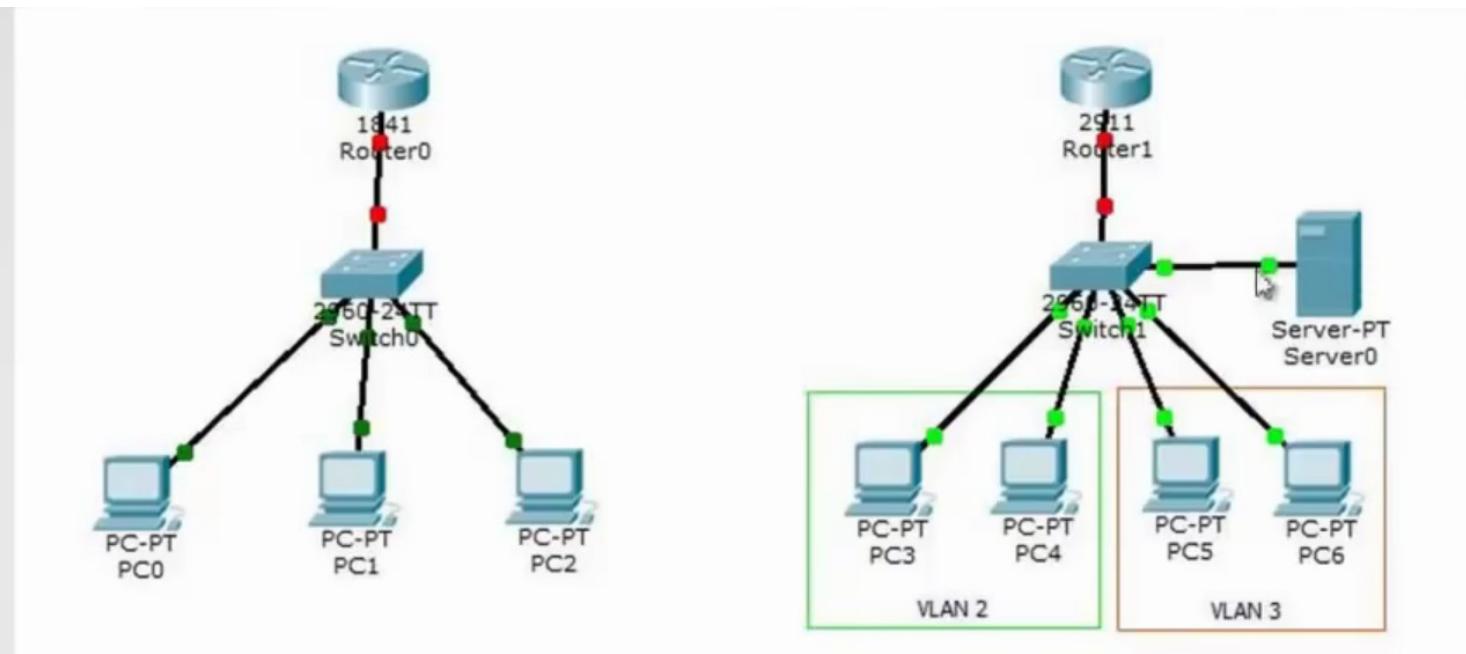


DHCP



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

```

```

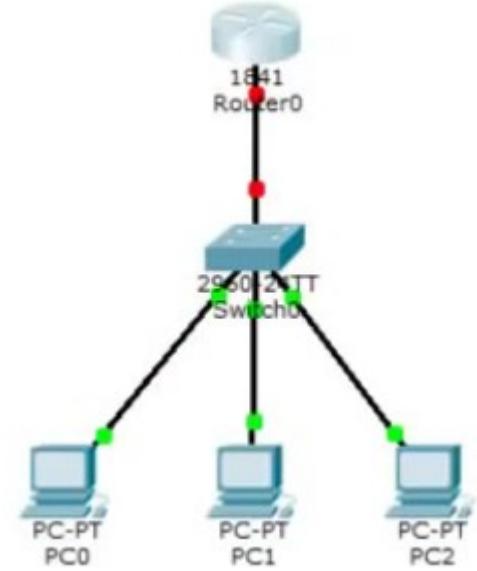
exit
interface GigabitEthernet0/1.4
encapsulation dot1Q 4
ip address 192.168.4.1 255.255.255.0

```

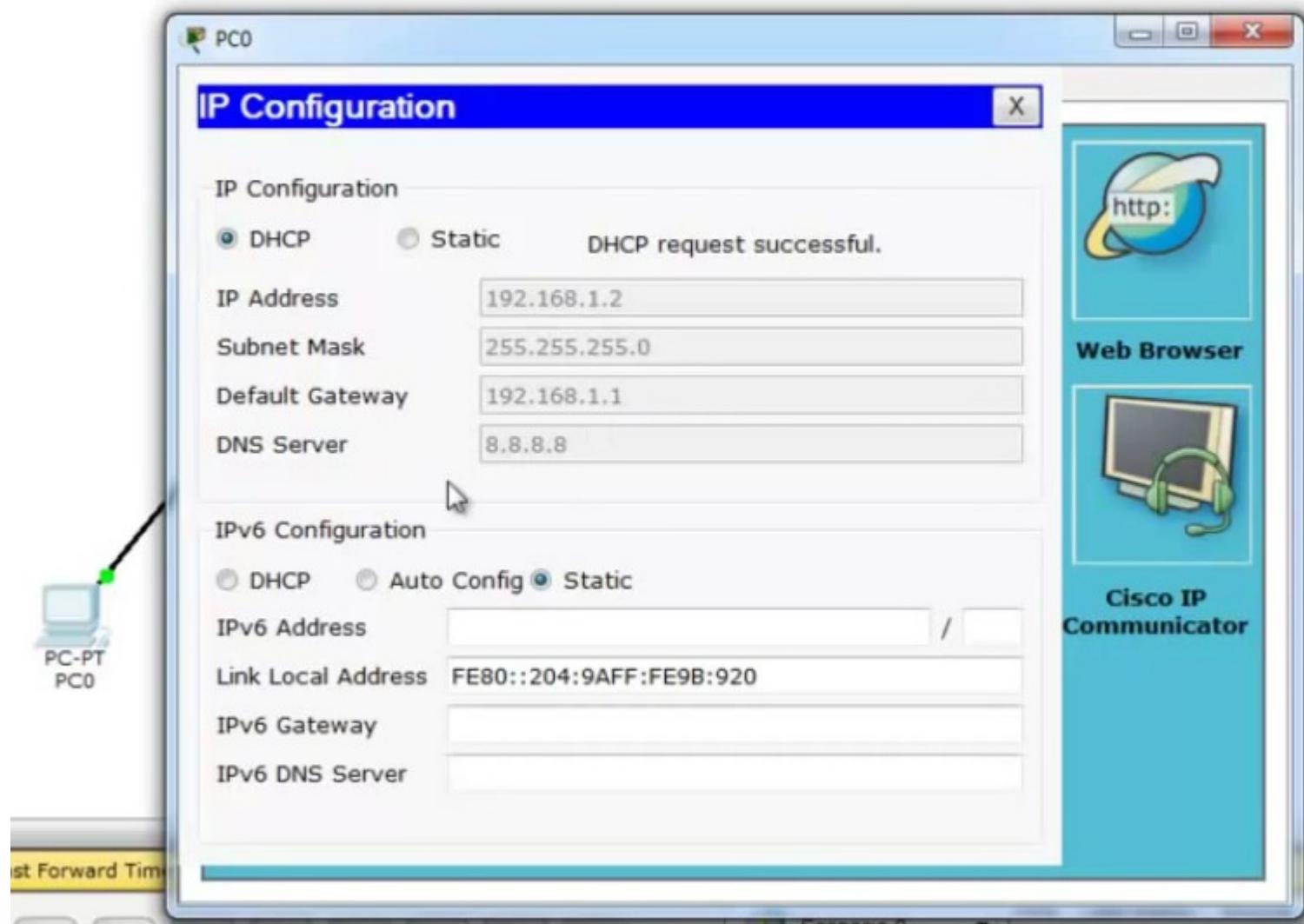
Настраиваем DHCP-сервер на Router0

Router0

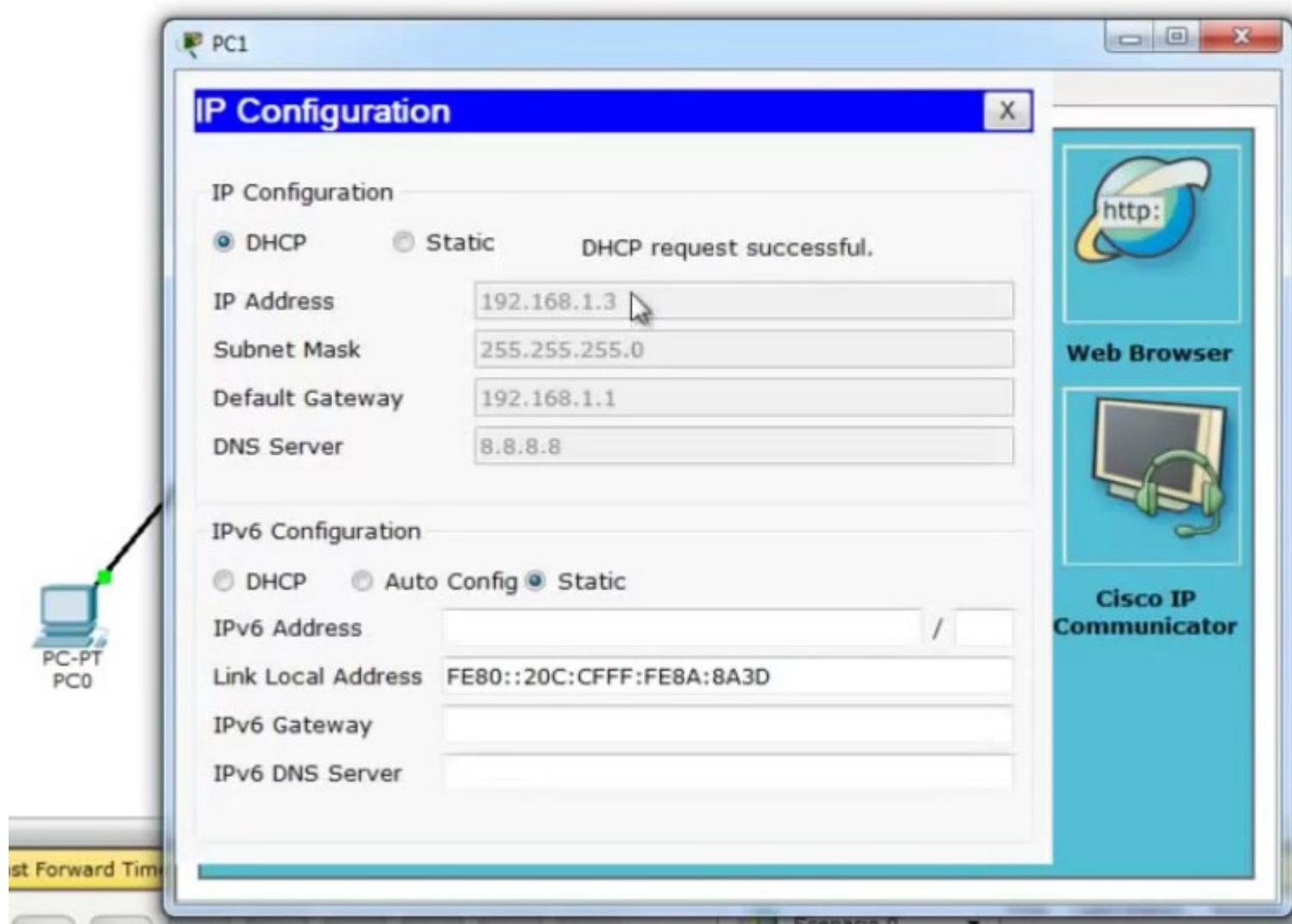
```
> no
> en
# conf t
(config)# int fa0/0
(config-if)# no shutdown
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# exit
(config)# ip dhcp pool DHCP
(dhcp-config)# network 192.168.1.0 255.255.255.0
(dhcp-config)# default-router 192.168.1.1
(dhcp-config)# dns-server 8.8.8.8
(dhcp-config)#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



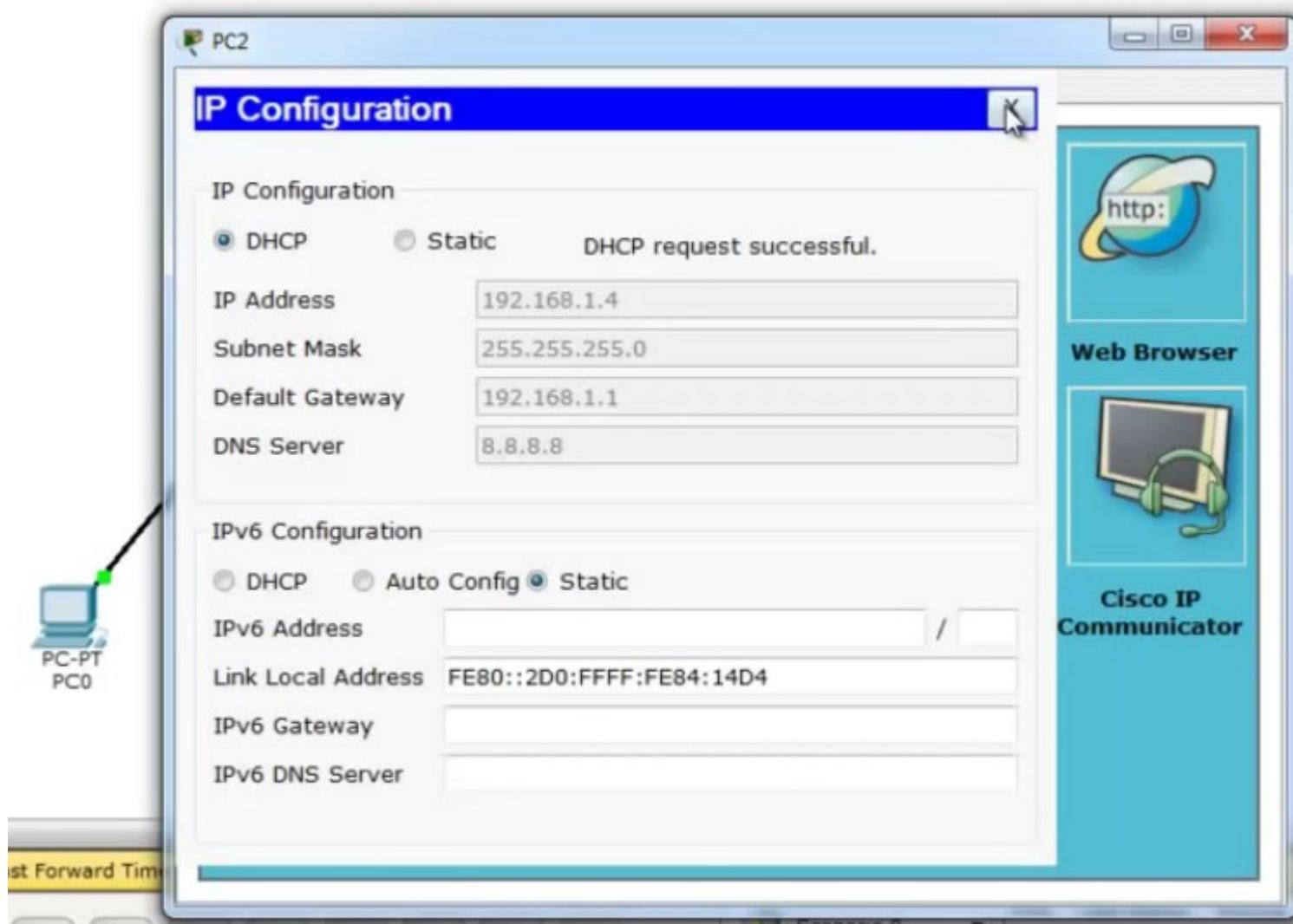
Включаем динамическое получение IP - DHCP на клиенте - PC0



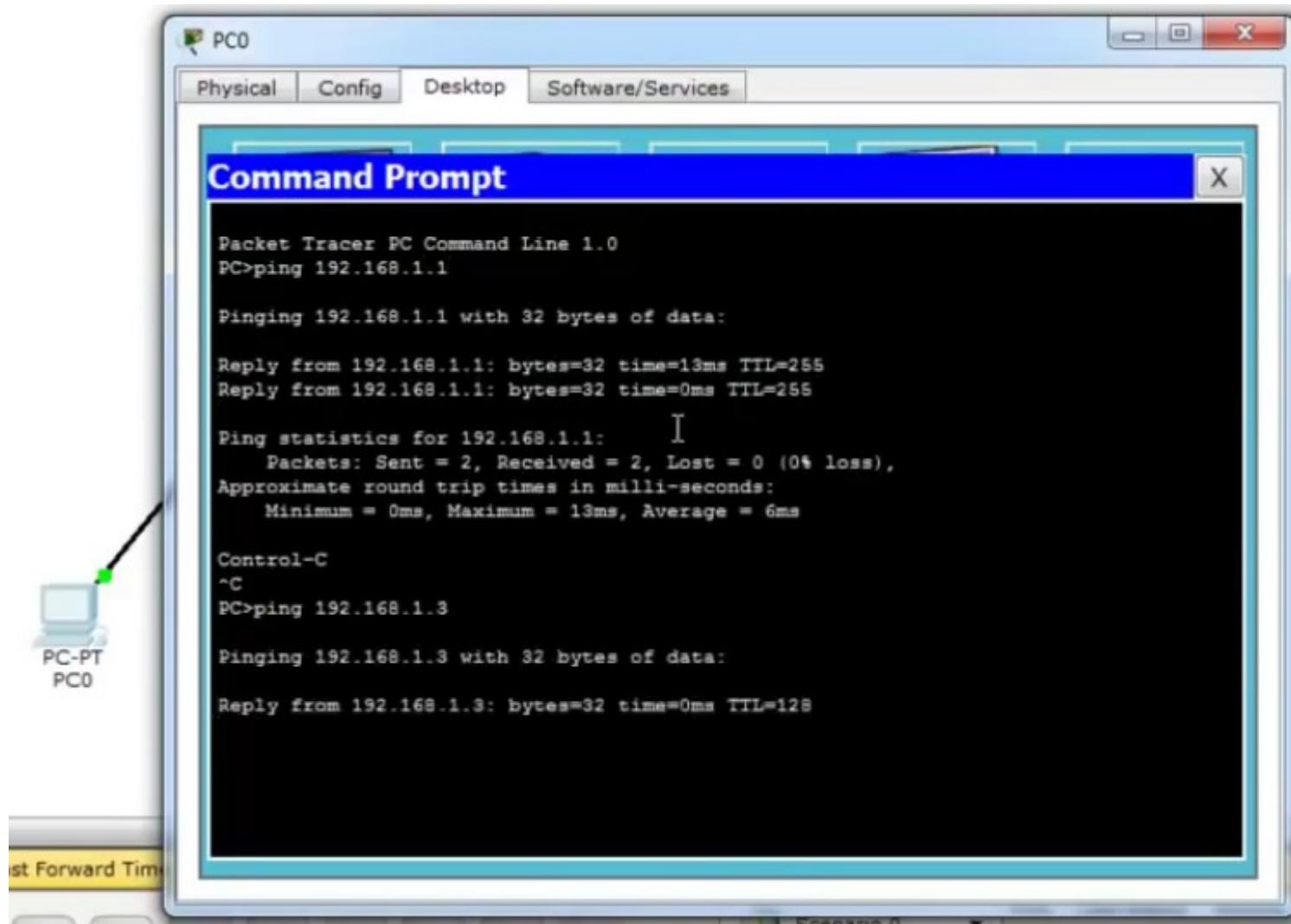
Аналогично поступаем на PC1



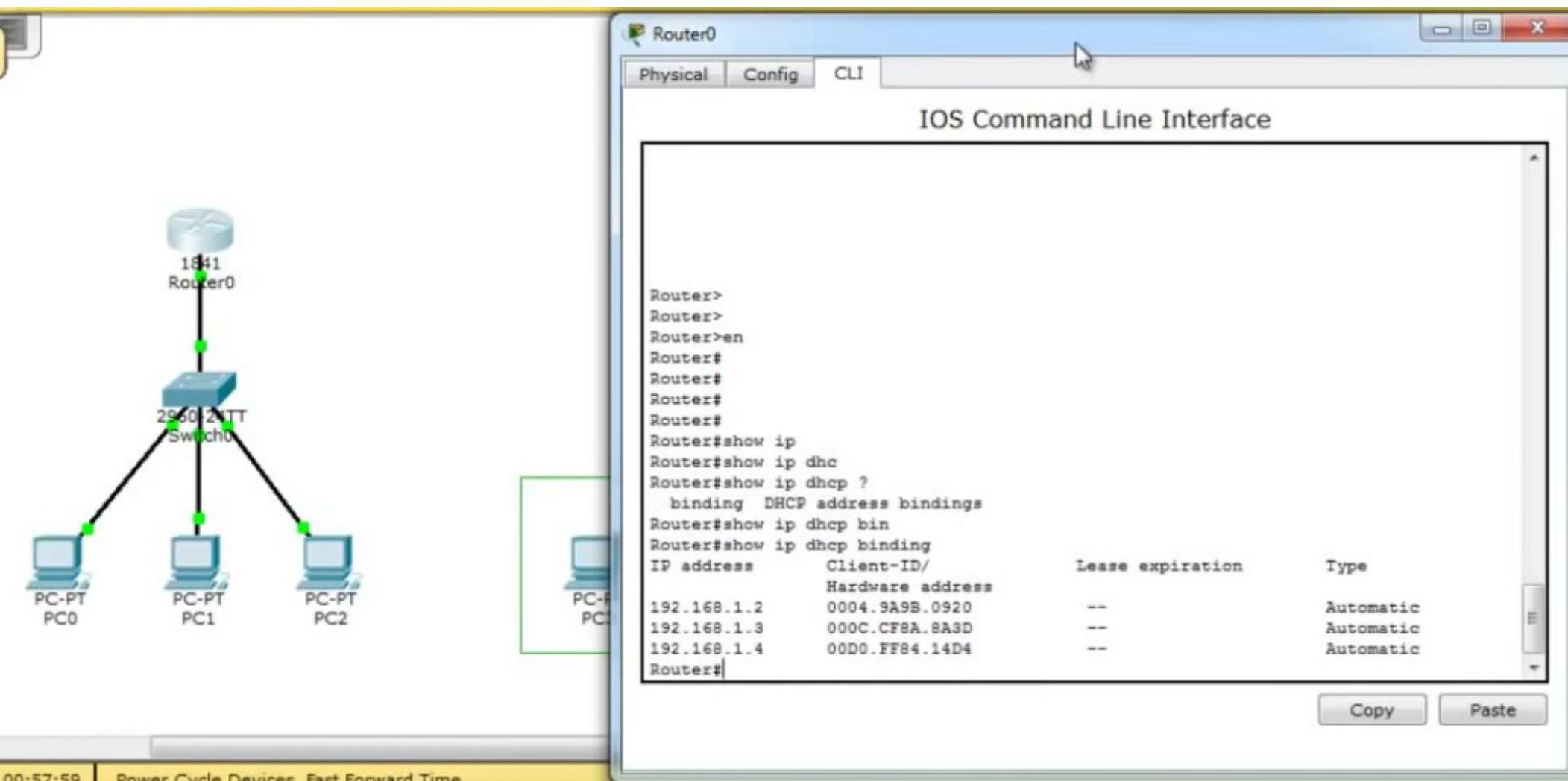
... и на PC2



Проверяем взаимодействие. Готово.



