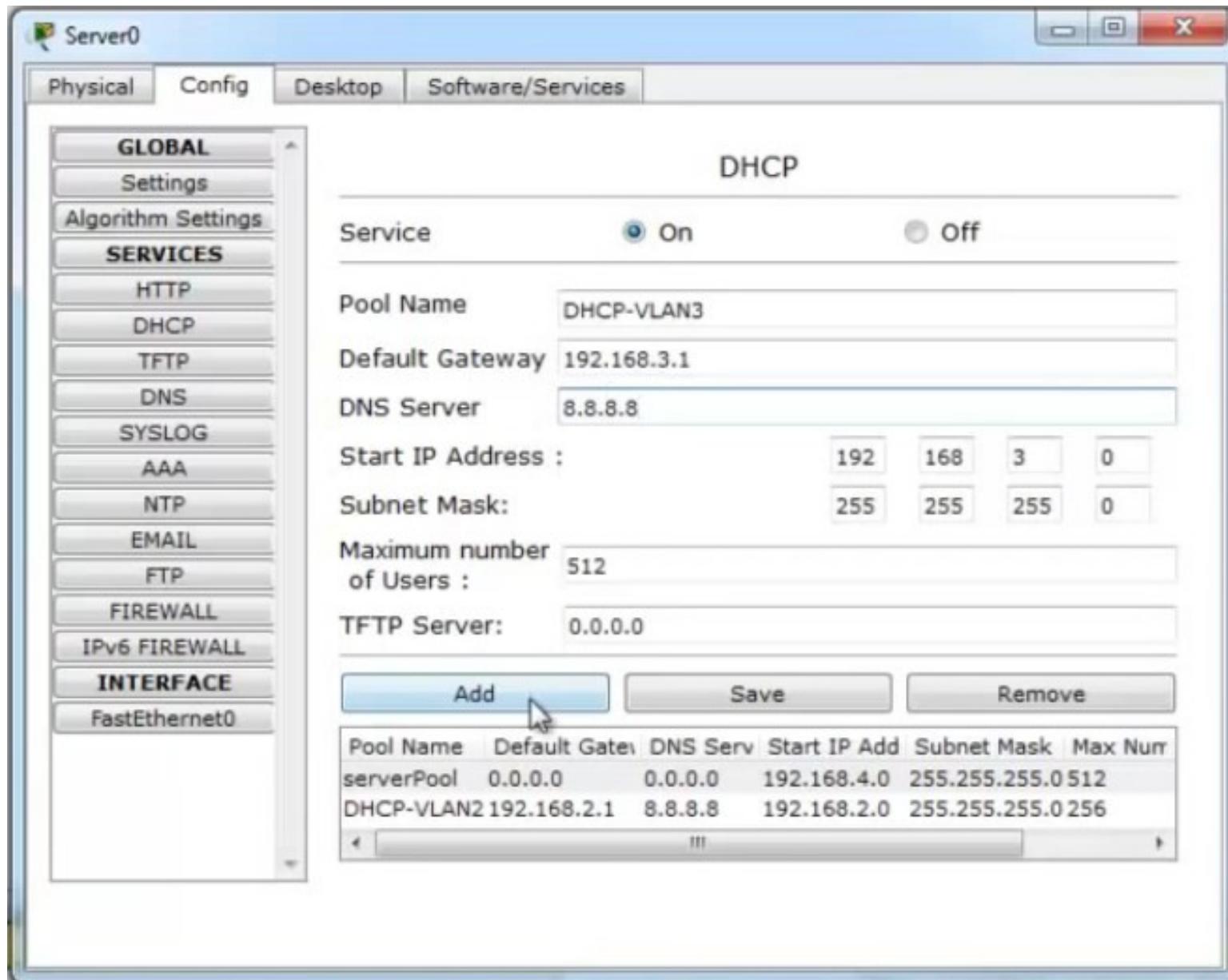
Проверим взаимодействие сервера Server0 и маршрутизатора Router1



Добавляем еще один DHCP-пул на Server 0.
Заходим в Config > DHCP ... заполняем, нажимаем Add



... аналогично добавляем пул для 3-го VLAN ...

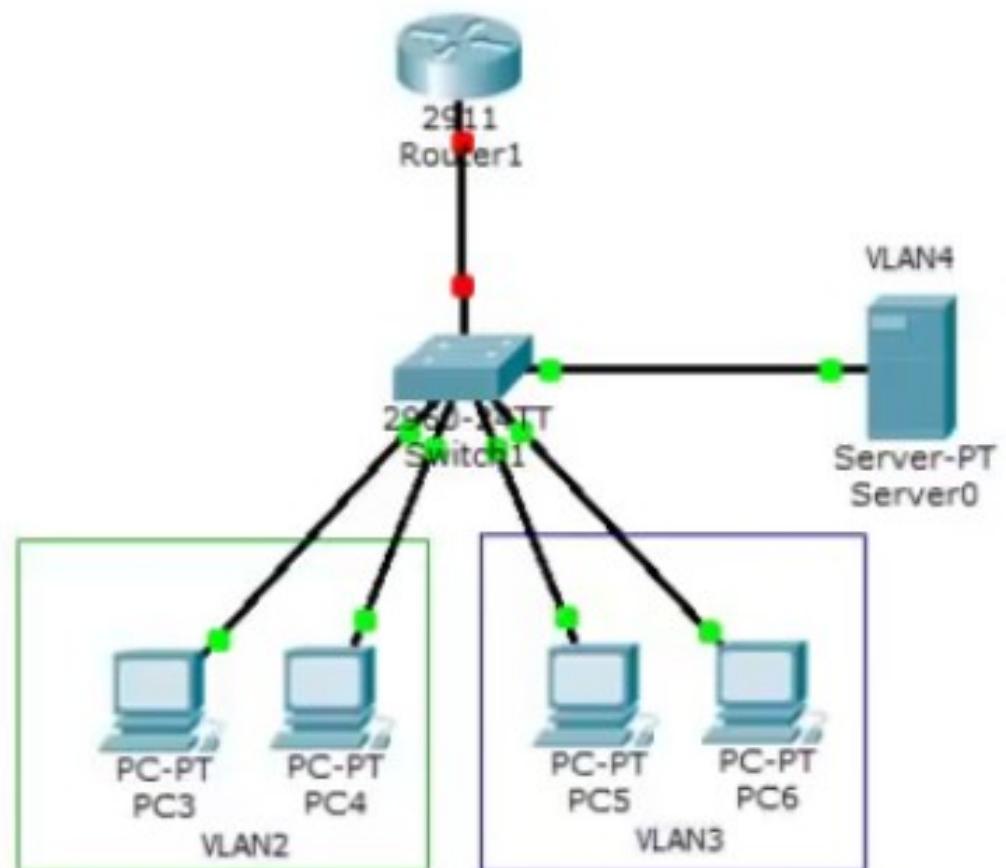


Настраиваем переадресацию DHCP запросов с компьютеров на сервер - на маршрутизаторе Router1

```
#conf t  
(config)# int gi 0/0.2  
(config-subif)# ip helper-address 192.168.4.2  
(config)# exit
```

```
#conf t  
(config)# int gi 0/0.3  
(config-subif)# ip helper-address 192.168.4.2  
(config)# end
```

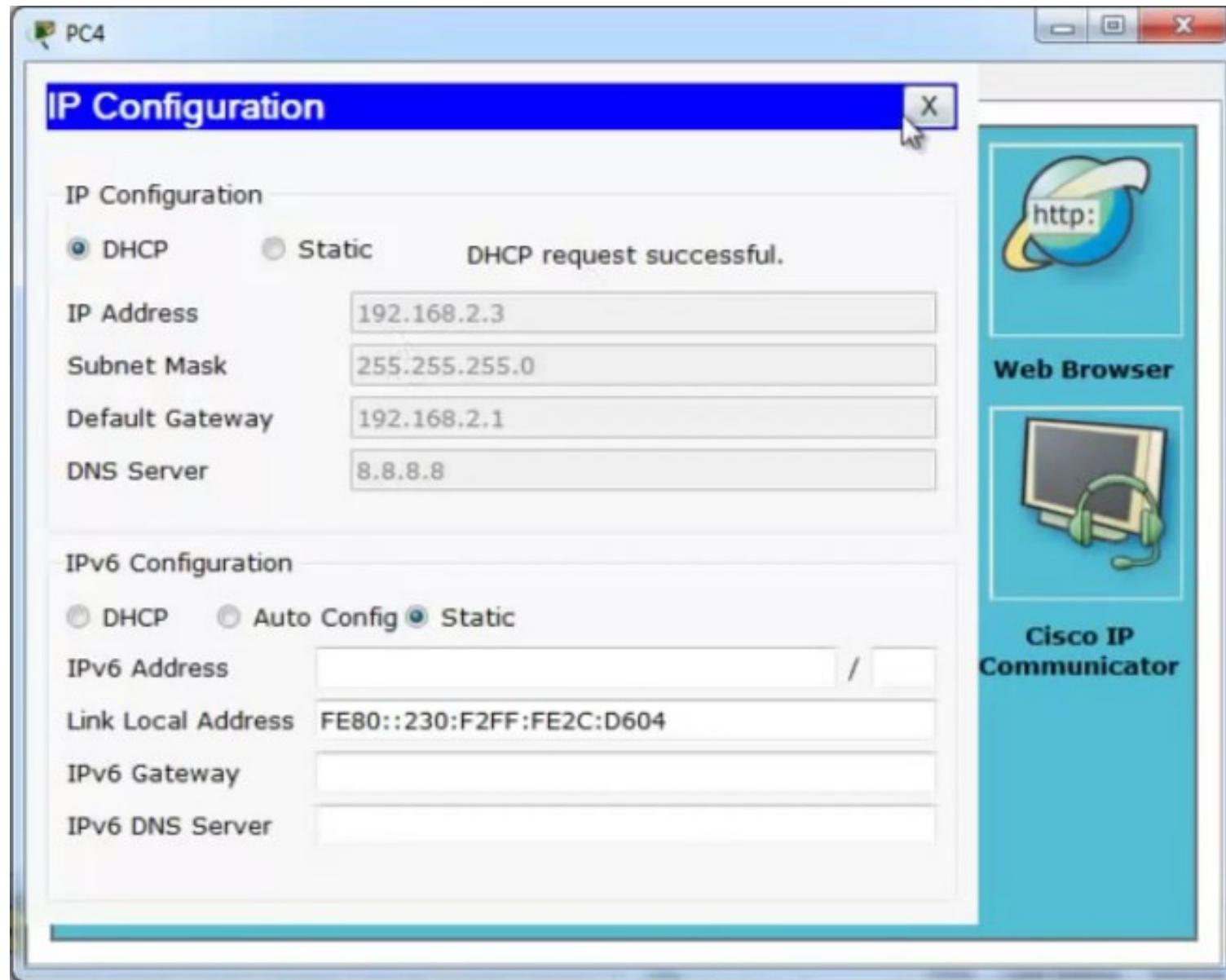
```
#wr mem
```



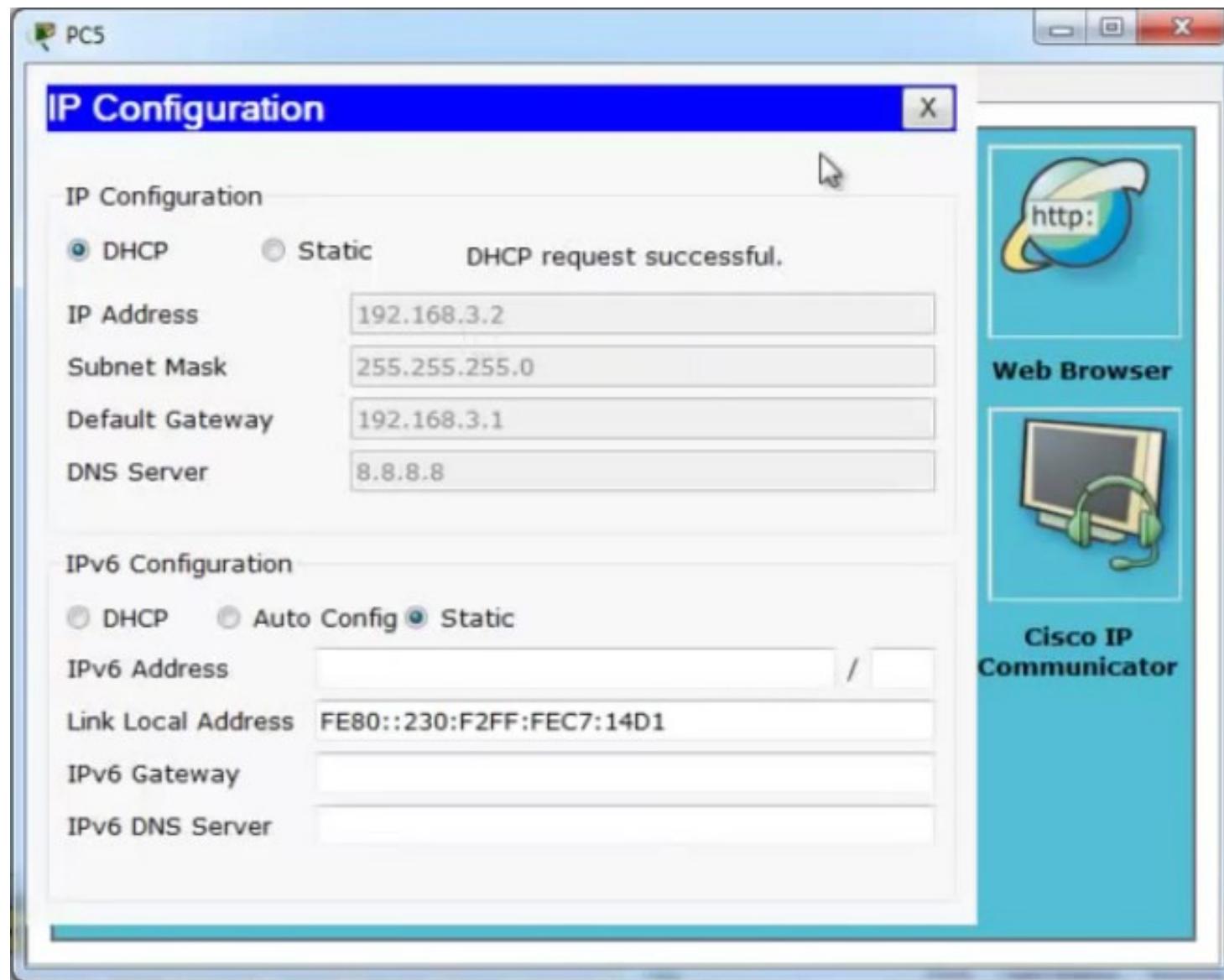
Пробуем получить IP адрес на компьютерах по DHCP



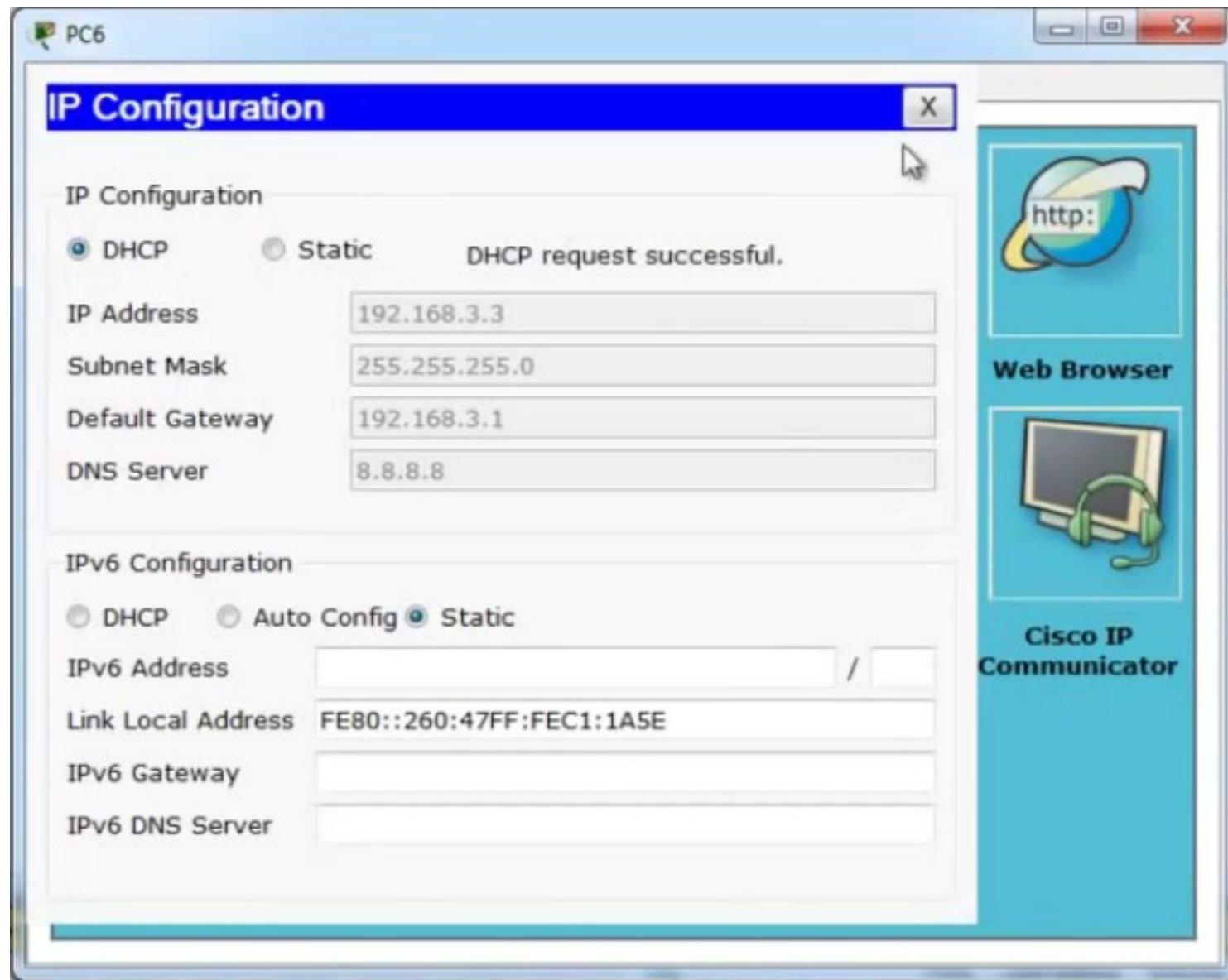
Пробуем получить IP адрес на компьютерах по DHCP



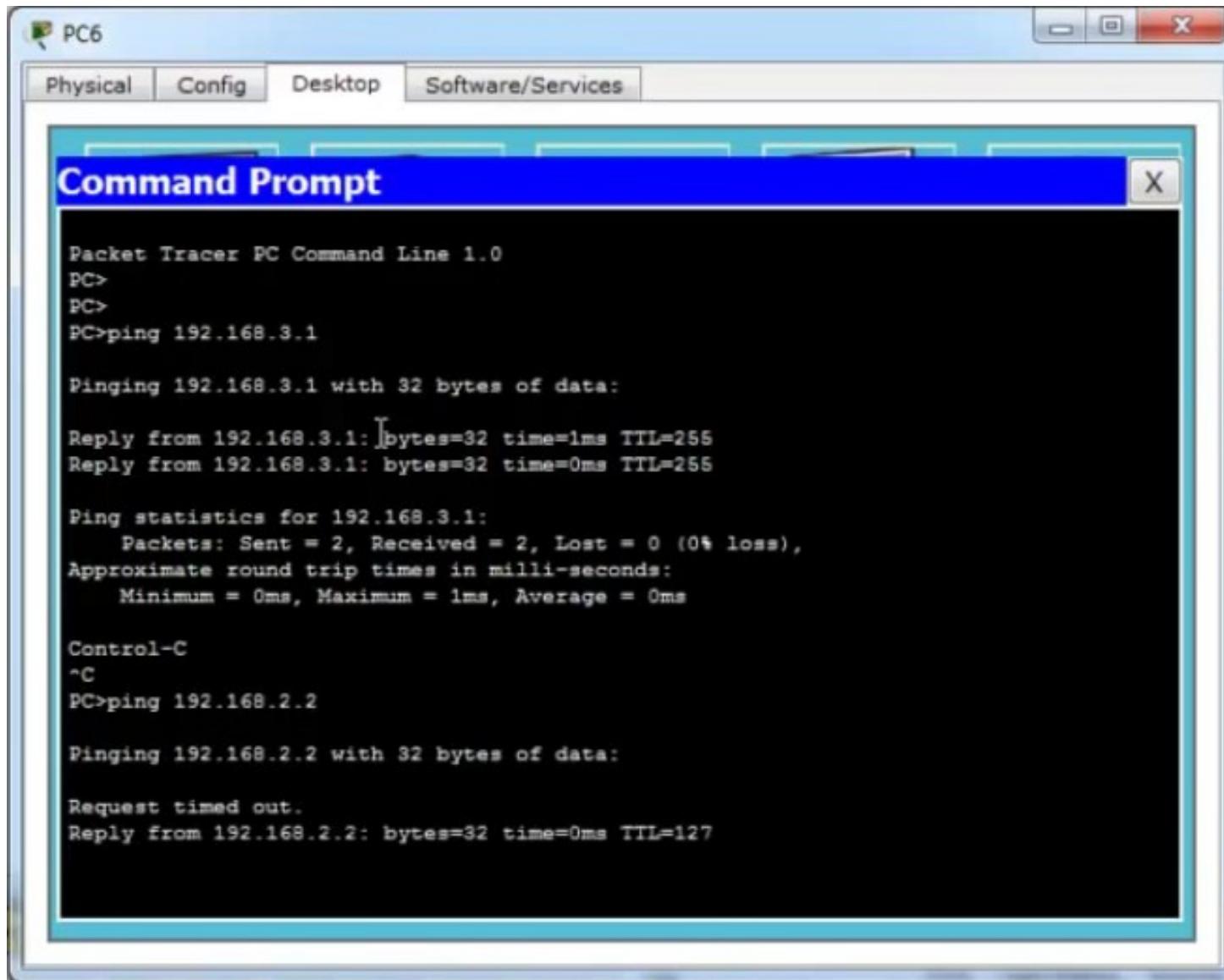
Пробуем получить IP адрес на компьютерах по DHCP



Пробуем получить IP адрес на компьютерах по DHCP



Проверим взаимодействие с коммутатором и соседними узлами



NAT — Network Address Translation

NAT - Network Address Translation

Более подробно читайте [здесь](#)

Публичный IP адрес (Белый IP)

Более подробно читайте [здесь](#)

Частный IP адрес (Серый IP)

От 10.0.0.0 до 10.255.255.255 с маской 255.0.0.0 (сеть класса A - около 16 млн. адресов)

От 172.16.0.0 до 172.31.0.0 с маской 255.255.0.0 (сеть класса B - около 65 тыс. адресов)

От 192.168.0.0 до 192.168.255.255 с маской 255.255.255.0 (сеть класса C - около 256 адресов)

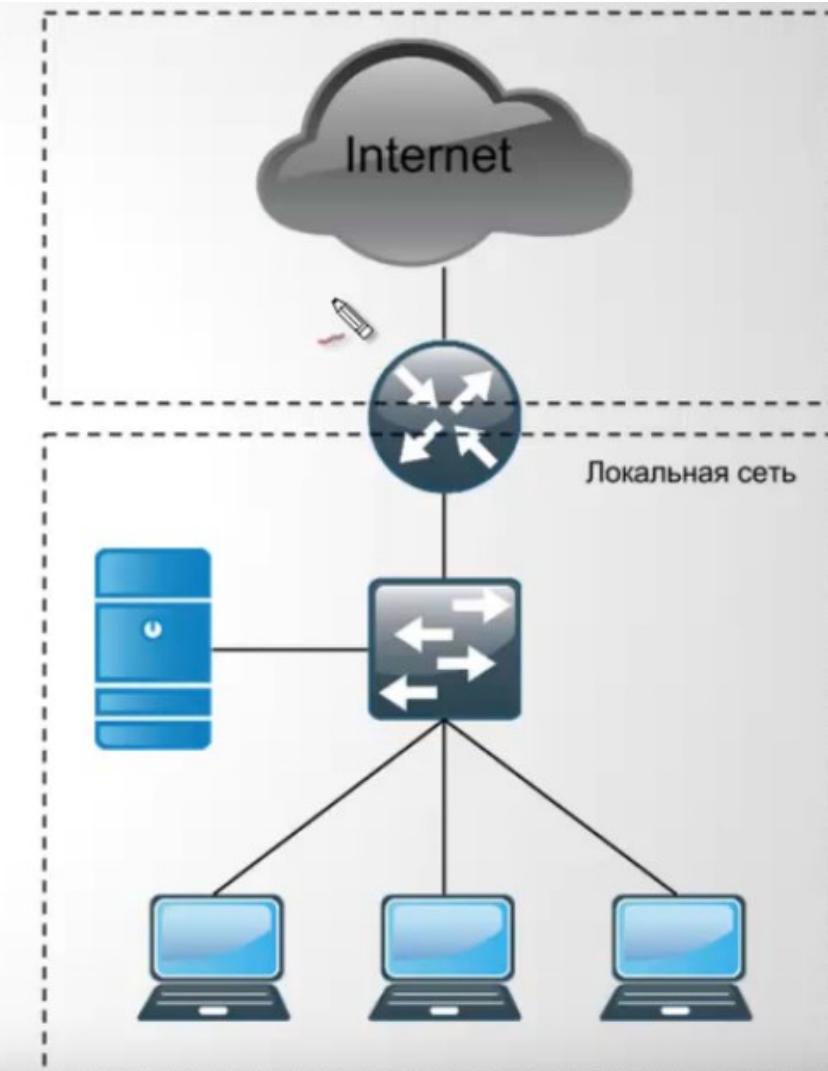
Более подробно читайте [здесь](#)

Статический NAT

Динамический NAT

Перегруженный NAT

Более подробно читайте [здесь](#)



NAT — Network Address Translation

Настройка PAT

```
interface FastEthernet0/0
 ip nat outside
interface FastEthernet0/1.2
 ip nat inside
interface FastEthernet0/1.3
 ip nat inside

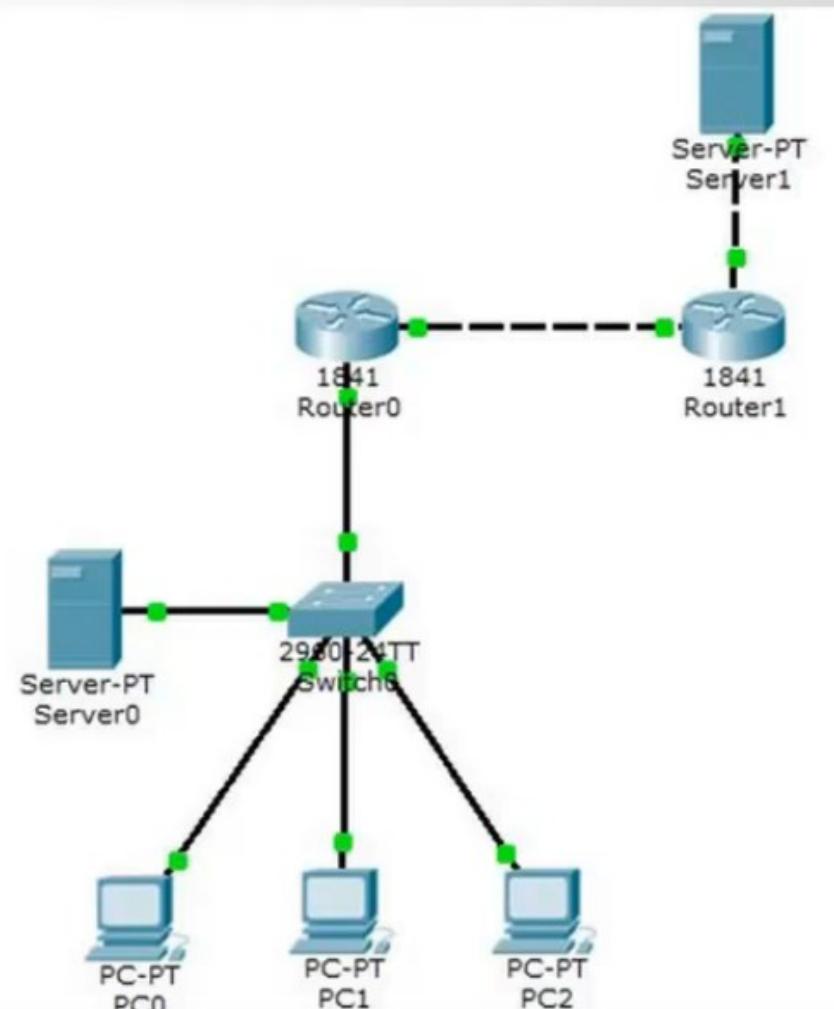
ip access-list standard FOR-NAT
permit 192.168.2.0 0.0.0.255
permit 192.168.3.0 0.0.0.255

ip nat inside source list FOR-NAT interface FastEthernet0/0 overload
```