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



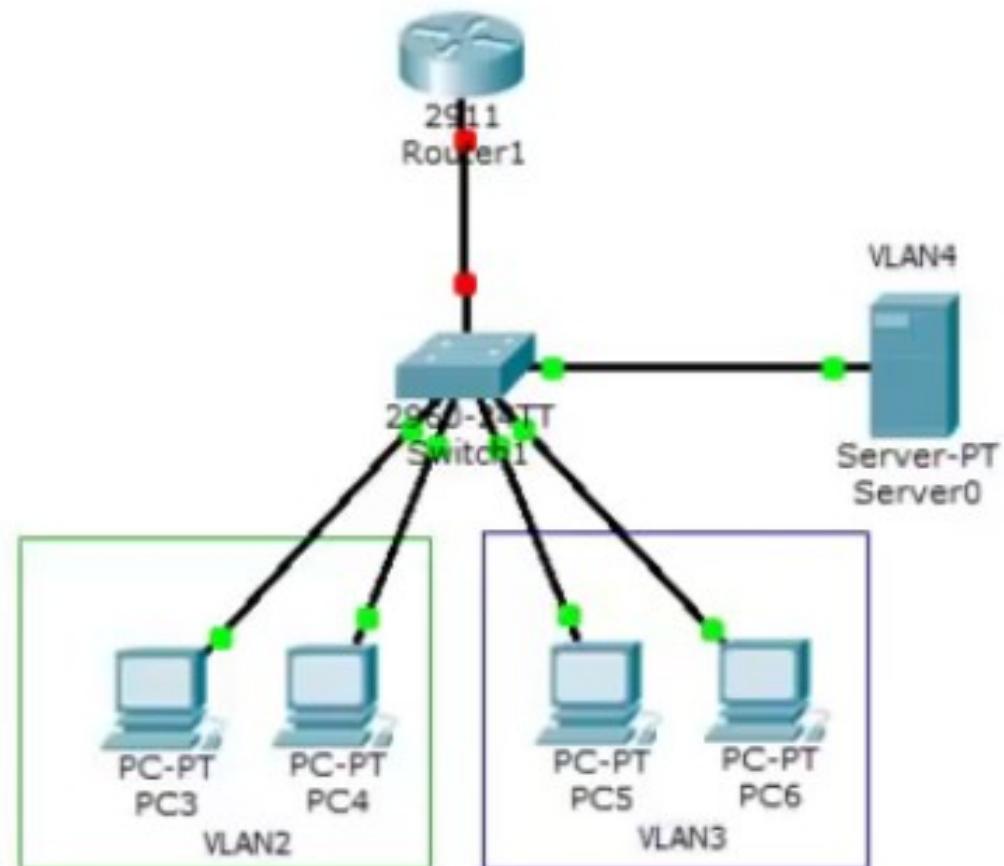
Второй пример.
Уже есть 2 VLAN'a.
(На самом деле Server-PT находится в 3-ем VLAN'e). Настраиваем
коммутатор Switch1

```
> 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

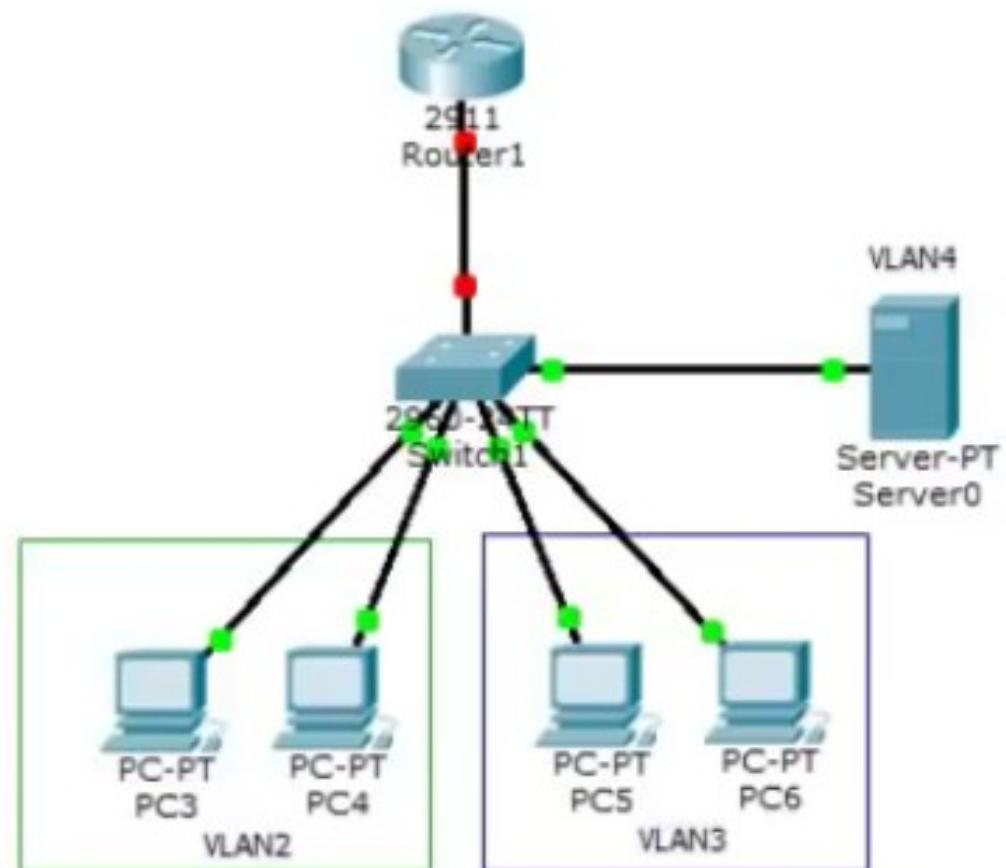
(config)# int range fastEthernet 0/6
(config-if)# switchport mode access
(config-if)# switchport access vlan 4
(config-if)# exit
```



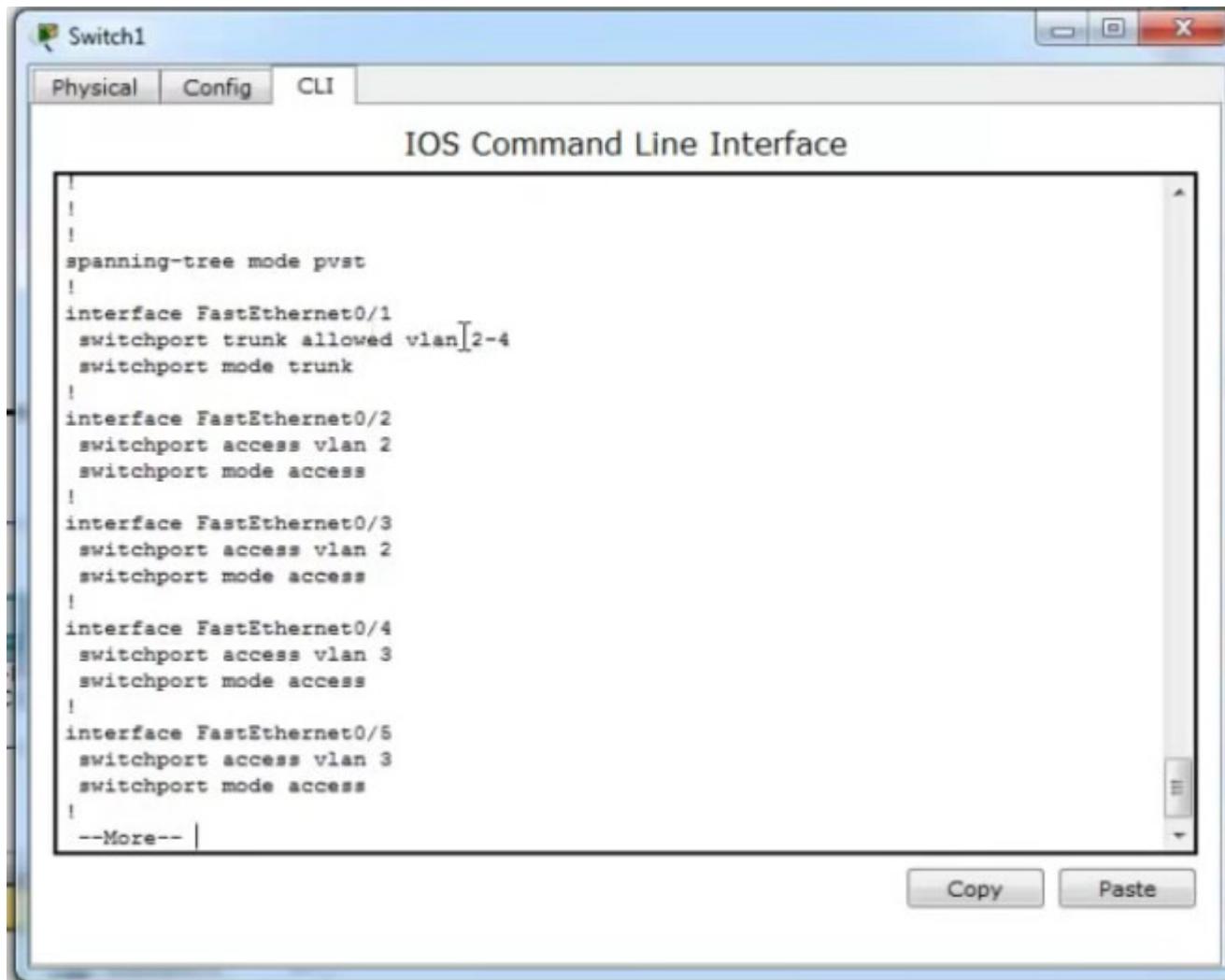
Настраиваем коммутатор Switch1

```
(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

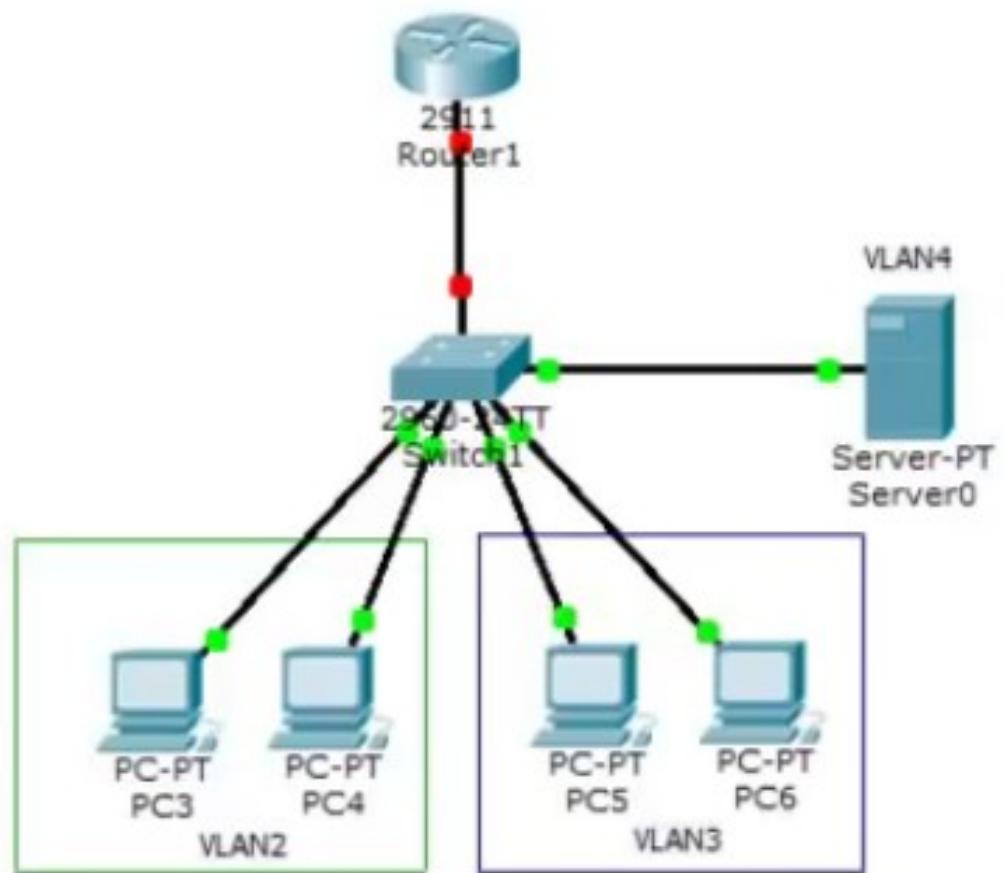
```
> en
# config t
(config)# int gi0/0.2
(config-subif)# encapsulation dot1Q 2
(config-subif)# ip address 192.168.2.1 255.255.255.0
(config-subif)# no shutdown
(config)# exit

(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

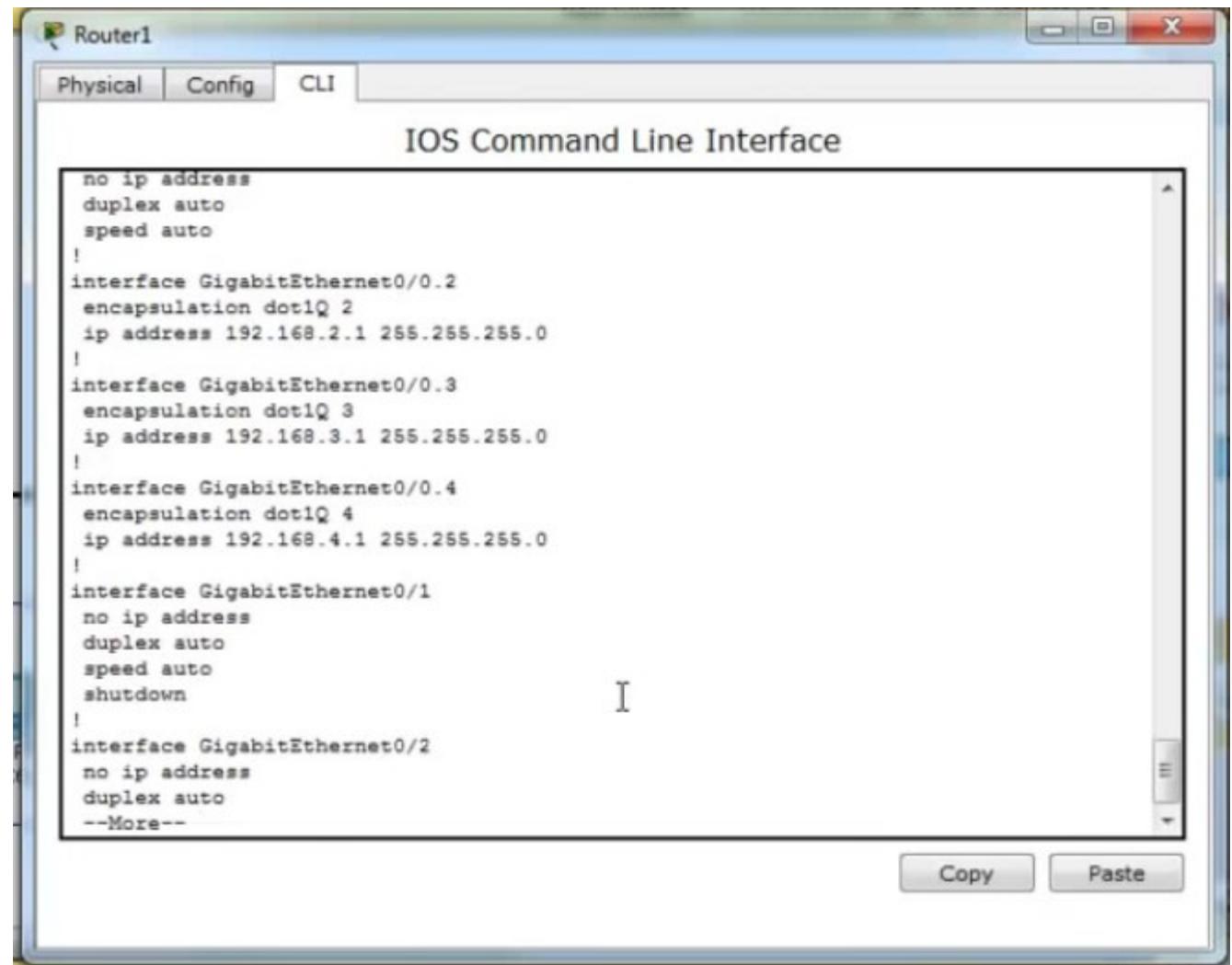
(config)# int gi0/0.4
(config-subif)# encapsulation dot1Q 4
(config-subif)# ip address 192.168.4.1 255.255.255.0
(config-subif)# no shutdown
(config)# end

# wr mem
```



Проверяем настройки маршрутизатора Router1

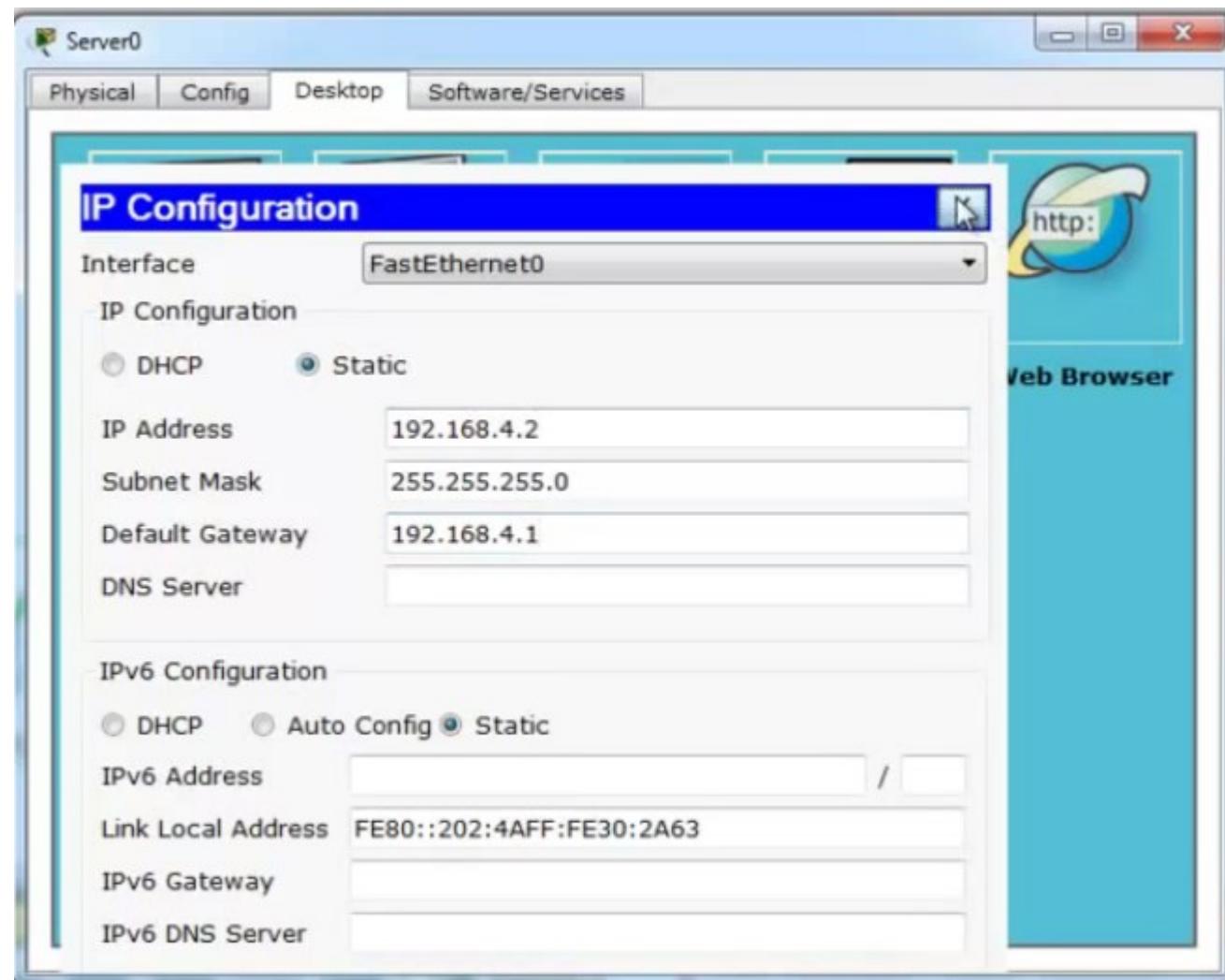
show run



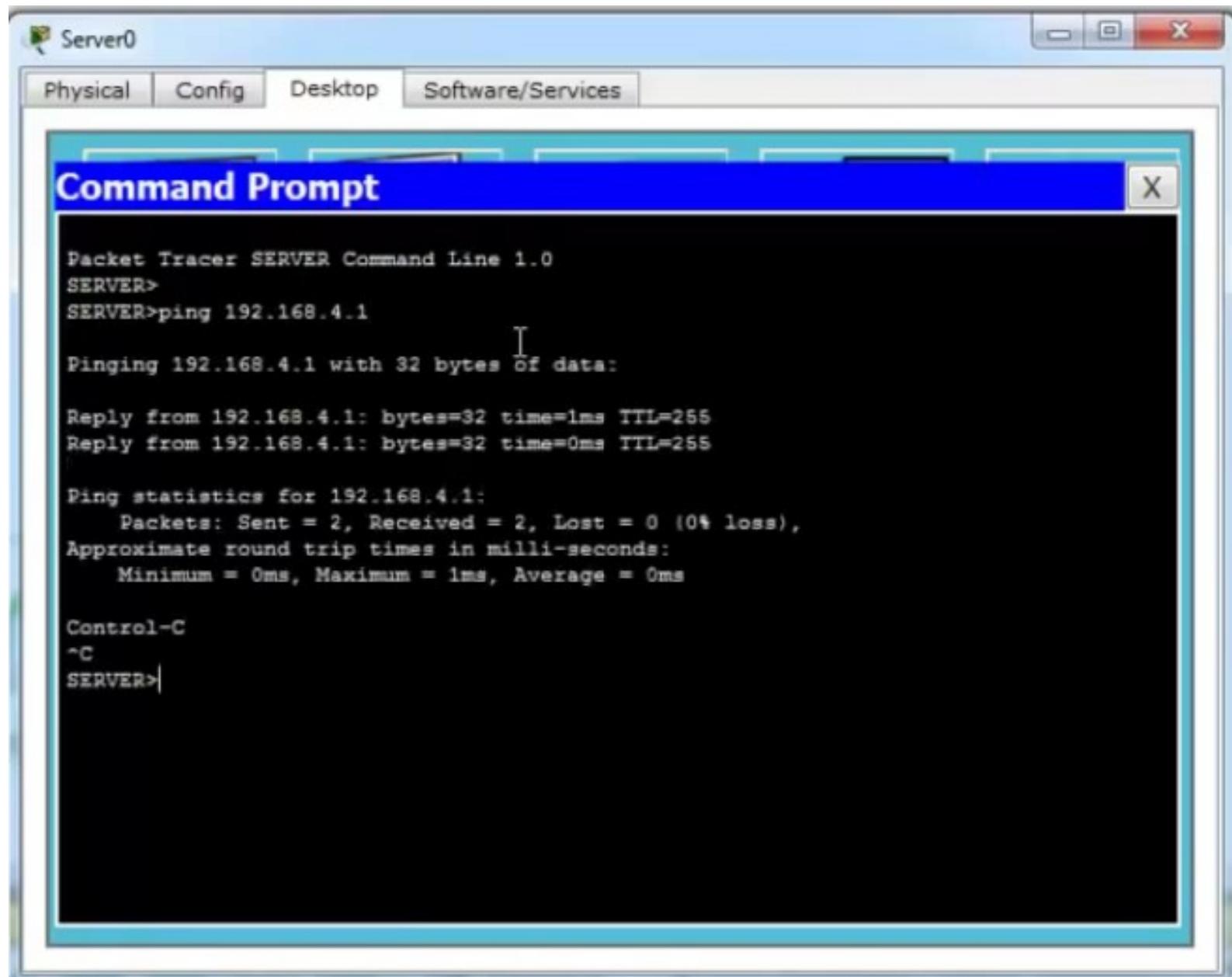
```
Router1
Physical Config CLI
IOS Command Line Interface
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/0.2
encapsulation dot1Q 2
ip address 192.168.2.1 255.255.255.0
!
interface GigabitEthernet0/0.3
encapsulation dot1Q 3
ip address 192.168.3.1 255.255.255.0
!
interface GigabitEthernet0/0.4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

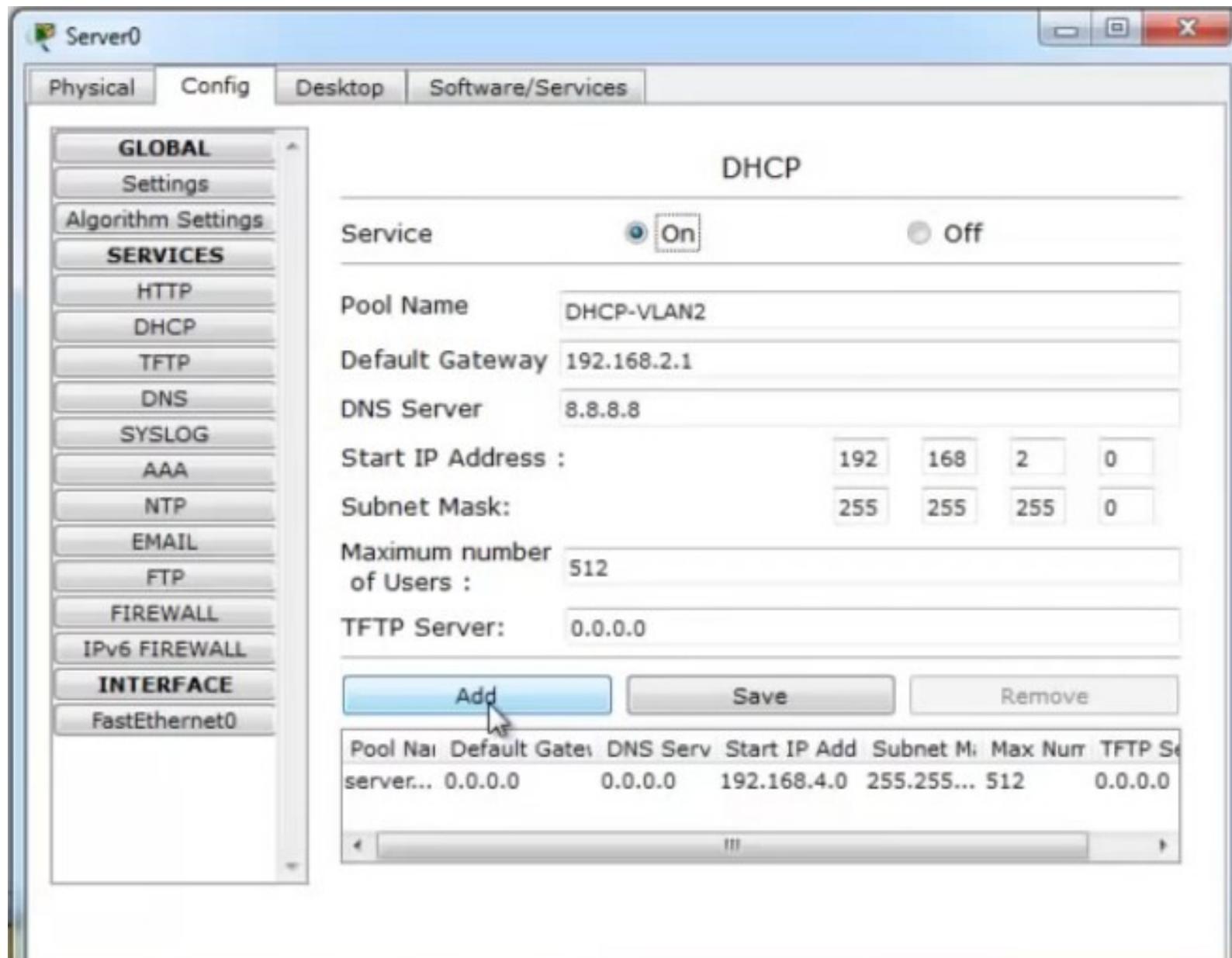
Зададим статический IP для сервера Server0



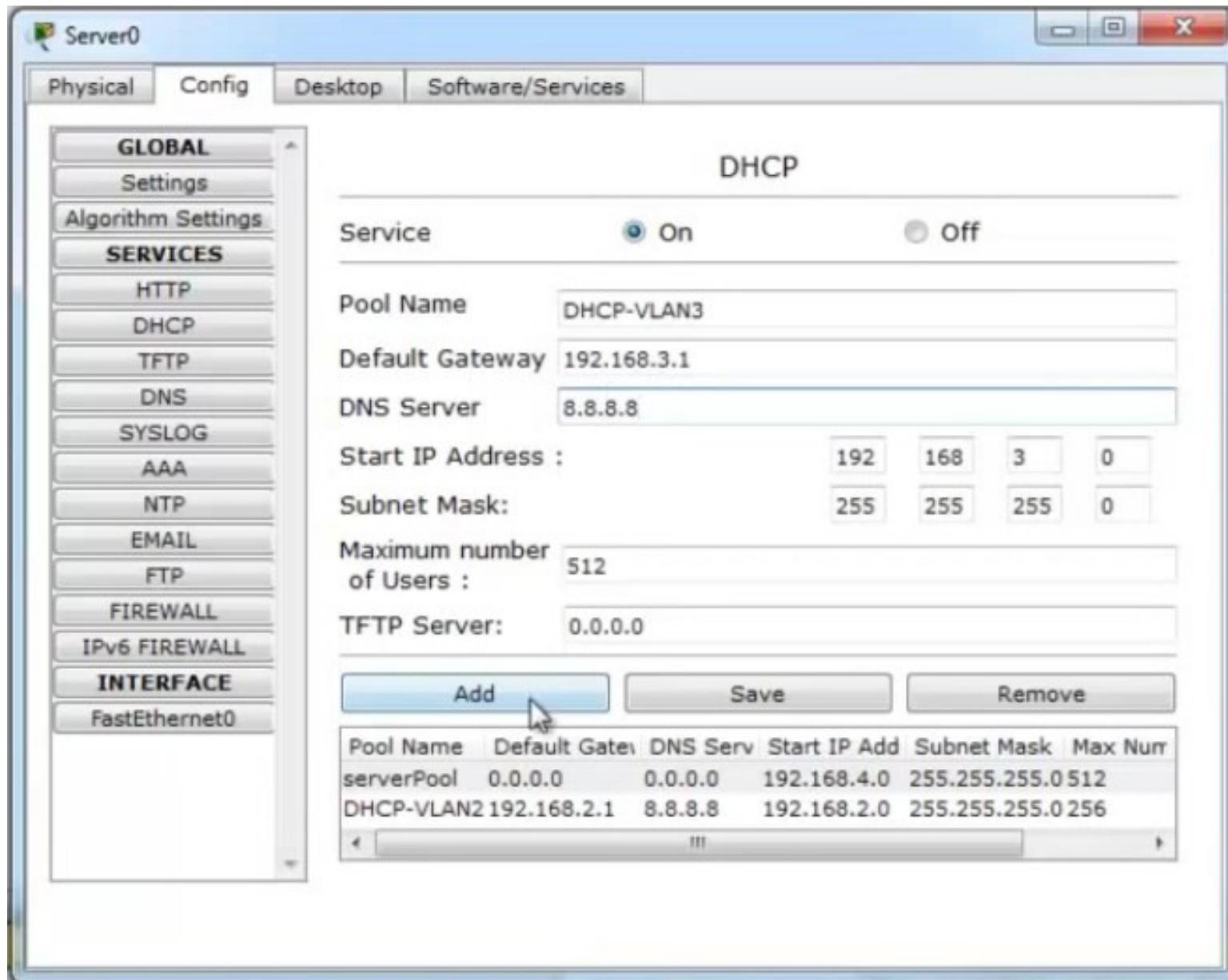
Проверим взаимодействие сервера Server0 и маршрутизатора Router1



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



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

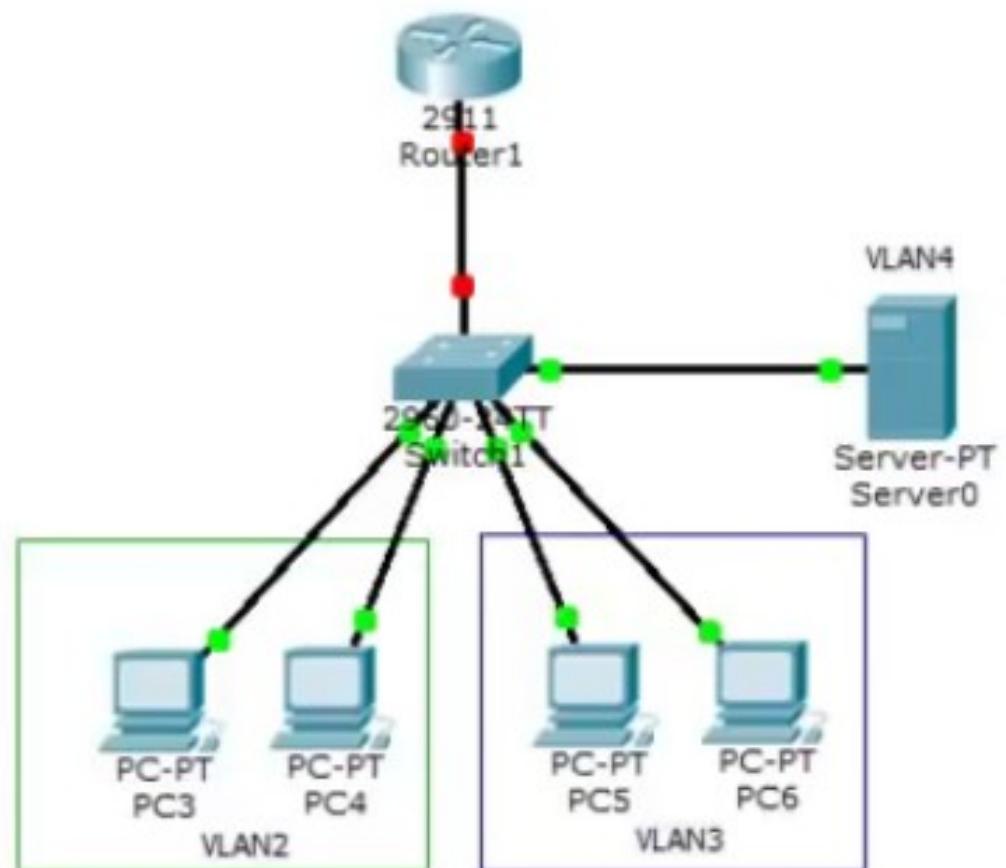


Настраиваем переадресацию DHCP запросов с компьютеров на сервер - на маршрутизаторе Router1

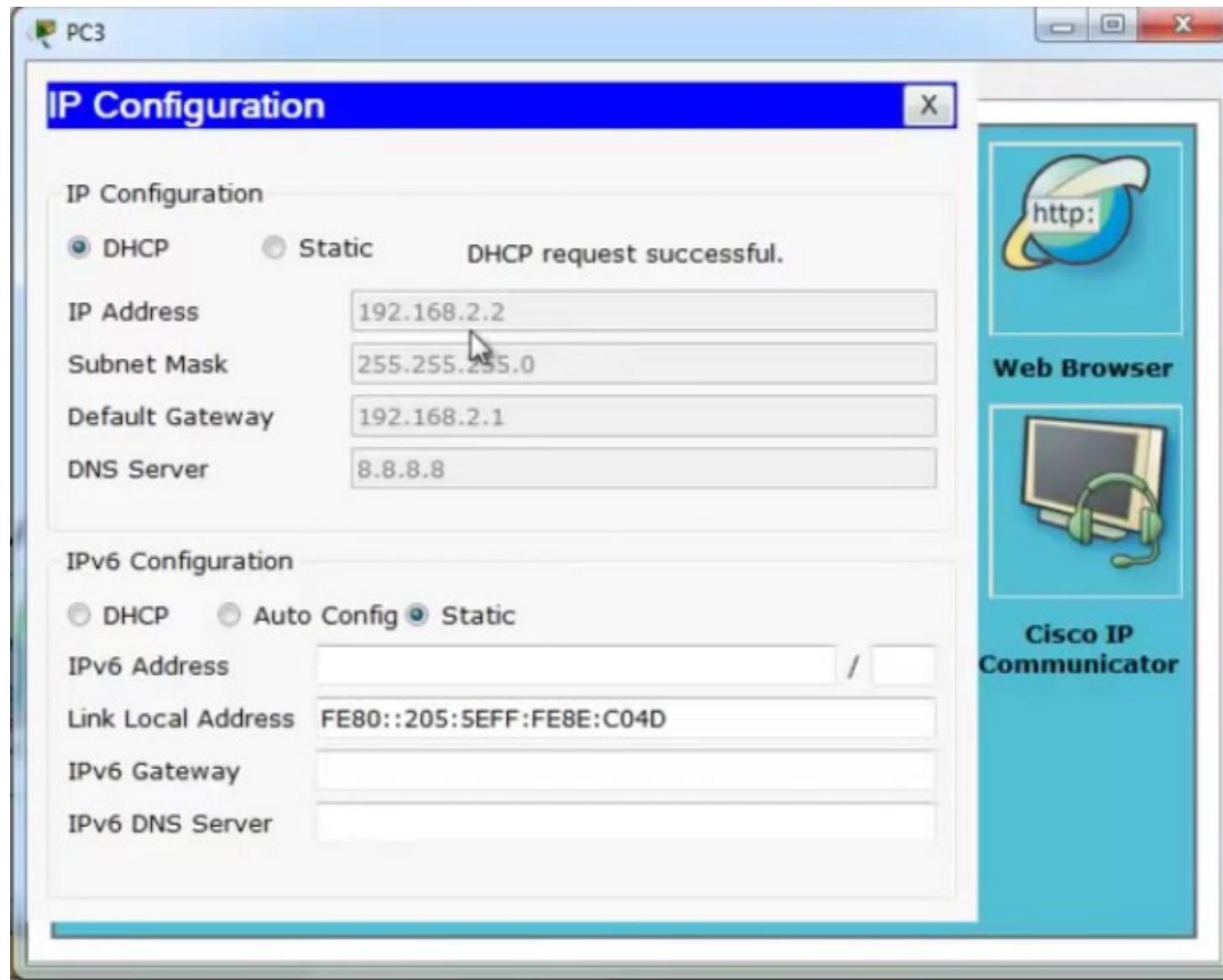
```
#conf t
(config)# int gi 0/0.2
(config-subif)# ip helper-address 192.168.4.2
(config)# exit
```

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

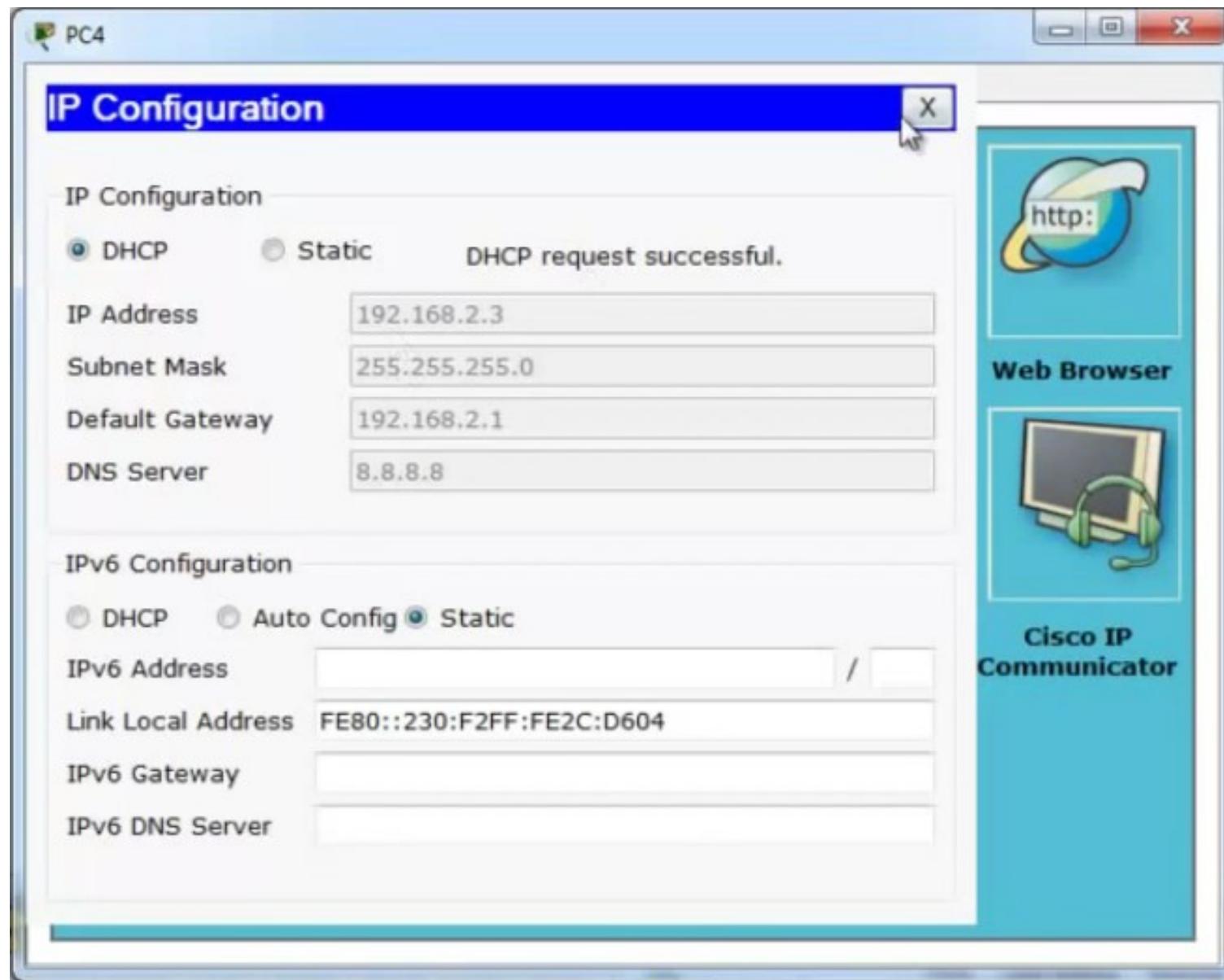
```
#wr mem
```



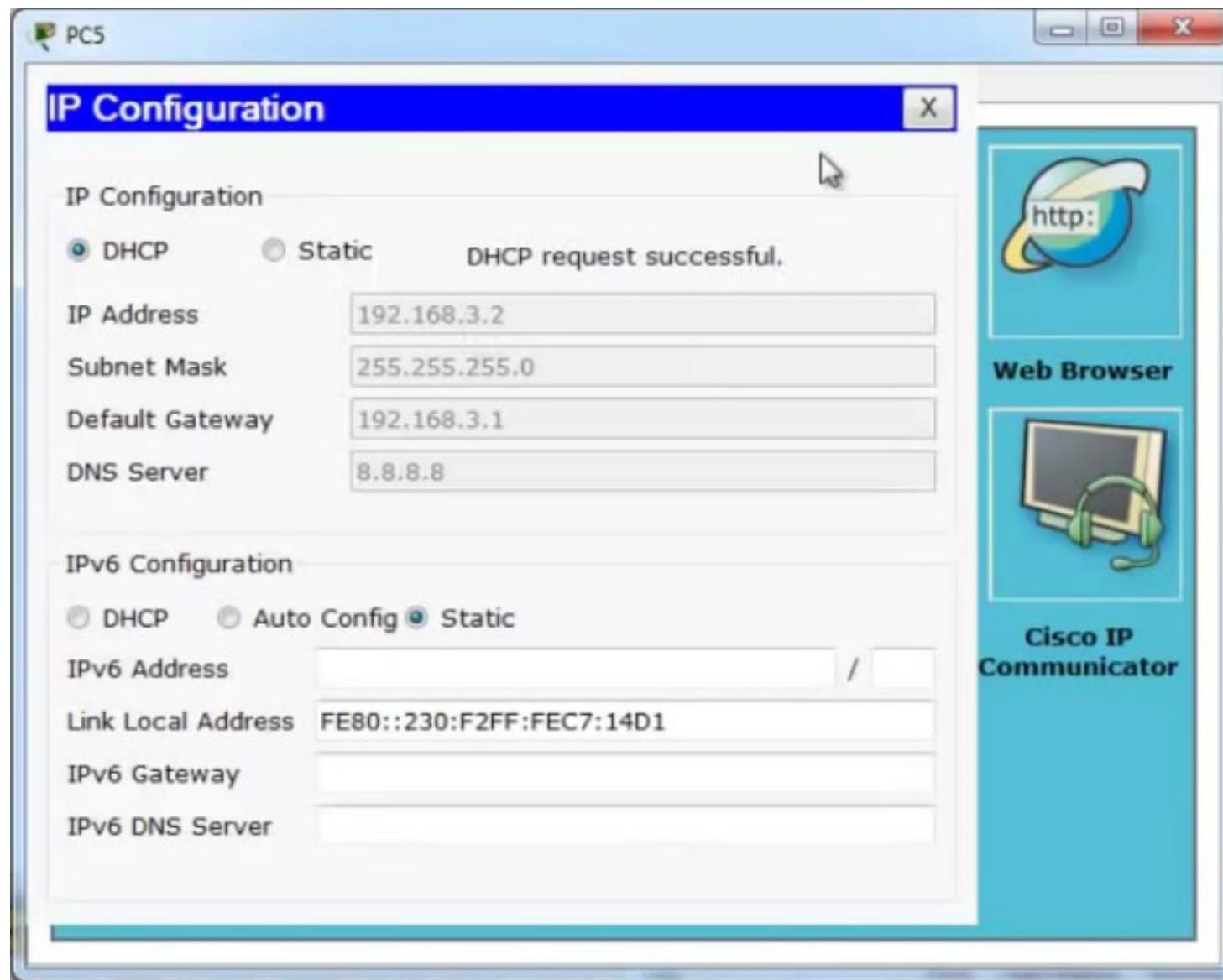
Пробуем получить IP адрес на компьютерах по DHCP



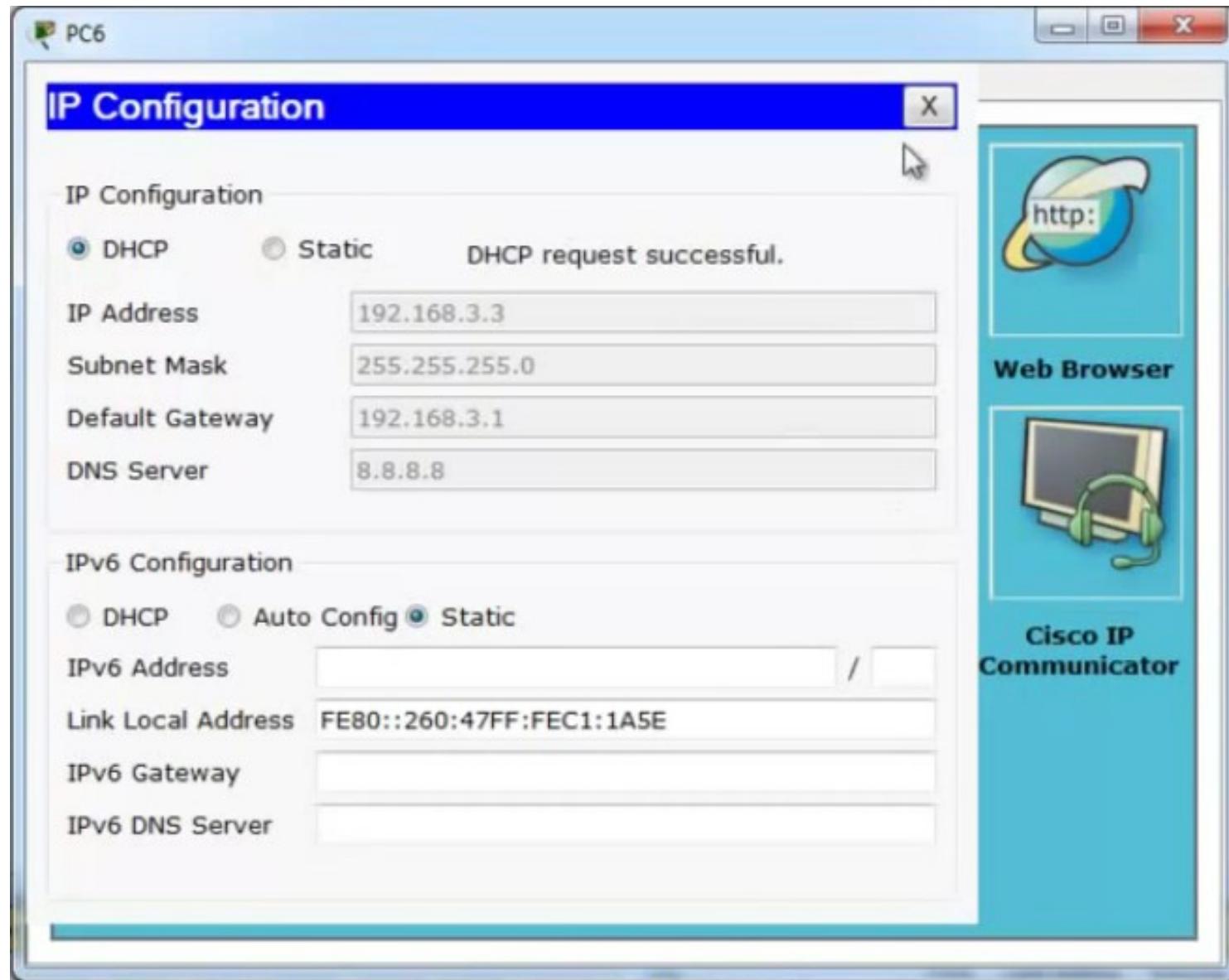
Пробуем получить IP адрес на компьютерах по DHCP



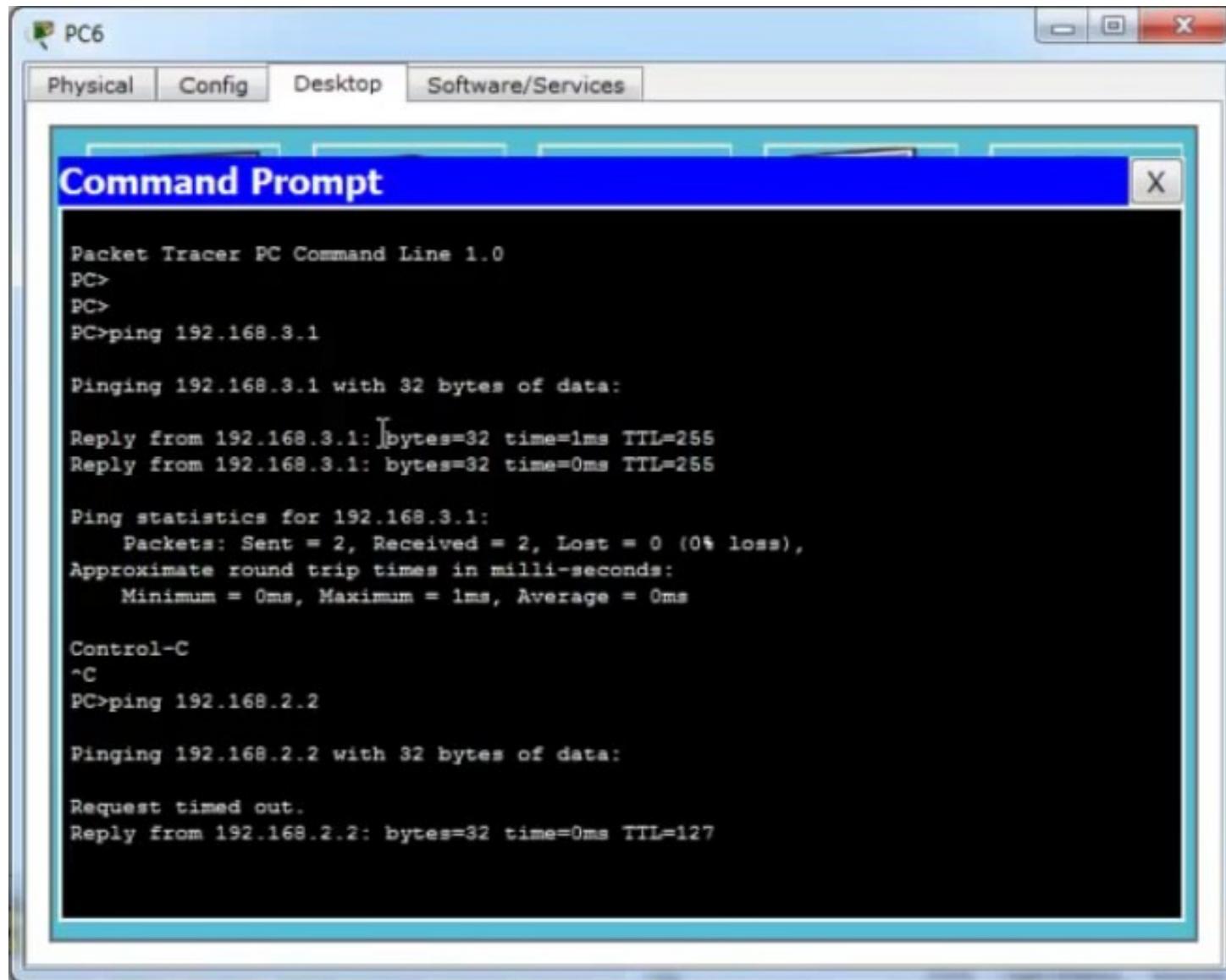
Пробуем получить IP адрес на компьютерах по DHCP



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)

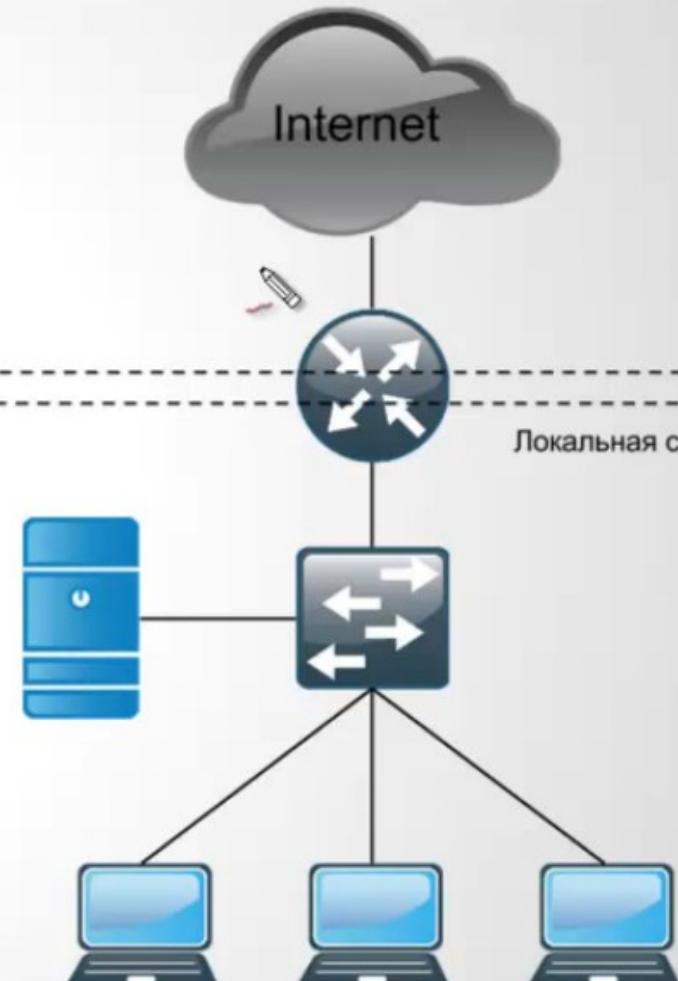
Более подробно читайте [здесь](#)