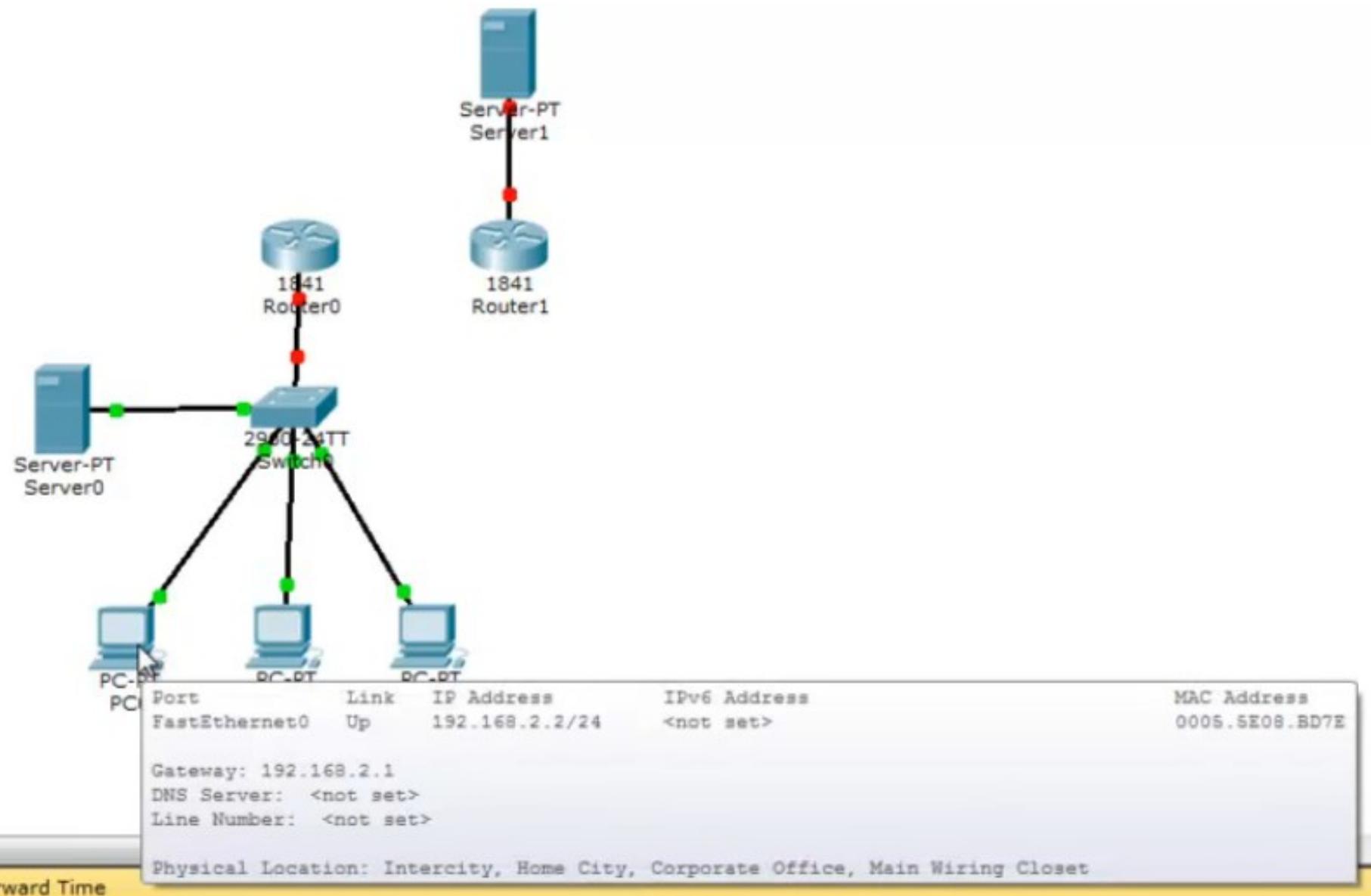
Настройка Static NAT

```
ip nat inside source static tcp 192.168.3.2 80 213.234.10.2 80
```

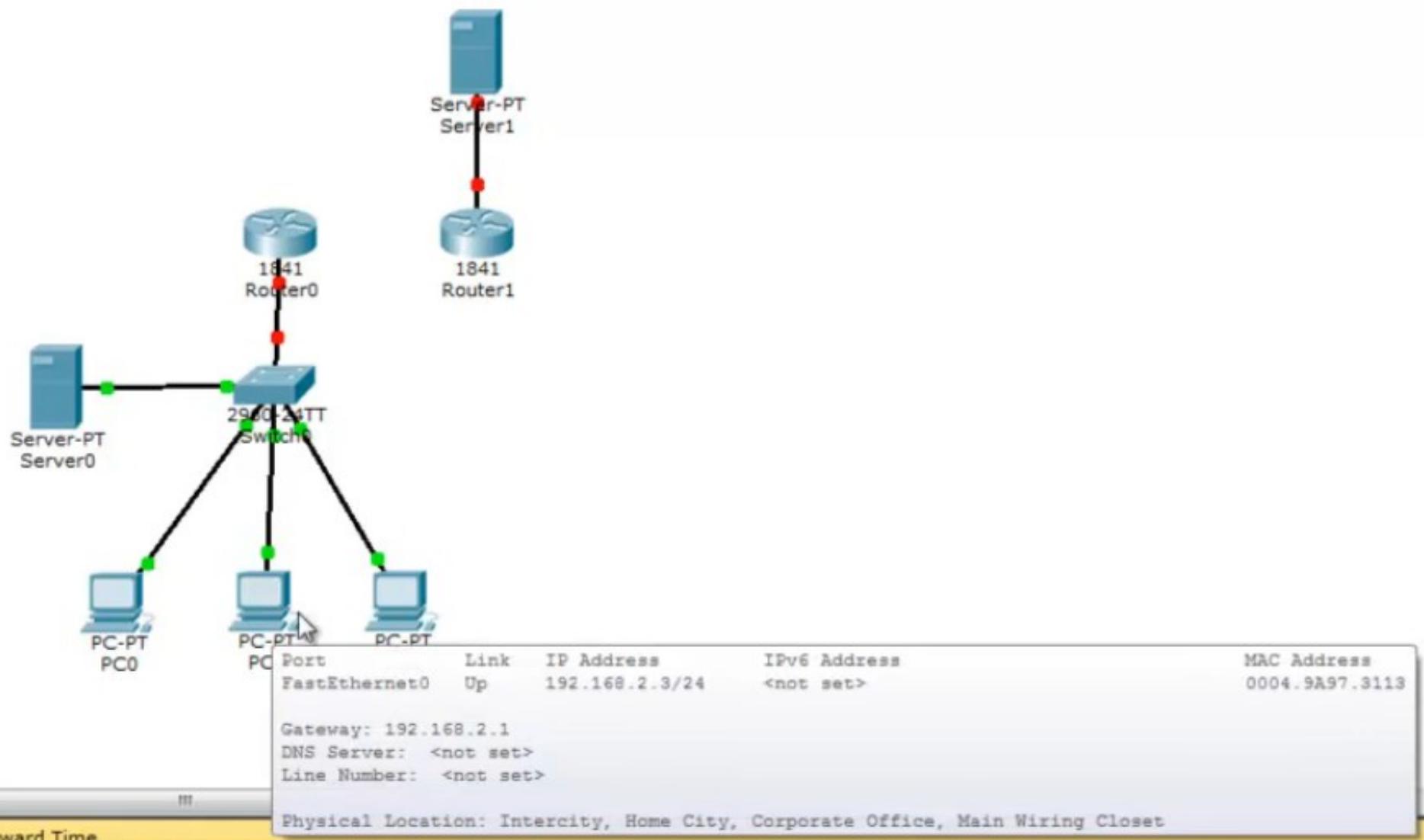
```
show ip nat translations
```



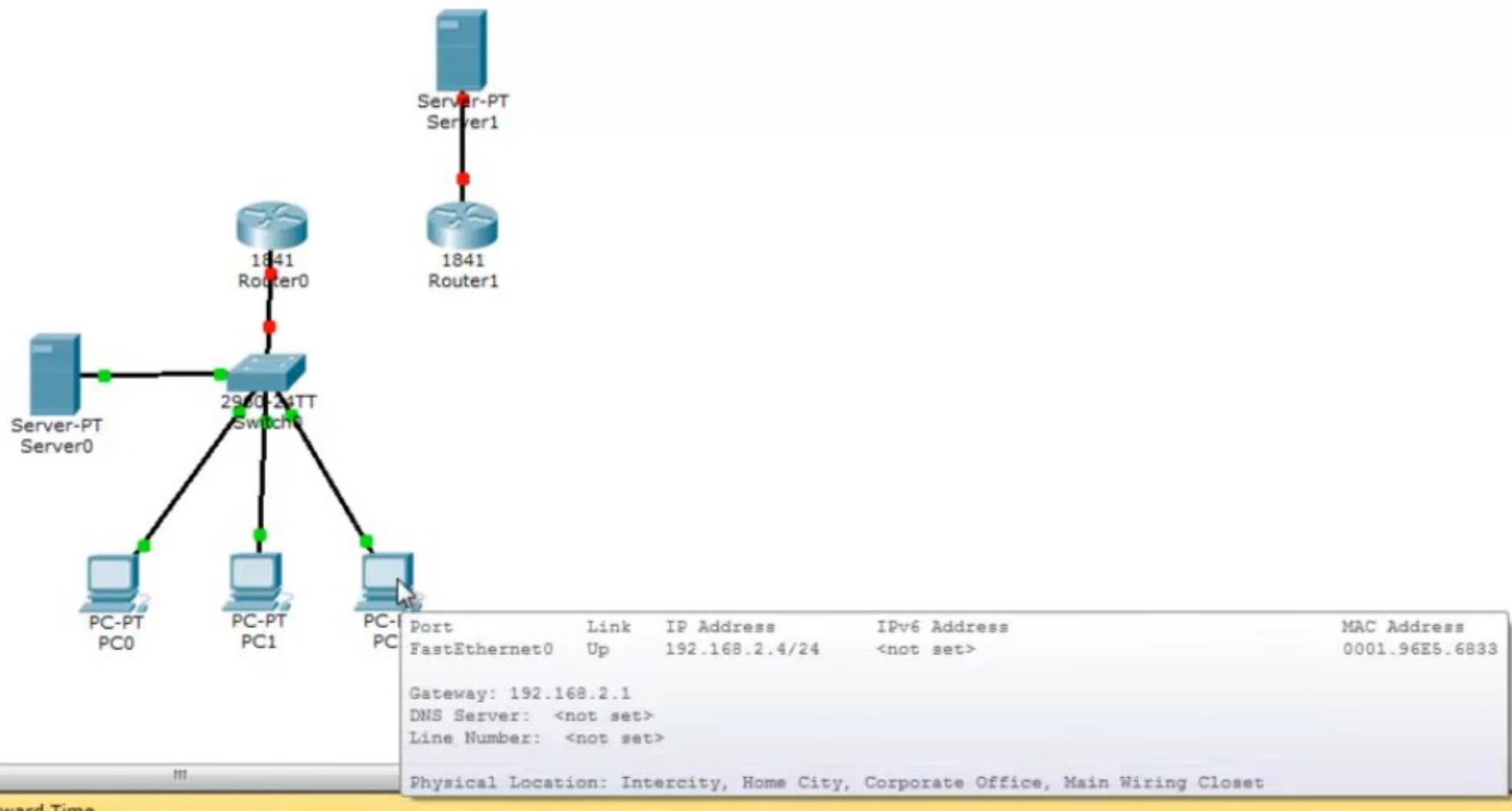
Ip адрес PC0



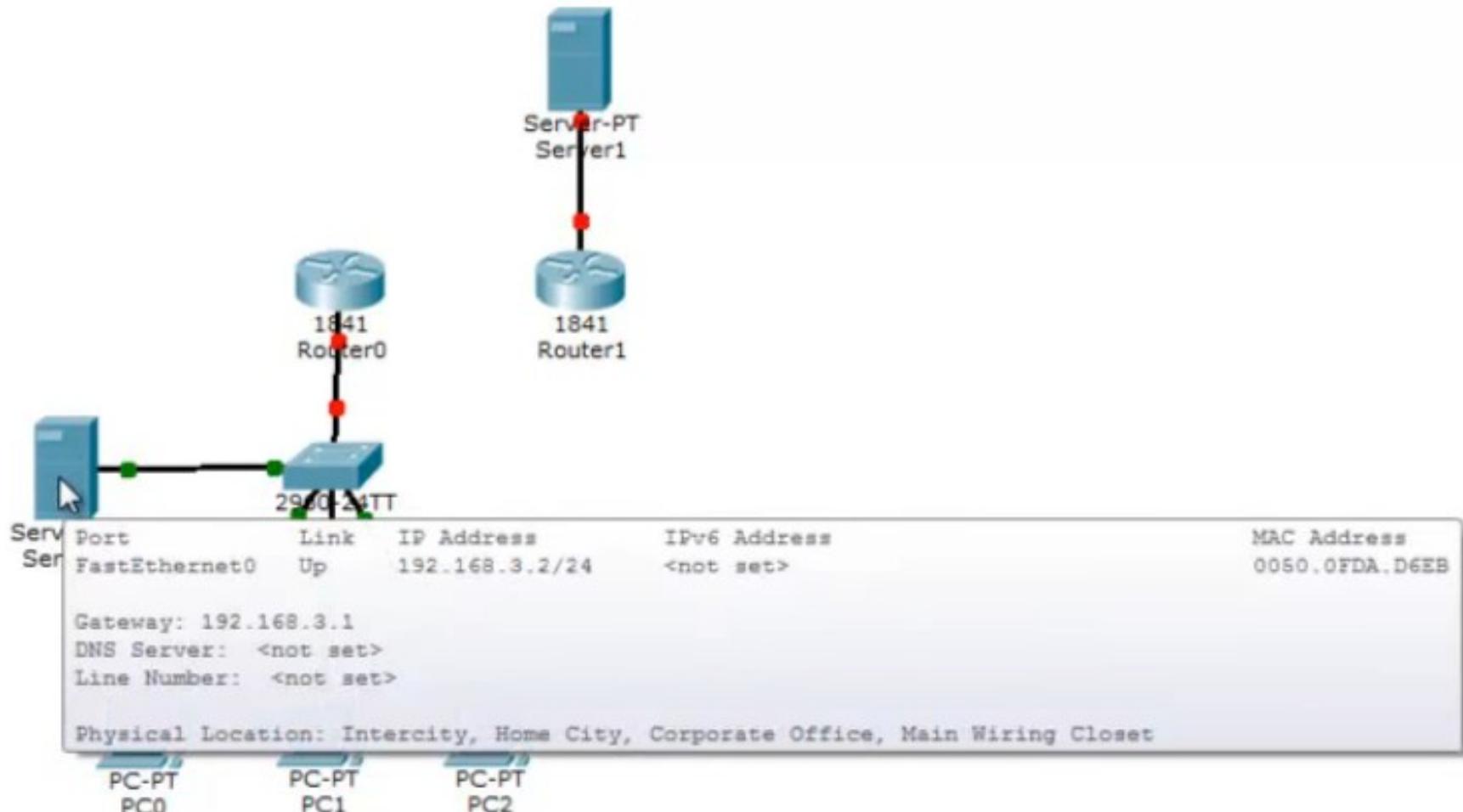
Ip адрес PC1



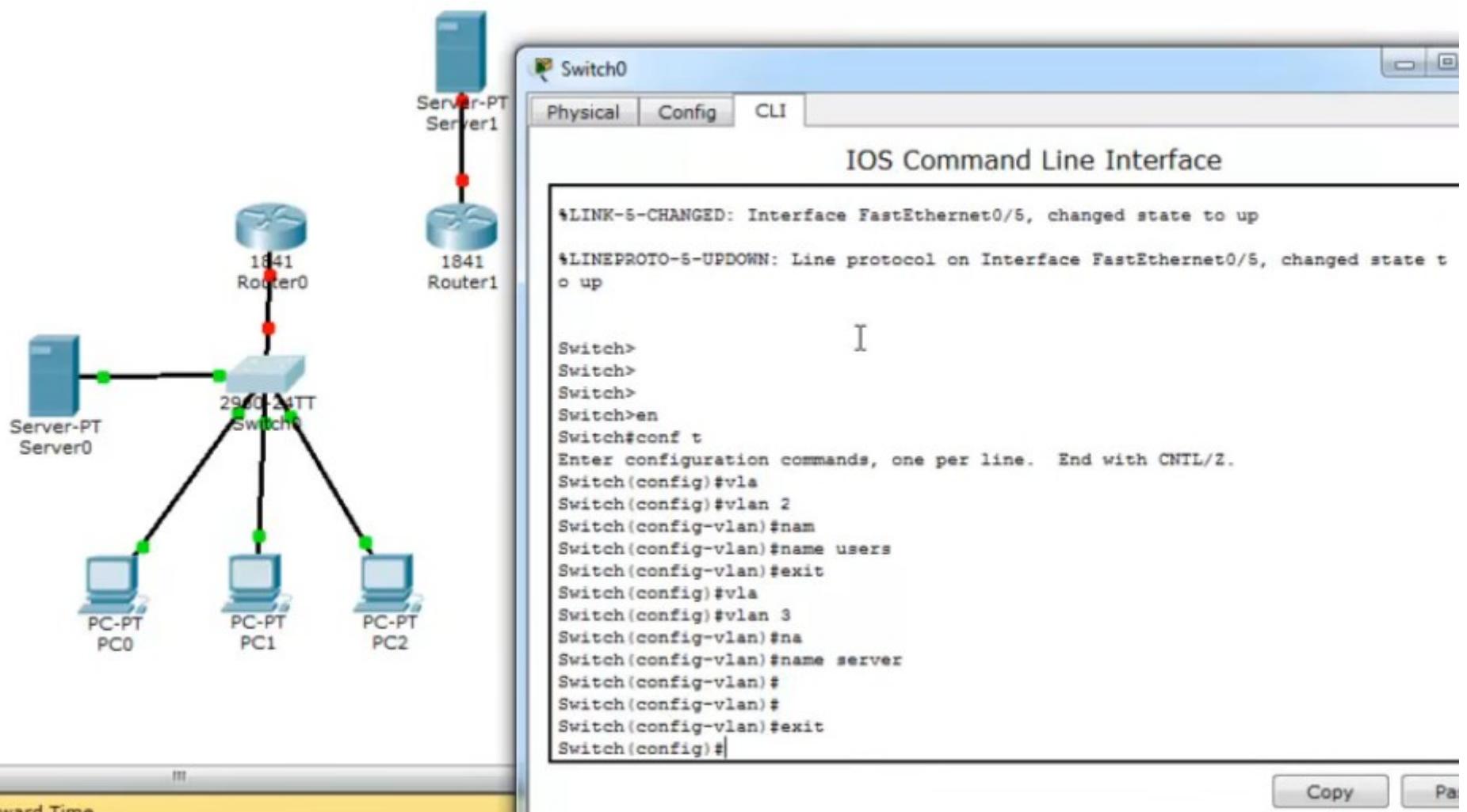
Ip адрес PC2



Ip адрес Sever0



На коммутаторе создадим VLAN 2 для компьютеров и VLAN 3 для серверов



Назначаем VLAN на порты коммутатора

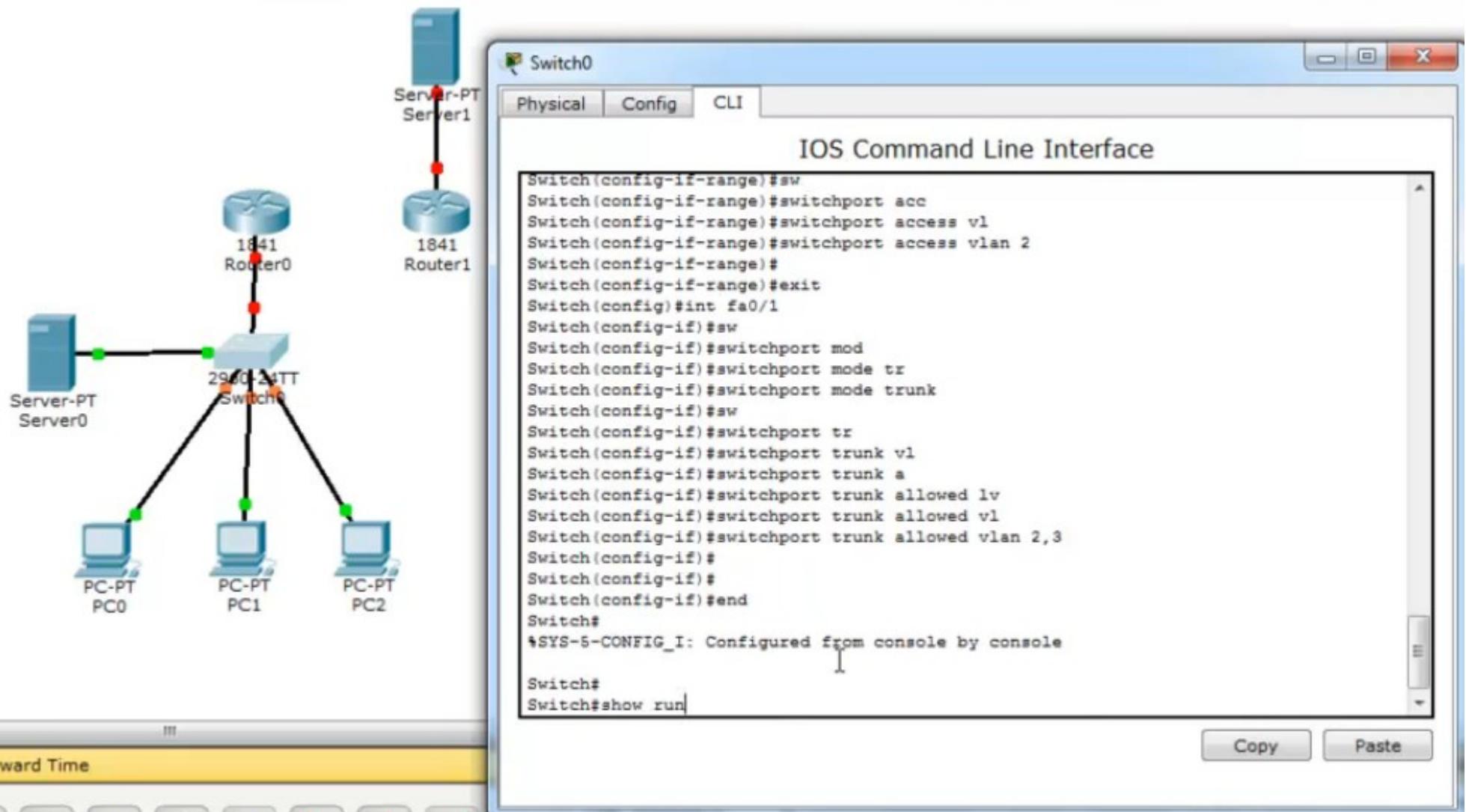
The network diagram illustrates a topology centered around a **Switch0**. It is connected to four devices: **Router0**, **Router1**, **Server0**, and three **PC-PT** (PC0, PC1, PC2) nodes. Router0 and Router1 are interconnected. Server0 is connected to Router0. The three PCs are connected directly to the **Switch0**.

The **Switch0** configuration window is open, showing the **Config** tab selected. The **IOS Command Line Interface** pane displays the following configuration script:

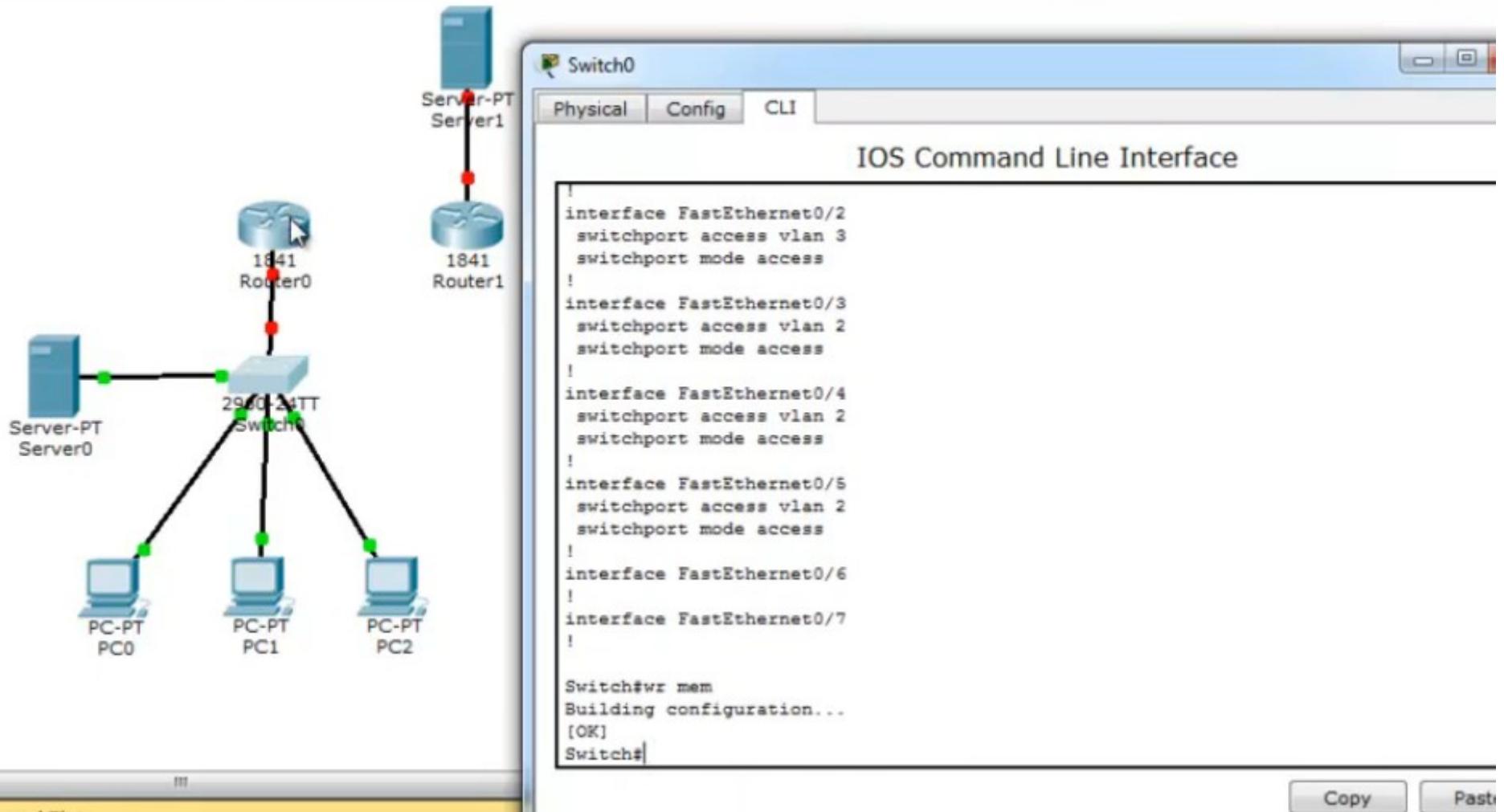
```
Switch(config)#  
Switch(config)#int fa0/2  
Switch(config-if)#sw  
Switch(config-if)#switchport mod  
Switch(config-if)#switchport mode acc  
Switch(config-if)#switchport mode access  
Switch(config-if)#sw  
Switch(config-if)#switchport acc  
Switch(config-if)#switchport access vl  
Switch(config-if)#switchport access vlan 3  
Switch(config-if)#exit  
Switch(config)#  
Switch(config)#  
Switch(config)#int ra  
Switch(config)#int range fa0/3-5  
Switch(config-if-range)#sw  
Switch(config-if-range)#switchport mod  
Switch(config-if-range)#switchport mode acc  
Switch(config-if-range)#switchport mode access  
Switch(config-if-range)#sw  
Switch(config-if-range)#switchport acc  
Switch(config-if-range)#switchport access vl  
Switch(config-if-range)#switchport access vlan 2  
Switch(config-if-range)#exit  
Switch(config)#int |
```

At the bottom right of the configuration window, there are **Copy** and **Paste** buttons.