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

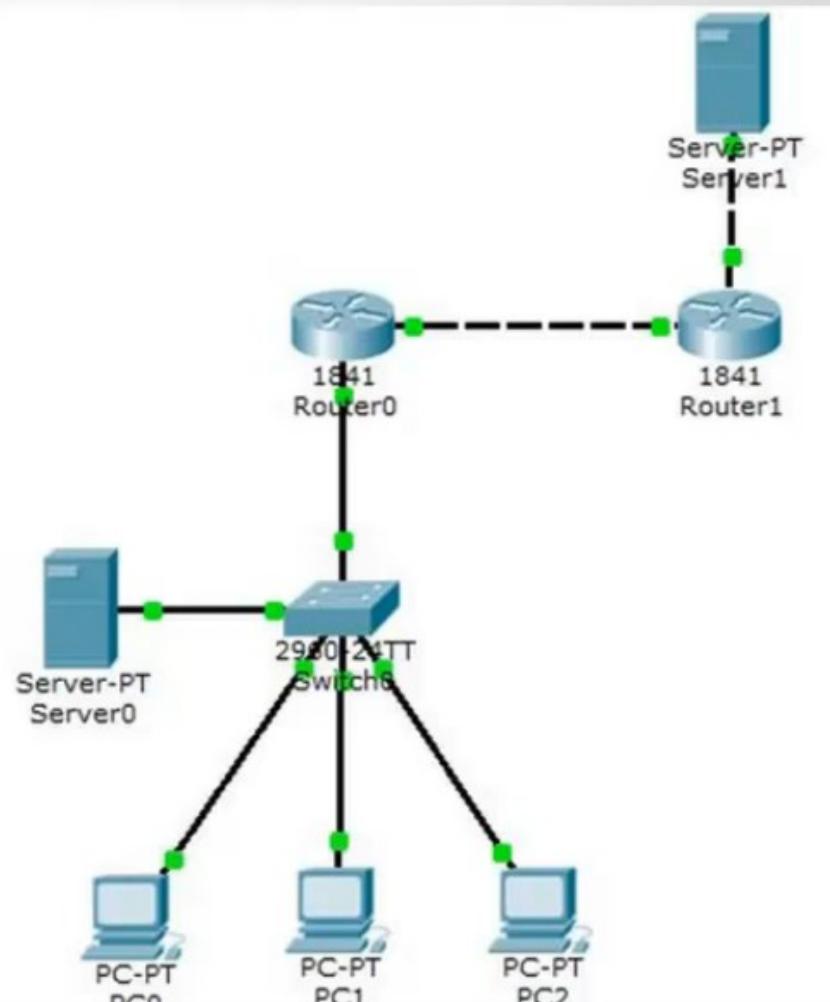
ip access-list standard FOR-NAT
permit 192.168.2.0 0.0.0.255
permit 192.168.3.0 0.0.0.255

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

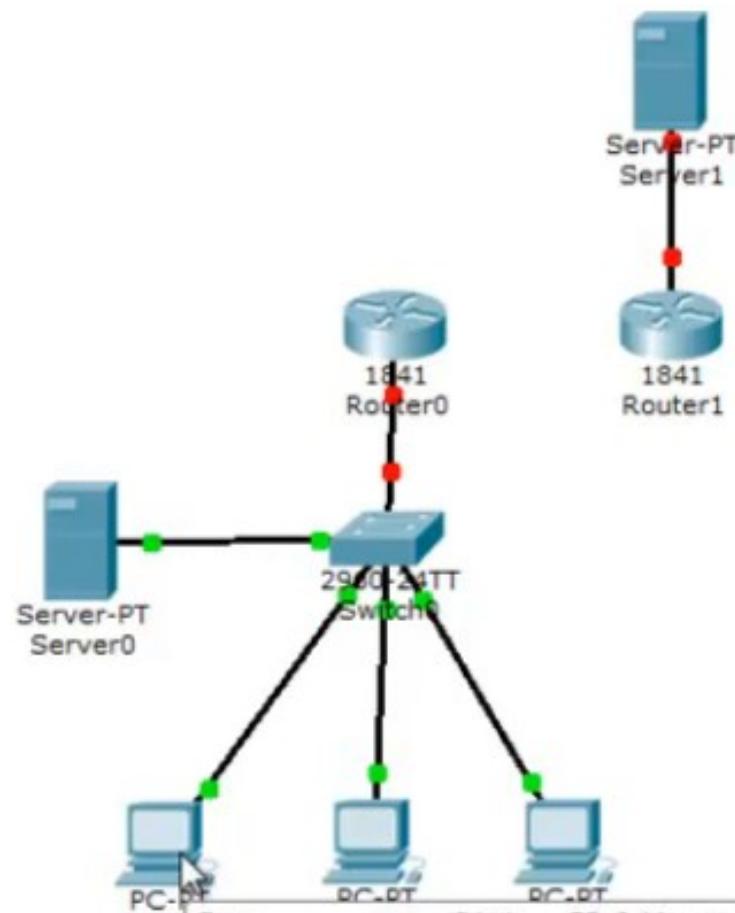
Настройка Static NAT

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

```
show ip nat translations
```



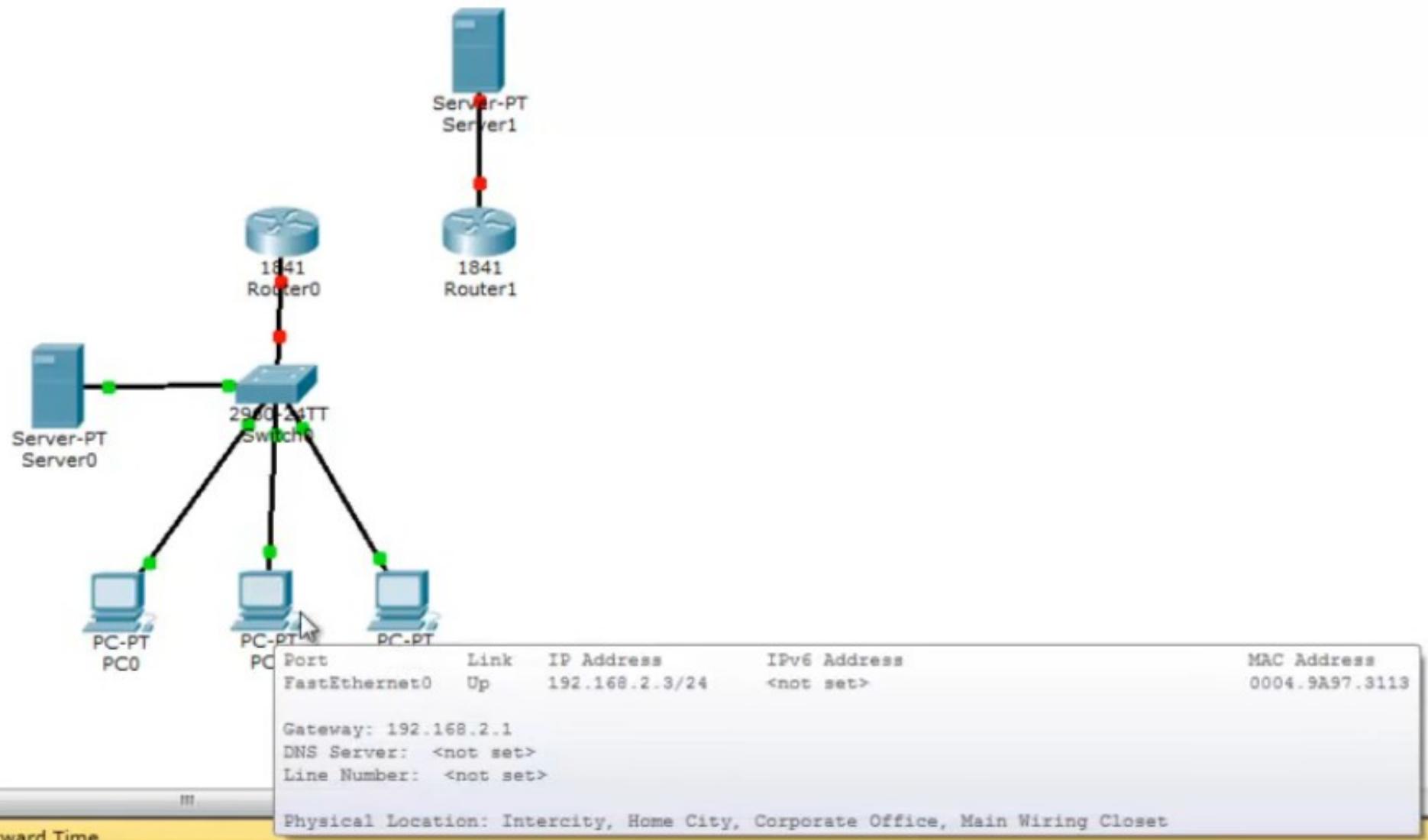
Ip адрес PC0



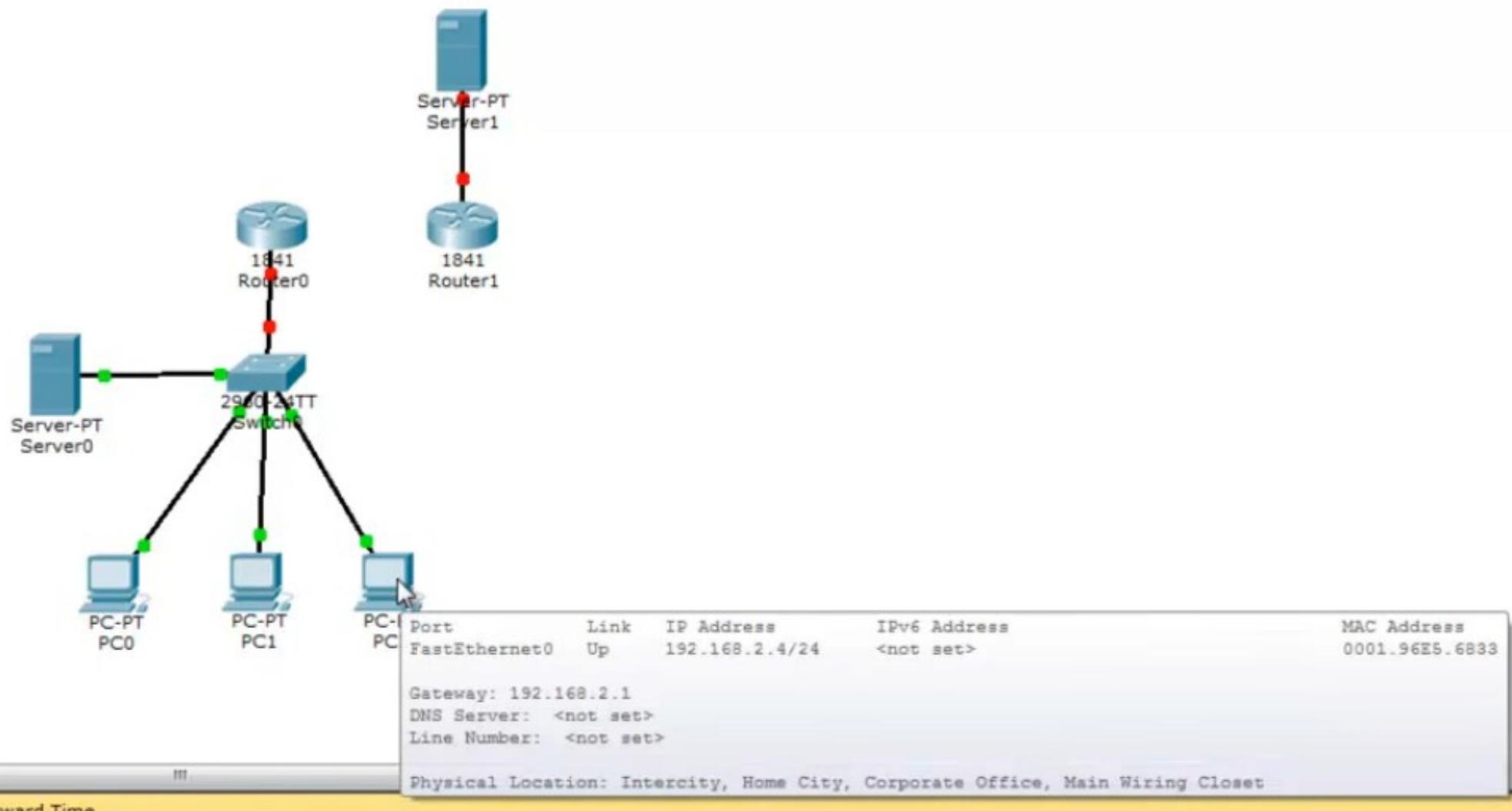
Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0	Up	192.168.2.2/24	<not set>	0005.5E08.BD7E
<hr/>				
Gateway: 192.168.2.1				
DNS Server: <not set>				
Line Number: <not set>				
<hr/>				
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet				

Fast Forward Time

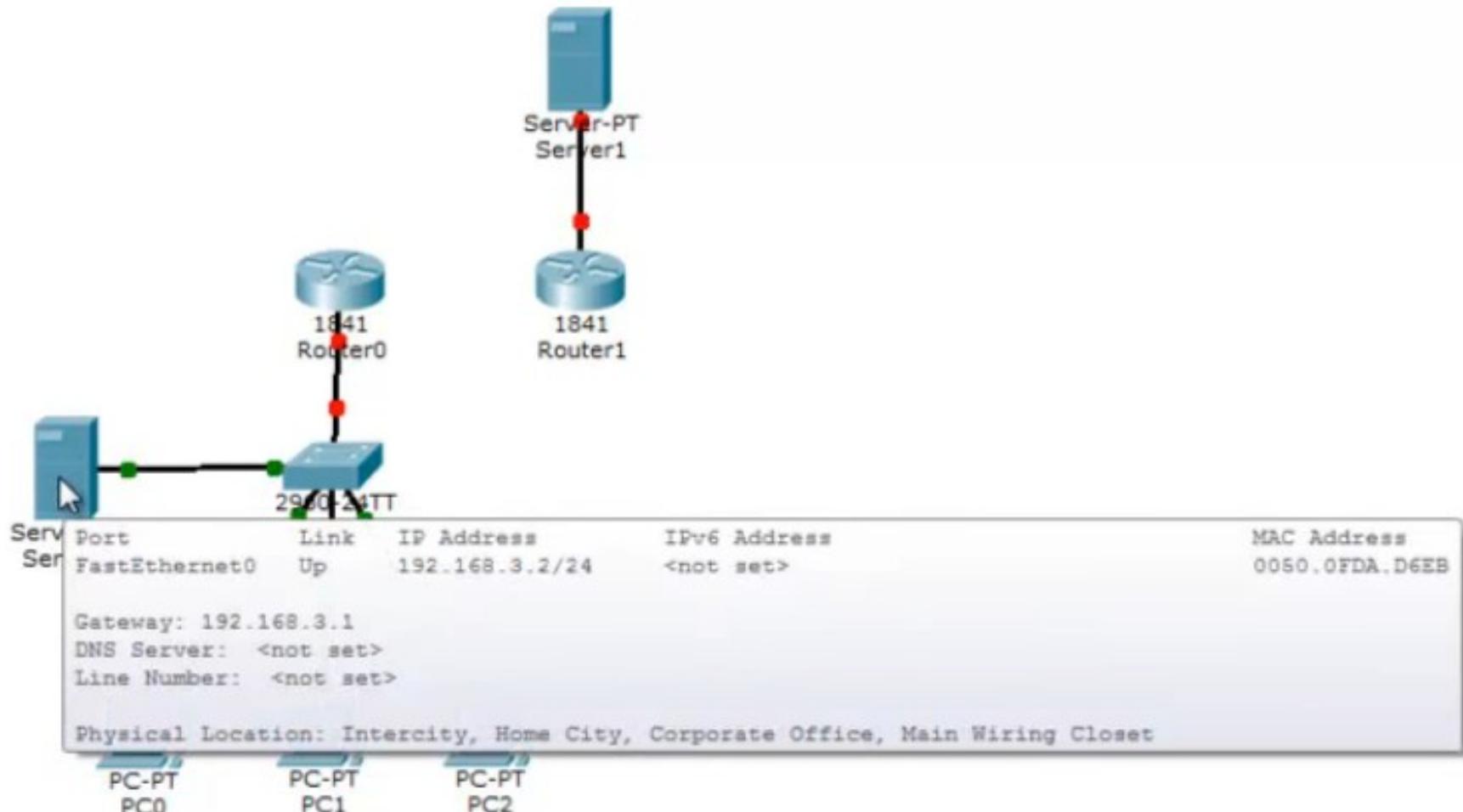
Ip адрес PC1



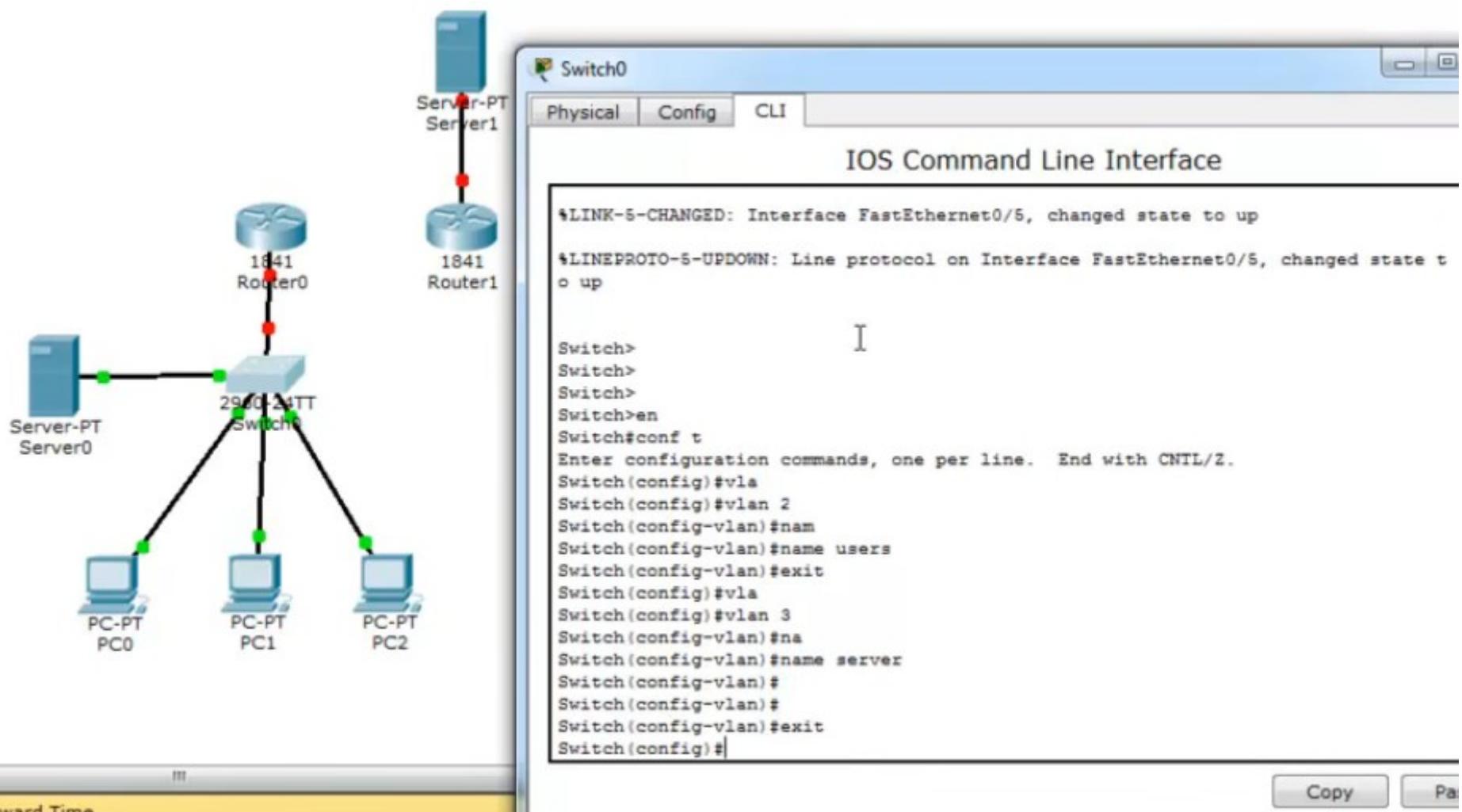
Ip адрес PC2



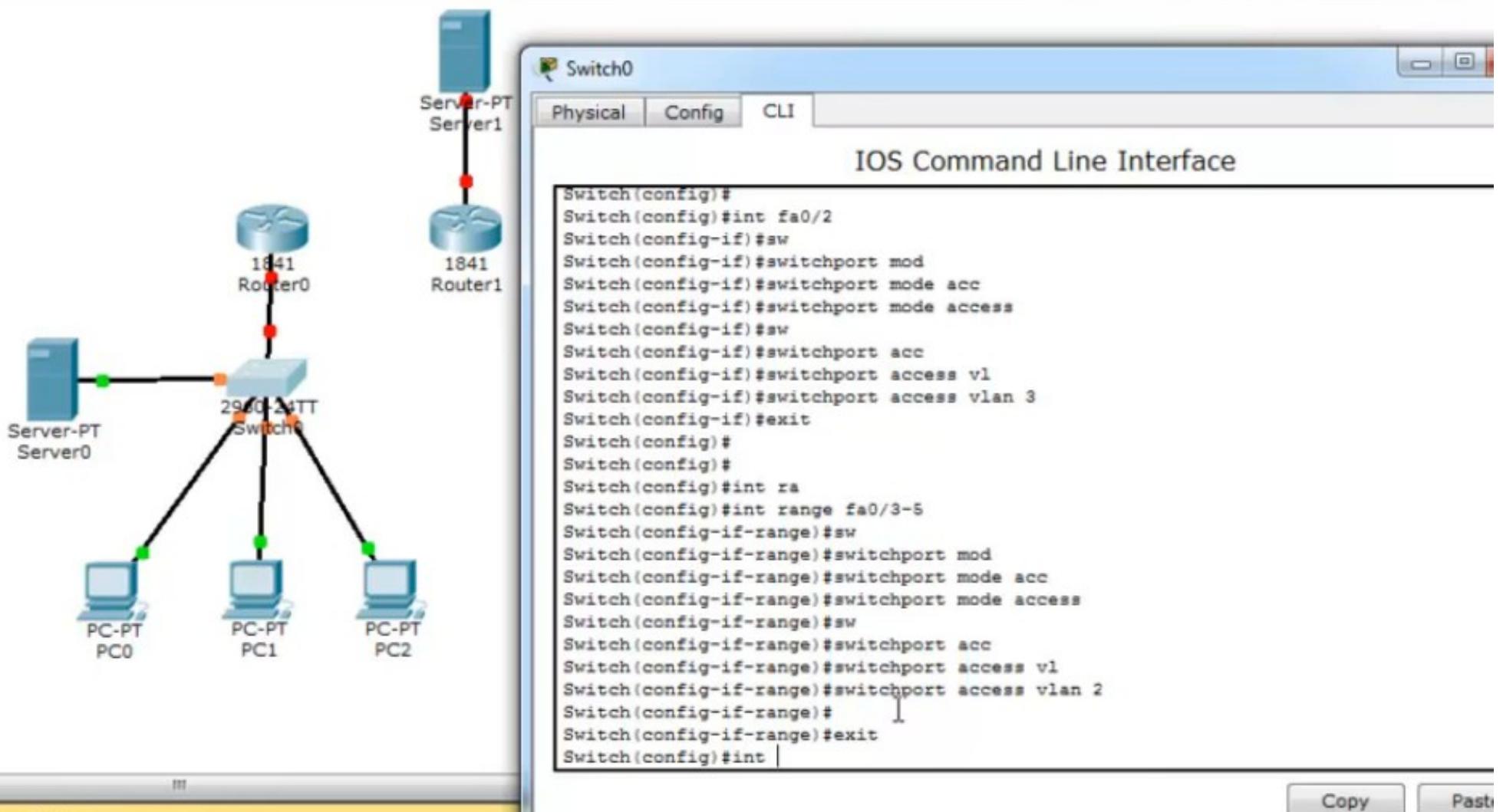
Ip адрес Sever0



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



Назначаем VLAN на порты коммутатора

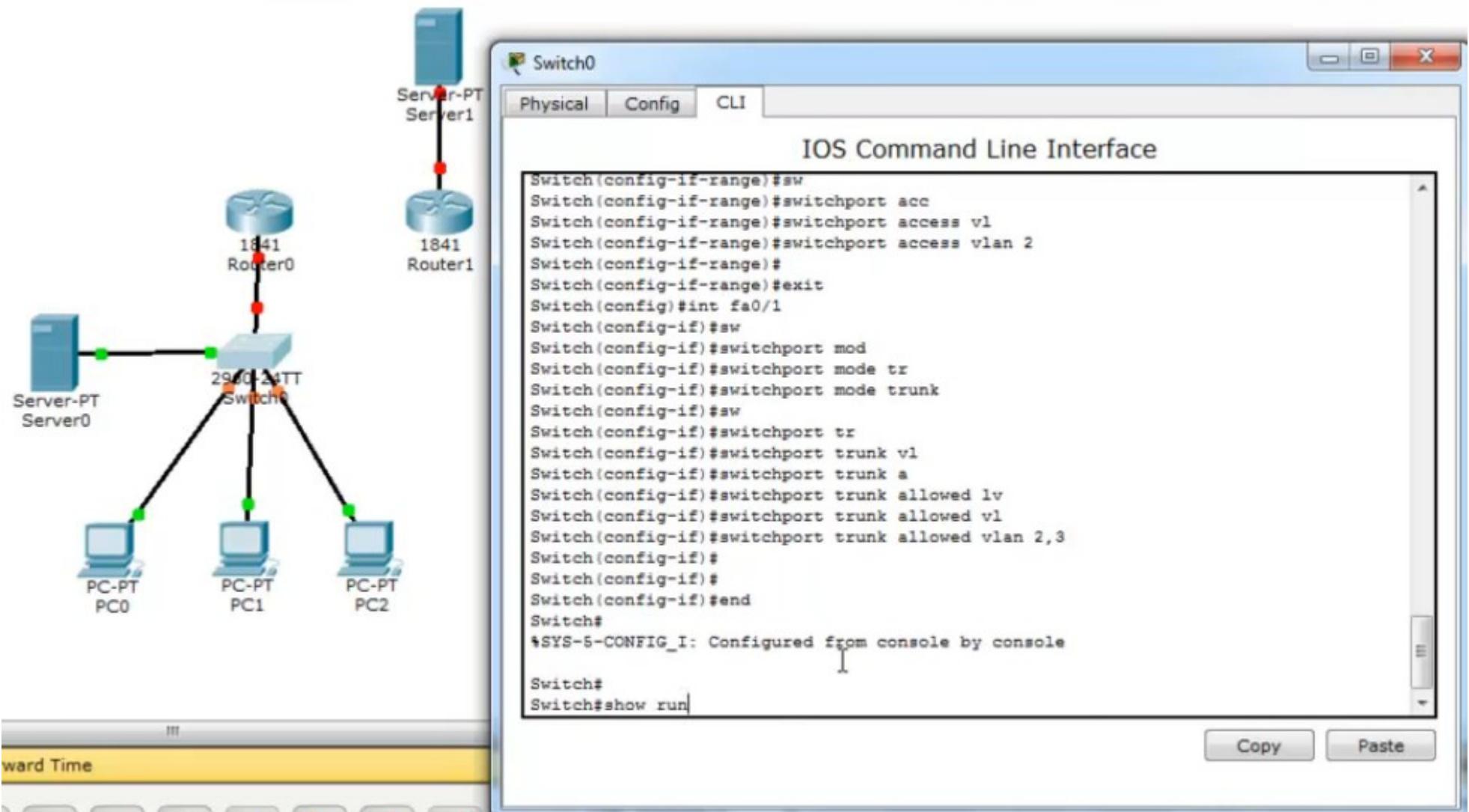


The image shows a network diagram on the left and a terminal window on the right. The network diagram includes a 2960-24 NTT Switch, Router0 (1841), Router1 (1841), Server0-PT (Server0), Server1-PT (Server1), and three PCs (PC0-PT, PC1-PT, PC2-PT). The switch is connected to the PCs, Router0, and Router1. Router0 is connected to Router1. Router1 is connected to Server1-PT. Server0-PT is connected to the switch. The terminal window shows the IOS Command Line Interface for the switch, with the 'Config' tab selected. The configuration script sets port fa0/2 to VLAN 1 and port ranges fa0/3-5 to VLAN 2.

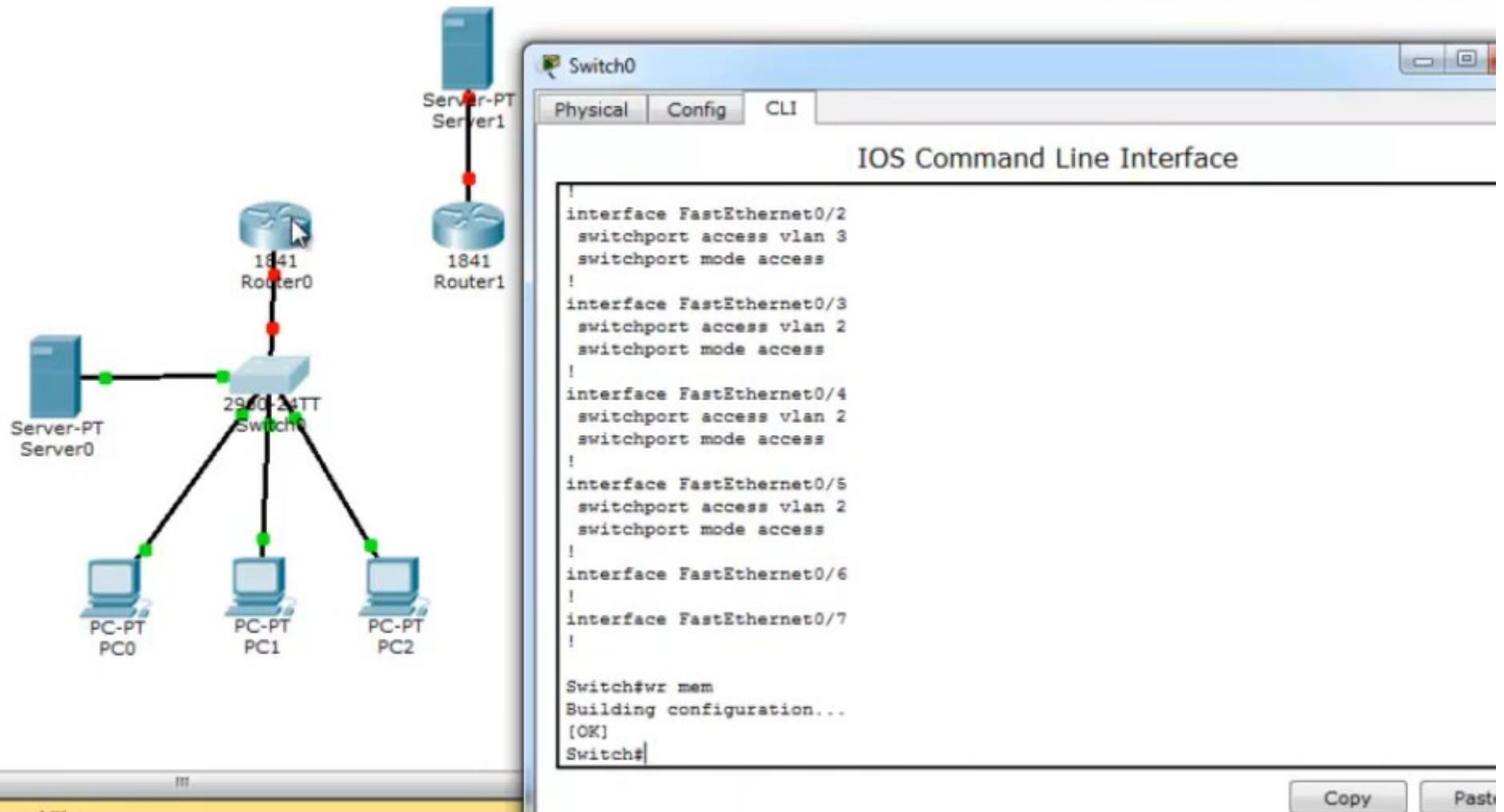
```
Switch(config)#  
Switch(config)#int fa0/2  
Switch(config-if)#sw  
Switch(config-if)#switchport mod  
Switch(config-if)#switchport mode acc  
Switch(config-if)#switchport mode access  
Switch(config-if)#sw  
Switch(config-if)#switchport acc  
Switch(config-if)#switchport access vl  
Switch(config-if)#switchport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

Copy Paste

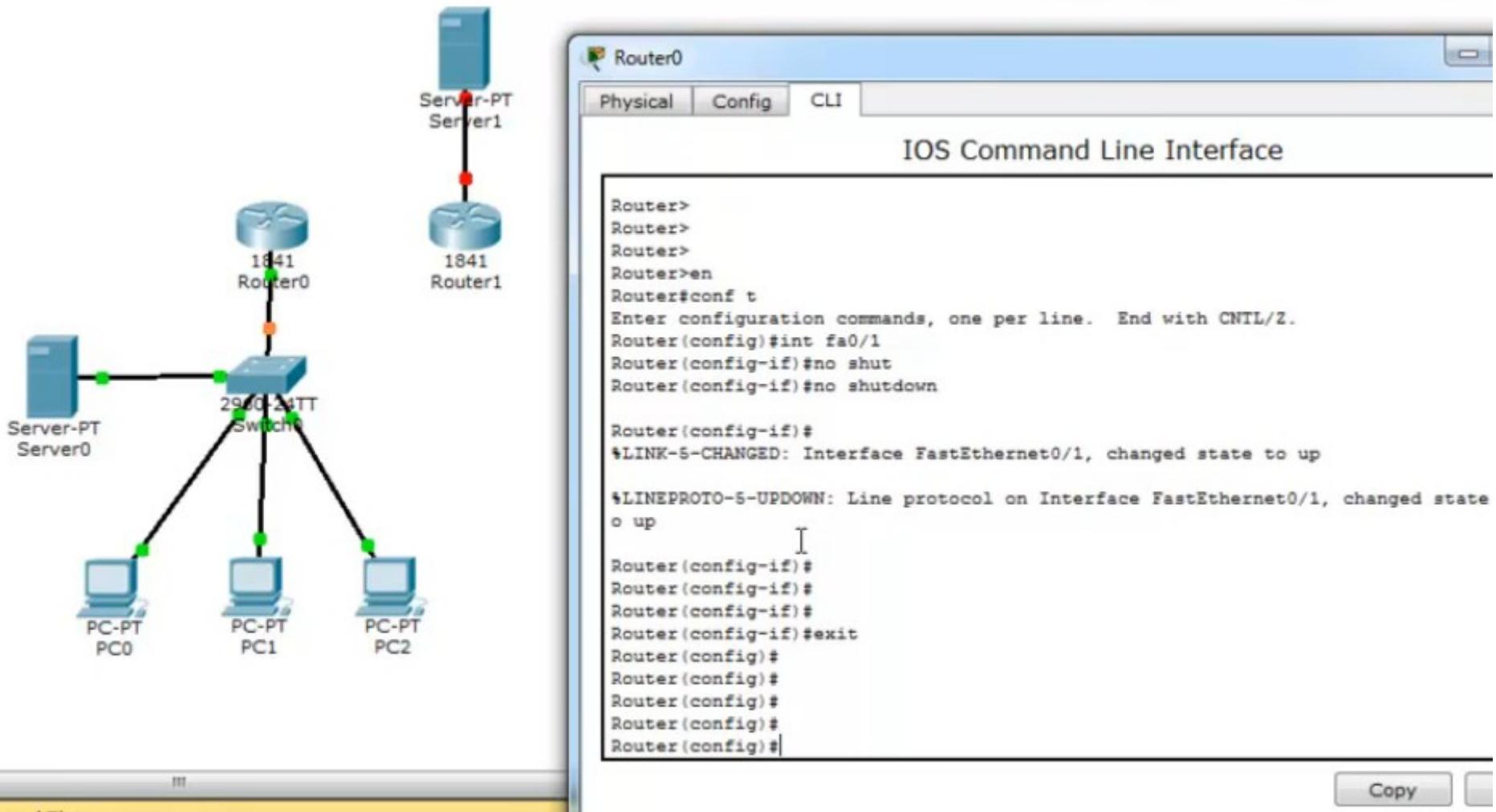
Назначаем trunk порт, проверяем конфигурацию



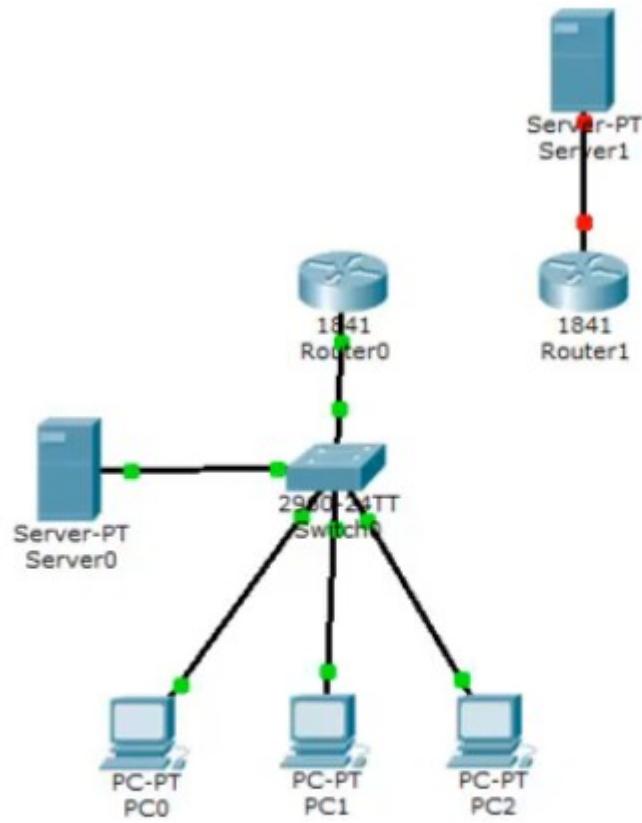
Проверяем конфигурацию, сохраняем



Настраиваем Router0, активируем интерфейс fa0/1



Создадим субинтерфейс для VLAN 2, назначим ip



Router0

Physical Config CLI

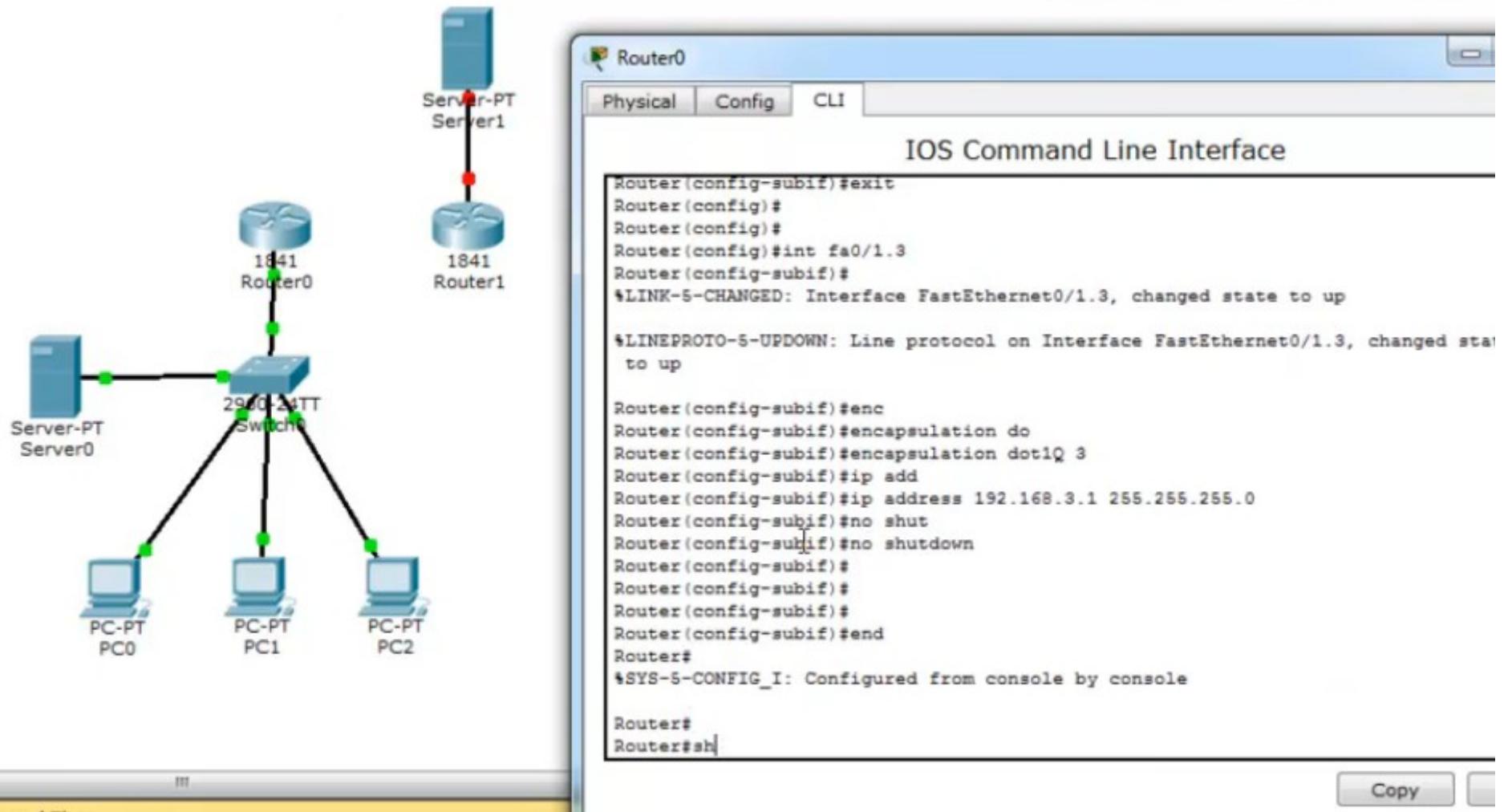
IOS Command Line Interface

```
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

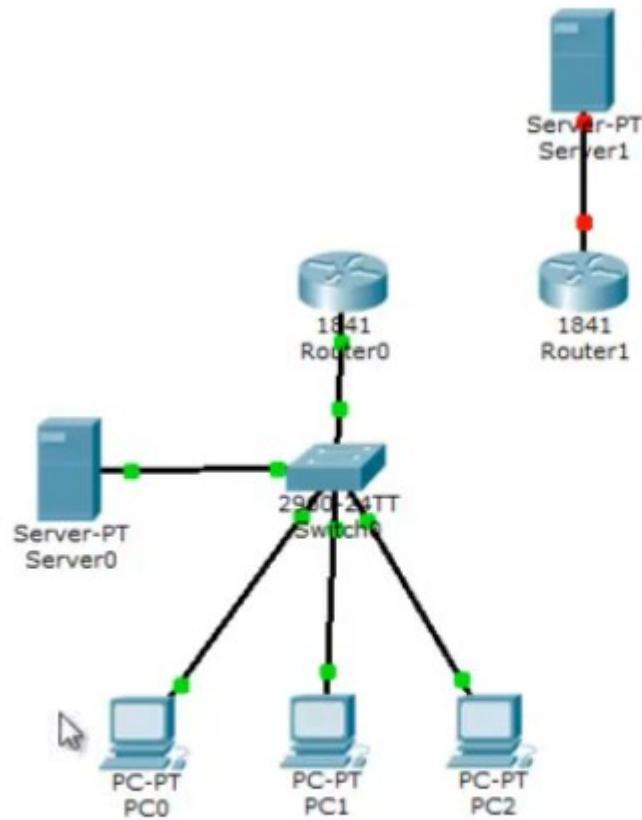
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.2, changed state to up

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

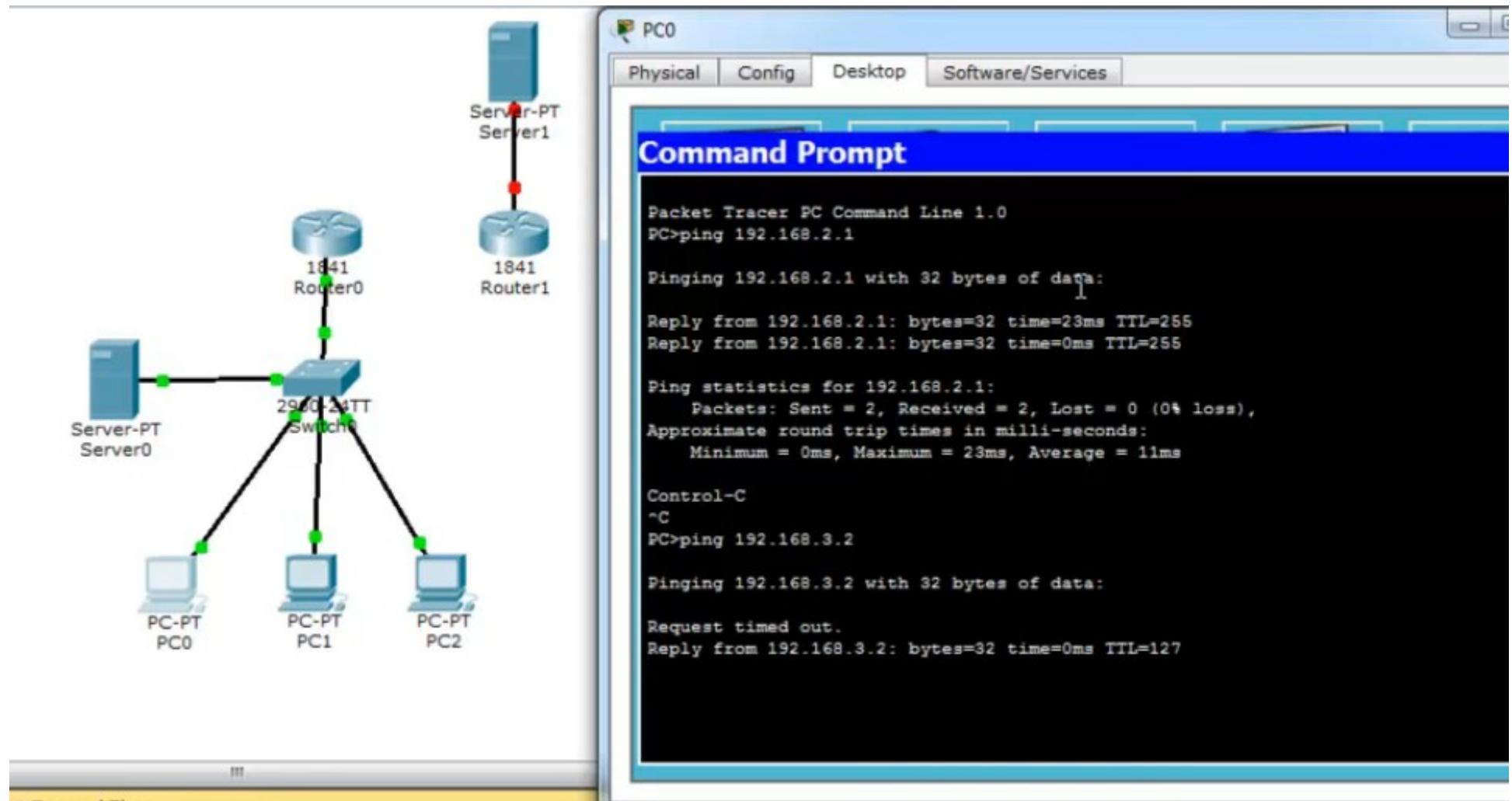
IOS Command Line Interface

```
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
!

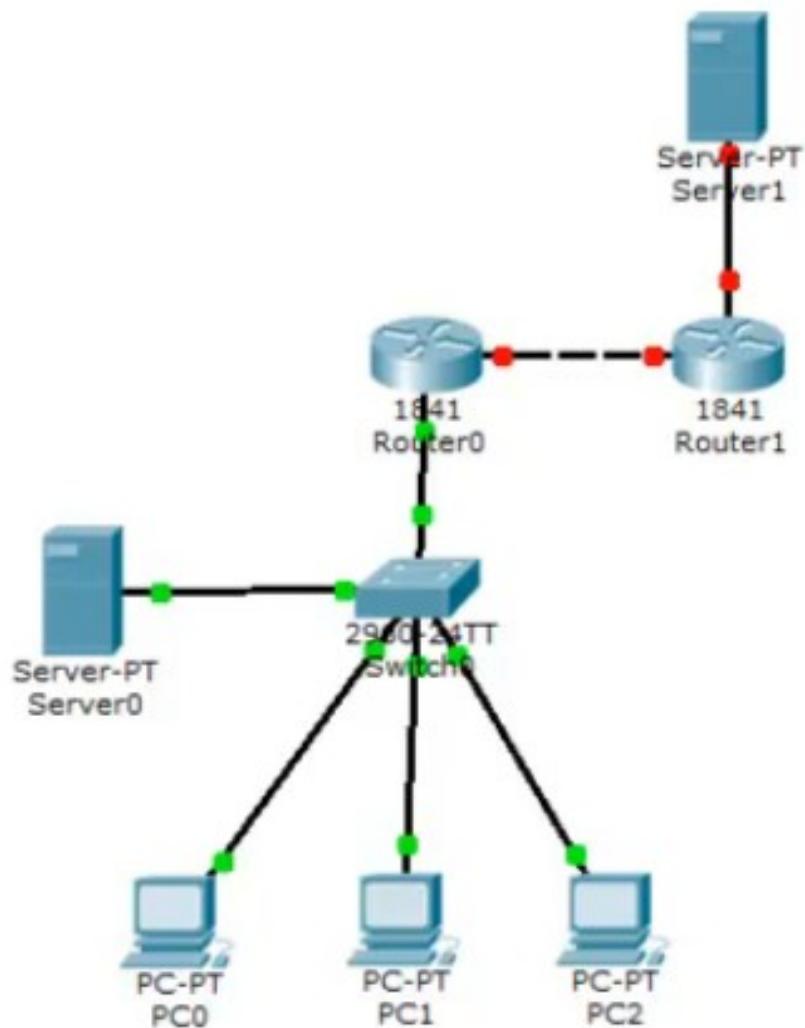
Router#wr mem
Building configuration...
[OK]
Router#
```

Copy

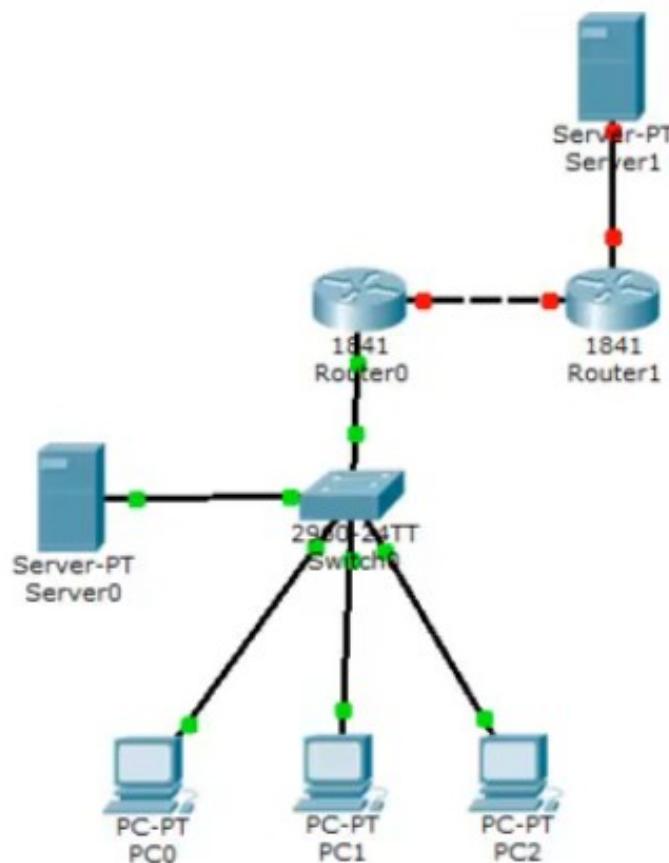
Проверяем, что шлюз и сервер доступны с PC0