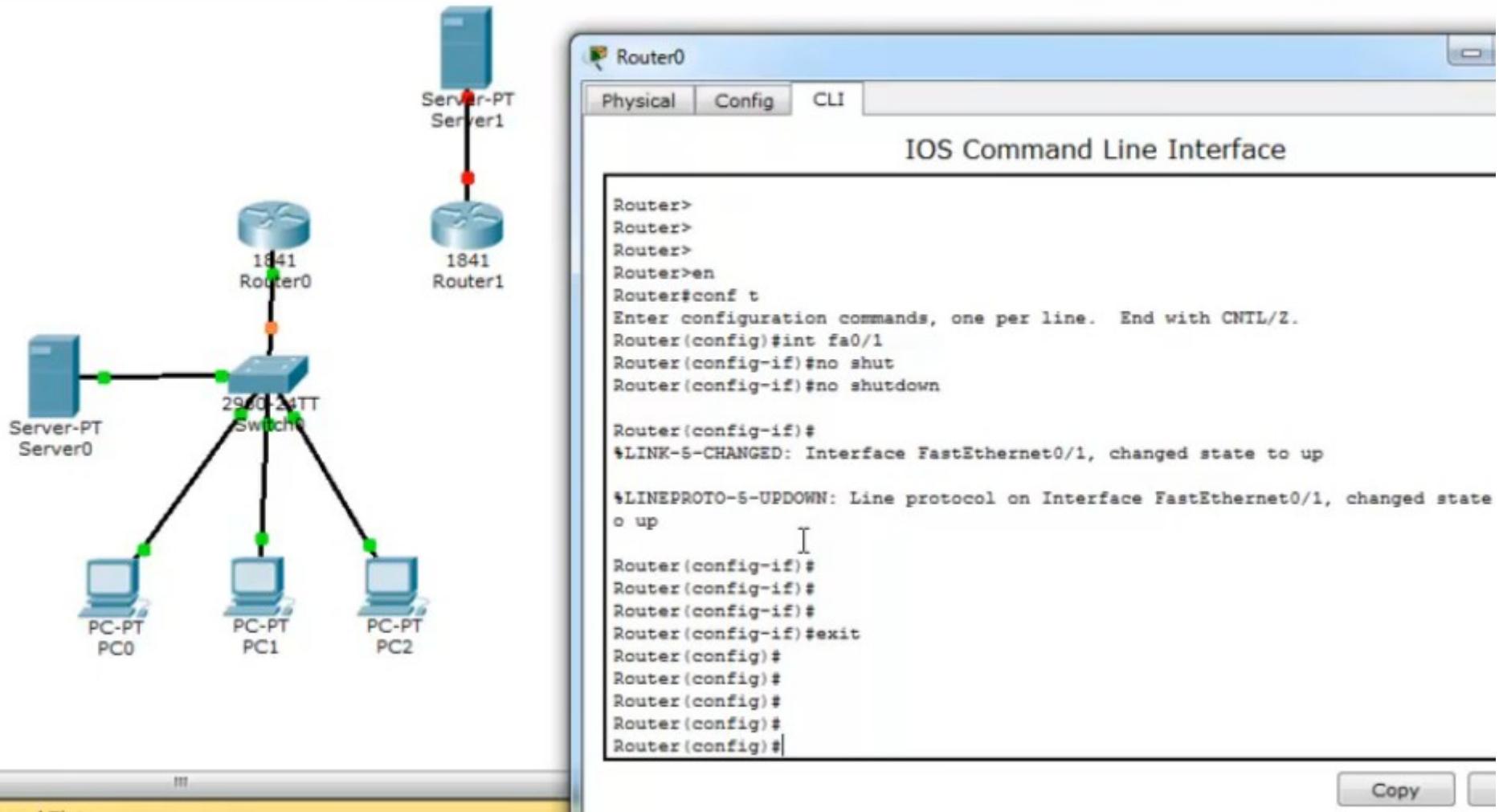
Назначаем trunk порт, проверяем конфигурацию



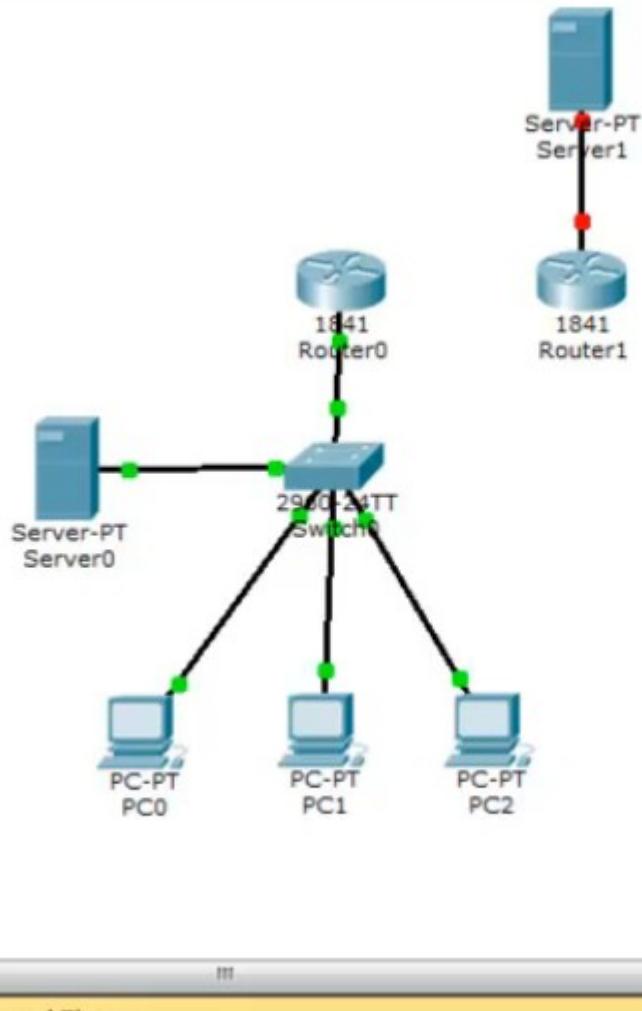
Проверяем конфигурацию, сохраняем



Настраиваем Router0, активируем интерфейс fa0/1



Создадим субинтерфейс для VLAN 2, назначим ip



Router0

Physical Config CLI

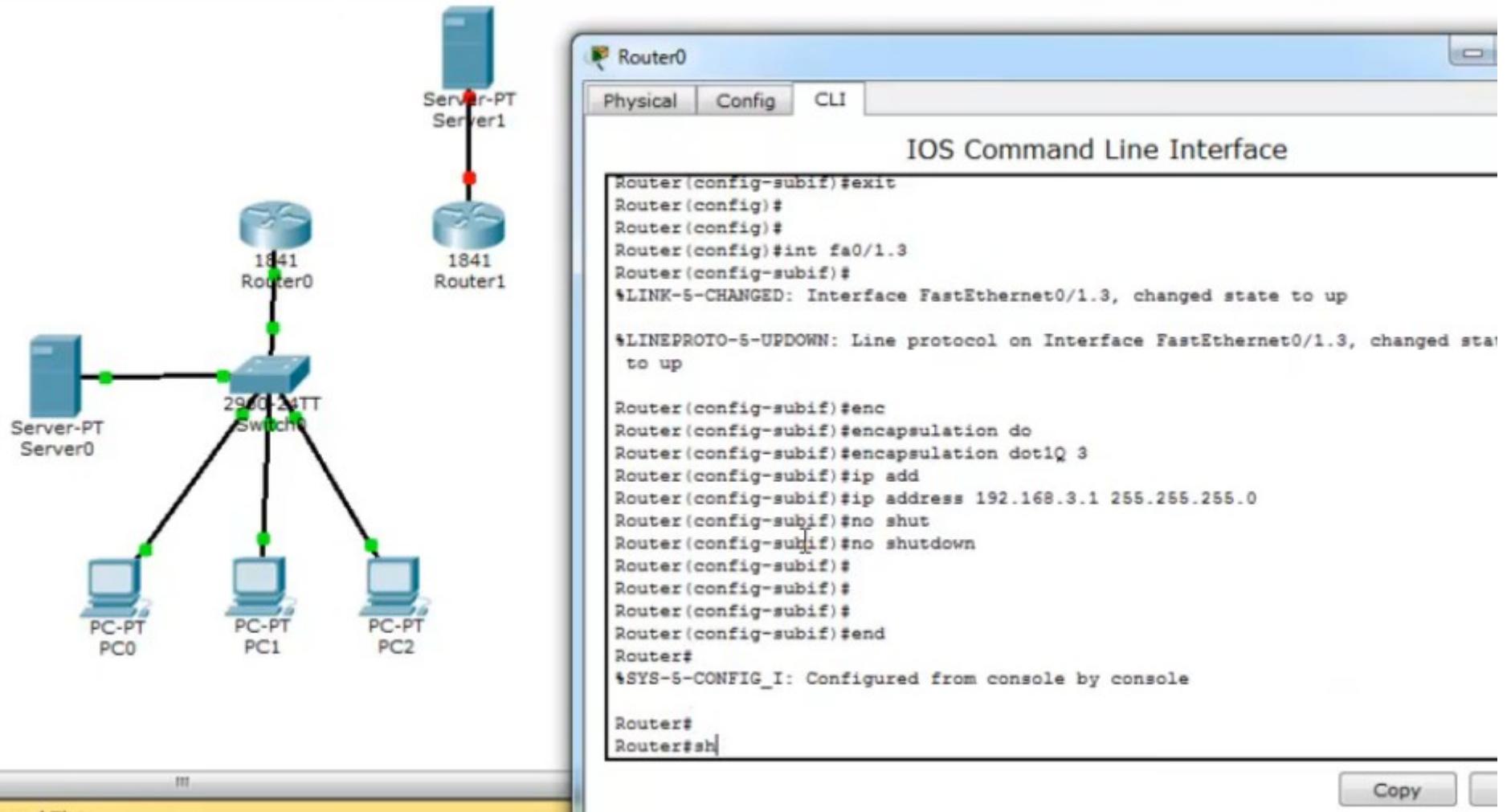
IOS Command Line Interface

```
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#int fa0/1.2
Router(config-subif)#
*LINK-5-CHANGED: Interface FastEthernet0/1.2, changed state to up

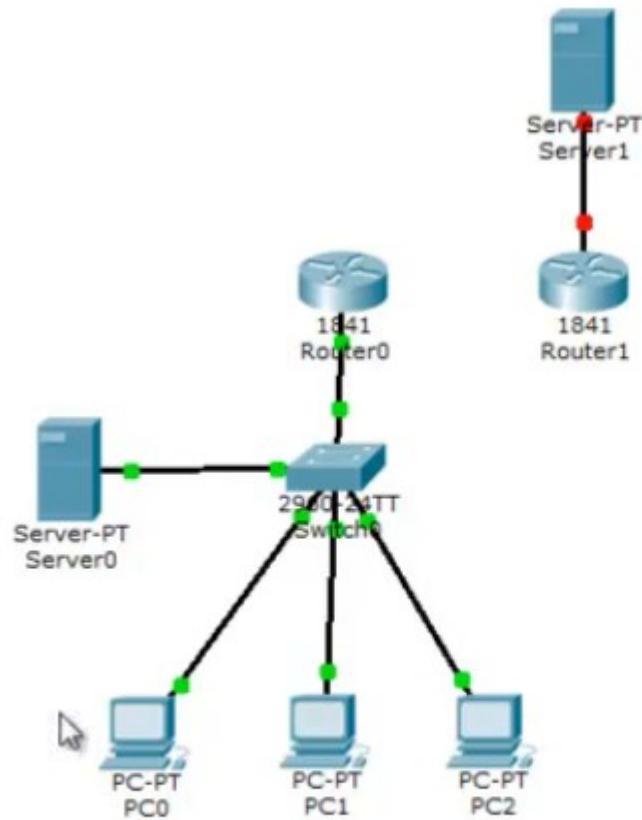
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.2, changed sta
to up

Router(config-subif)#
Router(config-subif)#
Router(config-subif)#enc
Router(config-subif)#encapsulation do
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip add
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#no shut
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#
Router(config)#
Router(config)#
```

Создадим еще один субинтерфейс для VLAN3, назначим ip



Проверяем, что созданы два субинтерфейса, записываем конфигурацию



Router0

Physical Config CLI

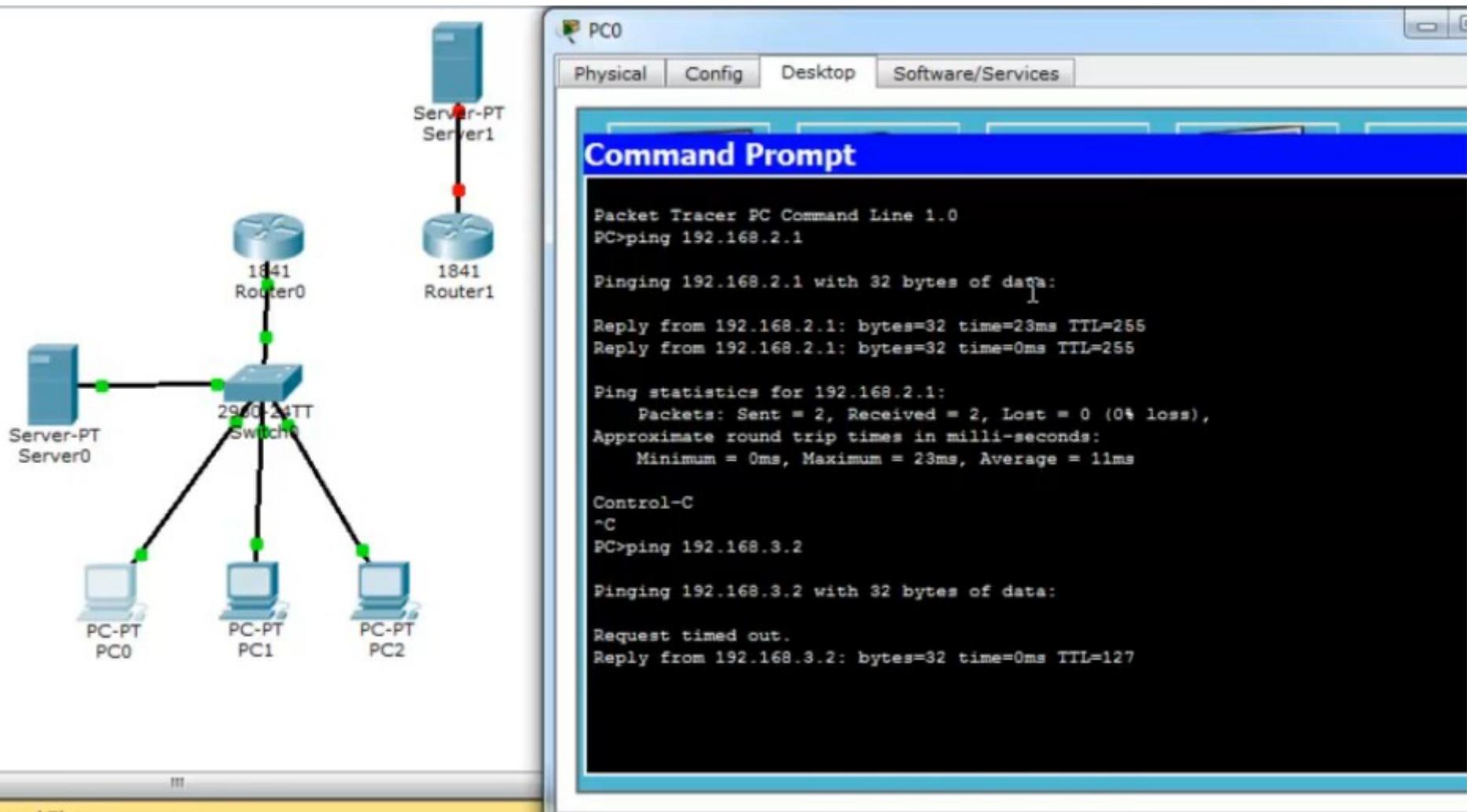
IOS Command Line Interface

```
shutdown
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
!
interface FastEthernet0/1.2
encapsulation dot1Q 2
ip address 192.168.2.1 255.255.255.0
!
interface FastEthernet0/1.3
encapsulation dot1Q 3
ip address 192.168.3.1 255.255.255.0
!
interface Vlan1
no ip address
shutdown
!
ip classless
!

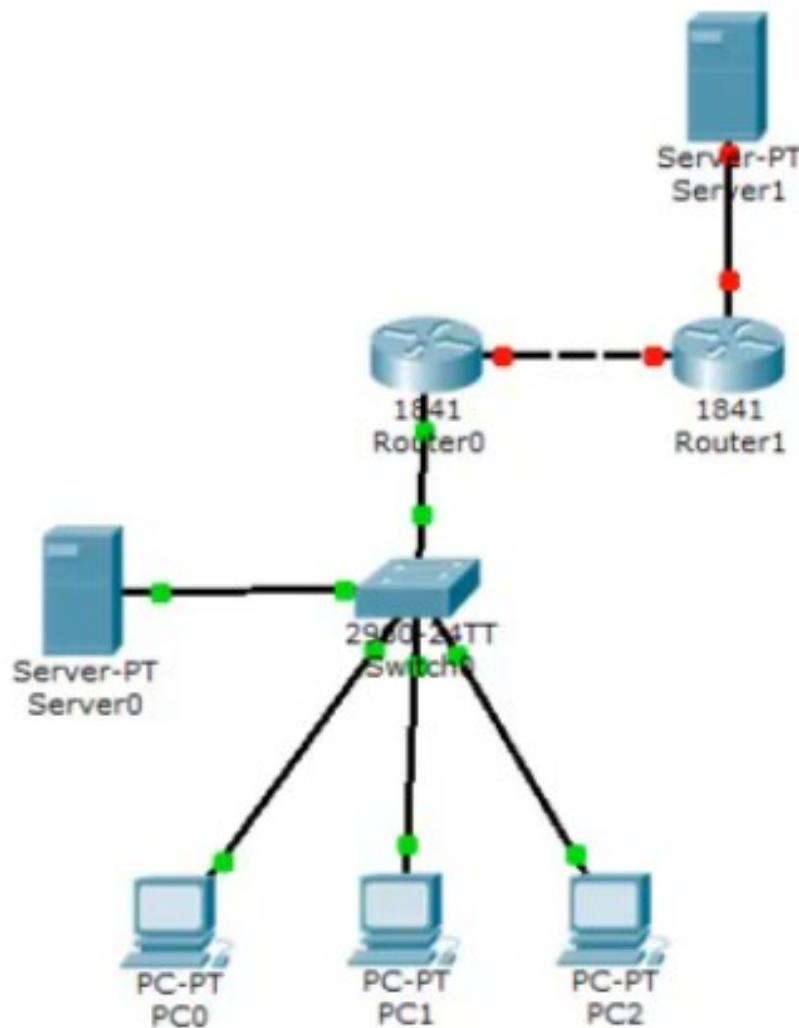
Router#wr mem
Building configuration...
[OK]
Router$
```

Copy

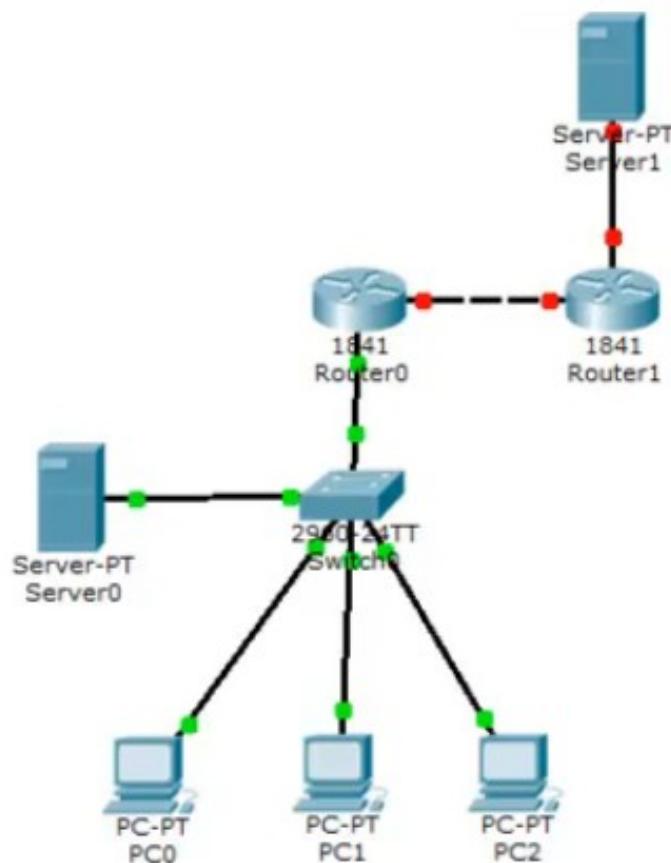
Проверяем, что шлюз и сервер доступны с PC0



Далее роутер нашей сети подсоединяют в к «интернету» в виде сервера и второго роутера, у которых есть статические белые ip адреса



Зададим ір адрес на интерфейсе Router1, обращенного к Router0



Router1

Physical Config CLI

IOS Command Line Interface

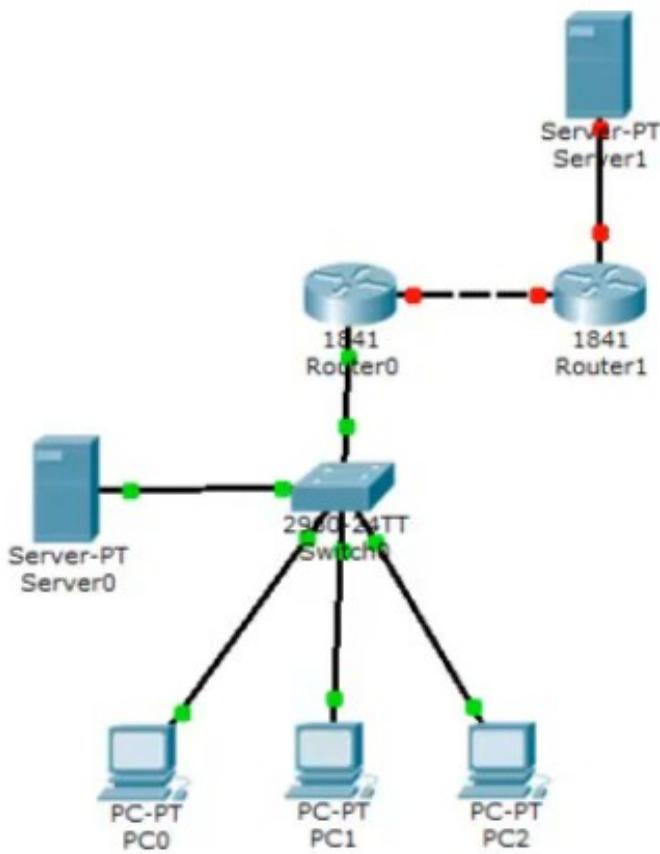
```
Router>
Router>en
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int
Router(config)#interface fa0/0
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)$ip add
Router(config-if)$ip address 213.234.10.1 255.255.255.252
Router(config-if)#
Router(config-if)$no shut
Router(config-if)$no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)$exit
Router(config)#

```

Зададим ip адрес на интерфейсе Router1, обращенного к Server1



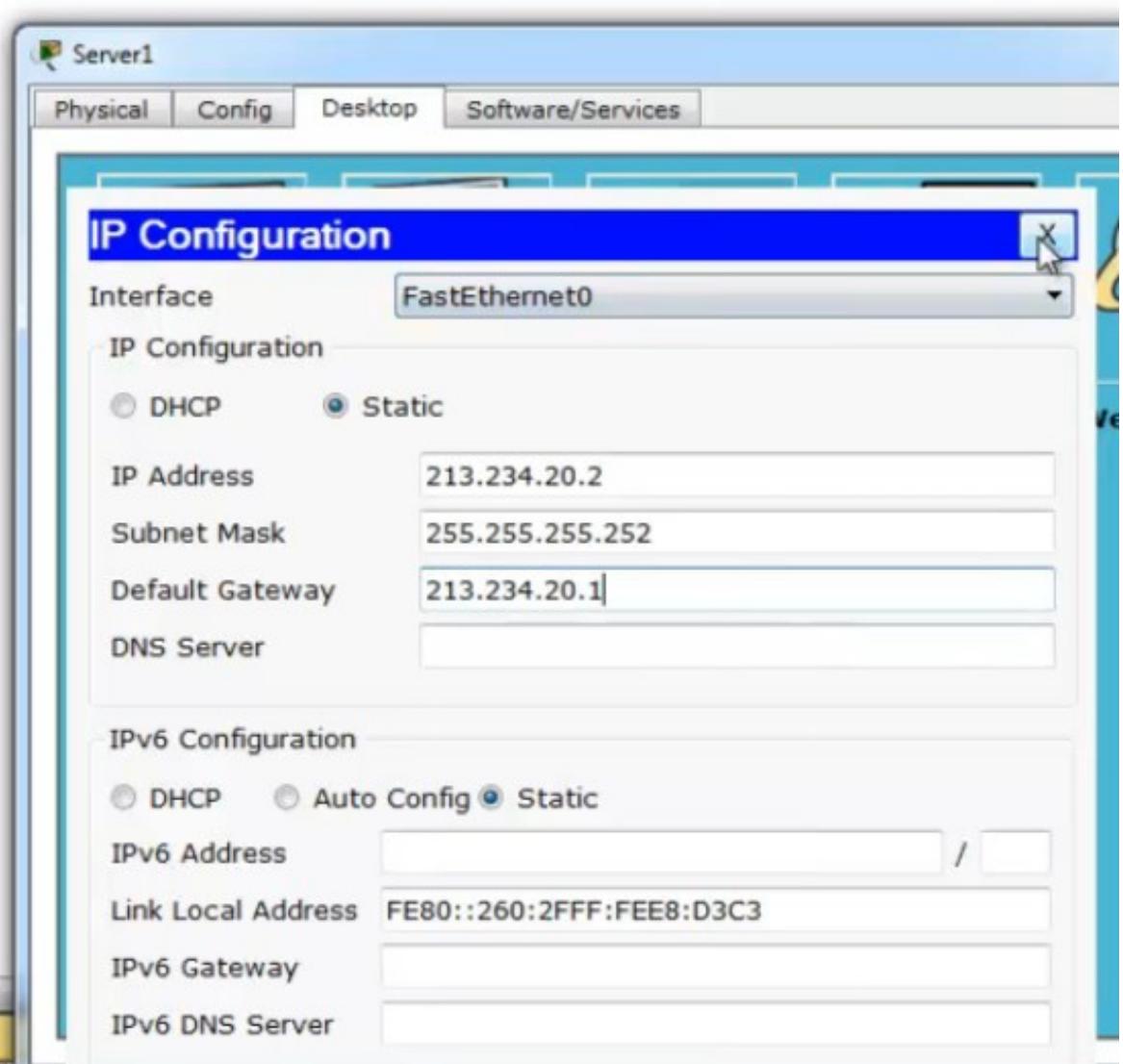
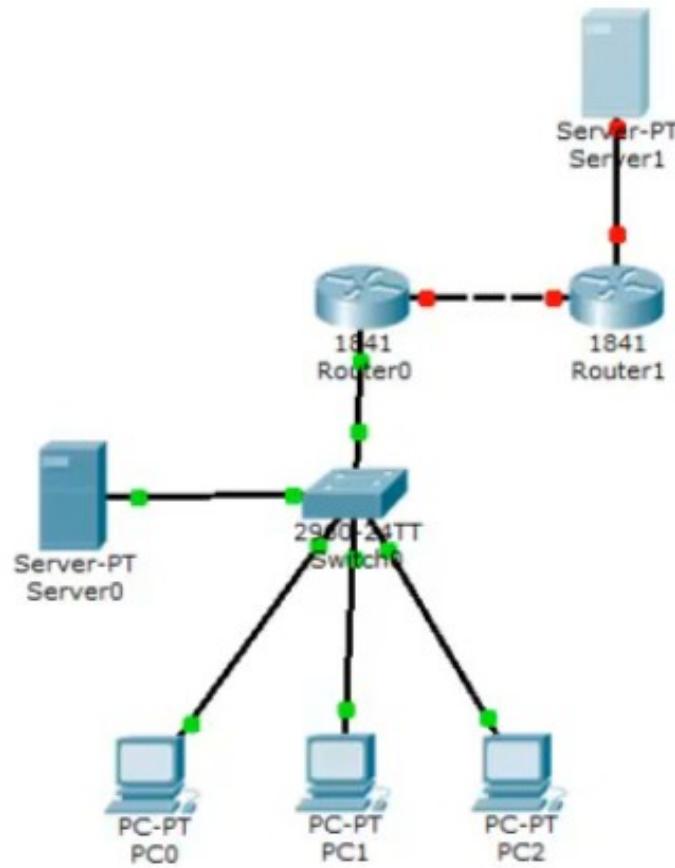
Router1

Physical Config CLI

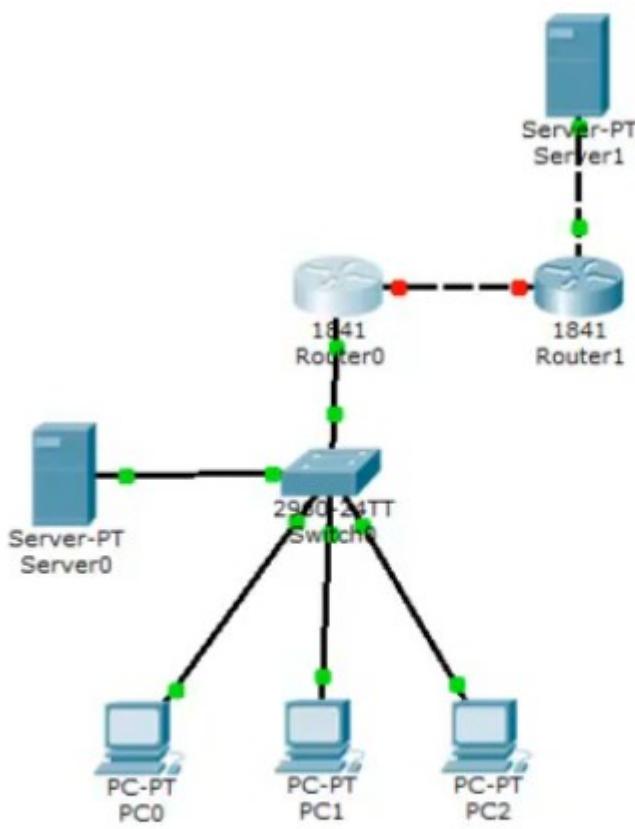
IOS Command Line Interface

```
Router(config)#  
Router(config)#int fa0/1  
Router(config-if)#  
Router(config-if)#ip a  
Router(config-if)#ip ad  
Router(config-if)#ip address 213.234.20.1 255.255.255.252  
Router(config-if)#no shut  
Router(config-if)#no shutdown  
  
Router(config-if)#  
*LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up  
  
Router(config-if)#  
Router(config-if)#  
Router(config-if)#  
Router(config-if)#  
Router(config-if)#exit  
Router(config)#  
Router(config)#  
Router(config)#  
Router(config)#wr mem  
~ [ ]  
* Invalid input detected at '^' marker.  
  
Router(config)#[/pre>
```

Зададим ір адрес для Server1



Заменим тип кабеля между Server1 и Router1. Зададим ip на Router0.



Router0

Physical Config CLI

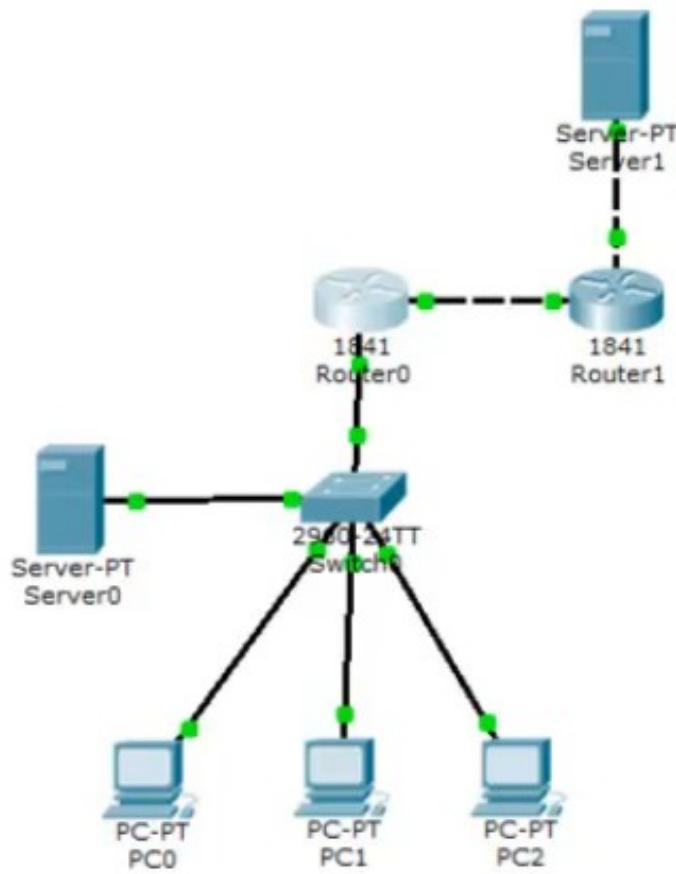
IOS Command Line Interface

```
Building configuration...
[OK]
Router#
Router#
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#
Router(config-if)#
Router(config-if)#ip add
Router(config-if)#ip address 213.234.10.2 255.255.255.252
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)$
```

Forward Time

Copy

Зададим шлюз по умолчанию на Router0



Router0

Physical Config CLI

IOS Command Line Interface

```
Router(config)#int fa0/0
Router(config-if)#no shut
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

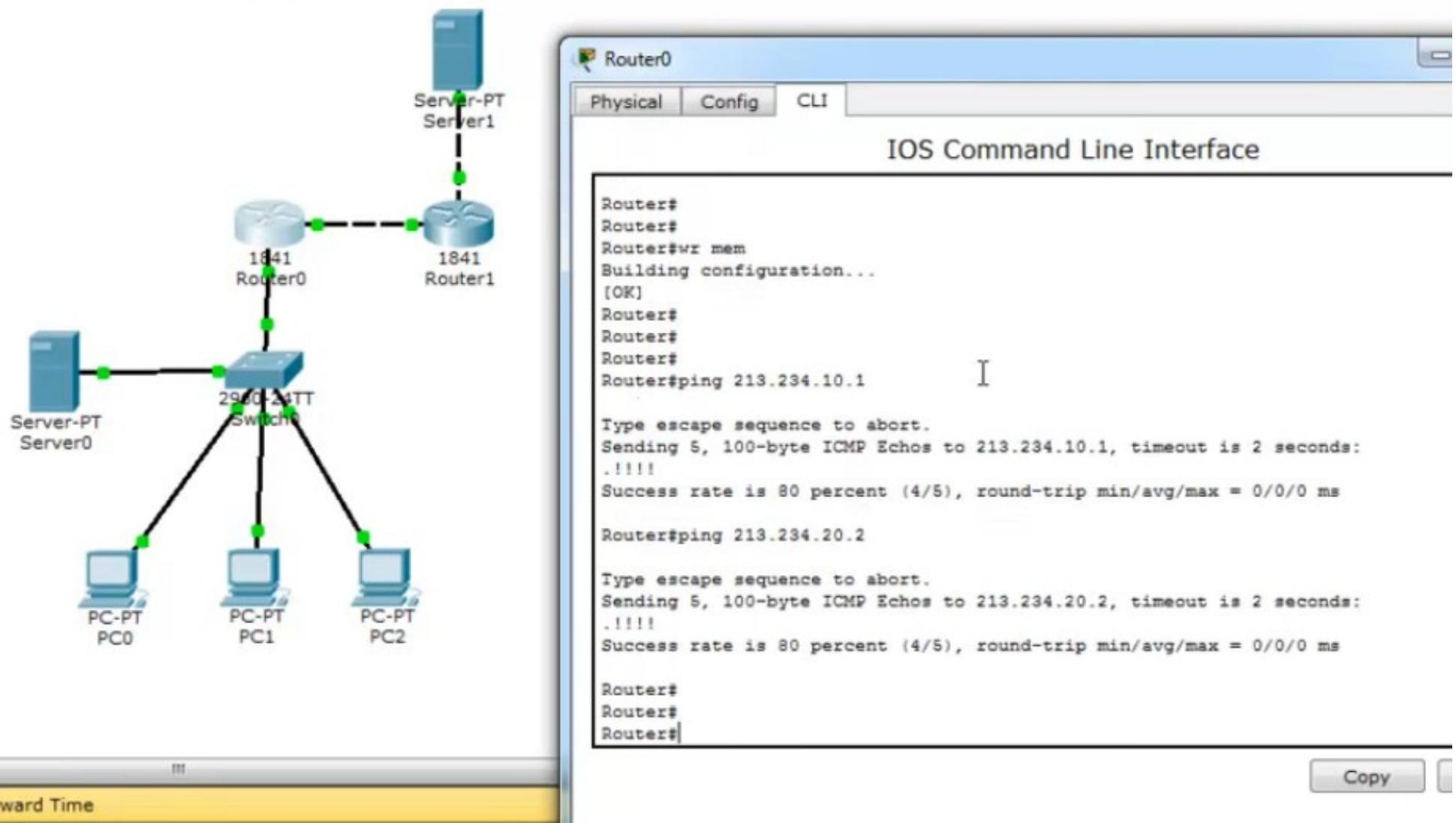
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#ip route 0.0.0.0 0.0.0.0 213.234.10.1
Router(config)#
Router(config)#
Router(config)#
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#
```

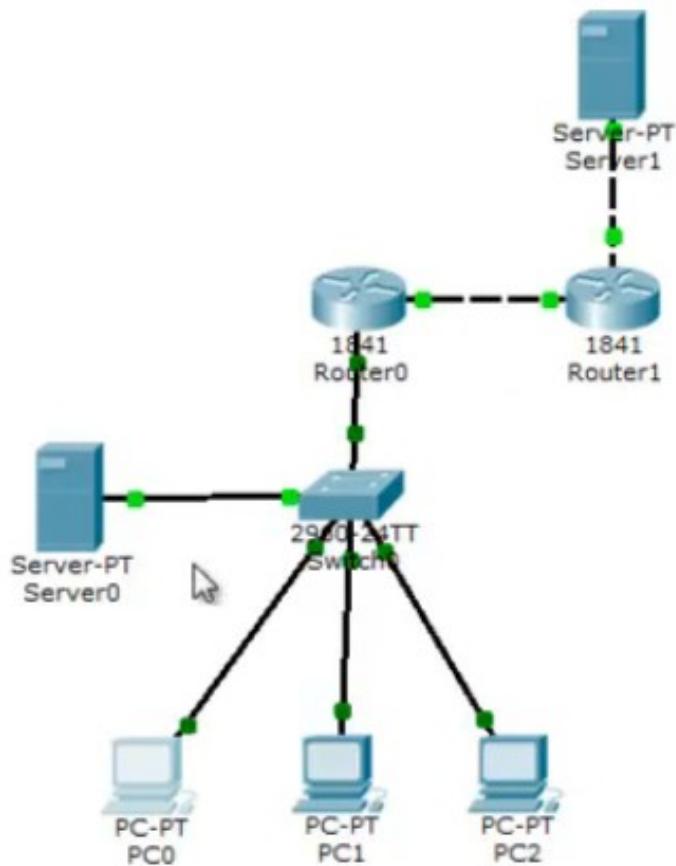
Copy

st Forward Time

Сохраняем. Проверяем связанность с Server1, Router1



Пингуем Server1 с PC0 — не проходит. Router1 не знает как работать с «серыми» ip адресами PC0, PC1, PC2



PC0

Physical Config Desktop Software/Services

Command Prompt

```
Control-C
~C
PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.2: bytes=32 time=0ms TTL=127
Reply from 192.168.3.2: bytes=32 time=0ms TTL=127
Reply from 192.168.3.2: bytes=32 time=1ms TTL=127

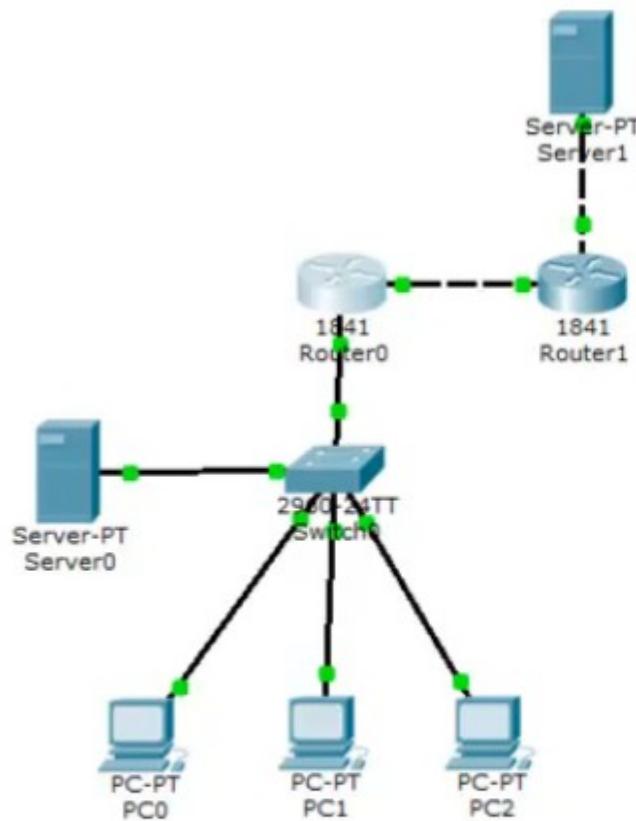
Ping statistics for 192.168.3.2:
  Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
PC>
PC>
PC>
PC>ping 213.234.20.2

Pinging 213.234.20.2 with 32 bytes of data:

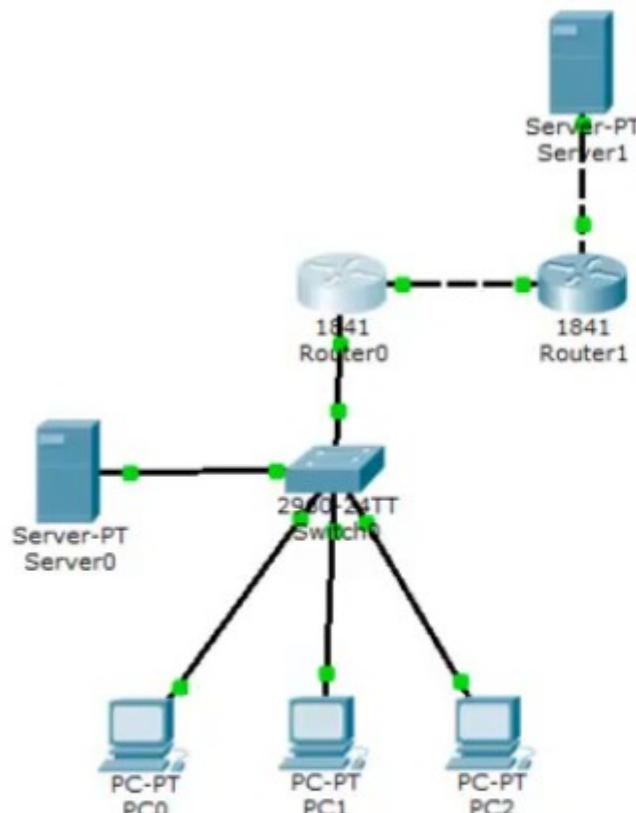
Request timed out.
Request timed out.
```

На Router0 определяем fa0/0 как внешний, fa0/1.2 как внутренний интерфейс



Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#int fa0/0
Router(config-if)#
Router(config-if)#
Router(config-if)#ip na
Router(config-if)#ip nat outs
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#int fa0/1.2
Router(config-subif)#ip na
Router(config-subif)#ip nat ins
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)#
Router(config)#
Router(config)#

определяем fa0/1.3 тоже как внутренний



Router0

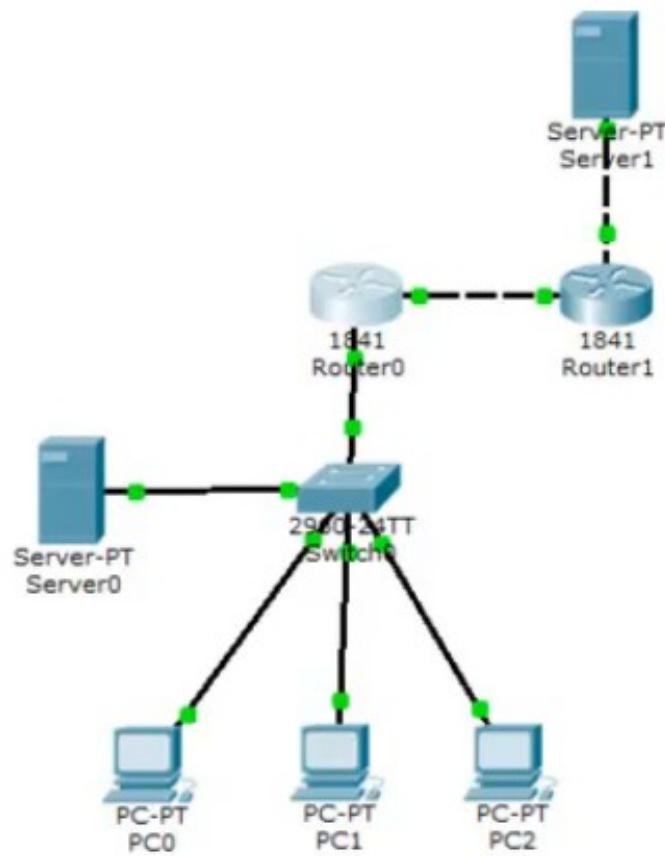
Physical Config CLI

IOS Command Line Interface

```
Router(config)#  
Router(config)#  
Router(config)#int fa0/1.2  
Router(config-subif)#ip na  
Router(config-subif)#ip nat ins  
Router(config-subif)#ip nat inside  
Router(config-subif)#exit  
Router(config)#  
Router(config)#  
Router(config)#int fa0/1.3  
Router(config-subif)#ip na  
Router(config-subif)#ip nat ins  
Router(config-subif)#ip nat inside  
Router(config-subif)#  
Router(config-subif)#  
Router(config-subif)#  
Router(config-subif)#end  
Router#  
%SYS-5-CONFIG_I: Configured from console by console  
  
Router#  
Router#  
Router#  
Router#  
Router#  
Router#
```

Copy

Добавляем acces-list, указывающий, какие сети за NAT. Проверяем.



Router#

Router#

Router#

Router#

Router#

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

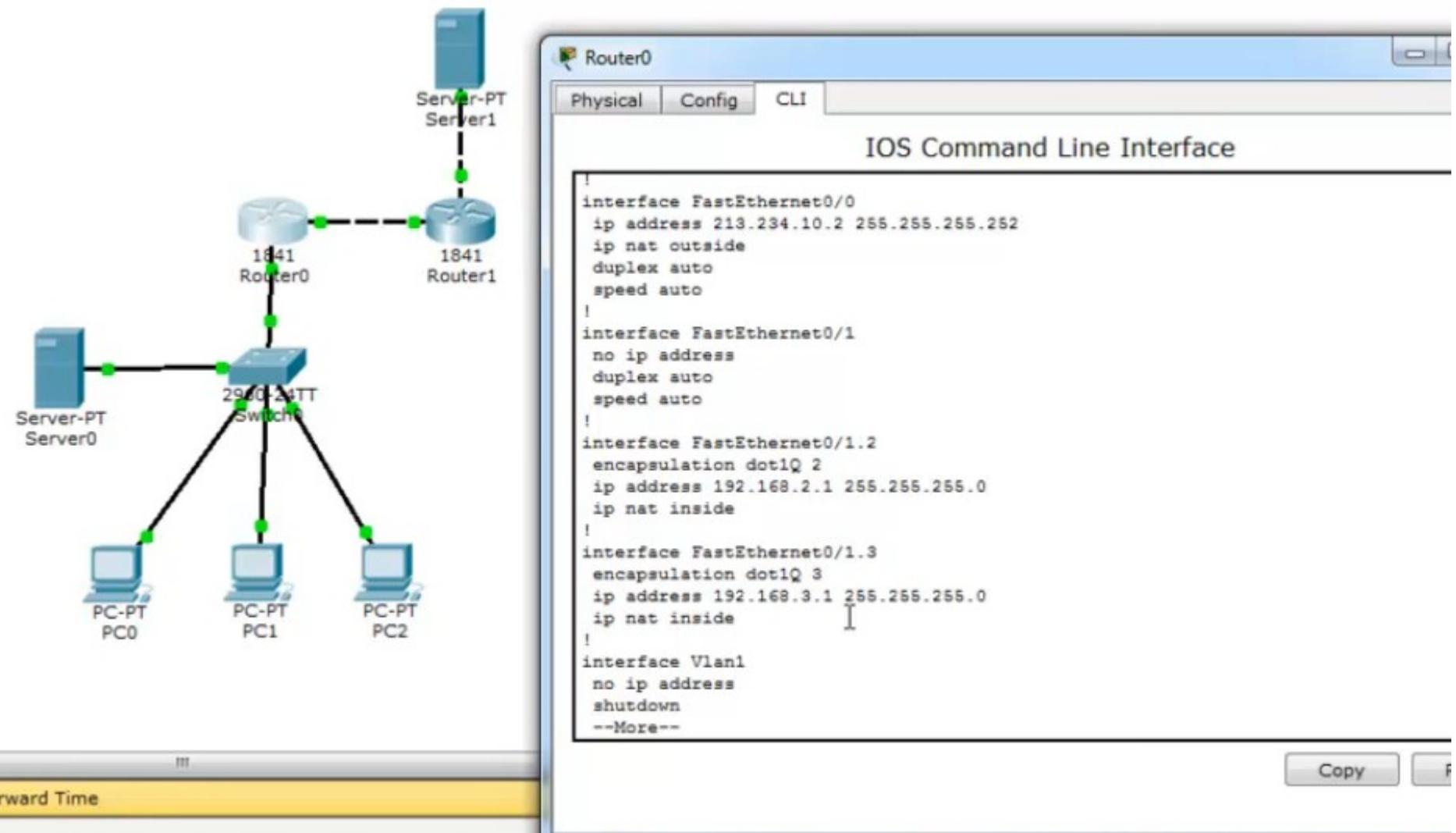
```
Router(config)#ip acc
Router(config)#ip access-list st
Router(config)#ip access-list standard FOR-NAT
Router(config-std-nacl)#per
Router(config-std-nacl)#permit 192.168.2.0 ?
A.B.C.D Wildcard bits
<cr>
Router(config-std-nacl)#permit 192.168.2.0 0.0.0.255
Router(config-std-nacl)#permit 192.168.3.0 0.0.0.255
Router(config-std-nacl)#
Router(config-std-nacl)#
Router(config-std-nacl)#
Router(config-std-nacl)#end
Router#
*SYS-5-CONFIG_I: Configured from console by console
```

Router#

Router#

Router\$show run

В конфигурации — какие интерфейсы inside, какие outside.



Настраиваем Port-Address-Translation

Настройка PAT

```
interface FastEthernet0/0
ip nat outside
interface FastEthernet0/1.2
ip nat inside
interface FastEthernet0/1.3
ip nat inside
```

```
ip access-list standard FOR-NAT
permit 192.168.2.0 0.0.0.255
permit 192.168.3.0 0.0.0.255
```

```
ip nat inside source list FOR-NAT interface FastEthernet0/0 overload
```

Настройка Static NAT

```
ip nat inside source static tcp 192.168.3.2 80 213.234.10.2 80
```

```
show ip nat translations
```

The screenshot shows a window titled "Router0" with tabs for "Physical", "Config", and "CLI". The "CLI" tab is selected, displaying the "IOS Command Line Interface". The command-line history shows the configuration of multiple interfaces (FastEthernet0/0, 0/1.2, 0/1.3) for NAT, the creation of an access list (FOR-NAT), and the application of this list to an overload source list on interface 0/0. The configuration ends with a "load" command to apply the changes.

```
!line aux 0!
line vty 0 4
login!
!
!
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#ip na
Router(config)#ip nat
Router(config)#ip nat in
Router(config)#ip nat inside so
Router(config)#ip nat inside source 1
Router(config)#ip nat inside source list FOR-NAT in
Router(config)#ip nat inside source list FOR-NAT interface fa
Router(config)#ip nat inside source list FOR-NAT interface fastEthernet 0/0 over
load
Router(config)#
Copy Paste
```

Сохраняем

Настройка PAT

```
interface FastEthernet0/0
ip nat outside
interface FastEthernet0/1.2
ip nat inside
interface FastEthernet0/1.3
ip nat inside

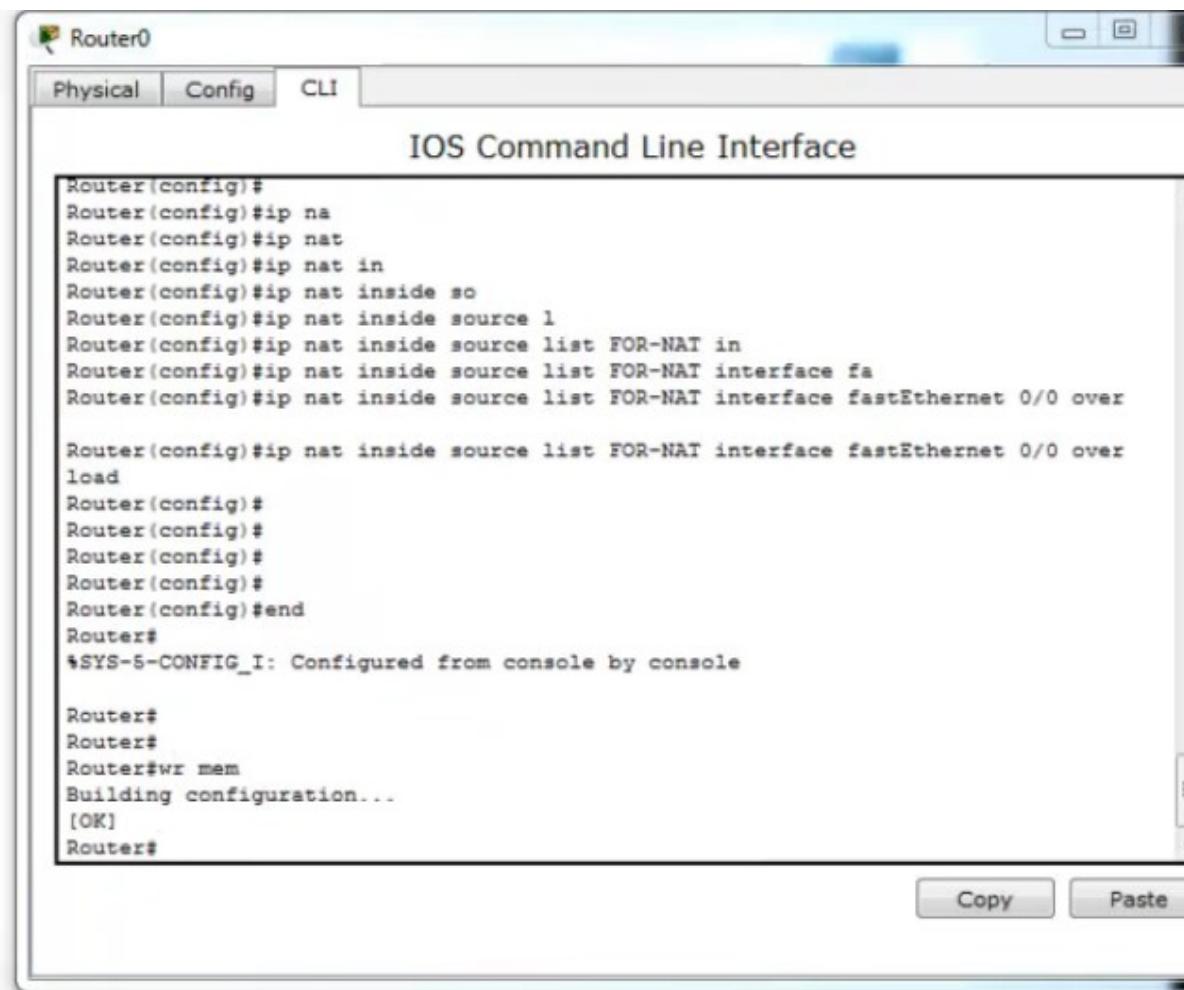
ip access-list standard FOR-NAT
permit 192.168.2.0 0.0.0.255
permit 192.168.3.0 0.0.0.255

ip nat inside source list FOR-NAT interface FastEthernet0/0 overload
```

Настройка Static NAT

```
ip nat inside source static tcp 192.168.3.2 80 213.234.10.2 80
```

```
show ip nat translations
```



IOS Command Line Interface

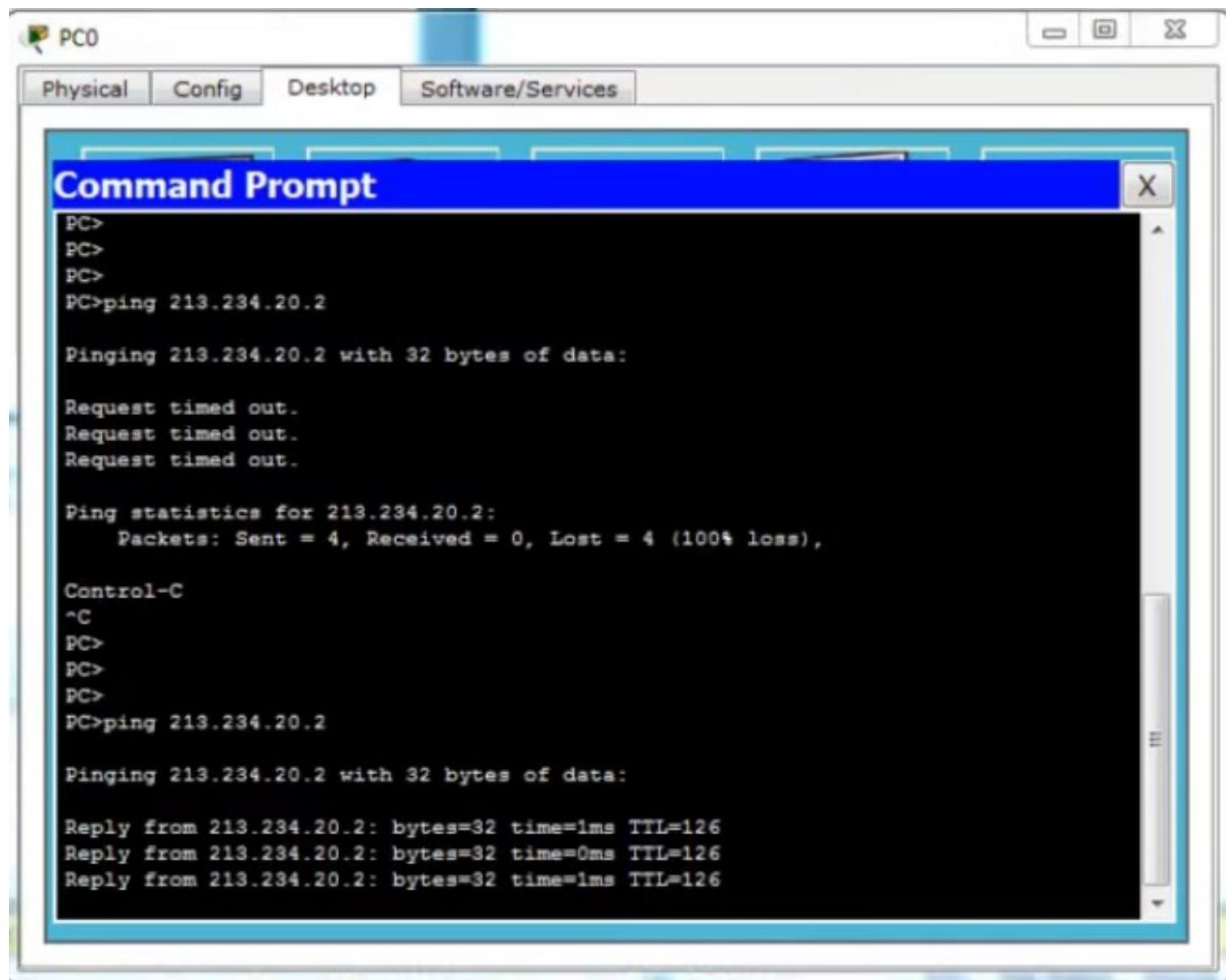
```
Router(config)#
Router(config)#ip na
Router(config)#ip nat
Router(config)#ip nat in
Router(config)#ip nat inside so
Router(config)#ip nat inside source 1
Router(config)#ip nat inside source list FOR-NAT in
Router(config)#ip nat inside source list FOR-NAT interface fa
Router(config)#ip nat inside source list FOR-NAT interface fastEthernet 0/0 over

Router(config)#ip nat inside source list FOR-NAT interface fastEthernet 0/0 over
load
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router#
*SYS-5-CONFIG_I: Configured from console by console

Router#
Router#
Router#wr mem
Building configuration...
[OK]
Router#
```

Copy Paste

Проверяем доступность Sever1 с PC0 — пинг проходит.