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

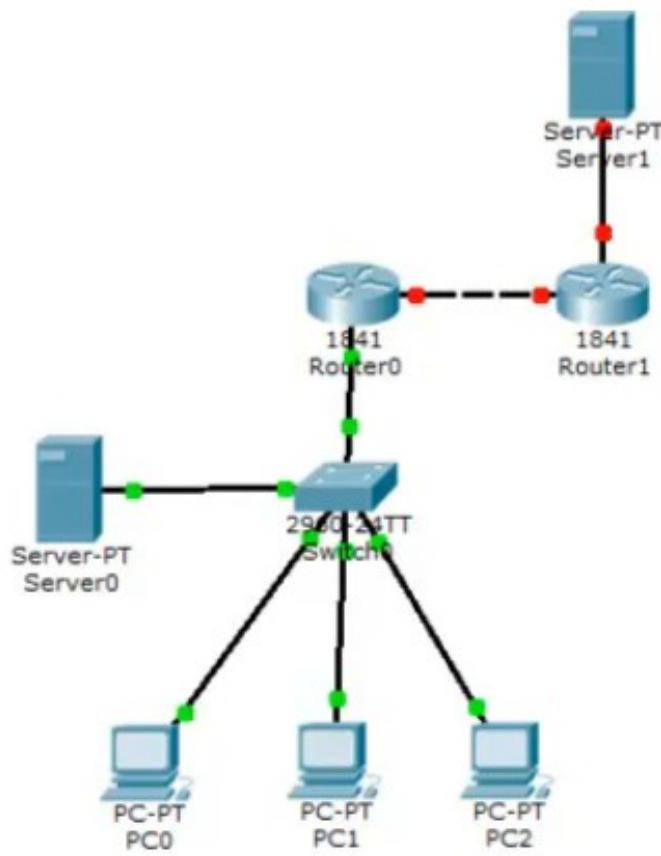
```
Router>
Router>en
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int
Router(config)#interface fa0/0
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)$ip add
Router(config-if)$ip address 213.234.10.1 255.255.255.252
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



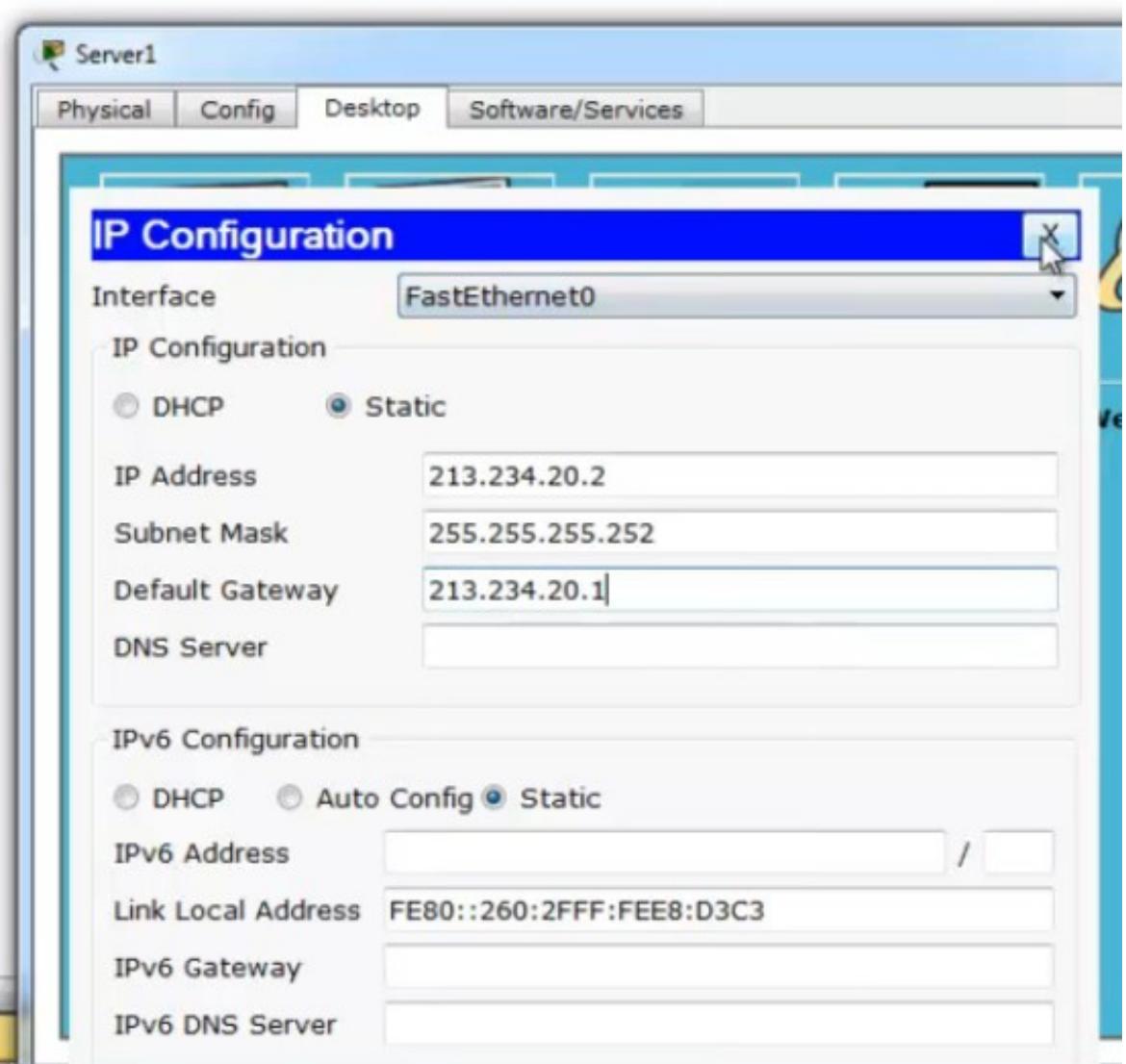
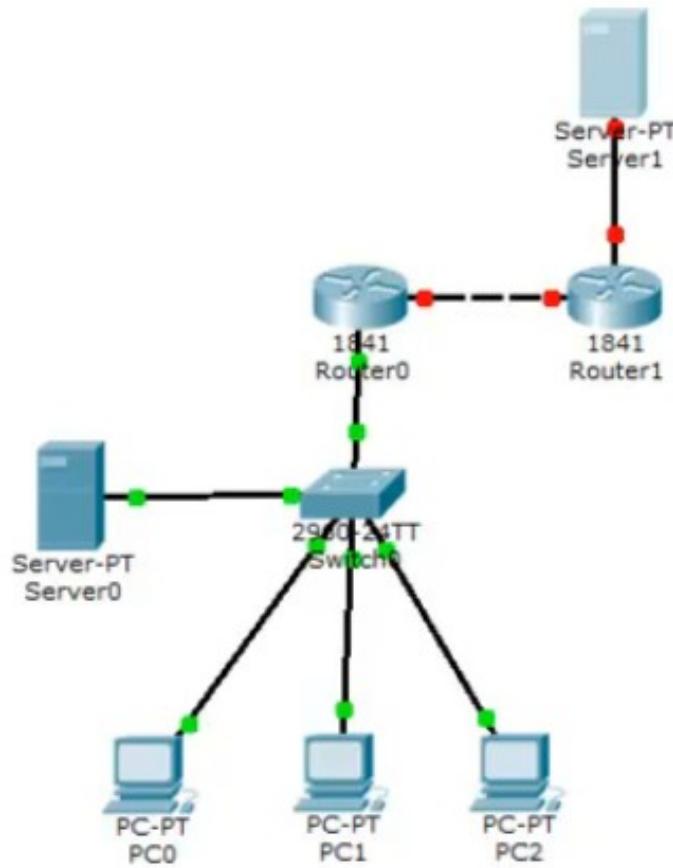
Router1

Physical Config CLI

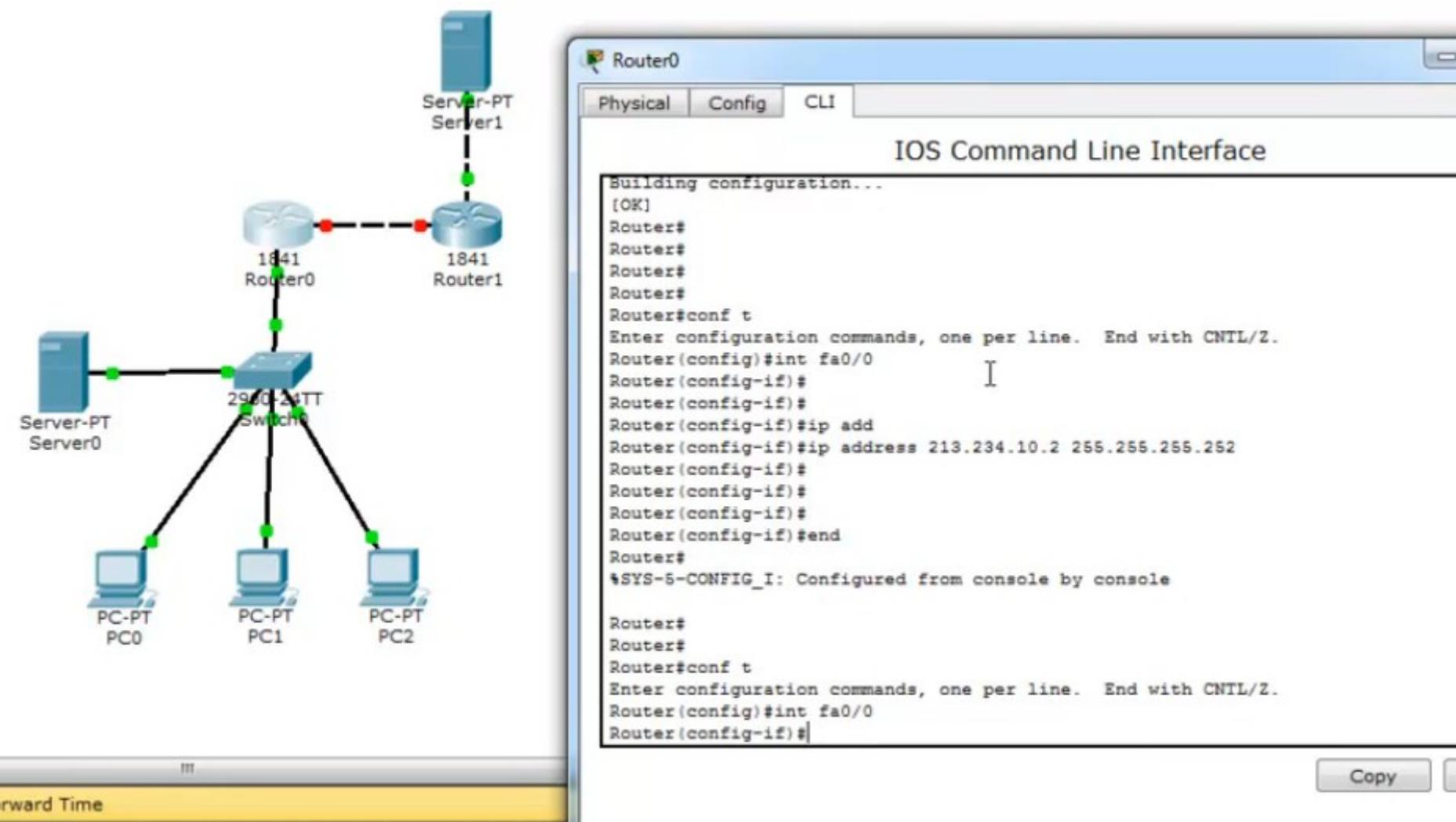
IOS Command Line Interface

```
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)#
```

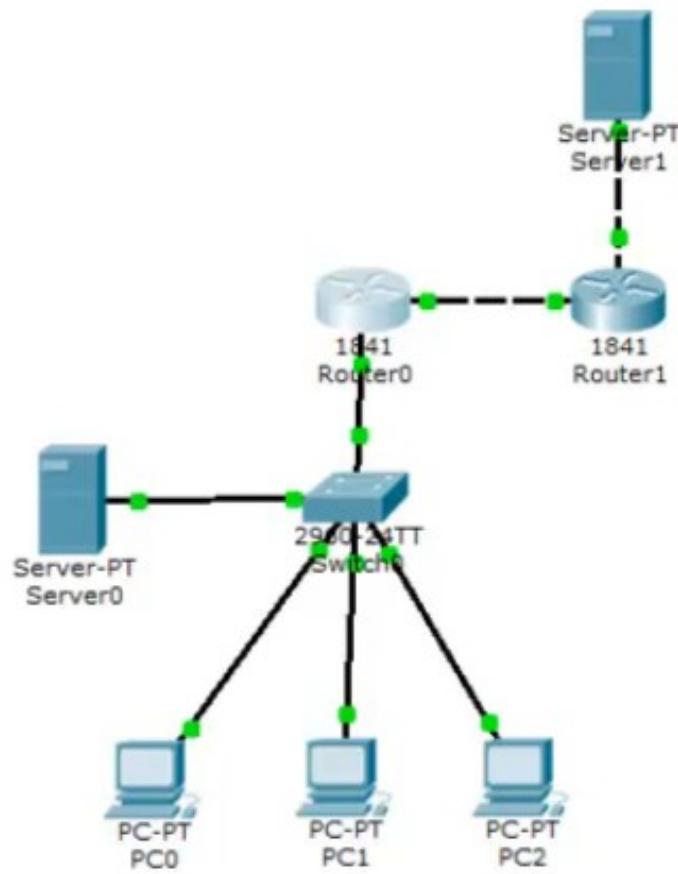
Зададим ір адрес для Server1



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



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

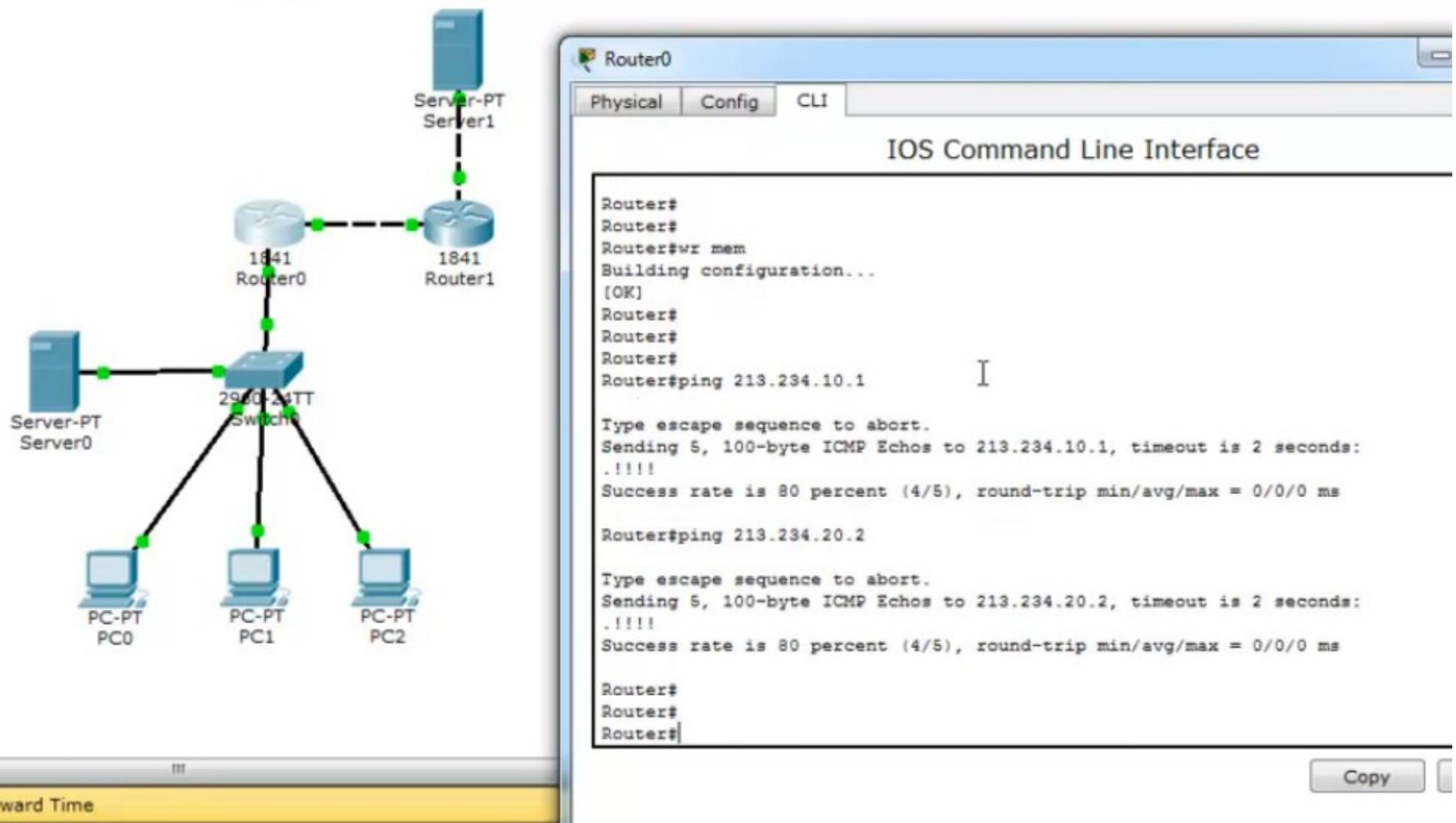
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

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

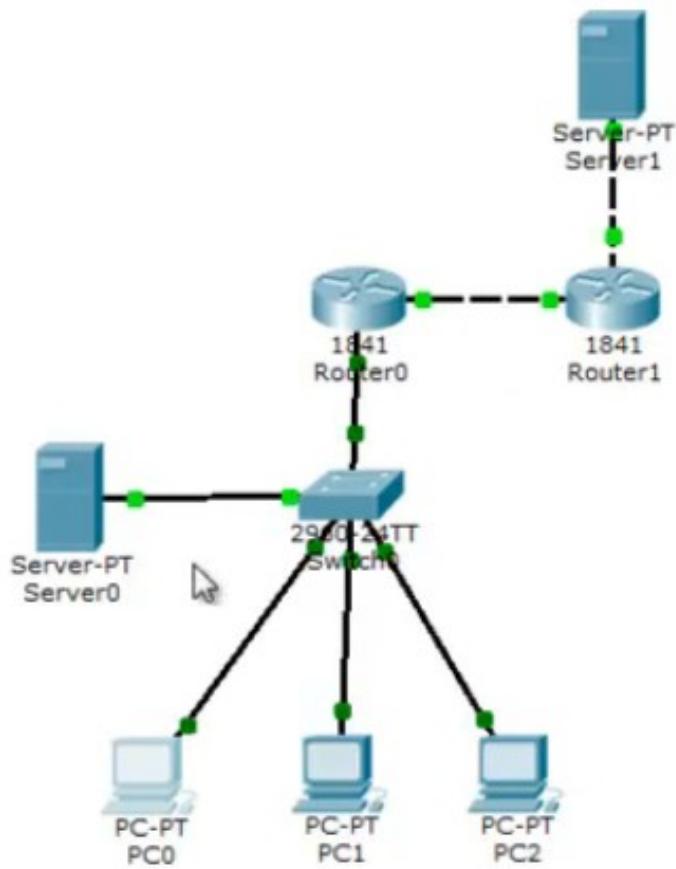
Router#
Router#
```

Copy

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

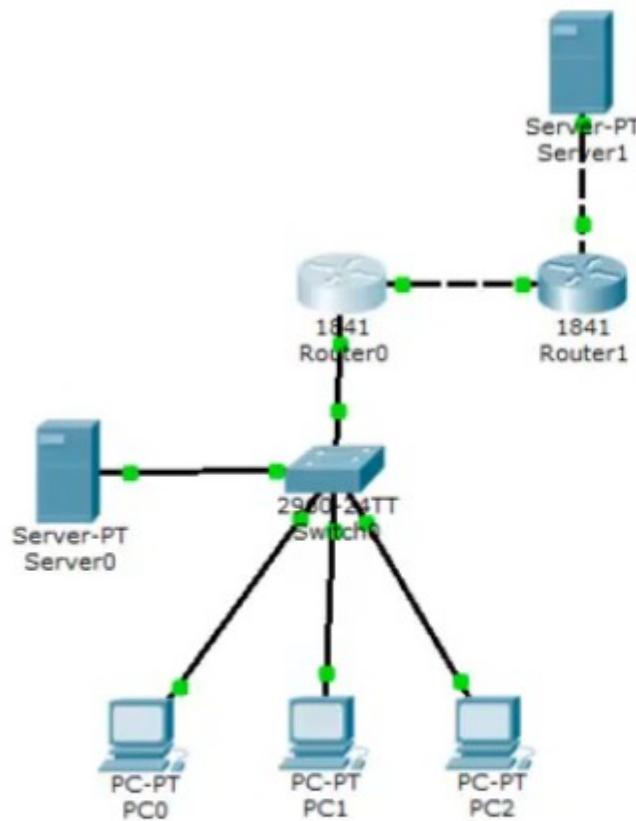
Ping statistics for 192.168.3.2:
  Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

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



Router0

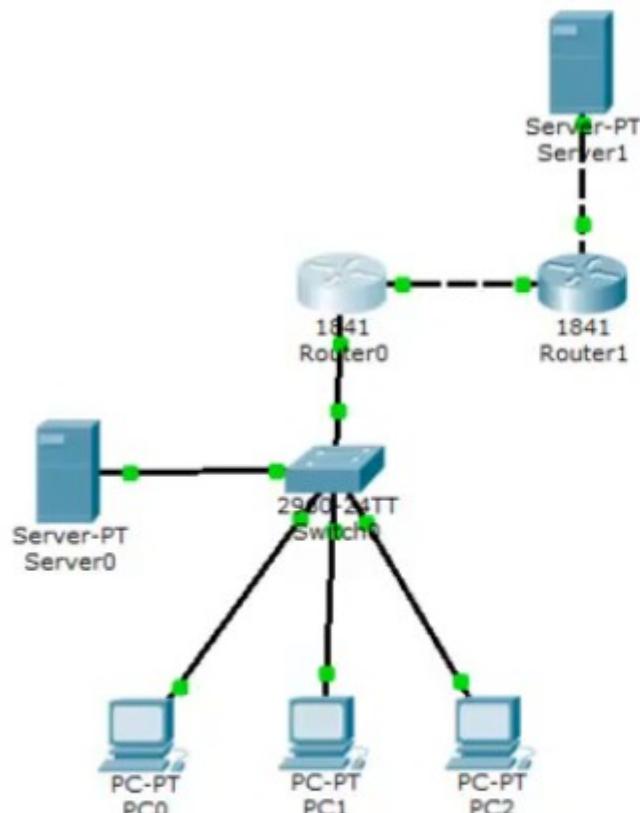
Physical Config CLI

IOS Command Line Interface

```
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)#
```

Copy

определяем fa0/1.3 тоже как внутренний



Router0

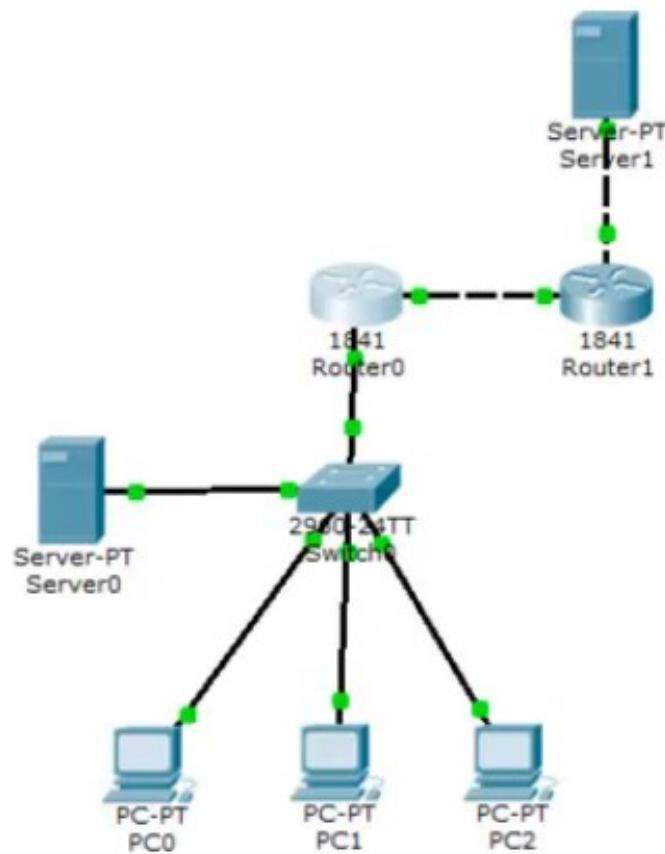
Physical Config CLI

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.



Router0

Physical Config CLI

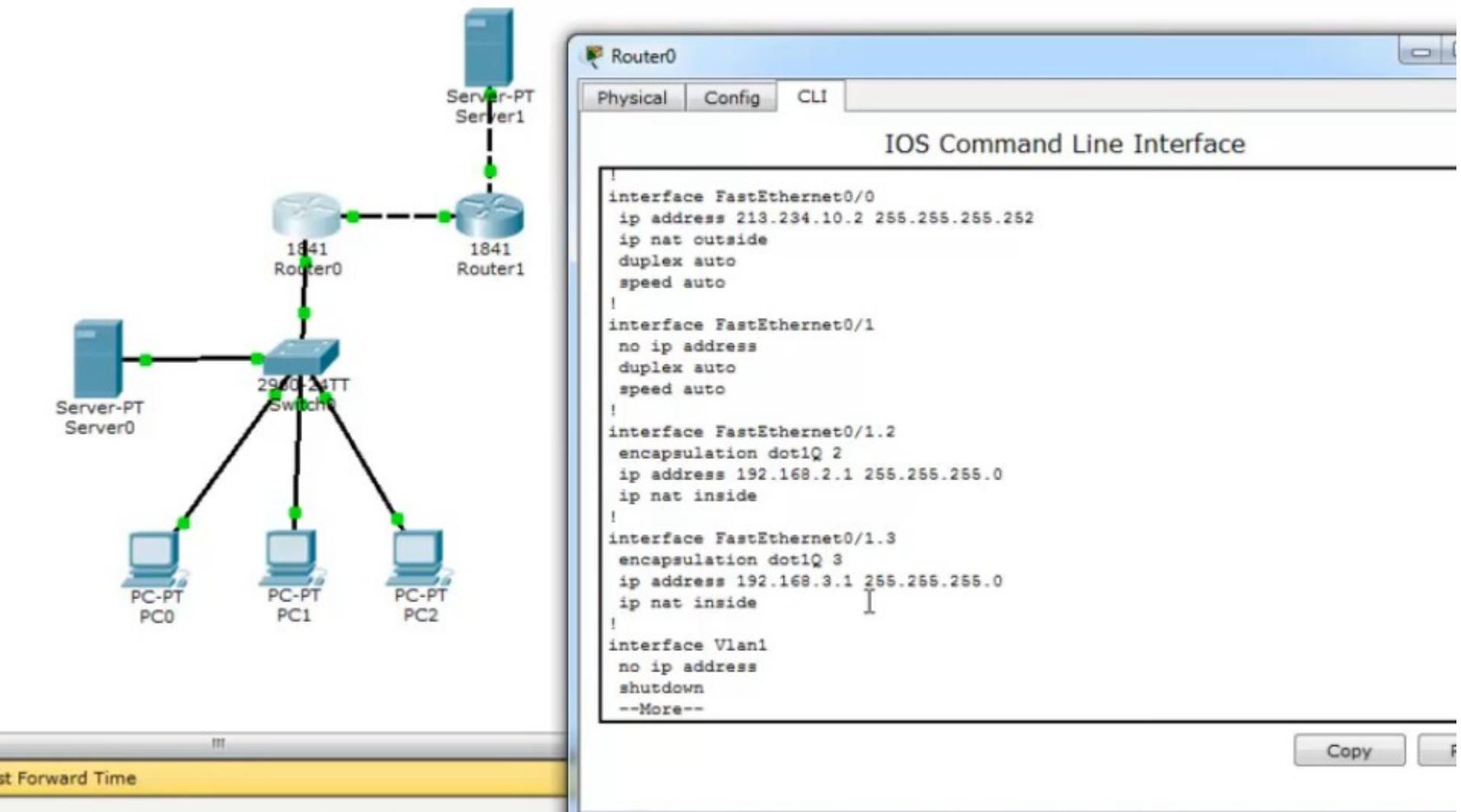
IOS Command Line Interface

```
Router#  
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
```

Copy

Forward Time

В конфигурации — какие интерфейсы inside, какие outside.