На Router0 видим настройки NAT

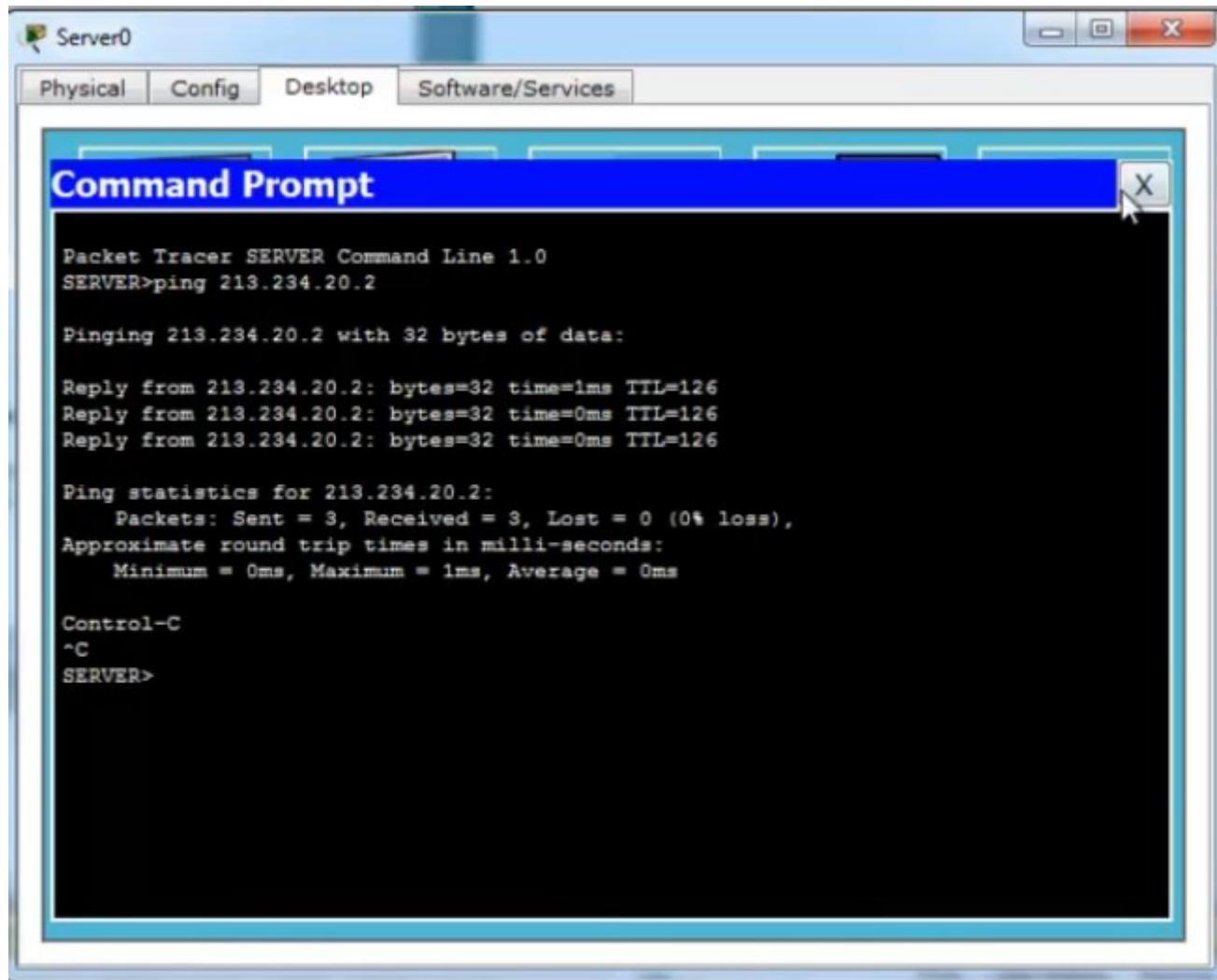
Router(config)#
Router(config)#
Router(config)#
Router(config)#end
Router#
*SYS-5-CONFIG_I: Configured from console by console

Router#
Router#
Router#wr mem
Building configuration...
[OK]
Router#
Router#
Router#
Router#
Router#
Router#
Router#show ip na
Router#show ip nat tr
Router#show ip nat translations

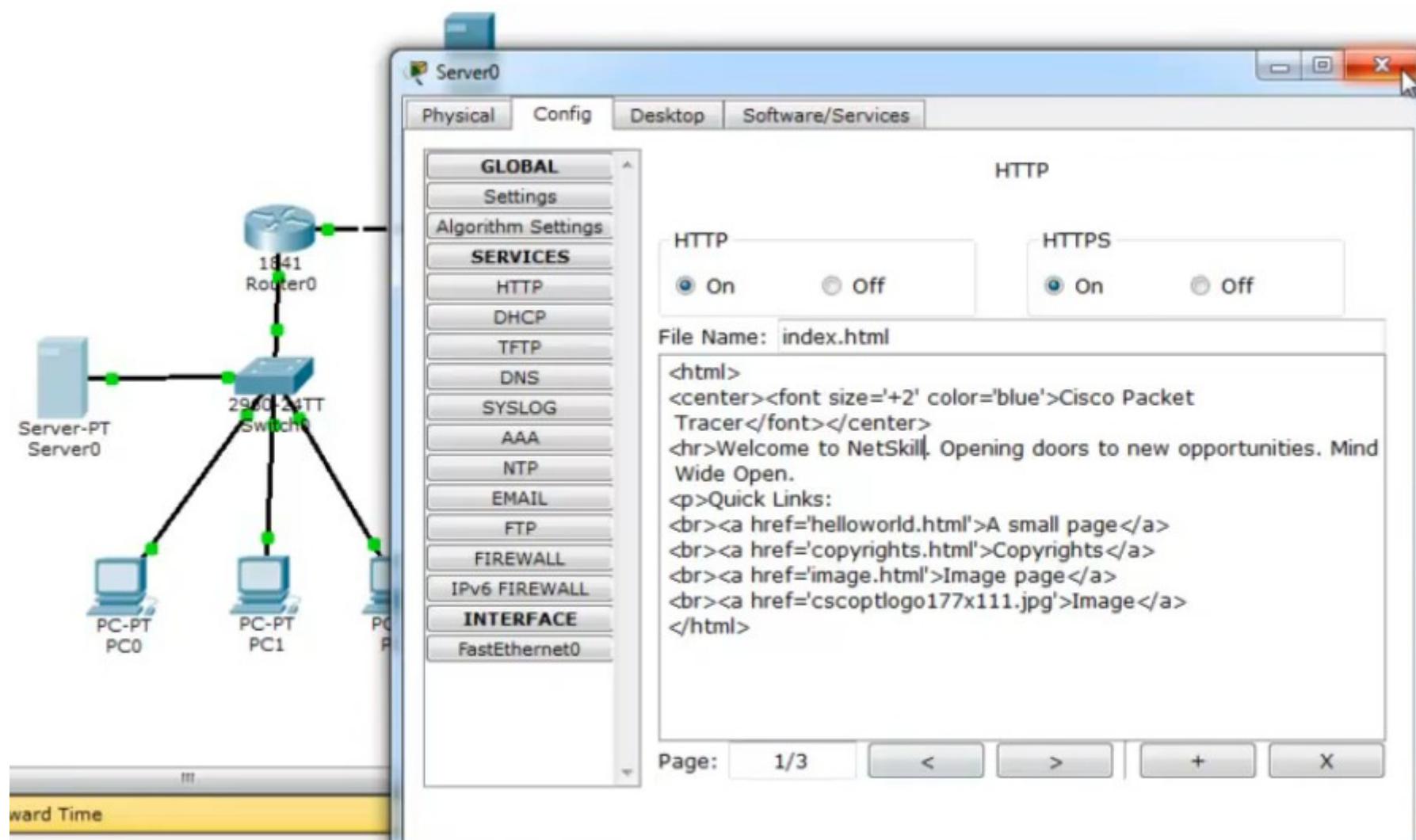
Protocol	Inside global	Inside local	Outside local	Outside global
icmp	213.234.10.2:11	192.168.2.2:11	213.234.20.2:11	213.234.20.2:11
icmp	213.234.10.2:12	192.168.2.2:12	213.234.20.2:12	213.234.20.2:12
icmp	213.234.10.2:13	192.168.2.2:13	213.234.20.2:13	213.234.20.2:13
icmp	213.234.10.2:14	192.168.2.2:14	213.234.20.2:14	213.234.20.2:14

Router#

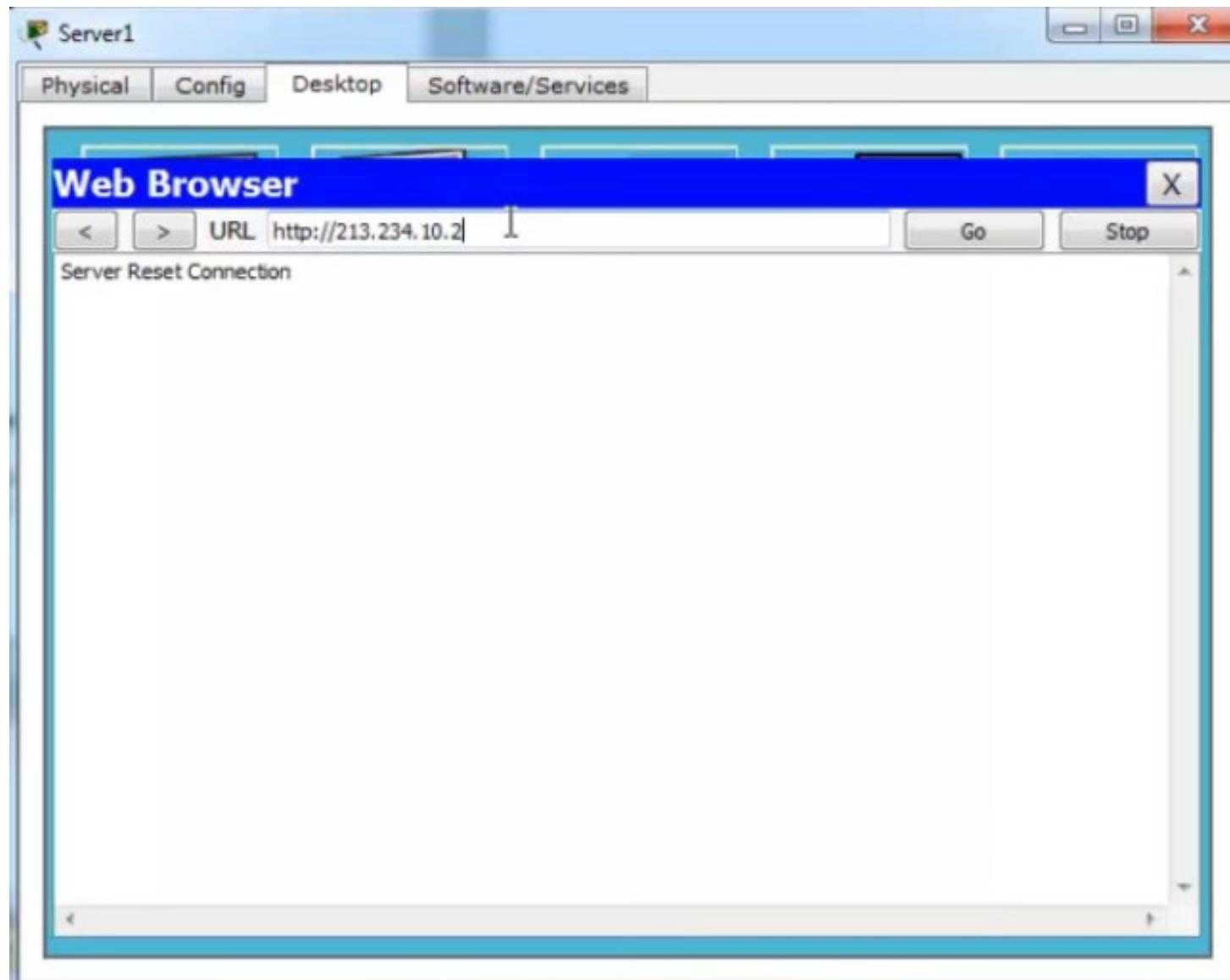
Проверяем, что с Server1 доступен PC0



Далее настроим статический NAT для доступа к Server0 из внешней сети. Изменим содержание index.html в Config > HTTP у Server0



Проверяем доступность веб-сервера на Server0 с Server1 — недоступен.



Настроим static NAT на Router0

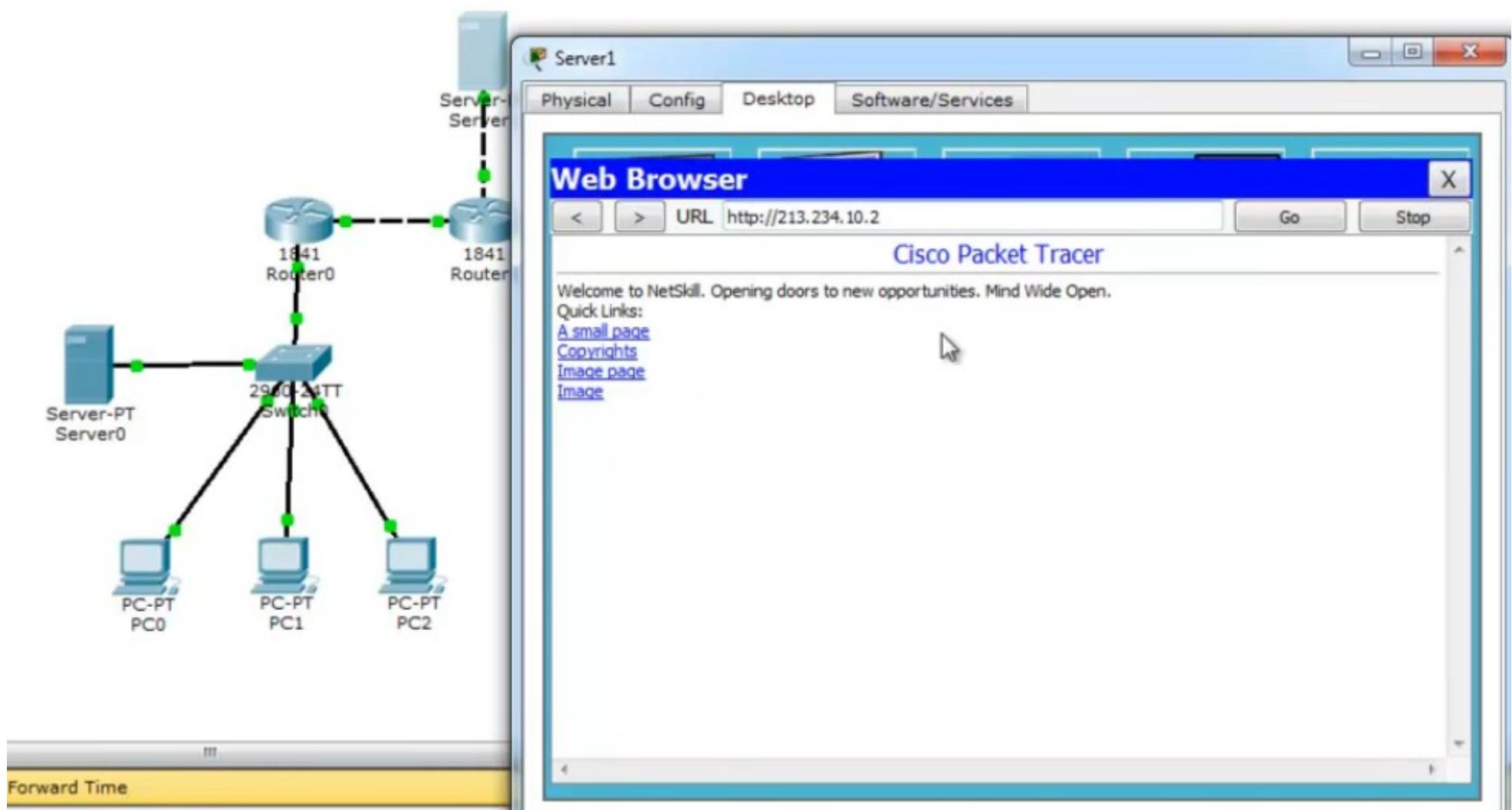
The screenshot shows a Windows application window titled "Router0". The window has three tabs at the top: "Physical", "Config", and "CLI". The "CLI" tab is selected, displaying the "IOS Command Line Interface". The terminal window contains the following configuration commands:

```
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip na
Router(config)#ip nat
Router(config)#ip nat ins
Router(config)#ip nat inside so
Router(config)#ip nat inside source stat
Router(config)#ip nat inside source static 192.168.3.2 80 213.234.10.2 80
           ^
* Invalid input detected at '^' marker.

Router(config)#ip nat inside source static 192.168.3.2 ?
      A.B.C.D Inside global IP address
Router(config)#ip nat inside source static tcp 192.168.3.2 80 213.234.10.2 80
Router(config)#
Router(config)#
Router(config)#
Router(config)#end
Router#
*SYS-5-CONFIG_I: Configured from console by console
wr mem
Building configuration...
[OK]
Router#
```

At the bottom of the window are two buttons: "Copy" and "Paste".

Снова пробуем обратиться к веб-серверу на Server0 с сервера Server1 — получилось.



VPN — Virtual Private Network

Lesson18 - VPN

Как дать доступ к локальным серверам?

1. Static NAT
2. DMZ
3. VPN

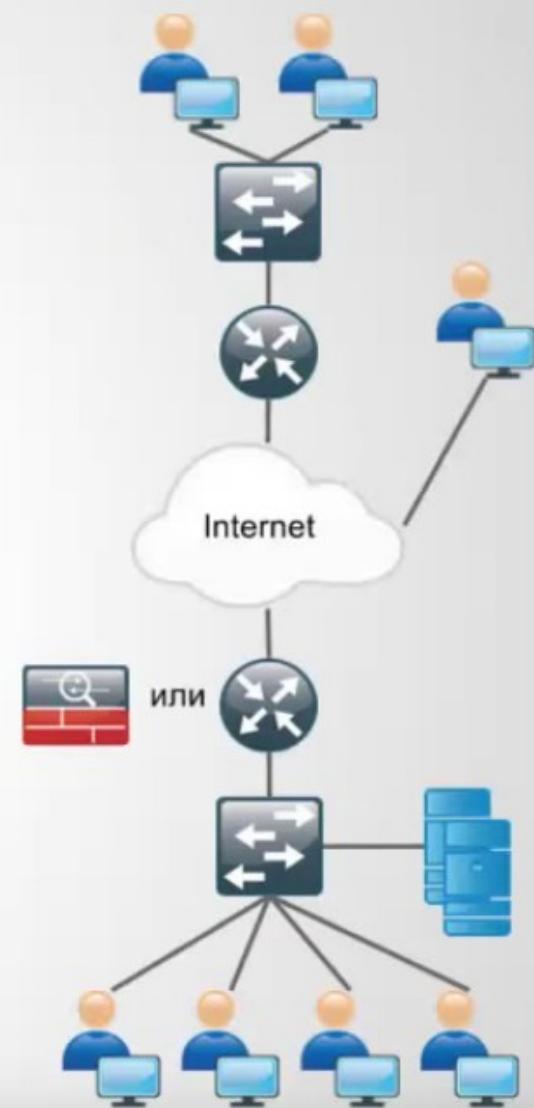
VPN - Virtual Private Network - виртуальная частная сеть

- IPsec Site-to-Site VPN - объединение сетей
- IPsec RA VPN - подключение удаленного пользователя

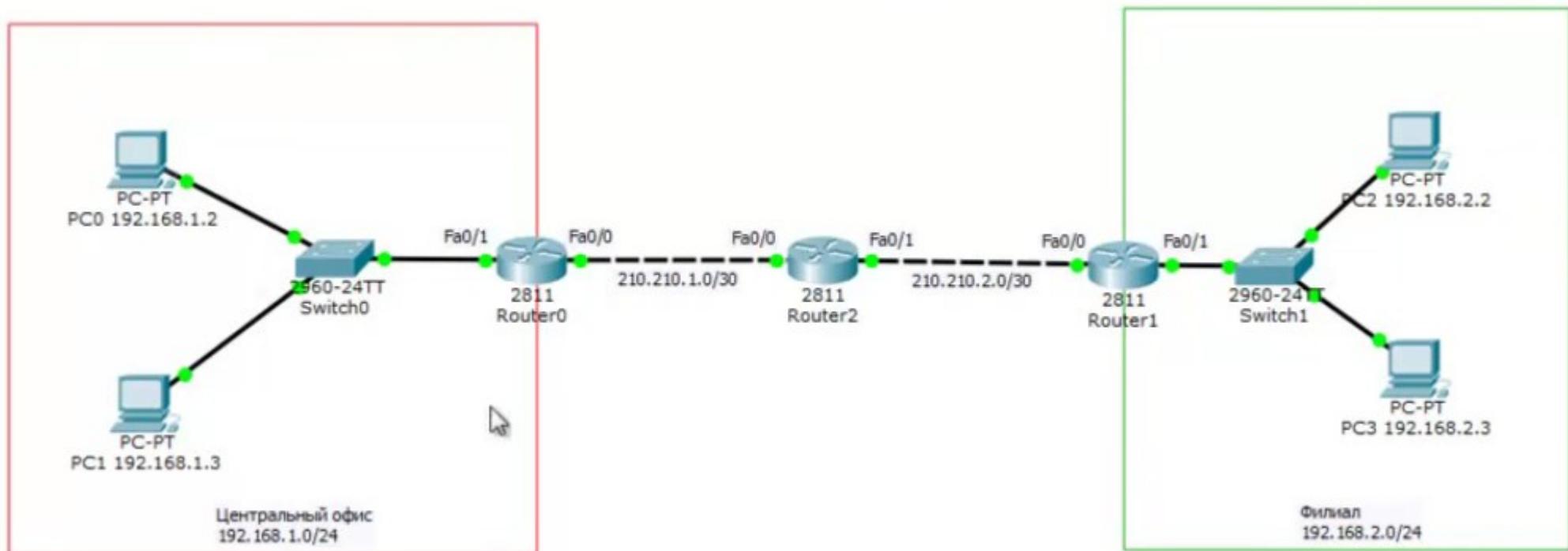
Построение туннеля в две фазы (IKE)

1. Первая фаза (установка SA и ISAKMP Tunnel)
2. Вторая фаза (IPsec Tunnel)

Более подробно о приведенных технологиях можно почитать [здесь](#) и [здесь](#)



VPN, пример. Есть центральный офис и филиал



Смотрим настройки на Router0 в центральном офисе

The image shows a network diagram and a Cisco IOS Command Line Interface (CLI) window.

Network Diagram:

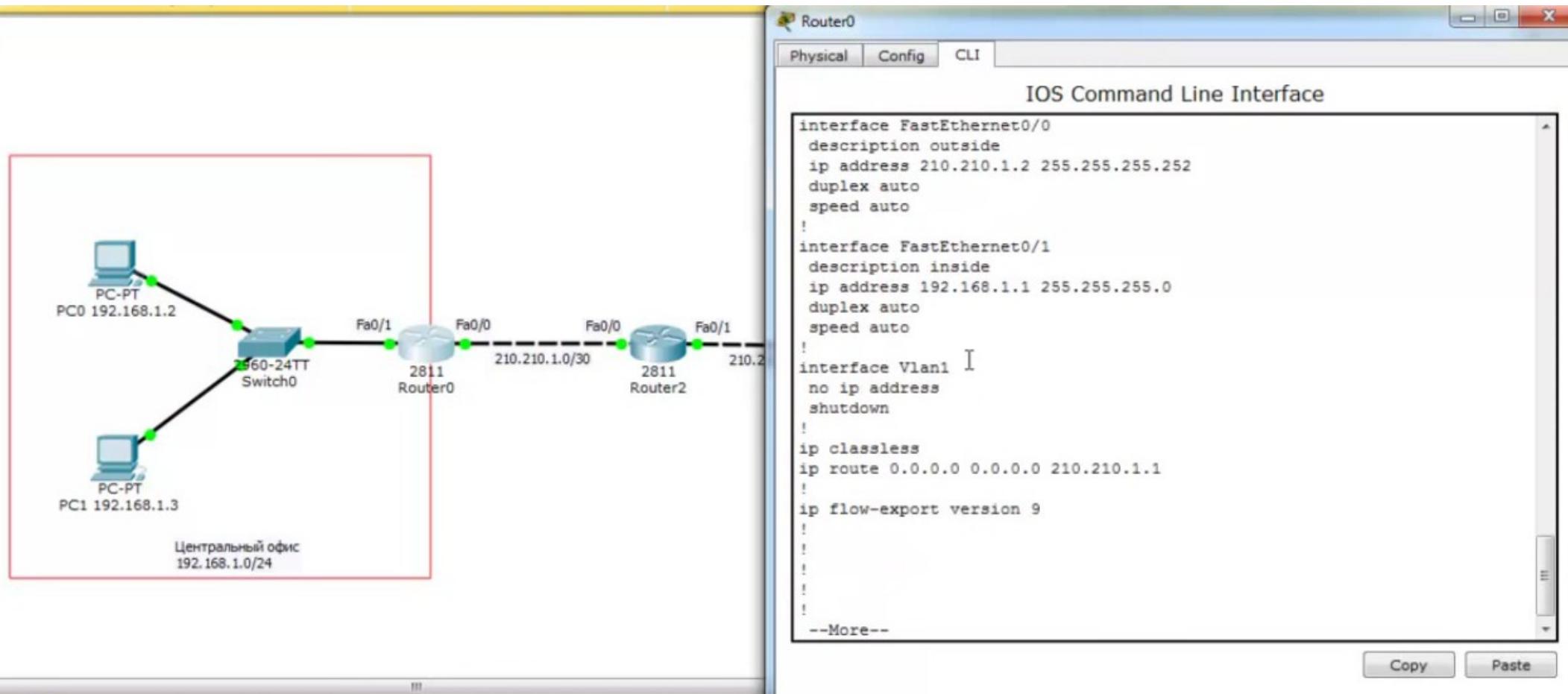
- A red box labeled "Центральный офис 192.168.1.0/24" contains:
 - A computer icon labeled "PC-PT PC0 192.168.1.2".
 - A switch icon labeled "2960-24TT Switch0".
 - A router icon labeled "2811 Router0".
 - A computer icon labeled "PC-PT PC1 192.168.1.3".
- Router0 is connected to Switch0 via port Fa0/1 and to Router2 via port Fa0/0.
- Router2 is connected to Router0 via port Fa0/0 and to an external network via port Fa0/1, with the IP address 210.210.1.0/30.
- The external network is connected to Router2 via port Fa0/1, with the IP address 210.210.1.1.

IOS Command Line Interface (CLI) Window:

- Title Bar:** Router0
- Tab Bar:** Physical, Config, CLI (selected)
- Text Area:**

```
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version  
12.4(15)T1, RELEASE SOFTWARE (fc2)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2007 by Cisco Systems, Inc.  
Compiled Wed 18-Jul-07 06:21 by pt_rel_team  
  
Press RETURN to get started!  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed  
state to up  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed  
state to up  
  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>en  
Router#  
Router#  
Router#  
Router#show run
```
- Buttons:** Copy, Paste

На Router0 настроено 2 ip адреса, маршрут по умолчанию.



На Router0 настроим NAT

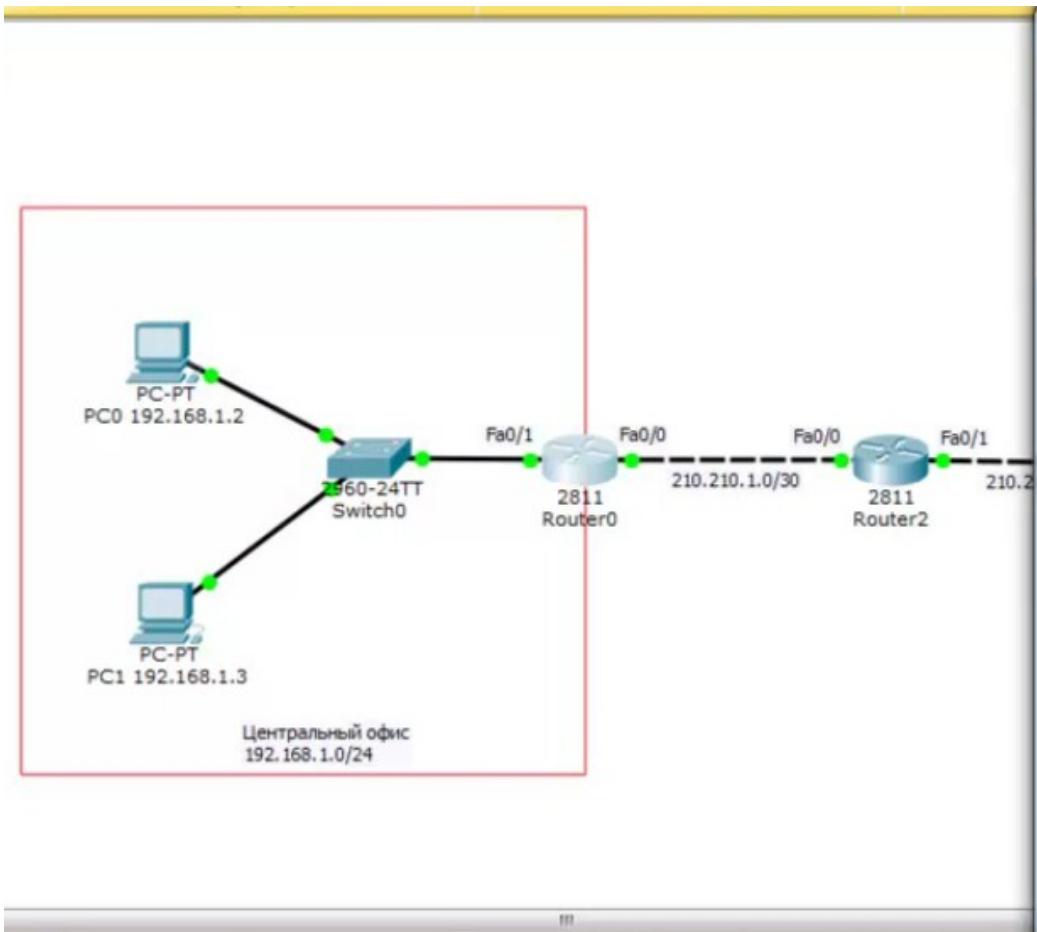
The network diagram illustrates a central office setup. A red box encloses a central area where two PCs (PC0 and PC1) are connected to a Switch0. This switch is connected to Router0 via two FastEthernet interfaces (Fa0/0 and Fa0/1). Router0 has two more FastEthernet interfaces (Fa0/0 and Fa0/1) connected to Router2 via a dashed line. Router2 has two FastEthernet interfaces (Fa0/0 and Fa0/1) connected to the Internet (IP 210.210.1.0/30 and 210.210.2.0/30). The entire central office network is assigned the IP range 192.168.1.0/24.

IOS Command Line Interface

```
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip nat
Router(config-if)#ip nat ou
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#int fa0/1
Router(config-if)#ip na
Router(config-if)#ip nat ins
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#ip acc
Router(config)#ip access-list s
Router(config)#ip access-list standard FOR-NAT
Router(config-std-nacl)#per
Router(config-std-nacl)#permit 192.168.1.0 ?
  A.B.C.D Wildcard bits
  <cr>
Router(config-std-nacl)#permit 192.168.1.0 0.0.0.255
Router(config-std-nacl)#exit
Router(config)#
Router(config)#
Router(config)#ip
```

Copy Paste

На Router0 настроим NAT



Router0

Physical Config CLI

IOS Command Line Interface

```
Router(config-std-nacl)#exit
Router(config)#
Router(config)#
Router(config)#ip nat
Router(config)#ip nat so
Router(config)#ip nat so
Router(config)#ip nat ?
    inside   Inside address translation
    outside  Outside address translation
    pool     Define pool of addresses
Router(config)#ip nat in
Router(config)#ip nat inside ?
    source   Source address translation
Router(config)#ip nat inside s
Router(config)#ip nat inside source 1
Router(config)#ip nat inside source list FOR-NAT ?
    interface Specify interface for global address
    pool      Name pool of global addresses
Router(config)#ip nat inside source list FOR-NAT in
Router(config)#ip nat inside source list FOR-NAT interface fa0/0 ?
    overload  Overload an address translation
<cr>
Router(config)#ip nat inside source list FOR-NAT interface fa0/0 over
Router(config)#ip nat inside source list FOR-NAT interface fa0/0
overload
Router(config)#

```

Сохраняем настройки

PC0 192.168.1.2
PC1 192.168.1.3
Центральный офис 192.168.1.0/24

Router0

Physical Config CLI

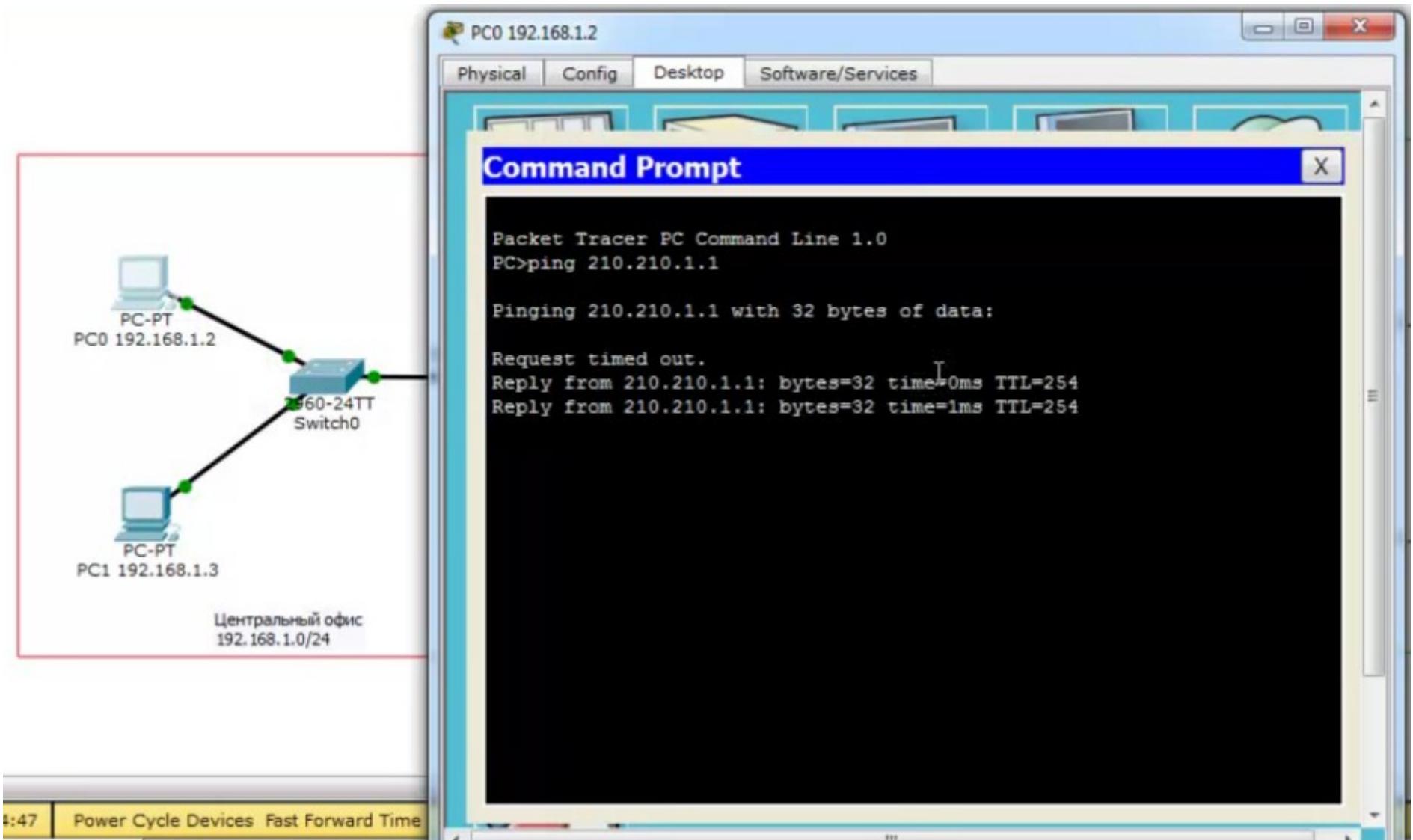
IOS Command Line Interface

```
Router(config)#ip nat inside ?
  source  Source address translation
Router(config)#ip nat inside s
Router(config)#ip nat inside source 1
Router(config)#ip nat inside source list FOR-NAT ?
  interface Specify interface for global address
  pool      Name pool of global addresses
Router(config)#ip nat inside source list FOR-NAT in
Router(config)#ip nat inside source list FOR-NAT interface fa0/0 ?
  overload Overload an address translation
<cr>
Router(config)#ip nat inside source list FOR-NAT interface fa0/0 over
Router(config)#ip nat inside source list FOR-NAT interface fa0/0
overload
Router(config)#
Router(config)#
Router(config)#
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#wr mem
Building configuration...
[OK]
Router#
```

Copy Paste

Проверяем доступ роутера провайдера с PC0. Доступно



Настраиваем NAT на Router1 филиала

Router>
Router>en
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip na
Router(config-if)#ip nat ou
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#int fa0/1
Router(config-if)#ip nat
Router(config-if)#ip nat in
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#
Router(config)#ip acc
Router(config)#ip access-list st
Router(config)#ip access-list standard FOR-NAT
Router(config-std-nacl)#per
Router(config-std-nacl)#permit 192.168.2.0 0.0.0.255
Router(config-std-nacl)#
Router(config-std-nacl)#exit
Router(config)#
Router(config)#
Router(config)#ip

Copy Paste

```
graph LR; Router1[2811 Router1] --- S1[2960-24 Switch1]; Router1 --- Link0_30["0/30"]; S1 --- PC2[PC-PT 192.168.2.2]; S1 --- PC3[PC-PT 192.168.2.3]; subgraph BranchOffice [Филиал 192.168.2.0/24]; Router1; S1; end;
```

Настраиваем NAT на Router1 филиала, и сохраняем настройки.

Router1

Physical Config CLI

IOS Command Line Interface

```
Router(config)#  
Router(config)#  
Router(config)#ip nat  
Router(config)#ip nat in  
Router(config)#ip nat inside so  
Router(config)#ip nat inside source li  
Router(config)#ip nat inside source list FOR-NAT ?  
  interface Specify interface for global address  
  pool      Name pool of global addresses  
Router(config)#ip nat inside source list FOR-NAT in  
Router(config)#ip nat inside source list FOR-NAT interface fa0/0 over  
Router(config)#ip nat inside source list FOR-NAT interface fa0/0  
overload  
Router(config)#  
Router(config)#  
Router(config)#  
Router(config)#end  
Router#  
%SYS-5-CONFIG_I: Configured from console by console  
  
Router#  
Router#  
Router#wr mem  
Building configuration...  
[OK]  
Router#
```

```
graph LR; Router1[2811 Router1] ---|Fa0/0| 0_30[0/30]; Router1 ---|Fa0/1| Switch1[2960-24 Switch1]; Switch1 --- PC1[PC1-PT 192.168.2.2]; Switch1 --- PC2[PC2-PT 192.168.2.2]; Switch1 --- PC3[PC3-PT 192.168.2.3];
```

Филиал
192.168.2.0/24

Проверяем с PC2 доступность интерфейса провайдера

PC2 192.168.2.2

Physical Config Desktop Software/Services

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 210.210.2.1

Pinging 210.210.2.1 with 32 bytes of data:

Request timed out.
Reply from 210.210.2.1: bytes=32 time=0ms TTL=254
Reply from 210.210.2.1: bytes=32 time=0ms TTL=254
```

The network diagram illustrates a topology with three main components: Router1, Switch1, and two PCs. Router1 is connected to a PC (PC-PT) with IP 210.210.2.1. Router1 is also connected to Switch1 via its Fa0/0 interface. The connection between Router1 and Switch1 is labeled with the subnet mask 210.210.2.0/30. Switch1 is connected to two PCs: PC-PT (IP 192.168.2.2) and PC3 (IP 192.168.2.3). A green box encloses the Router1-Switch1-PC-PT segment, with the label 'Файл' and '192.168.2.0/24' at the bottom right.

Краткий список команд для настройки VPN

Lesson18 - VPN

Типовые настройки роутера:

Настройка первой фазы

```
crypto isakmp policy 1
```

```
encr 3des
```

```
hash md5
```

```
authentication pre-share
```

```
group 2
```

Настройка ключа аутентификации и пира

```
crypto isakmp key cisco address 210.210.2.2
```

Вторая фаза

```
crypto ipsec transform-set TS esp-3des esp-md5-
```

```
hmac
```

Определяем какой трафик шифровать

```
ip access-list extended FOR-VPN
```

```
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Создание криптокарты

```
crypto map CMAP 10 ipsec-isakmp
```

```
set peer 210.210.2.2
```

```
set transform-set TS
```

```
match address FOR-VPN
```

Привязка к интерфейсу

```
interface FastEthernet0/0
```

```
crypto map CMAP
```

Типовые настройки МЭ:

Настройка первой фазы

```
crypto ikev1 enable outside
```

```
crypto ikev1 policy 1
```

```
encr 3des
```

```
hash md5
```

```
authentication pre-share
```

```
group 2
```

```
lifetime 43200
```

Настройка ключа аутентификации и пира

```
tunnel-group 210.210.2.2 type ipsec-l2l
```

```
tunnel-group 210.210.2.2 ipsec-attributes
```

```
ikev1 pre-shared-key cisco
```

Вторая фаза

```
crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac
```

Определяем какой трафик шифровать

```
access-list FOR-VPN extended permit icmp 192.168.1.0
```

```
255.255.255.0 192.168.2.0 255.255.255.0
```

Создание криптокарты

```
crypto map To-Site2 1 match address FOR-VPN
```

```
crypto map To-Site2 1 set peer 210.210.2.2
```

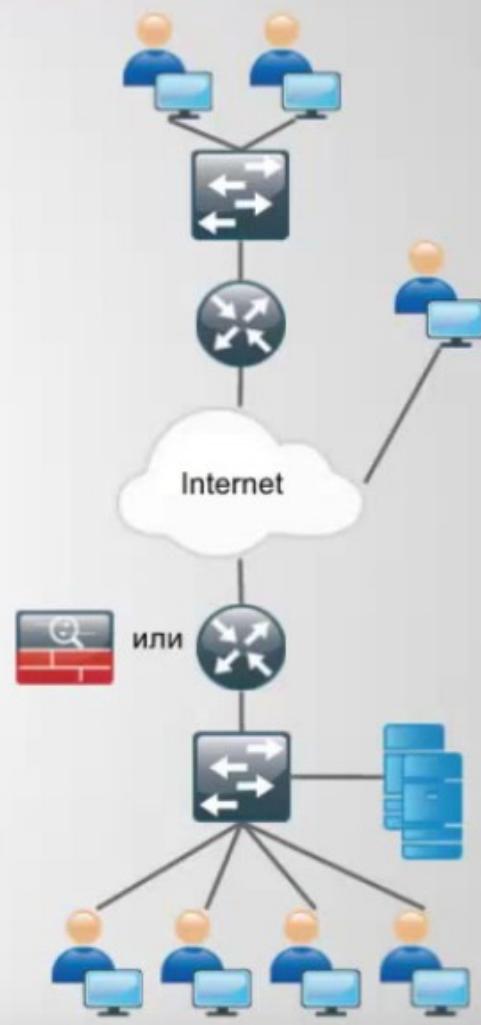
```
crypto map To-Site2 1 set security-association lifetime seconds
```

```
86400
```

```
crypto map To-Site2 1 set ikev1 transform-set TS
```

Привязка к интерфейсу

```
crypto map To-Site2 interface outside
```



На Router0 создаем политику, в которой задаем тип шифрования 3DES, и метод аутентификации с открытым ключом «pre-share»

Курс молодого бойца. Практическая часть

Типовые настройки роутера:

Настройка первой фазы

```
crypto isakmp policy 1
```

```
encr 3des
```

```
hash md5
```

```
authentication pre-share
```

```
group 2
```

Настройка ключа аутентификации и пира

```
crypto isakmp key cisco address 210.210.2.2
```

Вторая фаза

```
crypto ipsec transform-set TS esp-3des esp-md5-
```

```
hmac
```

Определяем какой трафик шифровать

```
ip access-list extended FOR-VPN
```

```
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Создание криптокарты

```
crypto map CMAP 10 ipsec-isakmp
```

```
set peer 210.210.2.2
```

```
set transform-set TS
```

```
match address FOR-VPN
```

Привязка к интерфейсу

```
interface FastEthernet0/0
```

```
crypto map CMAP
```

Router#
Router#wr mem
Building configuration...
[OK]
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#cry
Router(config)#crypto isa
Router(config)#crypto isakmp pol
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#enc
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#ha
Router(config-isakmp)#hash md
Router(config-isakmp)#hash md5
Router(config-isakmp)#au
Router(config-isakmp)#authentication pre
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#gr
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#
Router(config)#|

Copy Paste

На Router0 создаем открытый ключ, пароль cisco, и тип шифрования 3DES

курс молодого бойца. практическ

Типовые настройки роутера:

Настройка первой фазы

crypto isakmp policy 1

encl 3des

hash md5

authentication pre-share

group 2

Настройка ключа аутентификации и пароля

Page 10

crypto ipsec transform-set TS esp-3des esp-md5-

hmac

Определяем какой трафик шифровать

ip access-list extended FOR-VPN

```
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Создание криптокарты

съхранение на изображенията

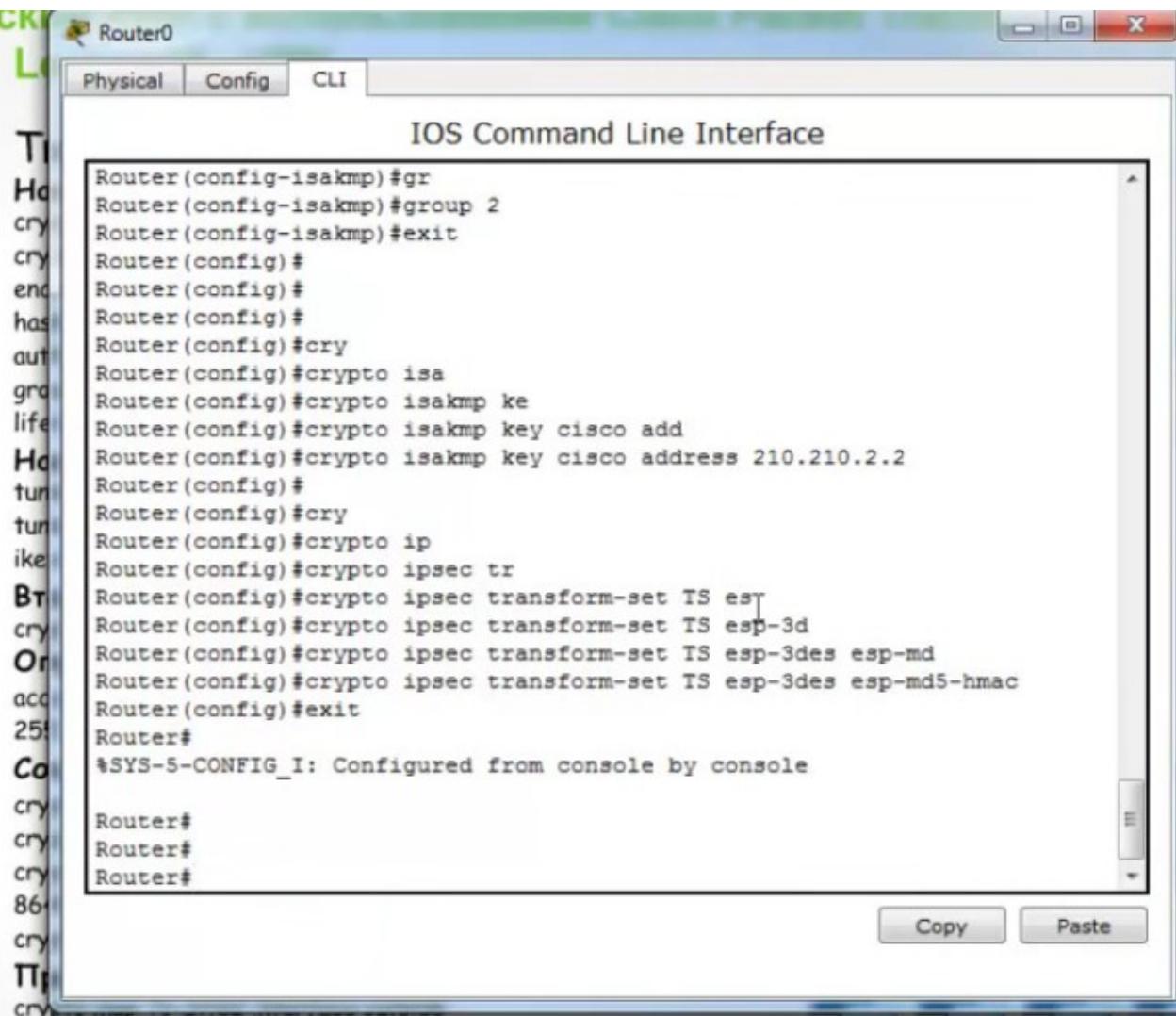
set peer 210 210 2 2

set transform-set TS

match address EOR VRF

match address FOR-VPN

Привязка к интерфейсу



На Router0 создаем access list, который задает какой траффик будет направляться в VPN-канал

курс молодого бойца. Практически

Типовые настройки роутера:

Настройка первой фазы

crypto isakmp policy 1

encl 3des

hash md5

authentication pre-share

group 2

Настройка ключа аутентификации и пира

```
crypto isakmp key cisco address 210.210.2.2
```

Вторая фаза

```
crypto ipsec transform-set TS esp-3des esp-md5-hmac
```

Определяем какой трафик шифровать

ip access-list extended FOR-VPN

```
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Создание криптокарты

СГУРТЫ ТАР СМАР 10 ІВСЕС-ІСАКМР

set peer 210 210 2 2

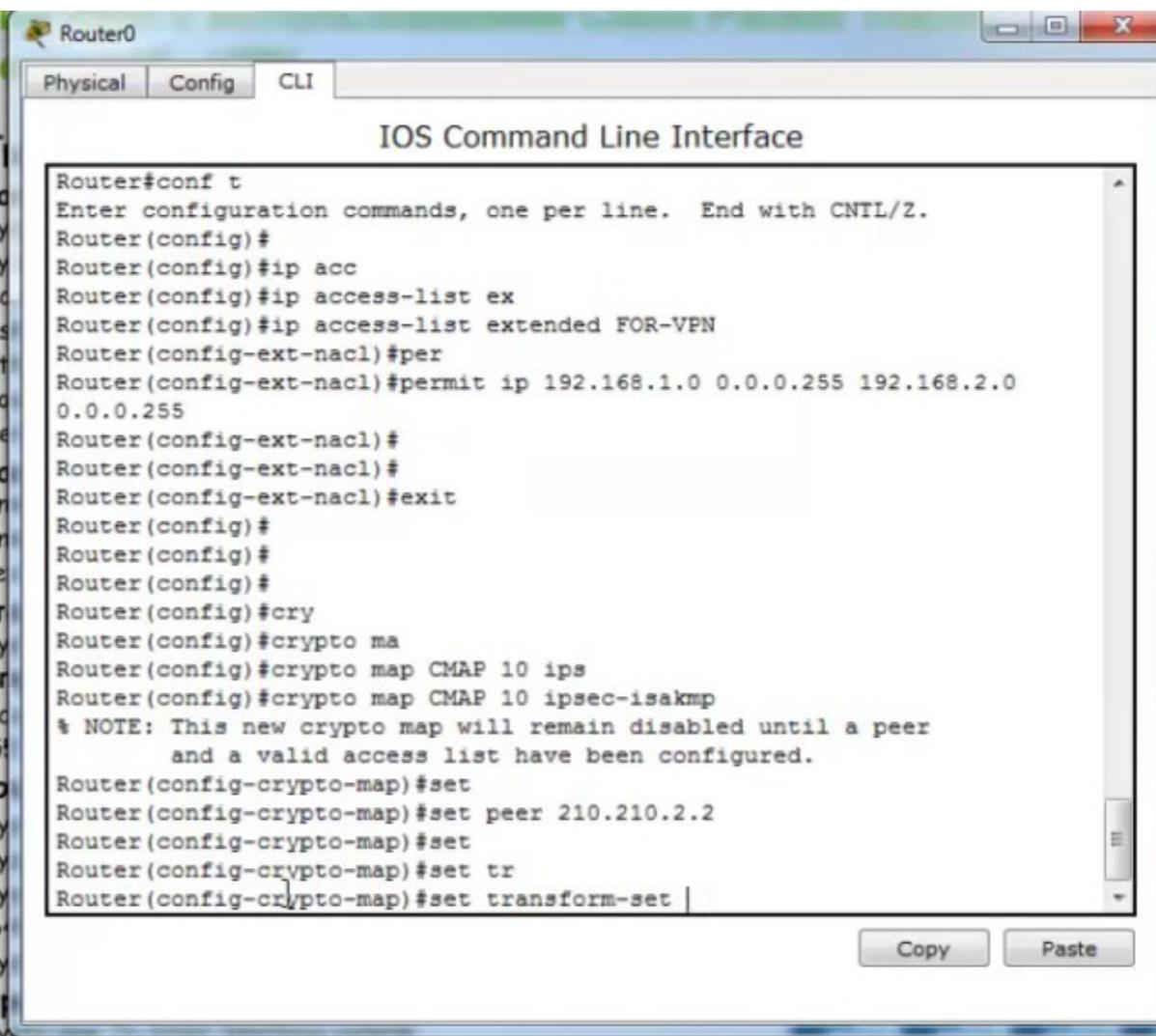
set transform-set TS

match address FOR VPN

match address FOR-VPN

Привязка к интерфейсу interface FastEthernet0/0

interface FASTEN
cripto-mon CMAP



На Router0 создаем крипто-карту с настройками шифрования

курс молодого бойца. практические

Типовые настройки роутера:

Настройка первой фазы

crypto isakmp policy 1

encl 3des

hash md5

authentication pre-share

group 2

Настройка ключа аутентификации и пира

```
crypto isakmp key cisco address 210.210.2.2
```

Вторая фаза

```
crypto ipsec transform-set T5 esp-3des esp-md5-hmac
```

Определяем какой трафик шифровать

ip access-list extended FOR-VPN

```
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Создание криптокарты

```
crypto map CMAP 10 ipsec-isakmp
```

set peer 210.210.2.2

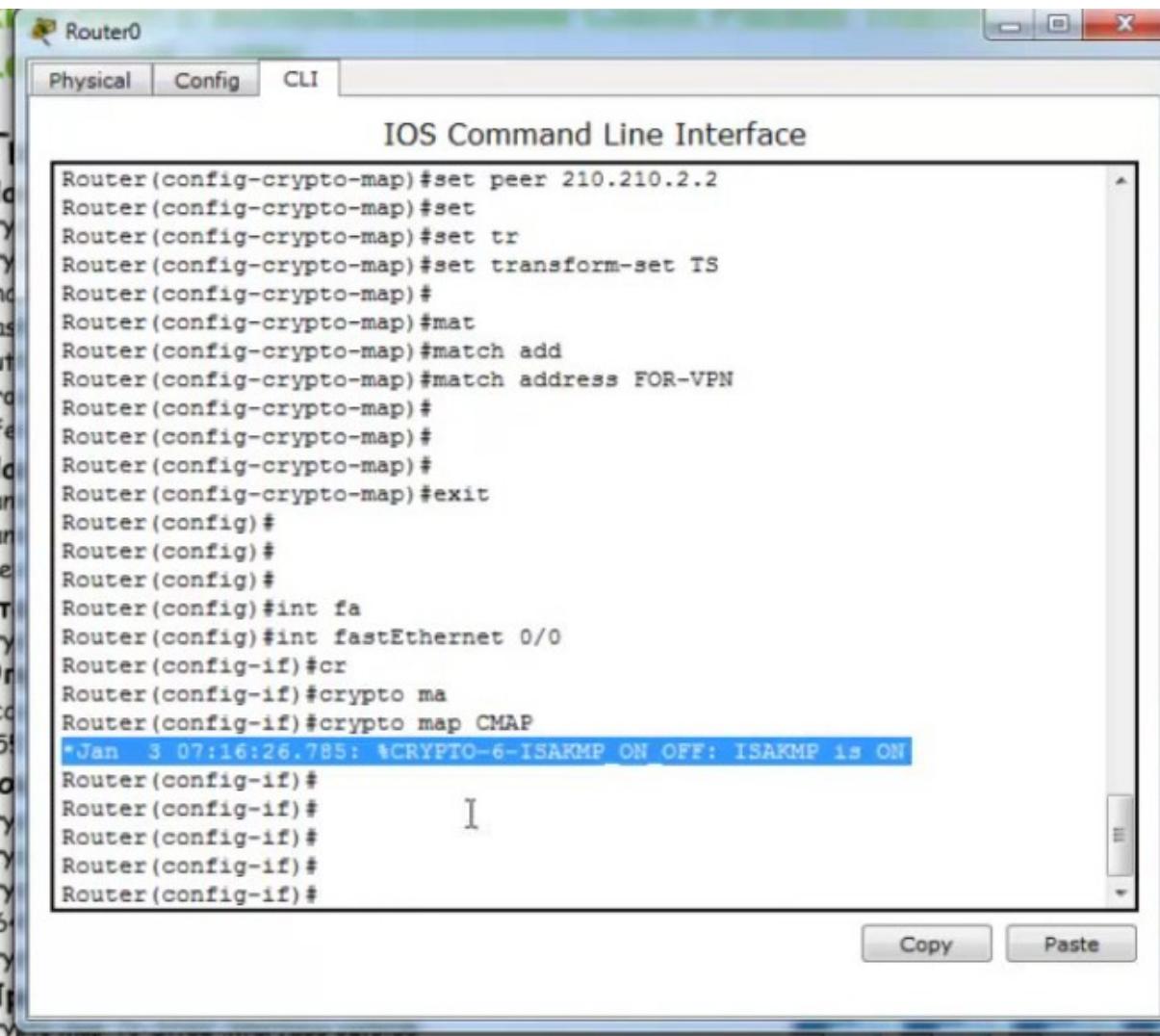
set transform-set TS

match address FOR-VPN

Привязка к интерфейсу

interface FastEthernet0/0

crypto map CMAP



На Router0 создаем крипто-карту с настройками шифрования

Курс молодого бойца. Практическ

The screenshot shows the Router0 CLI interface with the following configuration session:

```
Router(config-ext-nacl)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#cry
Router(config)#crypto ma
Router(config)#crypto map CMAP 10 ips
Router(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
       and a valid access list have been configured.
Router(config-crypto-map)#set
Router(config-crypto-map)#set peer 210.210.2.2
Router(config-crypto-map)#set
Router(config-crypto-map)#set tr
Router(config-crypto-map)#set transform-set TS
Router(config-crypto-map)#
Router(config-crypto-map)#mat
Router(config-crypto-map)#match add
Router(config-crypto-map)#match address FOR-VPN
Router(config-crypto-map)#
Router(config-crypto-map)#
Router(config-crypto-map)#
Router(config-crypto-map)#
Router(config)#
Router(config)#
Router(config)#[
```

At the bottom right, there are "Copy" and "Paste" buttons.