Настраиваем Port-Address-Translation

Настройка РАТ

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

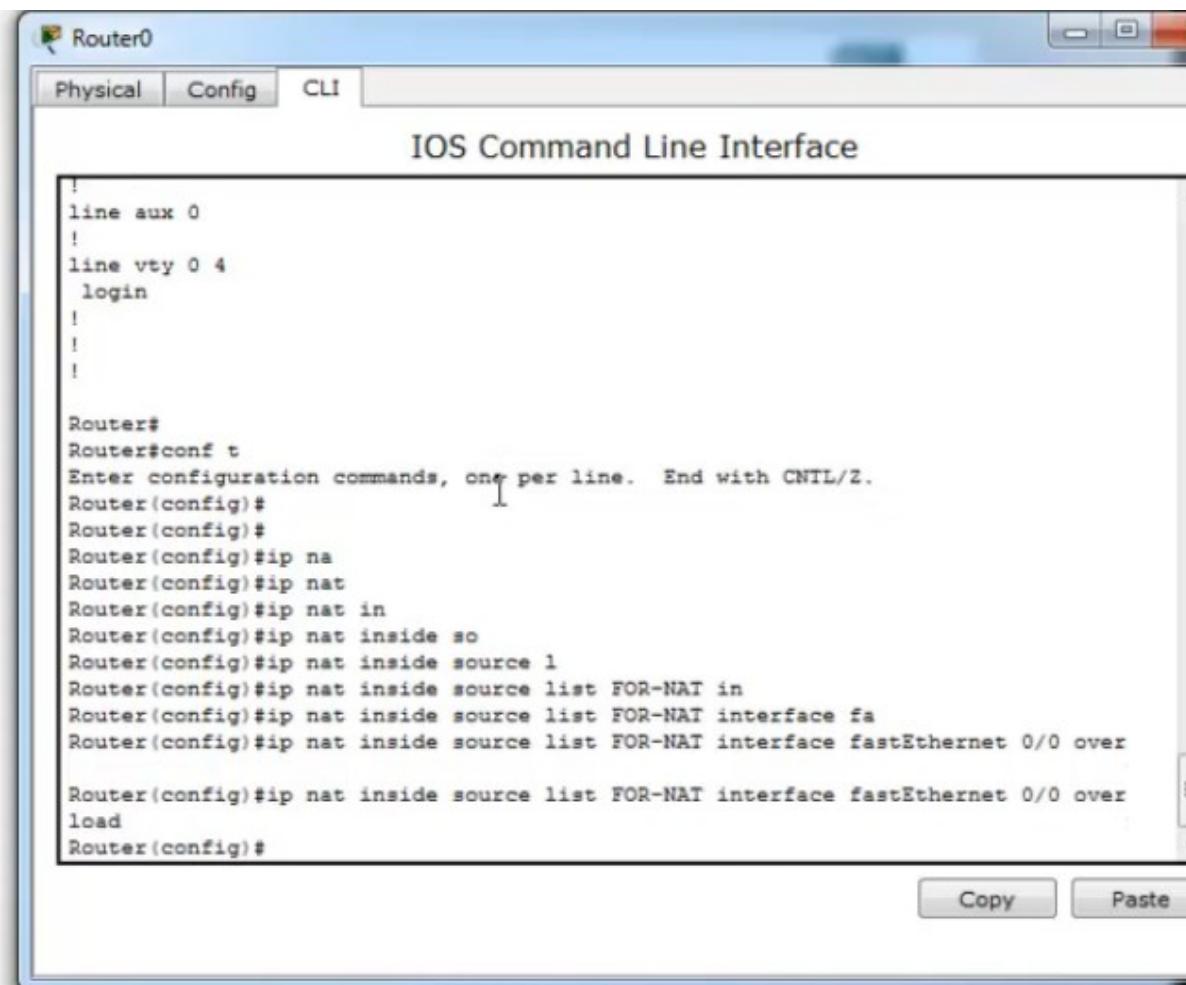
```
ip access-list standard FOR-NAT  
  permit 192.168.2.0 0.0.0.255  
  permit 192.168.3.0 0.0.0.255
```

```
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



Сохраняем

Настройка PAT

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

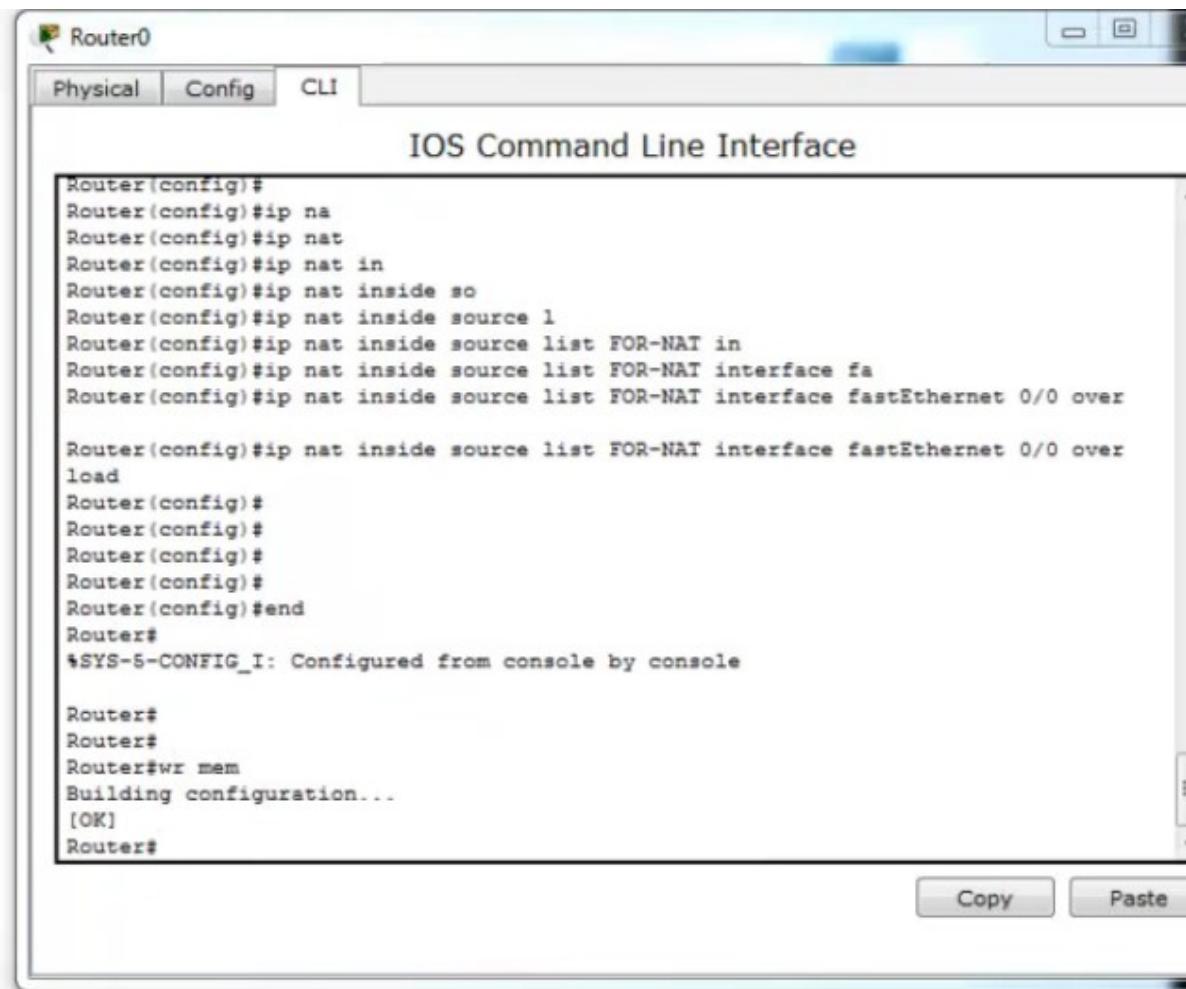
ip access-list standard FOR-NAT
permit 192.168.2.0 0.0.0.255
permit 192.168.3.0 0.0.0.255

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
```



Router0

Physical Config CLI

IOS Command Line Interface

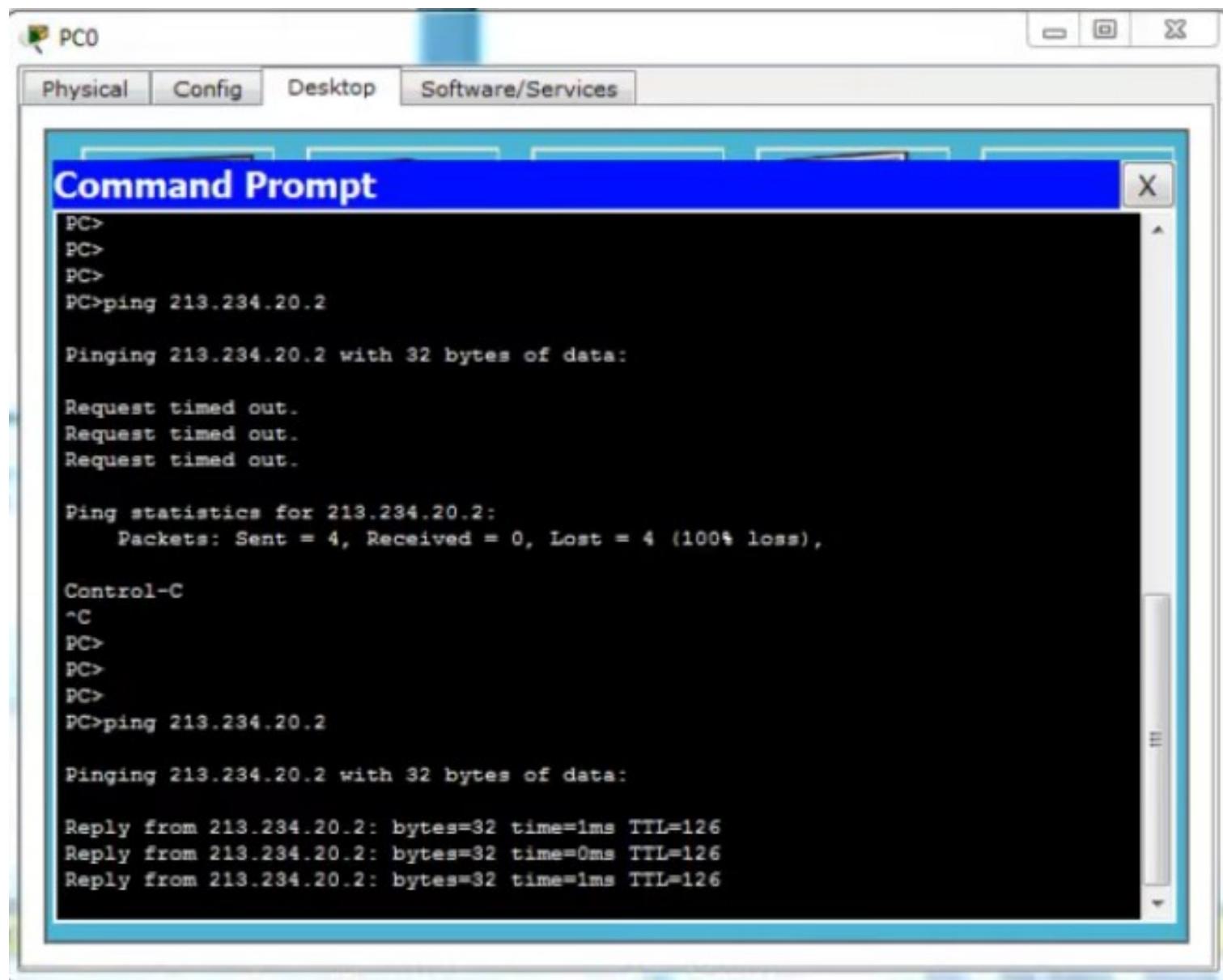
```
Router(config)#
Router(config)#ip na
Router(config)#ip nat
Router(config)#ip nat in
Router(config)#ip nat inside so
Router(config)#ip nat inside source 1
Router(config)#ip nat inside source list FOR-NAT in
Router(config)#ip nat inside source list FOR-NAT interface fa
Router(config)#ip nat inside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



PC0

Physical Config Desktop Software/Services

Command Prompt

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

Pinging 213.234.20.2 with 32 bytes of data:

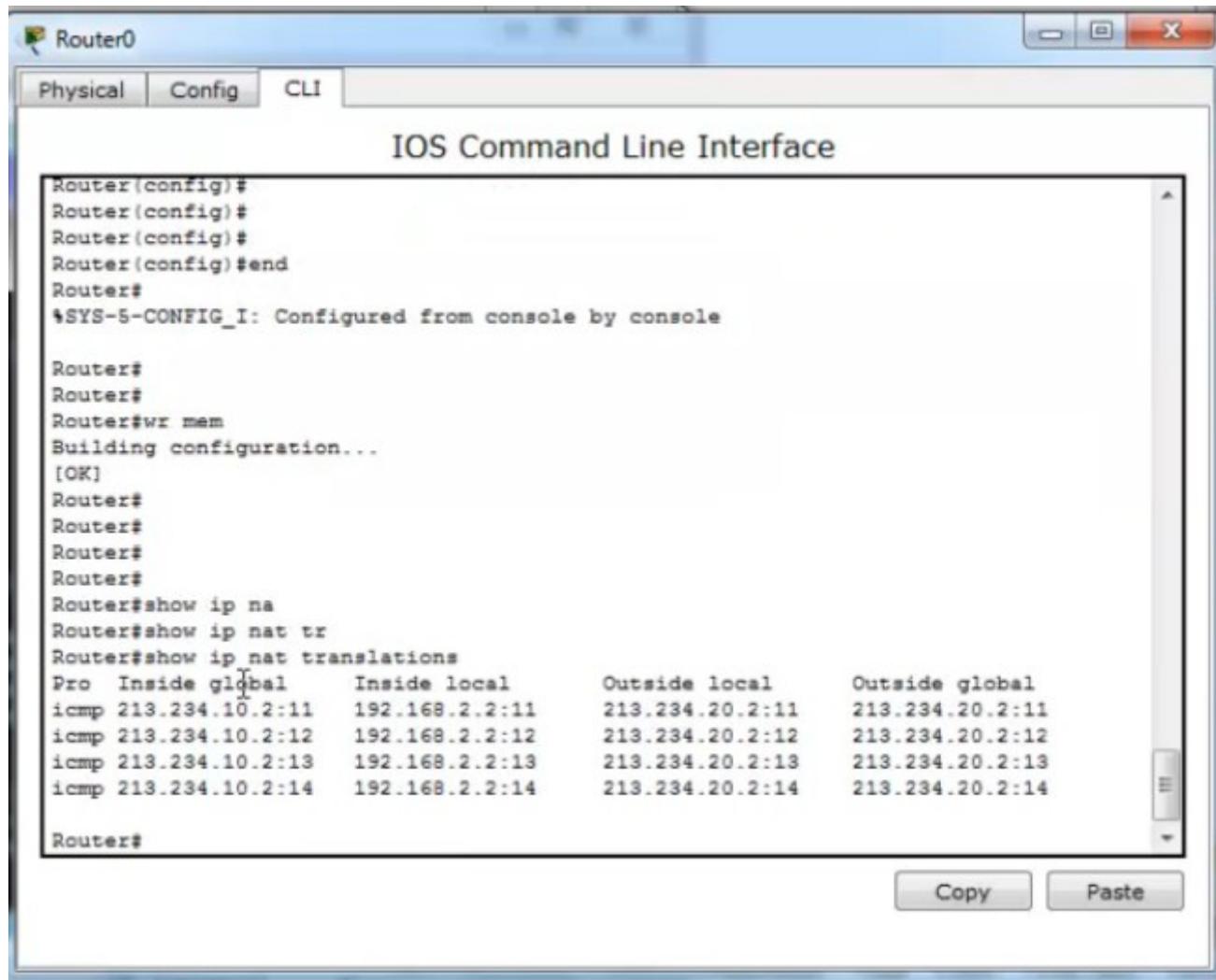
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 213.234.20.2:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
  Control-C
  ^C
PC>
PC>
PC>
PC>ping 213.234.20.2

Pinging 213.234.20.2 with 32 bytes of data:

Reply from 213.234.20.2: bytes=32 time=1ms TTL=126
Reply from 213.234.20.2: bytes=32 time=0ms TTL=126
Reply from 213.234.20.2: bytes=32 time=1ms TTL=126
```

На Router0 видим настройки NAT



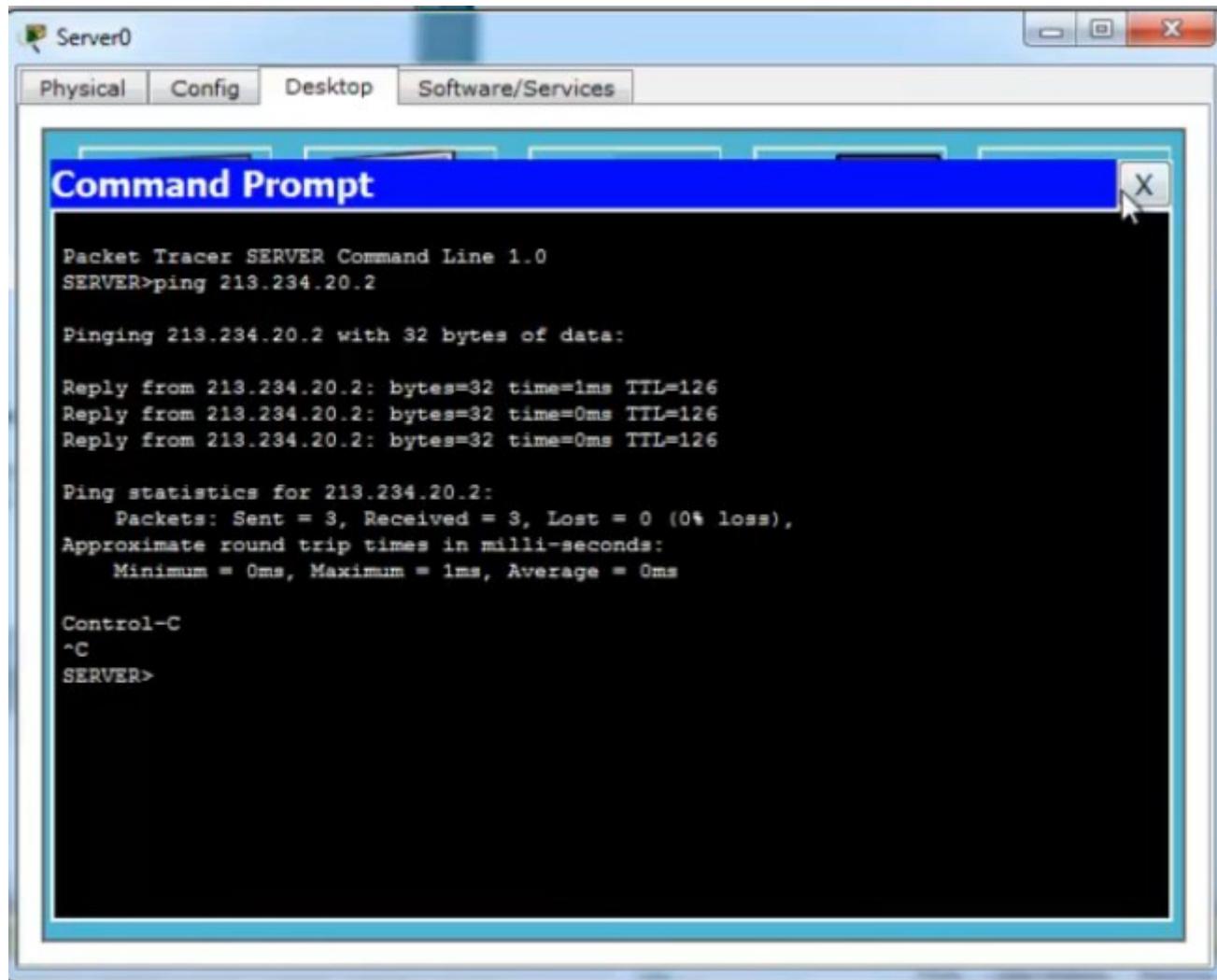
Router(config)#
Router(config)#
Router(config)#
Router(config)#end
Router#
*SYS-5-CONFIG_I: Configured from console by console

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

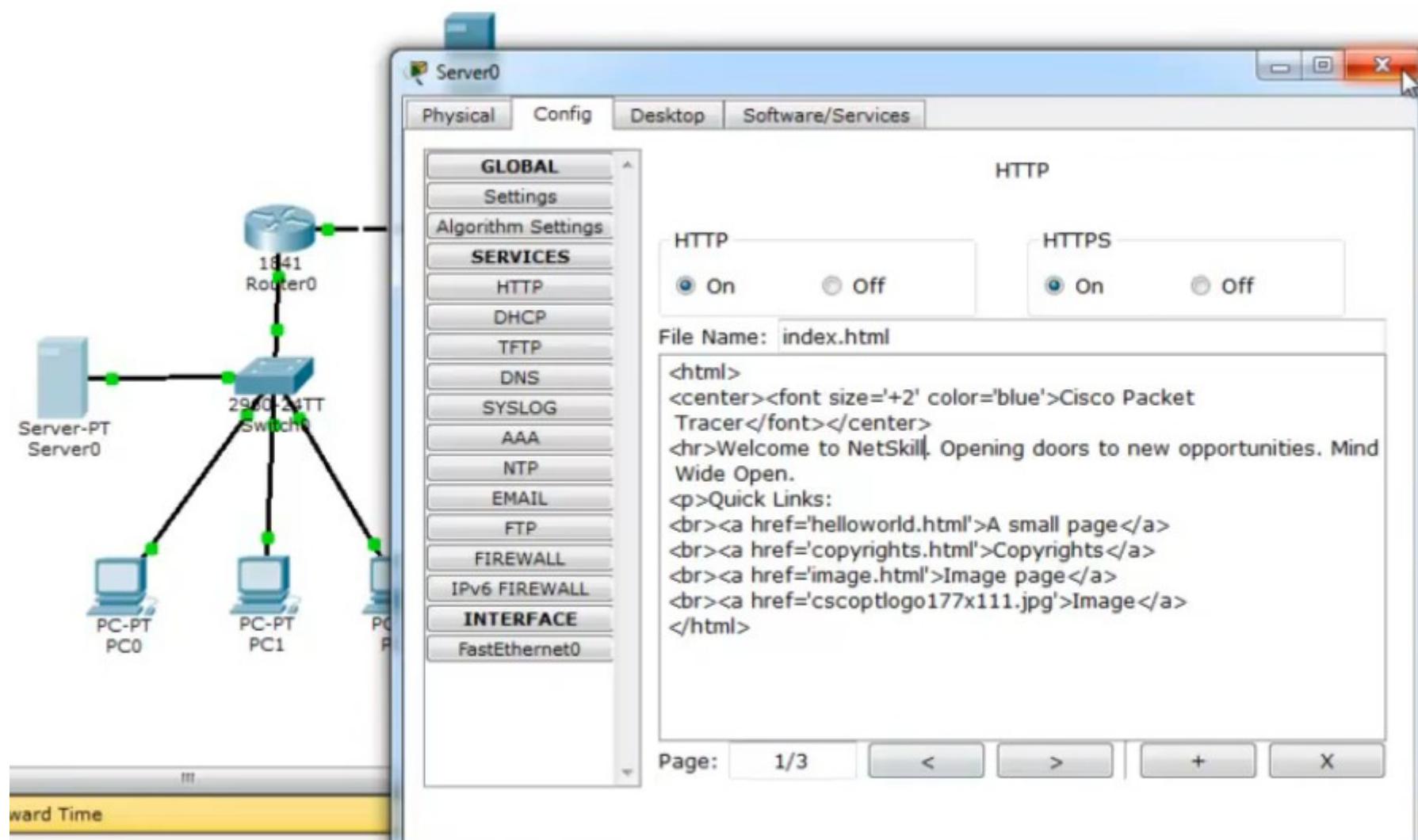
Router#

Copy Paste

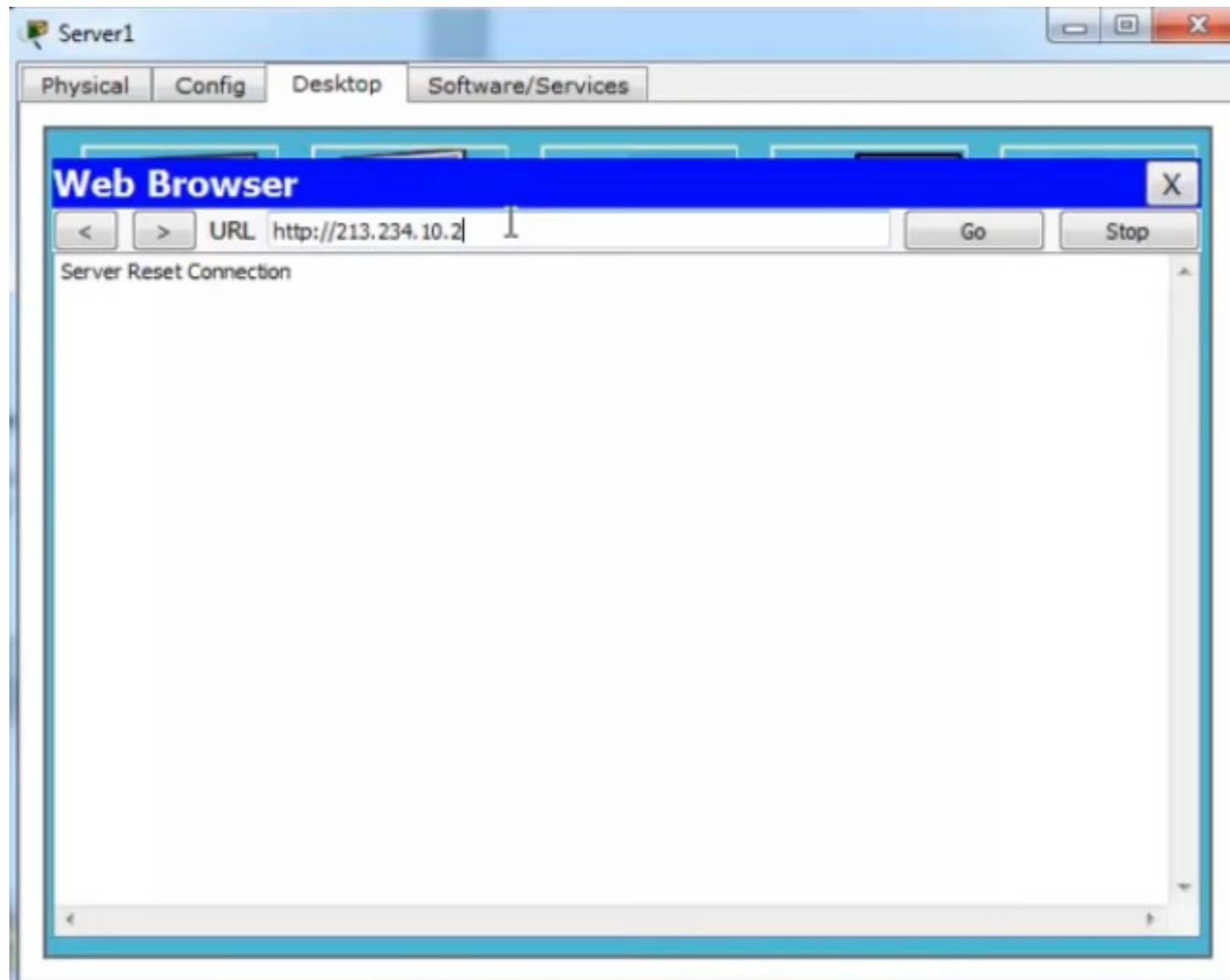
Проверяем, что с Server1 доступен PC0



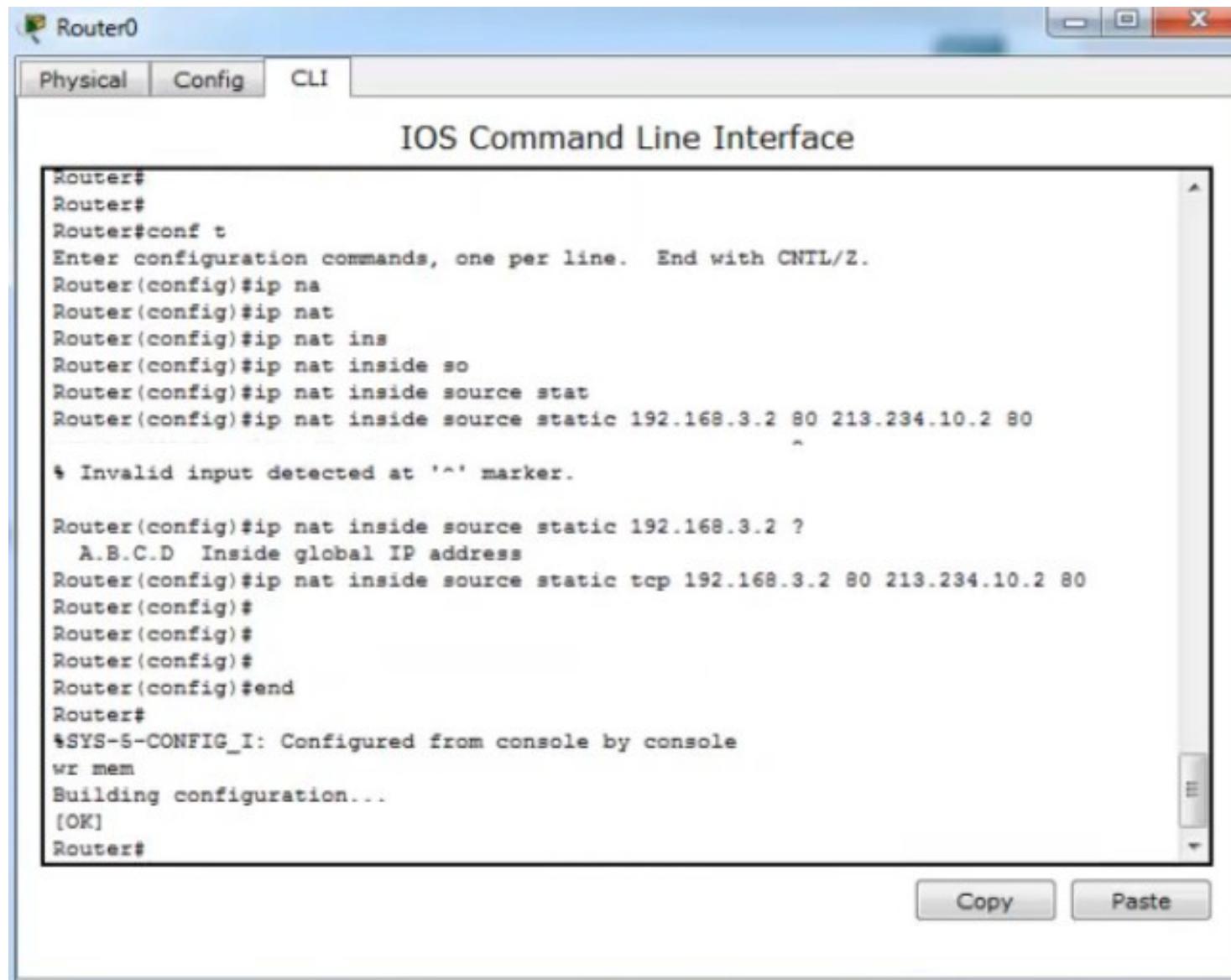
Далее настроим статический NAT для доступа к Server0 из внешней сети. Изменим содержание index.html в Config > HTTP у Server0