Типовые настройки роутера:

Настройка первой фазы

crypto isakmp policy 1

encl 3des

hash md5

authent

group 2

Настройка ключа аутентификации и права

crypto isakmp key cisco address 210.210.2.2

Вторая фаза

```
crypto ipsec transform-set TS esp-3des esp-md5-
```

hmac

Определяем какой трафик шифровать

ip access-list extended FOR-VPN

```
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Создание криптокарты

```
crypto map CMAP 10 ipsec-isakmp
```

set peer 210.210.2.2

set transform-set TS

match address EOR-VPN

Приязнь к инструментам

Привязка к интерфейсу interface FastEthernet0/

interface FastEthernet
switchport mode CMAC

Привязываем эту крипто-карту к интерфейсу fa0/0. Сохраняем

Курс молодого бойца. Практическое

Типовые настройки роутера:

Настройка первой фазы

crypto isakmp policy 1

encl 3des

hash md5

authentication pre-share

group 2

Настройка ключа аутентификации и пира

```
crypto isakmp key cisco address 210.210.2.2
```

Вторая фаза

```
crypto ipsec transform-set TS esp-3des esp-md5-
```

hmac

Определяем какой трафик шифровать

ip access-list extended FOR-VPN

```
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Создание криптокарты

```
crypto map CMAP 10 ipsec-isakmp
```

```
set peer 210.210.2.2
```

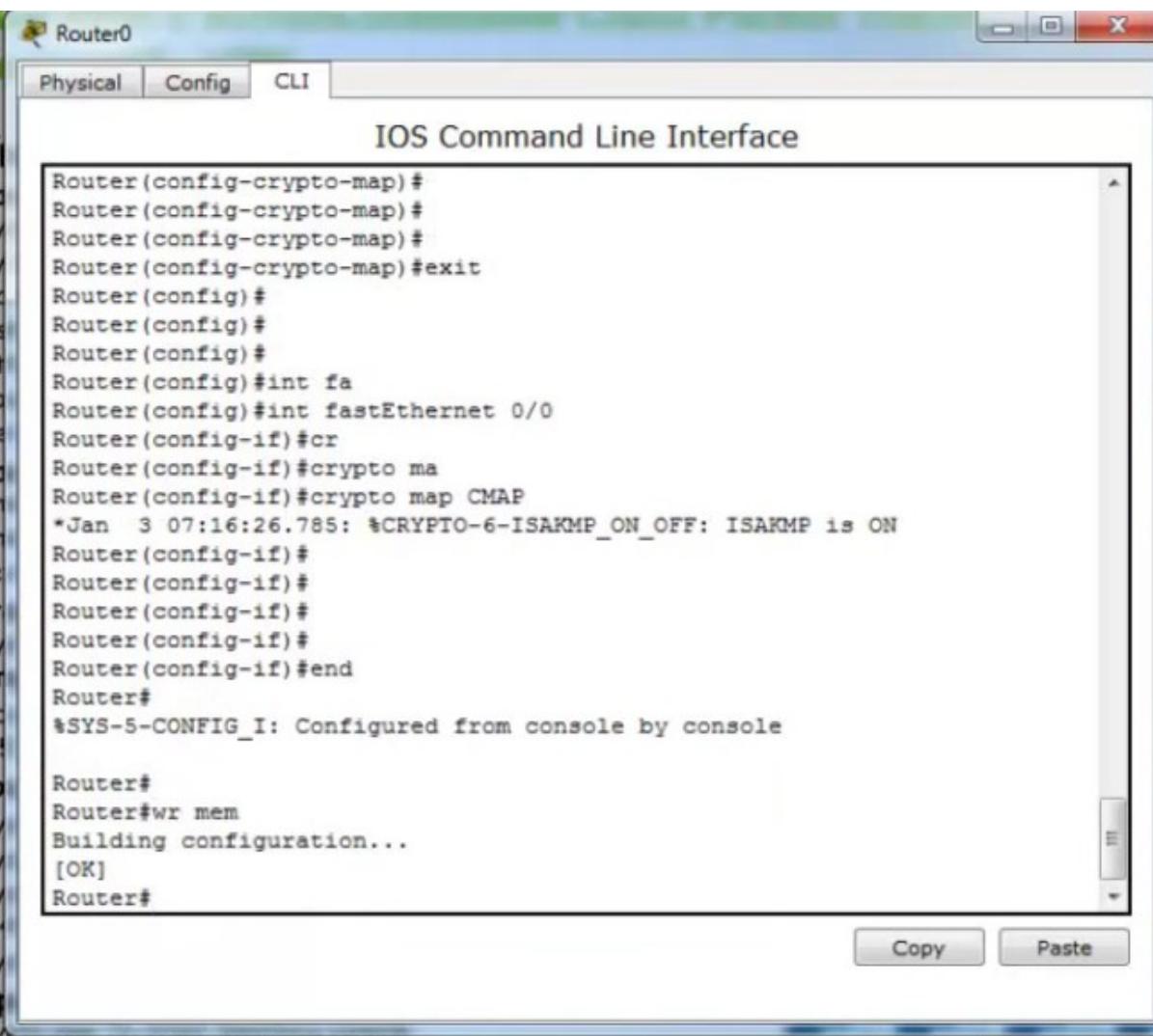
set transform-set TS

match address FOR-VPN

Привязка к интерфейсу

interface FastEthernet0/0

crypto map CMAP



Выполняем те же действия на Router1 роутере филиала

Типовые настройки роутера:

Настройка первой фазы

crypto isakmp policy 1

enctr 3des

hash md5

authentication pre-share

group 2

Настройка ключа аутентификации и пира

```
crypto isakmp key cisco address 210.210.2.2
```

Вторая фаза

```
crypto ipsec transform-set TS esp-3des esp-md5-hmac
```

Определяем какой трафик шифровать

ip access-list extended FOR-VPN

```
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Создание криптокарты

```
crypto map CMAP 10 ipsec-isakmp
```

```
set peer 210.210.2.2
```

set transform-set TS

match address FOR-VPN

Привязка к интерфейсу

interface FastEthernet0/0

crypto map CMAP

Выполняем те же действия на Router1 роутере филиала

Типовые настройки роутера:

Настройка первой фазы

```
crypto isakmp policy 1
```

```
encr 3des
```

```
hash md5
```

```
authentication pre-share
```

```
group 2
```

Настройка ключа аутентификации и пира

```
crypto isakmp key cisco address 210.210.2.2
```

Вторая фаза

```
crypto ipsec transform-set TS esp-3des esp-md5-hmac
```

Определяем какой трафик шифровать

```
ip access-list extended FOR-VPN
```

```
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Создание криптокарты

```
crypto map CMAP 10 ipsec-isakmp
```

```
set peer 210.210.2.2
```

```
set transform-set TS
```

```
match address FOR-VPN
```

Привязка к интерфейсу

```
interface FastEthernet0/0
```

```
crypto map CMAP
```

Router1

Physical Config CLI

IOS Command Line Interface

```
Router(config)#cry
Router(config)#crypto isa
Router(config)#crypto isakmp ke
Router(config)#crypto isakmp key cisco add
Router(config)#crypto isakmp key cisco address 210.210.1.2
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
cry
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#cry
Router(config)#crypto ip
Router(config)#crypto ipsec tr
Router(config)#crypto ipsec transform-set TS esp-3
Router(config)#crypto ipsec transform-set TS esp-3des esp
Router(config)#crypto ipsec transform-set TS esp-3des esp-m
Router(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
Router(config)#
Router(config)#ip acc
Router(config)#ip access-list ex
Router(config)#ip access-list extended FOR-VPN
Router(config-ext-nacl)#
Router(config-ext-nacl)#
Router(config-ext-nacl)#per
Router(config-ext-nacl)#permit |
```

Copy Paste

Выполняем те же действия на Router1 роутере филиала

Типовые настройки роутера:

Настройка первой фазы

```
crypto isakmp policy 1
```

```
encr 3des
```

```
hash md5
```

```
authentication pre-share
```

```
group 2
```

Настройка ключа аутентификации и пира

```
crypto isakmp key cisco address 210.210.2.2
```

Вторая фаза

```
crypto ipsec transform-set TS esp-3des esp-md5-
```

```
hmac
```

Определяем какой трафик шифровать

```
ip access-list extended FOR-VPN
```

```
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Создание криптокарты

```
crypto map CMAP 10 ipsec-isakmp
```

```
set peer 210.210.2.2
```

```
set transform-set TS
```

```
match address FOR-VPN
```

Привязка к интерфейсу

```
interface FastEthernet0/0
```

```
crypto map CMAP
```

Router1

Physical Config CLI

IOS Command Line Interface

```
Router(config-ext-nacl)#
Router(config-ext-nacl)#per
Router(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 192.168.1.0
0.0.0.255
Router(config-ext-nacl)#
Router(config-ext-nacl)#exit
Router(config)#cry
Router(config)#crypto ma
Router(config)#crypto map CMAP 10 ips
Router(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#set
Router(config-crypto-map)#set pee
Router(config-crypto-map)#set peer 210.210.1.2
Router(config-crypto-map)#set
Router(config-crypto-map)#set tr
Router(config-crypto-map)#set transform-set TS
Router(config-crypto-map)#ma
Router(config-crypto-map)#match add
Router(config-crypto-map)#match address FOR-VPN
Router(config-crypto-map)#exit
Router(config)#int fa0/0
Router(config-if)#cr
Router(config-if)#crypto ma
Router(config-if)#crypto map CMA
```

Copy Paste

Сохраняем настройки

Типовые настройки роутера:

Настройка первой фазы

crypto isakmp policy 1

encr 3des

hash md5

authentication pre-share

group 2

Настройка ключа аутентификации и пира

```
crypto isakmp key cisco address 210.210.2.2
```

Вторая фаза

```
crypto ipsec transform-set TS esp-3des esp-md5-hmac
```

Определяем какой трафик шифровать

ip access-list extended FOR-VPN

```
permit ip 192.168.1.0 0.0.0.255 19
```

Создание криптокарты

crypto map CMAP 10 ipse

```
set peer 210.210.2.2
```

set transform-set TS

match address FOR-VI

Привязка к интерфейсу

Приставка к интерфейсу
interface FastEthernet0/

interface Fa0/0 crypto map CMAP

Попробуем с компьютера PC0 центрального офиса пропинговать компьютер PC2 в филиале. Не проходит

PC0 192.168.1.2

Physical Config Desktop Software/Services

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 210.210.1.1

Pinging 210.210.1.1 with 32 bytes of data:

Request timed out.
Reply from 210.210.1.1: bytes=32 time=0ms TTL=254
Reply from 210.210.1.1: bytes=32 time=1ms TTL=254
Reply from 210.210.1.1: bytes=32 time=10ms TTL=254

Ping statistics for 210.210.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

PC>ping 192.168.2.2

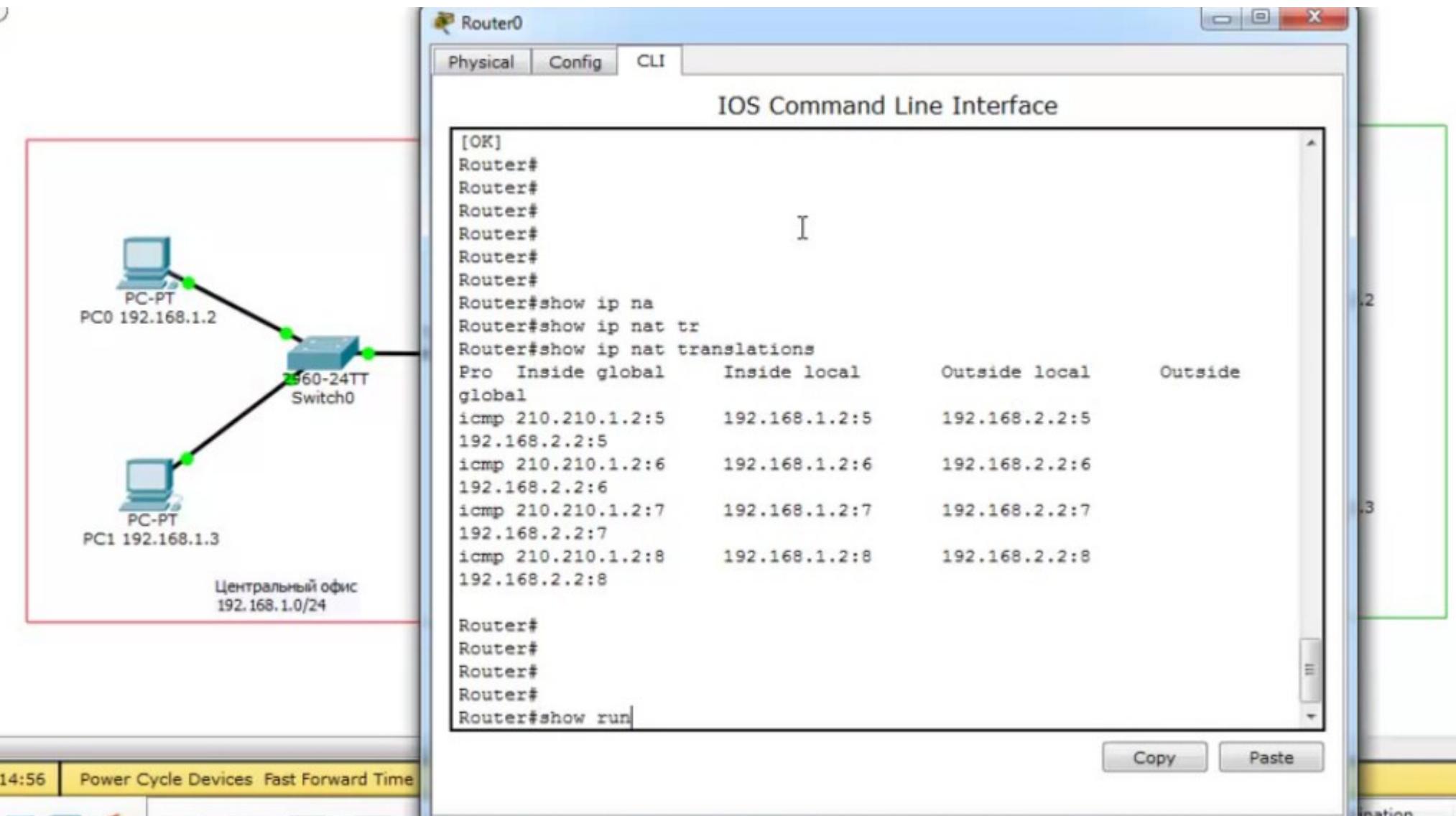
Pinging 192.168.2.2 with 32 bytes of data:

Reply from 210.210.1.1: Destination host unreachable.
Reply from 210.210.1.1: Destination host unreachable.
```

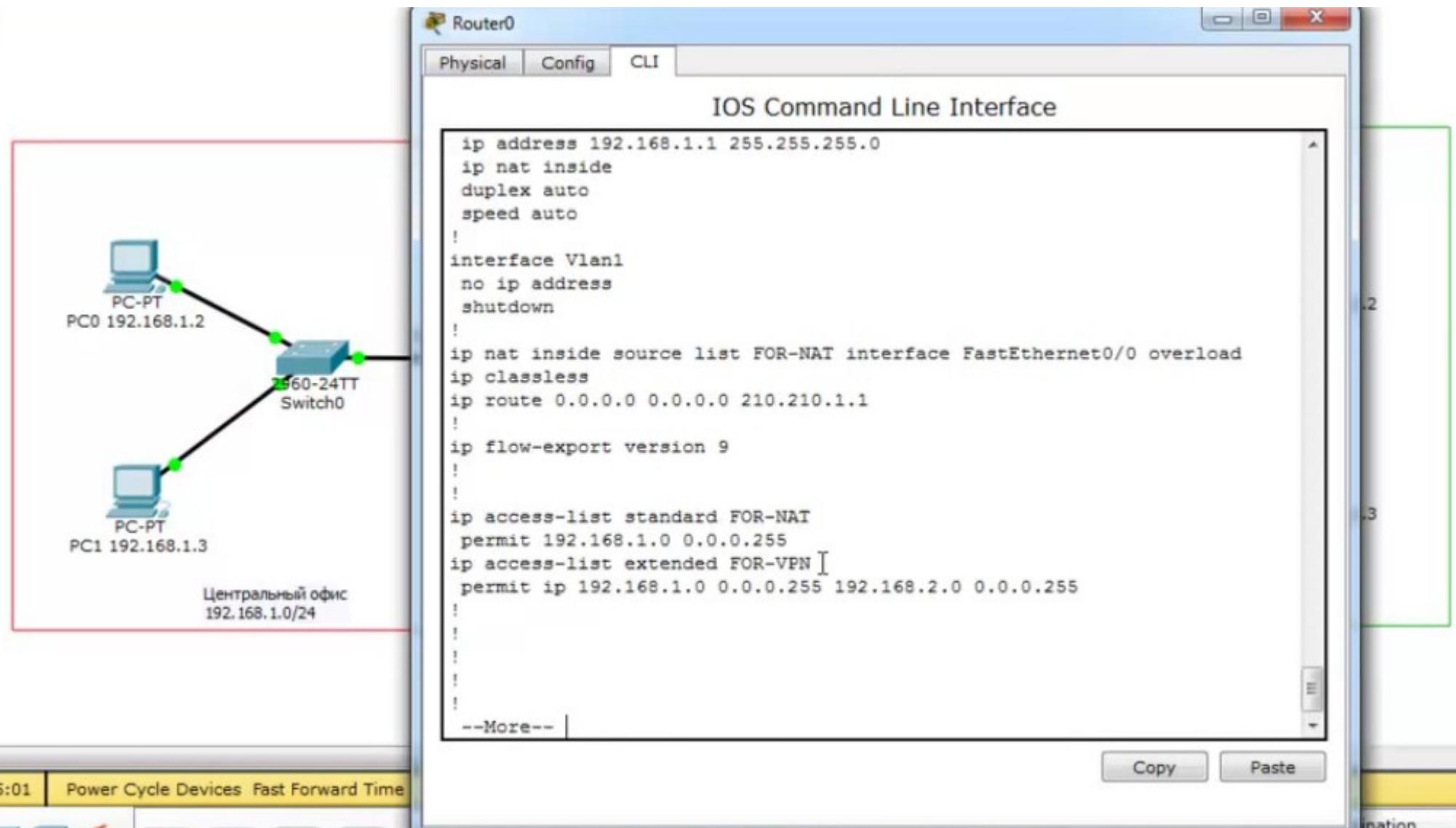
Филиал
192.168.2.0/24

Fire Last Status Source Destination T

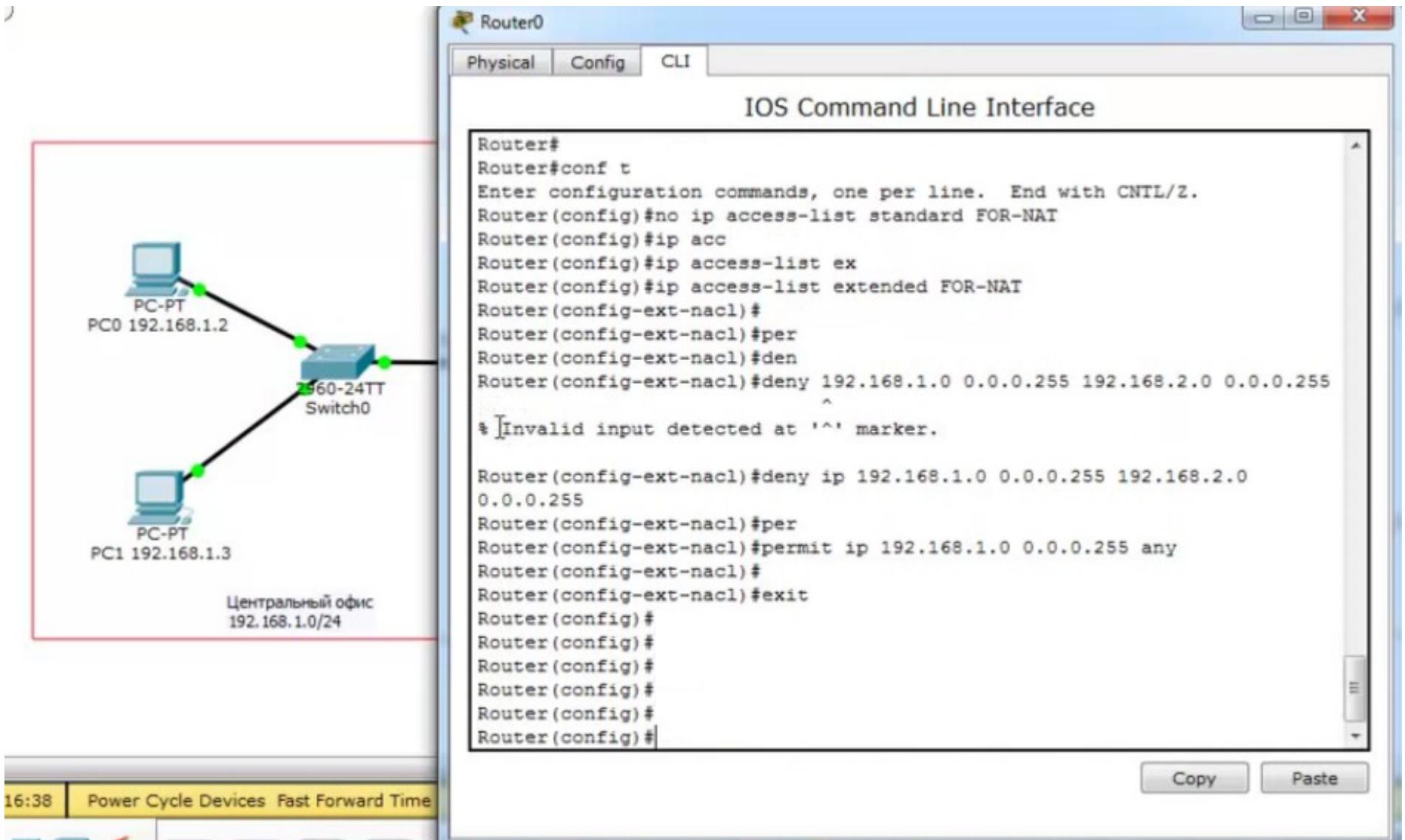
Смотрим настройки NAT на Router0. Траффик, который должен идти в VPN-канал, попадает под преобразования NAT. Посмотрим настройки access-list



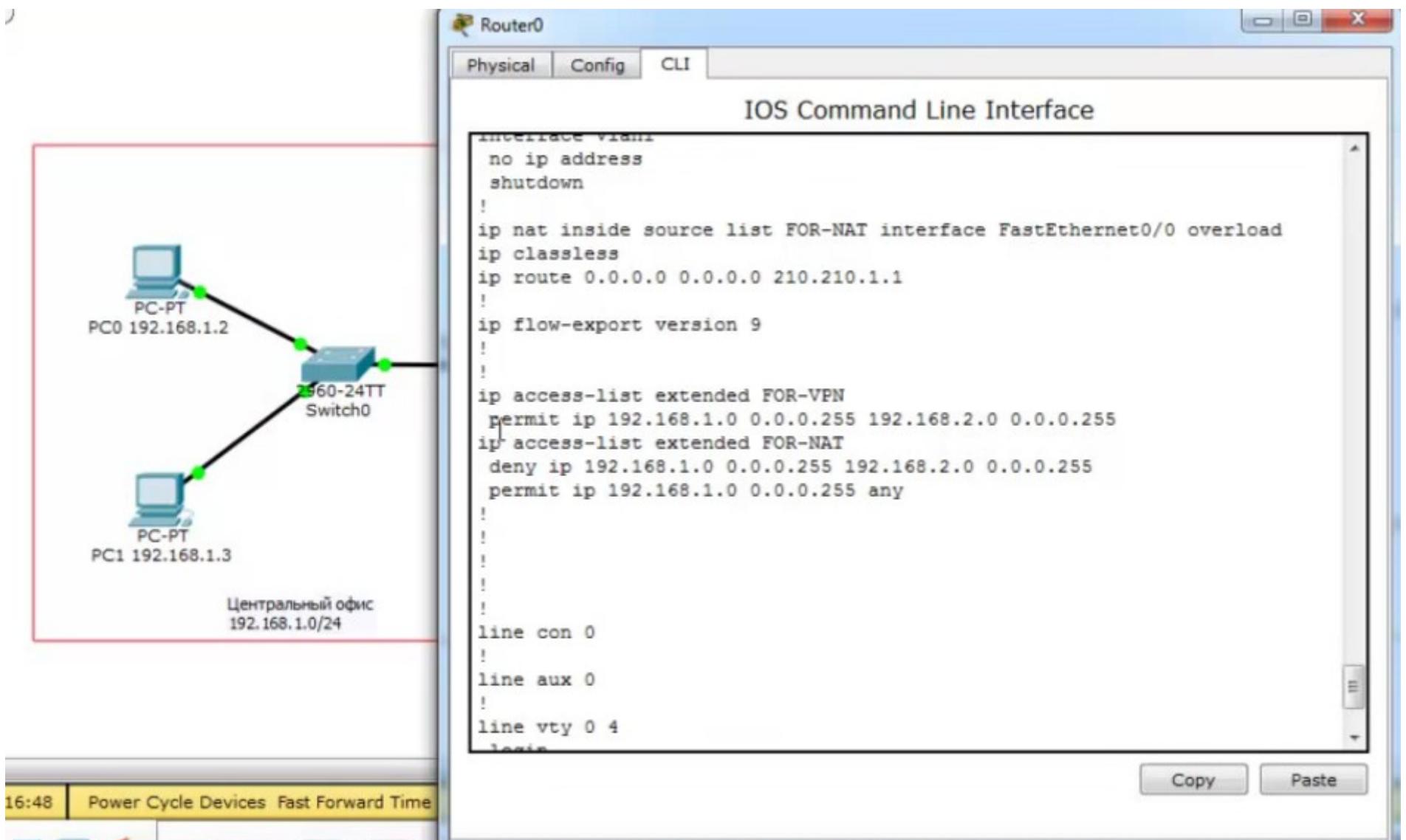
Под действие access-list попадает весь траффик 192.168.1.0, а это не совсем то, что нам нужно



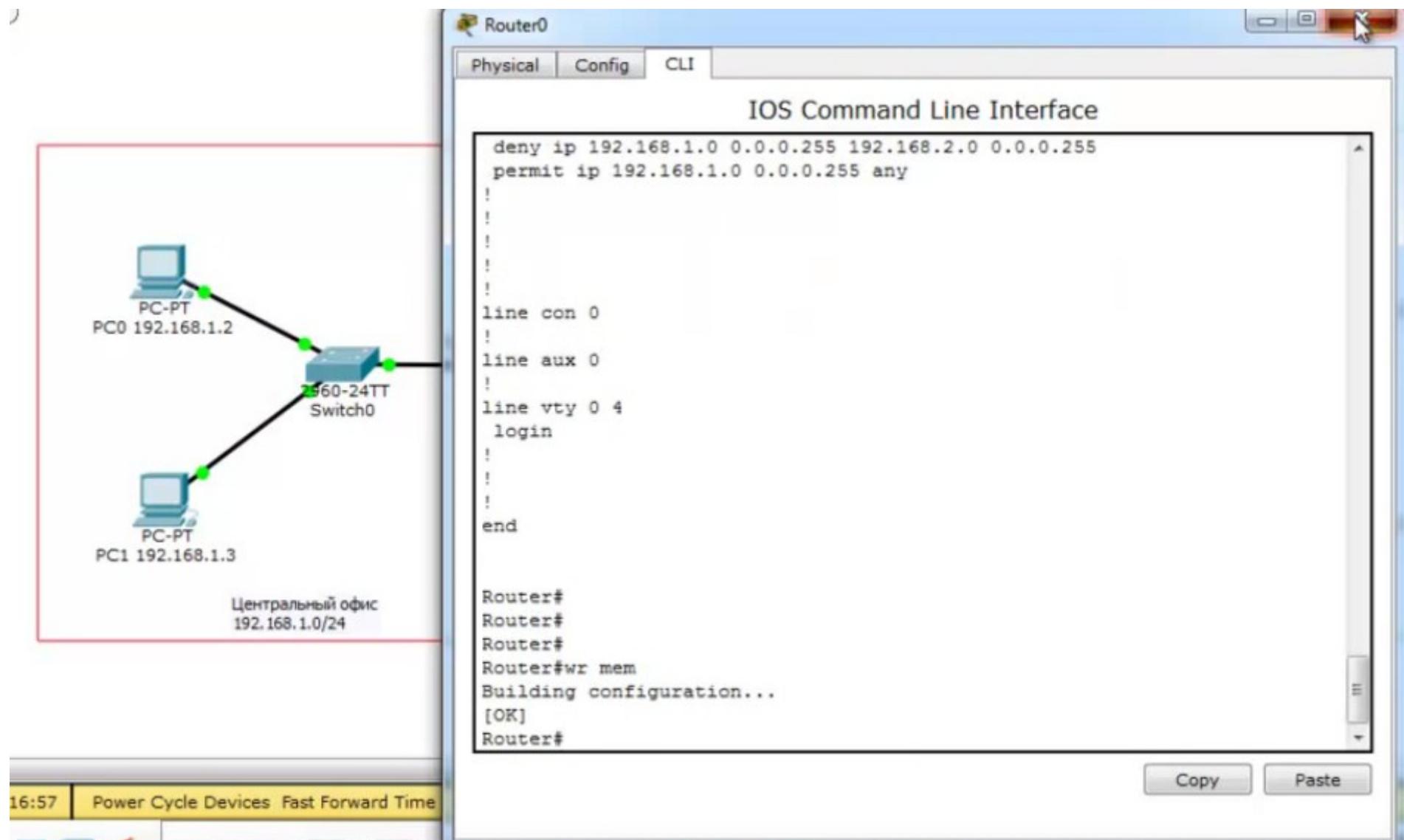
Удалим существующий access-list, добавим исправленный



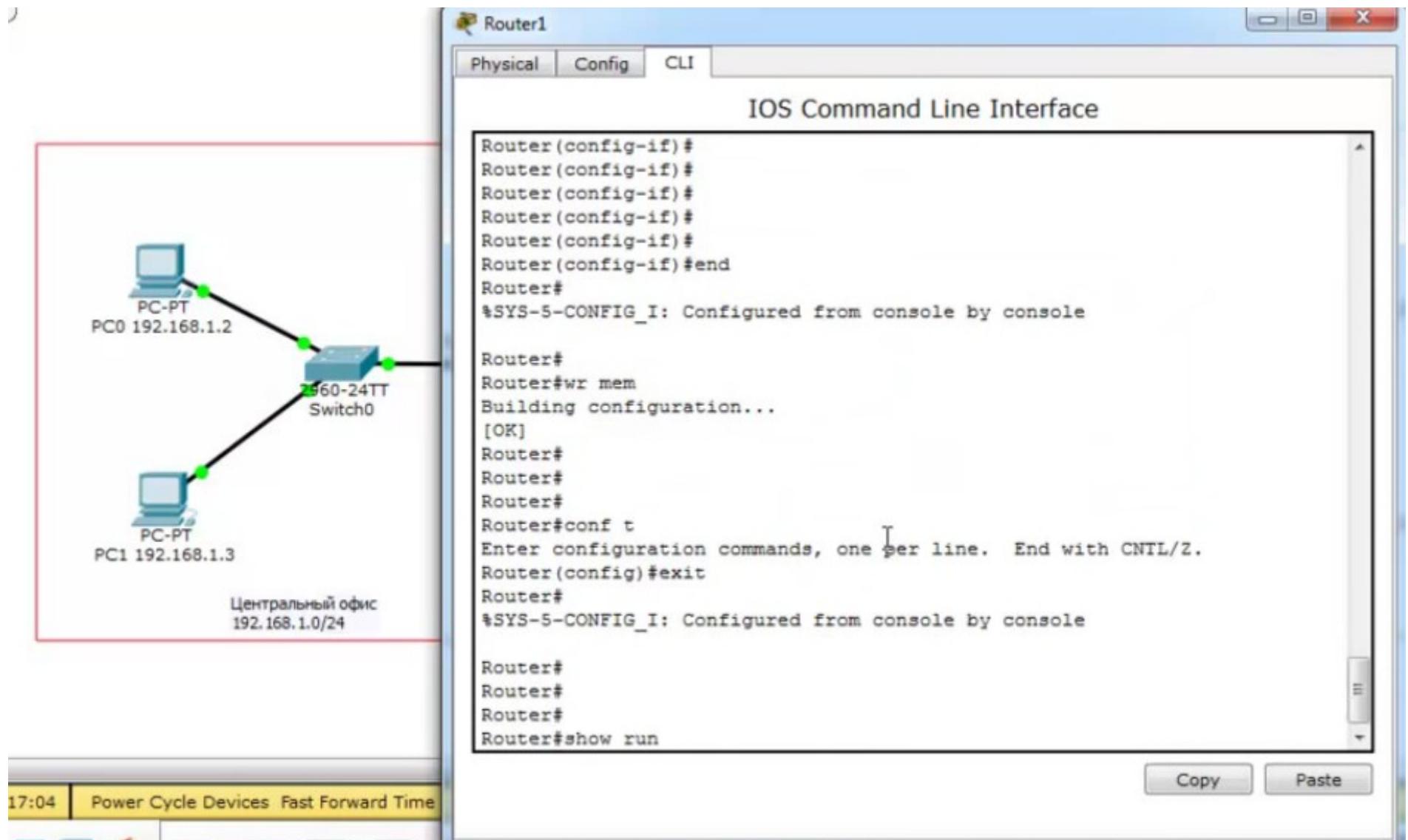
Проверим получившиеся настройки



Сохраняем



Зайдем на Router1 филиала, для выполнения тех же операций



Удалим существующий access list

The network diagram illustrates a topology where two PCs (PC-PT) are connected to a Switch0. The Switch0 is then connected to a Router1. The Router1 is also connected to a Central Office with the IP range 192.168.1.0/24.

Router1 Configuration (CLI):

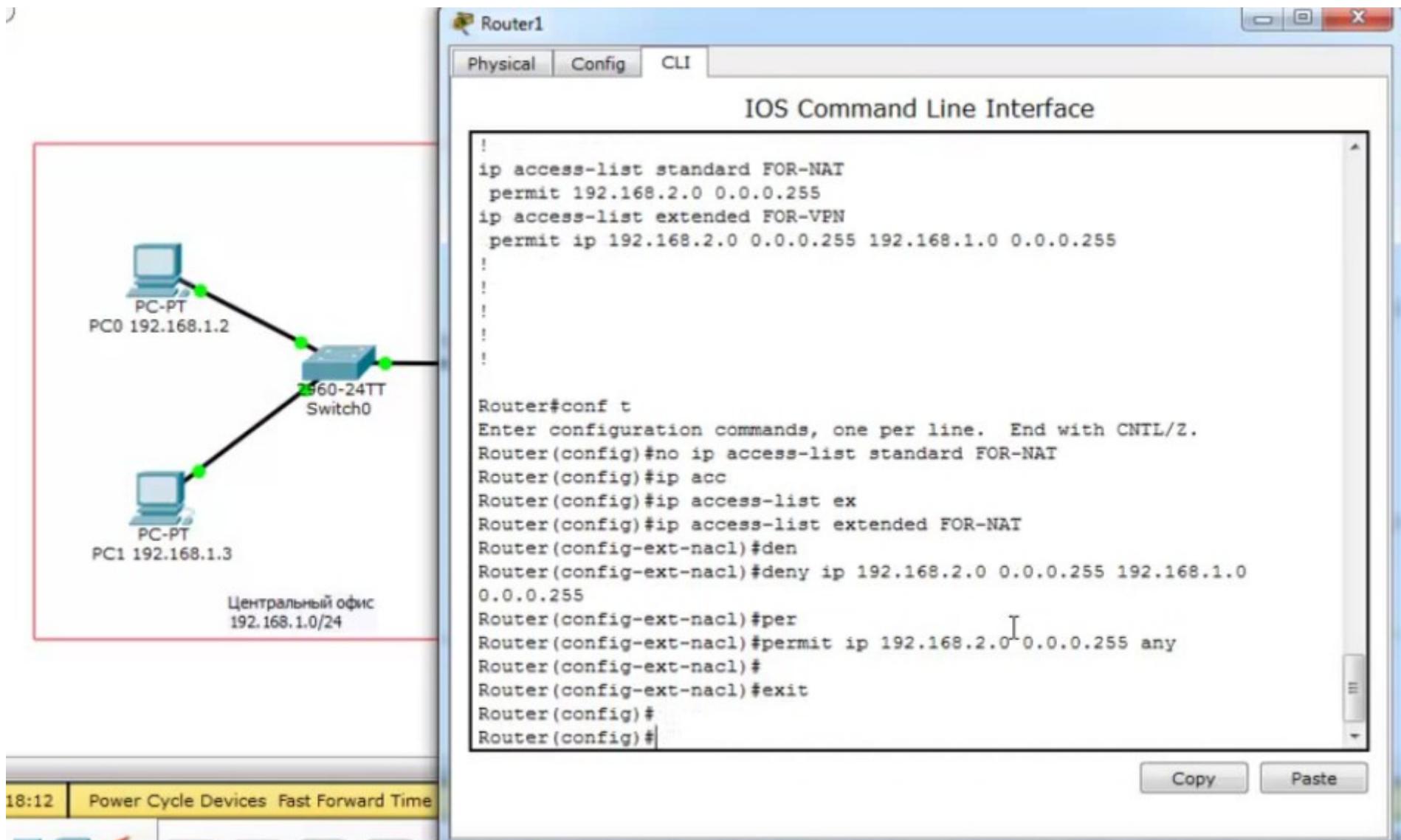
```
!
interface Vlan1
no ip address
shutdown
!
ip nat inside source list FOR-NAT interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 210.210.2.1
!
ip flow-export version 9
!
!
ip access-list standard FOR-NAT
permit 192.168.2.0 0.0.0.255
ip access-list extended FOR-VPN
permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
!
!
!
!
!
!
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip access-list standard FOR-NAT
Router(config)#

```

Toolbar Buttons:

- Copy
- Paste

и создадим расширенный



Проверим получившиеся настройки

Router1

Physical Config CLI

IOS Command Line Interface

```
ip address 192.168.2.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip nat inside source list FOR-NAT interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 210.210.2.1
!
ip flow-export version 9
!
!
ip access-list extended FOR-VPN
permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
ip access-list extended FOR-NAT
deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
permit ip 192.168.2.0 0.0.0.255 any
!
!
!
!
!--More--
```

PC-PT
PC0 192.168.1.2

PC-PT
PC1 192.168.1.3

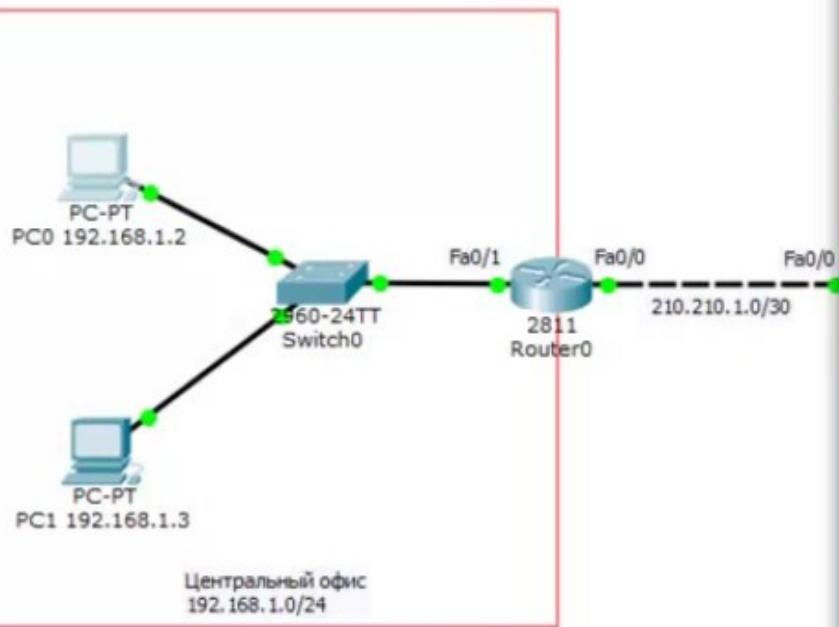
Центральный офис
192.168.1.0/24

560-24TT
Switch0

18:18 | Power Cycle Devices Fast Forward Time

Copy Paste

Проверим ping с PC0 на PC2 - идет



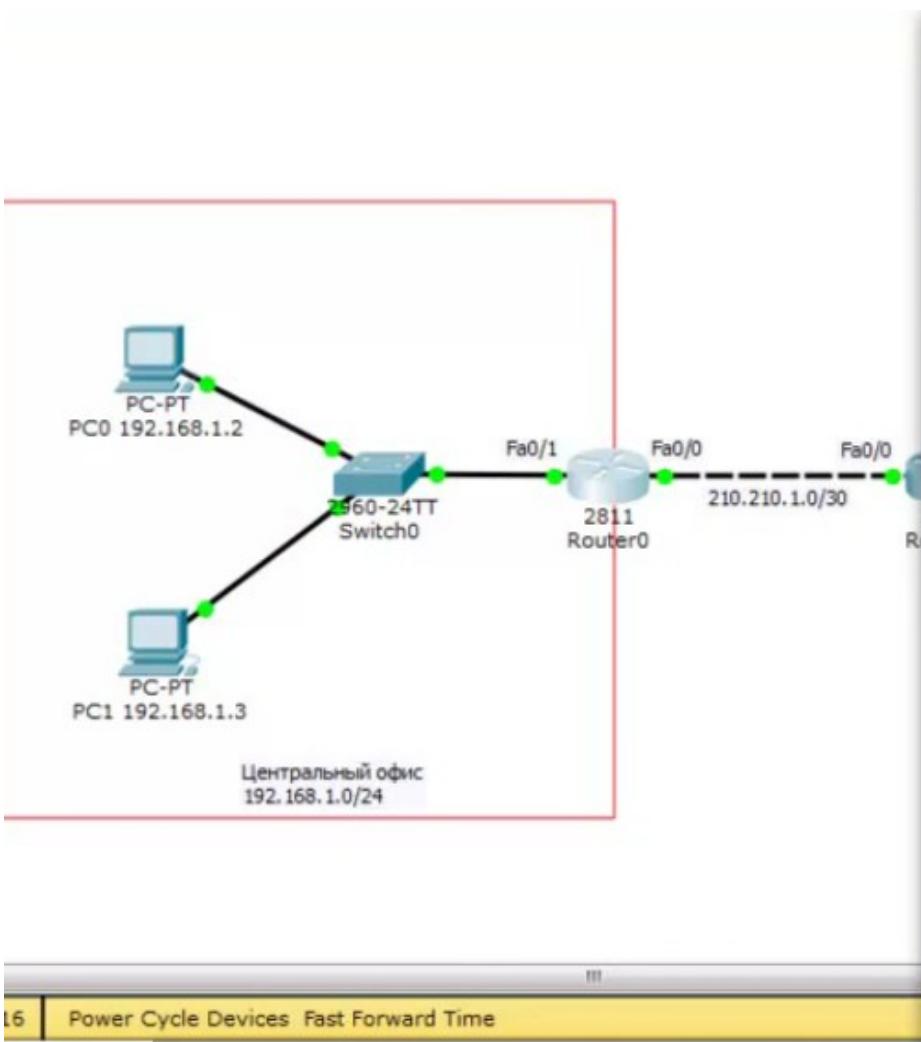
PC0 192.168.1.2

Physical Config Desktop Software/Services

Command Prompt

```
Pinging 192.168.2.2 with 32 bytes of data:  
Reply from 210.210.1.1: Destination host unreachable.  
  
Ping statistics for 192.168.2.2:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
PC>ping 192.168.2.2  
  
Pinging 192.168.2.2 with 32 bytes of data:  
  
Request timed out.  
Reply from 192.168.2.2: bytes=32 time=13ms TTL=126  
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126  
Reply from 192.168.2.2: bytes=32 time=11ms TTL=126  
  
Ping statistics for 192.168.2.2:  
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 10ms, Maximum = 13ms, Average = 11ms  
  
PC>
```

Проверим на роутере наличие «технологического» VPN тоннеля



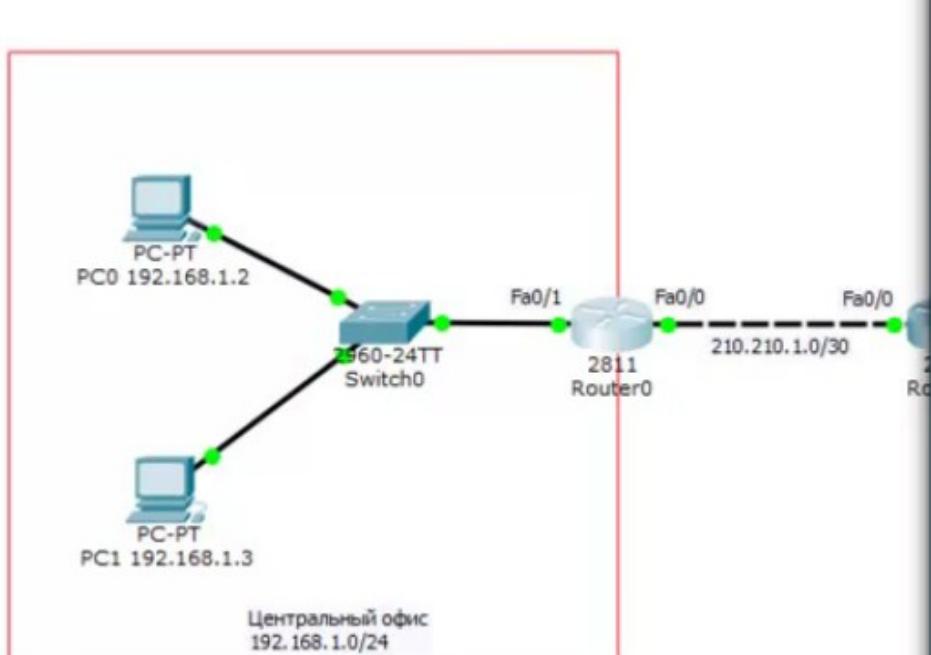
```
Router#
Router#
Router#
Router#wr mem
Building configuration...
[OK]
Router#
Router#
Router#
Router#
Router#
Router#show isa
Router#show cry
Router#show crypto isa
Router#show crypto isakmp sa
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state      conn-id slot status
210.210.2.2  210.210.1.2  QM_IDLE   1054     0 ACTIVE
                                         I
IPv6 Crypto ISAKMP SA

Router#
```

Copy Paste

16 Power Cycle Devices Fast Forward Time

и наличие ipsec VPN тоннеля



Router#show cr
Router#show crypto ip
Router#show crypto ipsec sa

interface: FastEthernet0/0
Crypto map tag: CMAP, local addr 210.210.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer 210.210.2.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 210.210.1.2, remote crypto endpt.: 210.210.2.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x170B5AB4(386620084)

inbound esp sas:
spi: 0x55DE26EA(1440622314)

--More-- |

Copy Paste

DMZ

DMZ - Demilitarized Zone - демилитаризованная зона

- Содержит общедоступные сервисы (web сервер, почтовый сервер, ftp сервер и т.д.)
- Отделяет публичные сервера от локальных сетей
- Предотвращает атаку на другие узлы сети



Возможна реализация на МЭ с помощью *security-level*

Возможна реализация на маршрутизаторе с использованием *zone based firewall* и более старой технологией *CBAC* (Context Based Access Control)

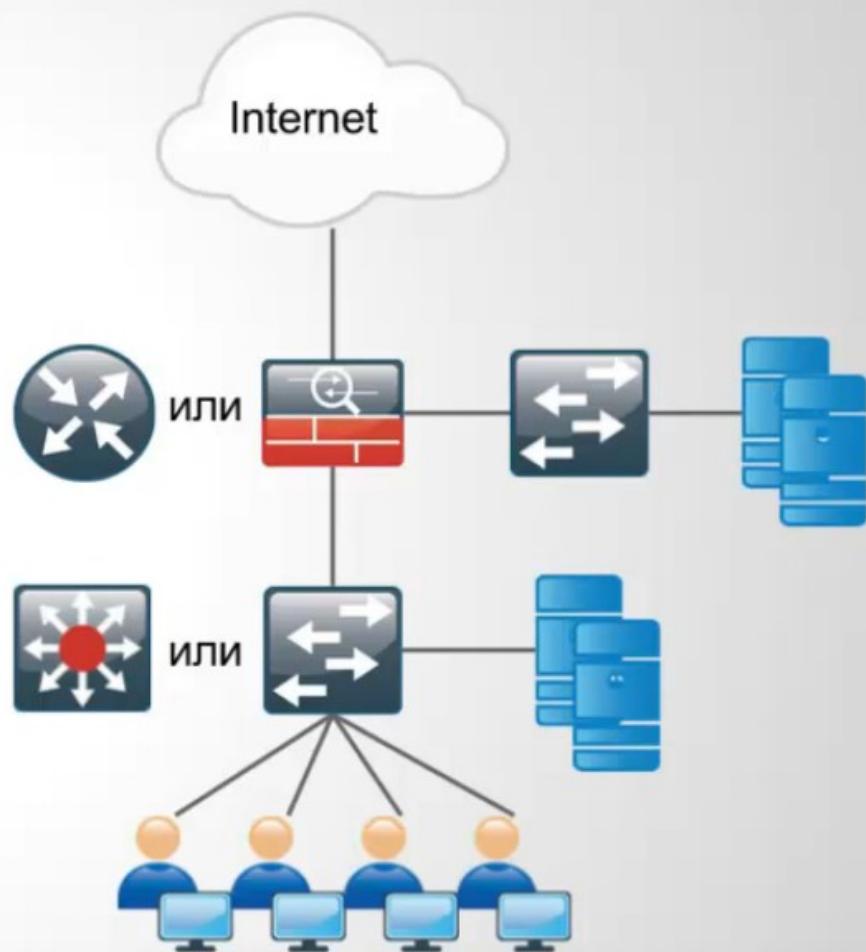
Как правило выделяют минимум три зоны:

- Внешний сегмент (*outside*)
- DMZ сегмент (*DMZ*)
- Внутренний сегмент (*inside*)

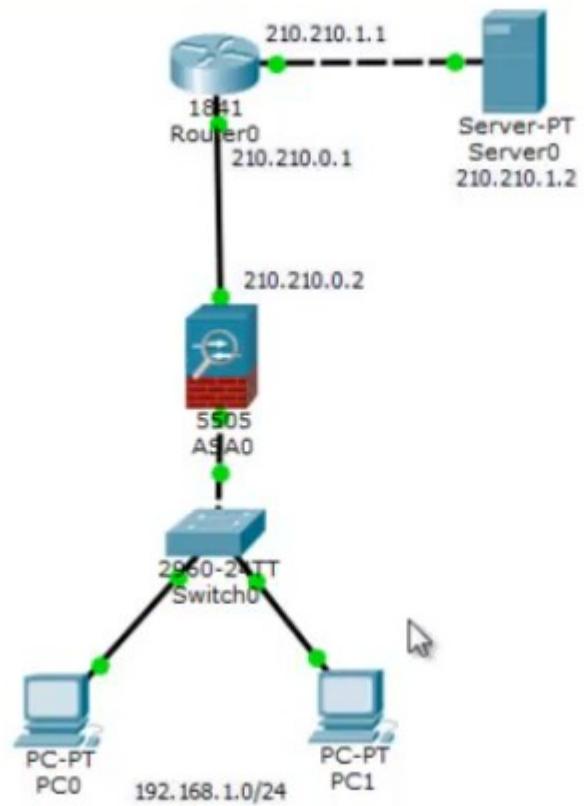
И три основные политики взаимодействия зон:

- inside* → *outside*
- inside* → DMZ
- outside* → DMZ

Более подробно о приведенных технологиях можно почитать [здесь](#), [здесь](#), [здесь](#) и [здесь](#)



Изначально используется схема Cisco ASA



На asa0 настроен пароль cisco

The screenshot shows a Windows application window titled "ASA0" with a tab bar containing "Physical", "Config", and "CLI". The "CLI" tab is selected, displaying the "ASA Command Line Interface". The terminal window contains the following text:

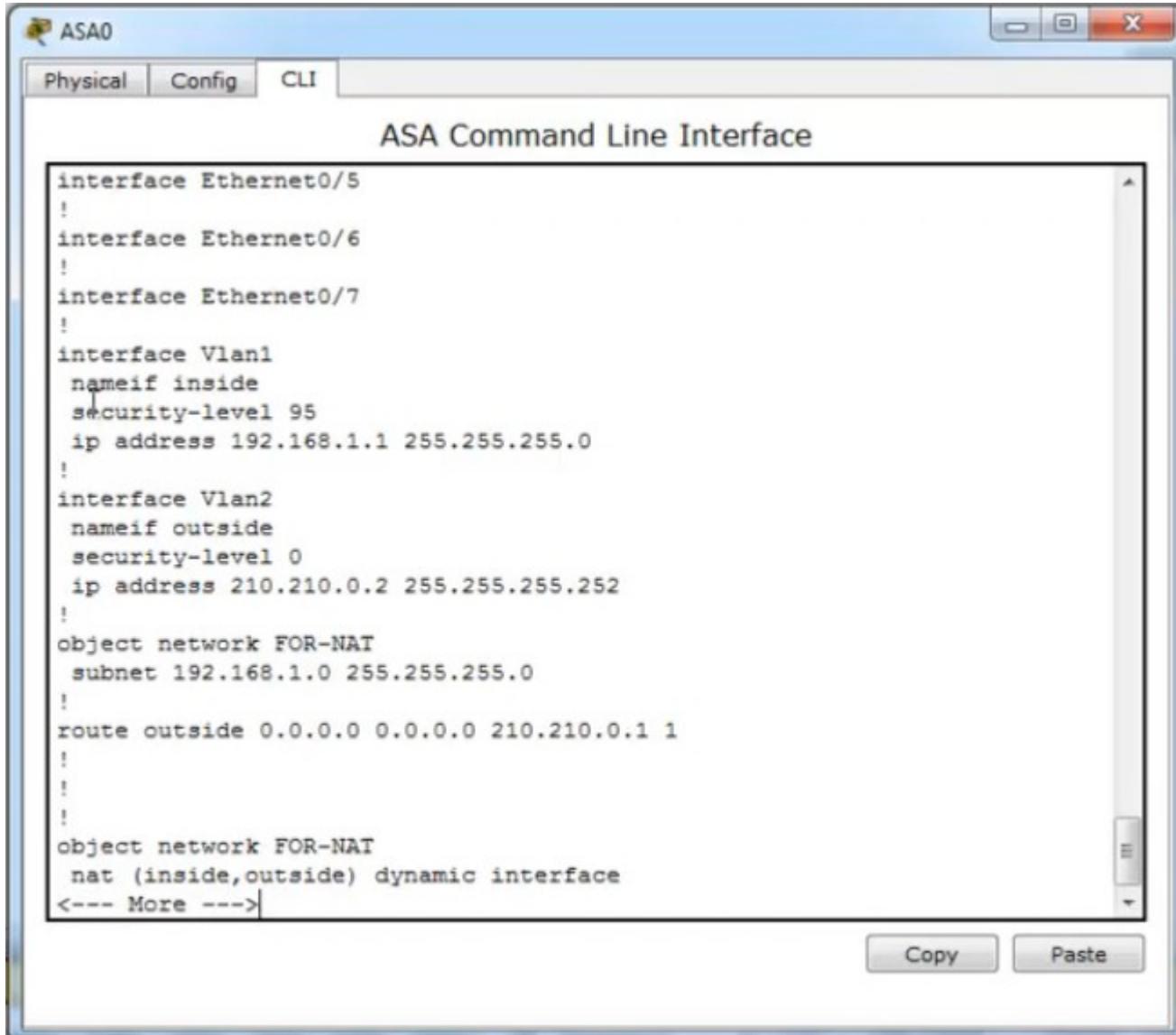
```
!
telnet timeout 5
ssh 192.168.1.0 255.255.255.0 inside
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.35 inside
dhcpd enable inside
!
!
!
!
!
ciscoasa#
ciscoasa#
ciscoasa#exit

Logoff
Type help or '?' for a list of available commands.

ciscoasa>en
Password:
ciscoasa#
ciscoasa#
ciscoasa#show run
```

At the bottom of the terminal window, there are "Copy" and "Paste" buttons.

На asa0 настроен NAT

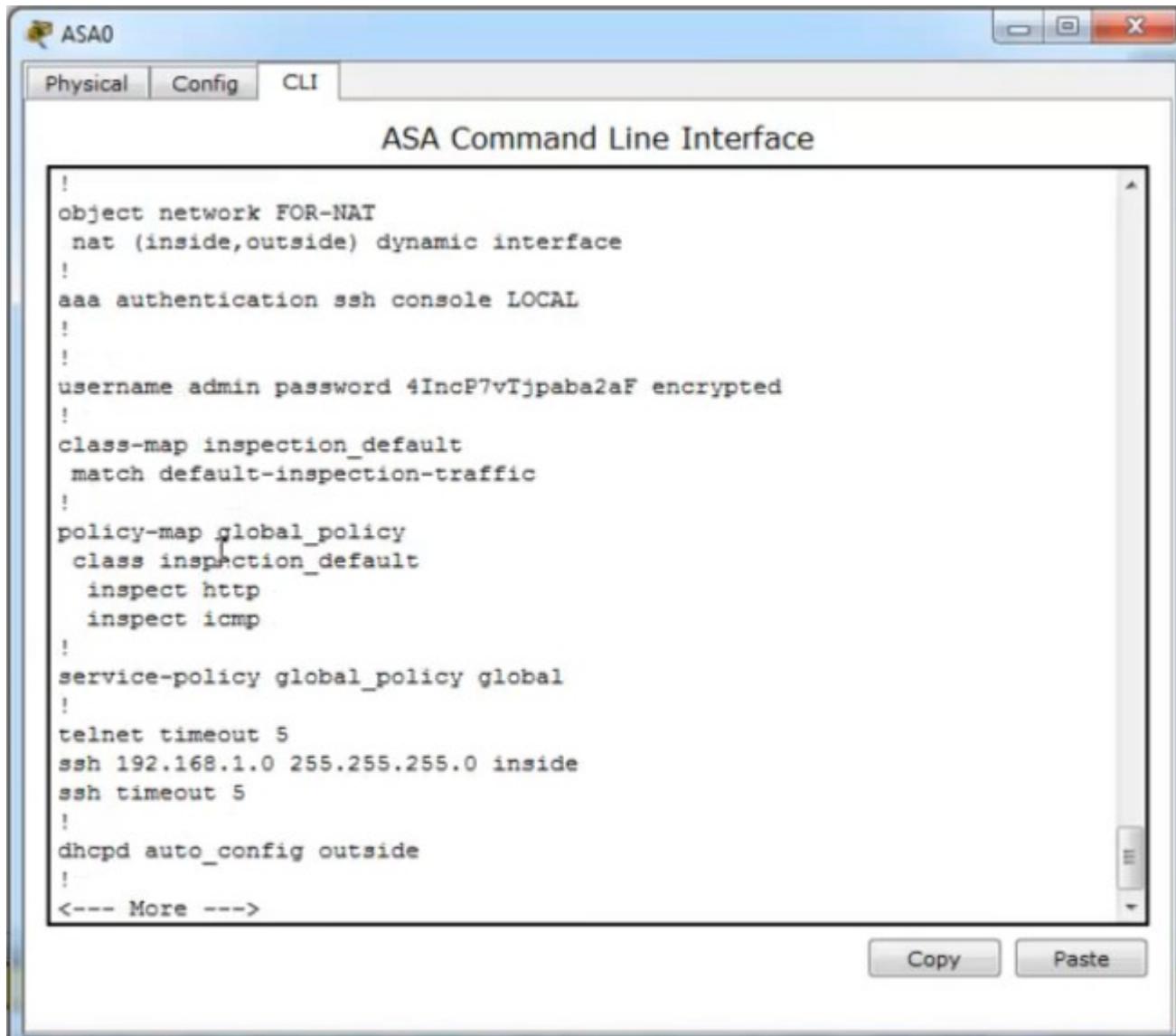


The screenshot shows the ASA Command Line Interface window titled "ASA0". The window has tabs for "Physical", "Config", and "CLI", with "Config" selected. The main area displays the following configuration script:

```
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
    nameif inside
    security-level 95
    ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
    nameif outside
    security-level 0
    ip address 210.210.0.2 255.255.255.252
!
object network FOR-NAT
    subnet 192.168.1.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 210.210.0.1 1
!
!
!
object network FOR-NAT
    nat (inside,outside) dynamic interface
<--- More --->
```

At the bottom of the configuration window are "Copy" and "Paste" buttons.

На аса0 настроено инспектирование трафика

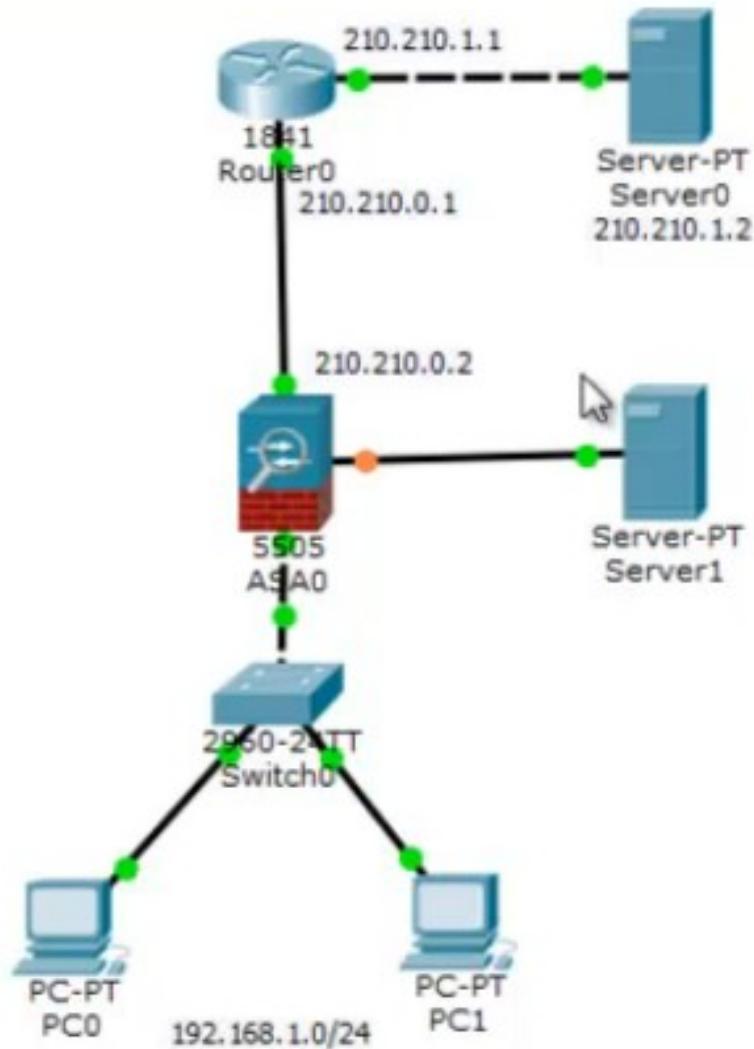


The screenshot shows the ASA Command Line Interface window titled "ASA0". The "Config" tab is selected. The main pane displays the following configuration script:

```
!
object network FOR-NAT
    nat (inside,outside) dynamic interface
!
aaa authentication ssh console LOCAL
!
!
username admin password 4Incp7vTjpaba2af encrypted
!
class-map inspection_default
    match default-inspection-traffic
!
policy-map global_policy
    class inspection_default
        inspect http
        inspect icmp
!
service-policy global_policy global
!
telnet timeout 5
ssh 192.168.1.0 255.255.255.0 inside
ssh timeout 5
!
dhcpd auto_config outside
!
<--- More --->
```

At the bottom right of the configuration pane are "Copy" and "Paste" buttons.

Добавим Server1, который мы будем выделять в DMZ



Зададим серверу Server1 статический ip адрес