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



Настроим static NAT на Router0

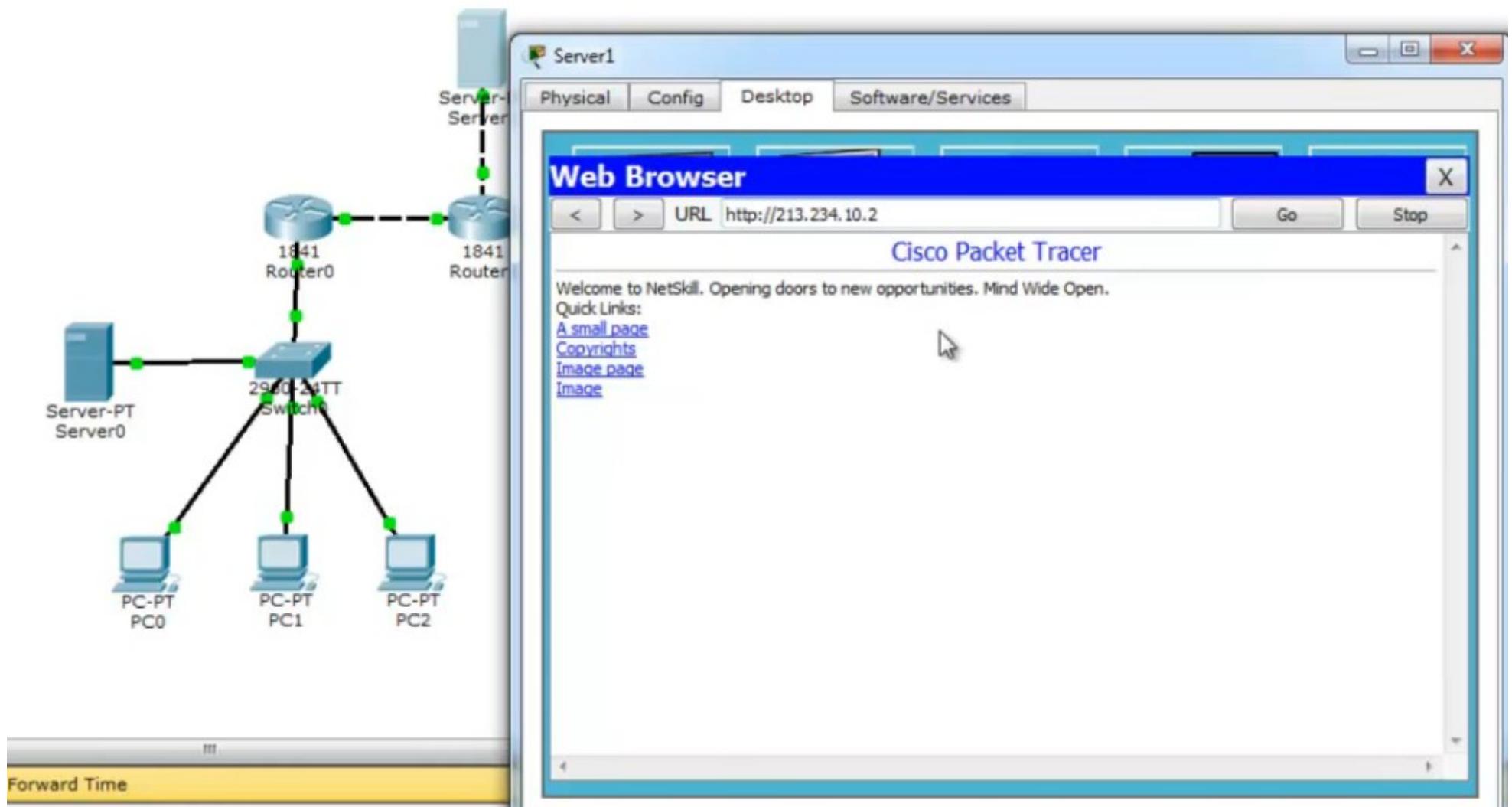


The screenshot shows the Router0 CLI interface. The title bar says "Router0". The tabs "Physical", "Config", and "CLI" are present, with "CLI" being the active tab. The main window title is "IOS Command Line Interface". The command-line session is as follows:

```
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 "Copy" and "Paste" buttons.

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

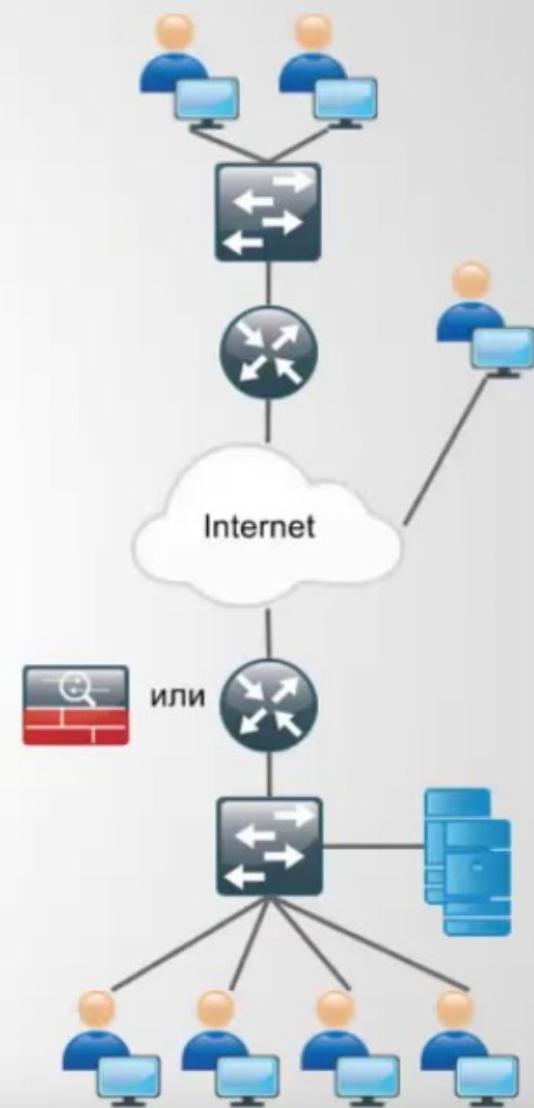
VPN - Virtual Private Network - виртуальная частная сеть

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

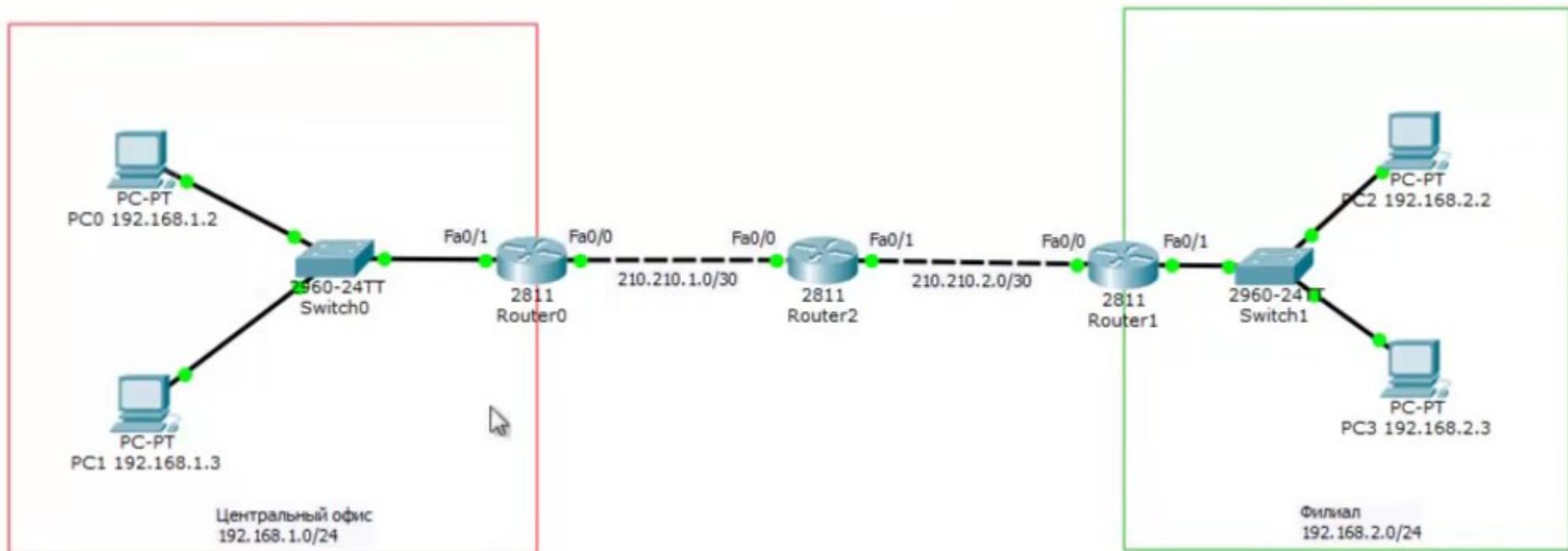
Построение туннеля в две фазы (IKE)

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

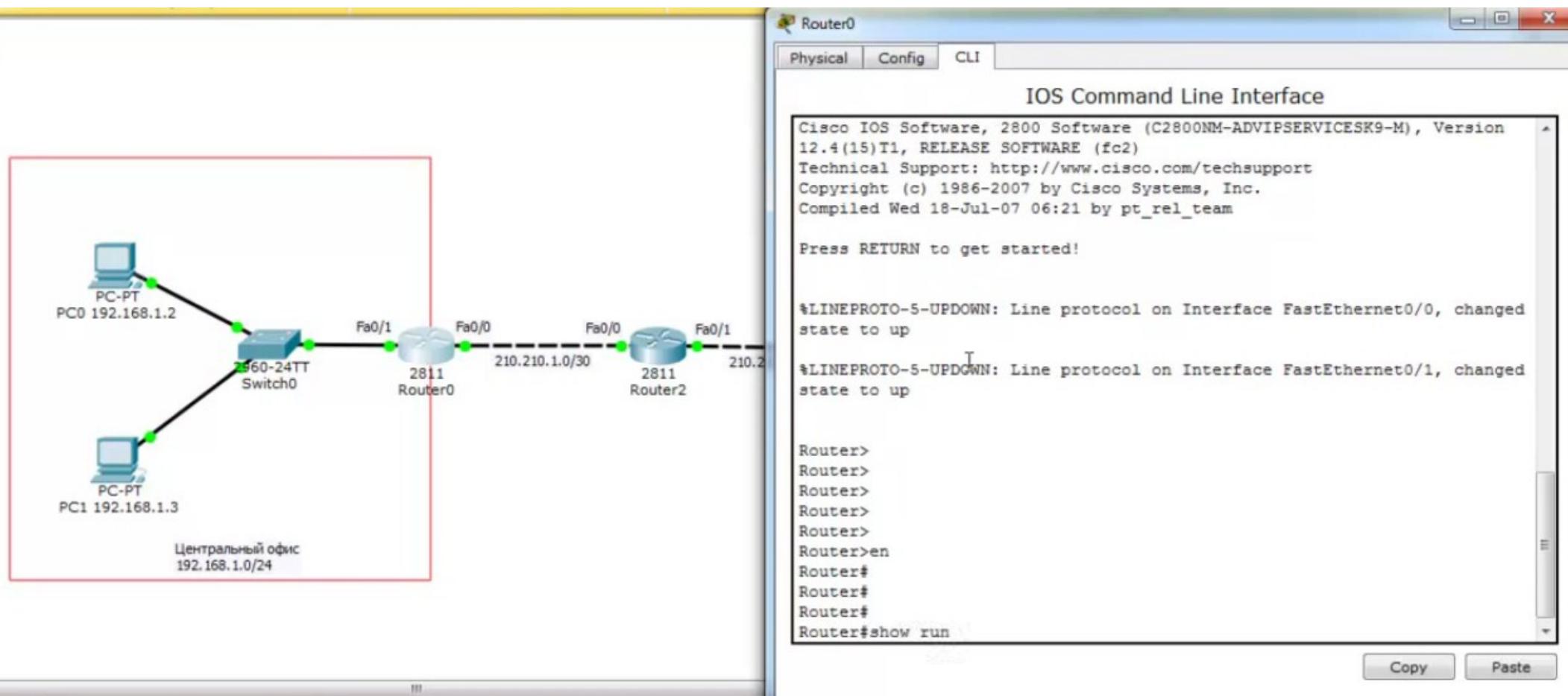
Более подробно о приведенных технологиях можно почитать [здесь](#) и [здесь](#)



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. The network diagram on the left illustrates a central office setup. It features a central Router0 (2811 model) connected to a Switch0 (2960-24TT) and another Router2 (2811 model). Router0 has two FastEthernet interfaces (Fa0/0 and Fa0/1) and a Serial interface (Serial0/0). Router2 also has two FastEthernet interfaces (Fa0/0 and Fa0/1). Two PCs, PC0 (192.168.1.2) and PC1 (192.168.1.3), are connected to the Switch0. A red box highlights the Router0 area. The text "Центральный офис 192.168.1.0/24" is displayed below the diagram. The right side shows the Router0 CLI window with the following content:

```
Router0
Physical Config CLI
IOS Command Line Interface
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!

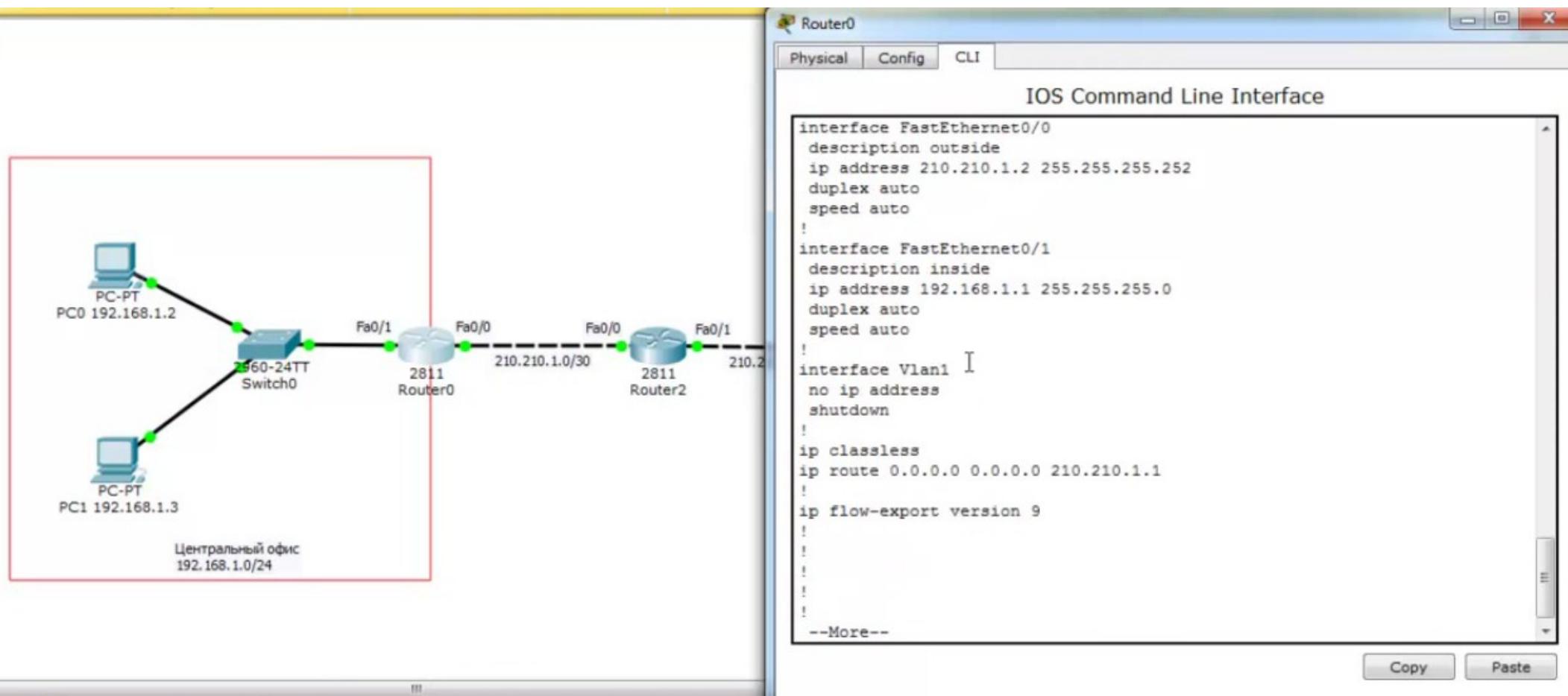
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

%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 for "Copy" and "Paste" are located at the bottom right of the CLI window.

На Router0 настроено 2 ip адреса, маршрут по умолчанию.



На Router0 настроим NAT

The diagram shows a network topology with a central Router0 and two external routers, Router1 and Router2. Router0 is connected to a Switch0 and two external routers. Router1 is connected to PC0 (192.168.1.2) and Router0. Router2 is connected to Router0 and PC1 (192.168.1.3). Router0 has two FastEthernet interfaces (Fa0/0, Fa0/1) and an access list (2811) applied to its Fa0/0 interface. The access list permits traffic from 192.168.1.0/24 and denies all other traffic. Router0 is configured with an IP address 210.210.1.0/30 on its Fa0/0 interface and 210.210.1.1 on its Fa0/1 interface. Router1 has an IP address 210.210.1.2 on its Fa0/0 interface and 210.210.1.3 on its Fa0/1 interface. Router2 has an IP address 210.210.1.4 on its Fa0/0 interface and 210.210.1.5 on its Fa0/1 interface. The network is labeled 'Центральный офис 192.168.1.0/24'.

The right side shows the 'Router0' window with the 'Config' tab selected. The 'IOS Command Line Interface' pane displays the configuration commands for setting up NAT on Router0:

```
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
```

Buttons for 'Copy' and 'Paste' are located at the bottom right of the CLI window.

На Router0 настроим NAT

The diagram shows a network topology. On the left, a red box encloses a PC-PT (IP 192.168.1.2) connected to a 60-24TT Switch0. Router0 (2811) is connected to Switch0 via Fa0/1 and to Router2 (2811) via Fa0/0. Router2 is connected to another device via Fa0/0 and to the right via Fa0/1. Router0 has an interface 210.210.1.0/30 connected to Router2. The text "Центральный офис 192.168.1.0/24" is written below the red box.

The right side shows the "Router0" window with the "Config" tab selected. The "IOS Command Line Interface" pane displays the following configuration script:

```
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)#

```

Buttons "Copy" and "Paste" are located at the bottom right of the CLI interface.

Сохраняем настройки

The diagram illustrates a network topology. On the left, a red box encloses a PC-PT (PC0) with IP 192.168.1.2, connected to a 260-24TT Switch0. The Switch0 is connected to Router0 (2811 model) via a Fa0/1 interface. Router0 is also connected to Router2 (2811 model) via a Fa0/0 interface. Router2 is connected to the Internet via a Fa0/0 interface with IP 210.210.1.0/30 and a Fa0/1 interface with IP 210.2. Router0 has a Fa0/0 interface with IP 210.210.1.0/30. The entire network is within a 'Центральный офис' (Central Office) with IP 192.168.1.0/24.

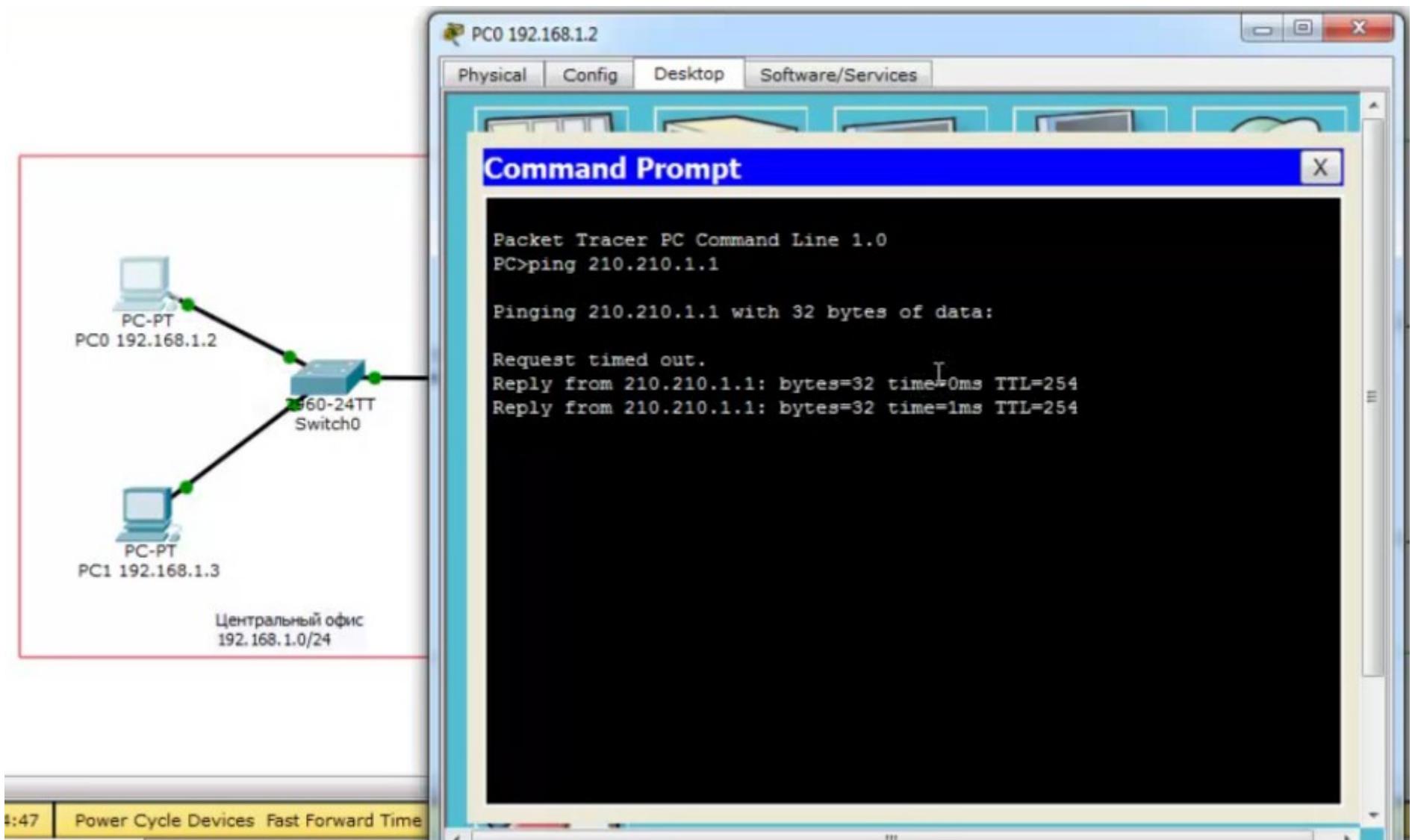
The right side shows the 'Router0' window with the 'Config' tab selected. The title bar says 'Router0' and the menu bar includes 'Physical', 'Config', and 'CLI'. The 'CLI' window displays the following configuration commands:

```
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#
```

At the bottom of the window are 'Copy' and 'Paste' buttons.

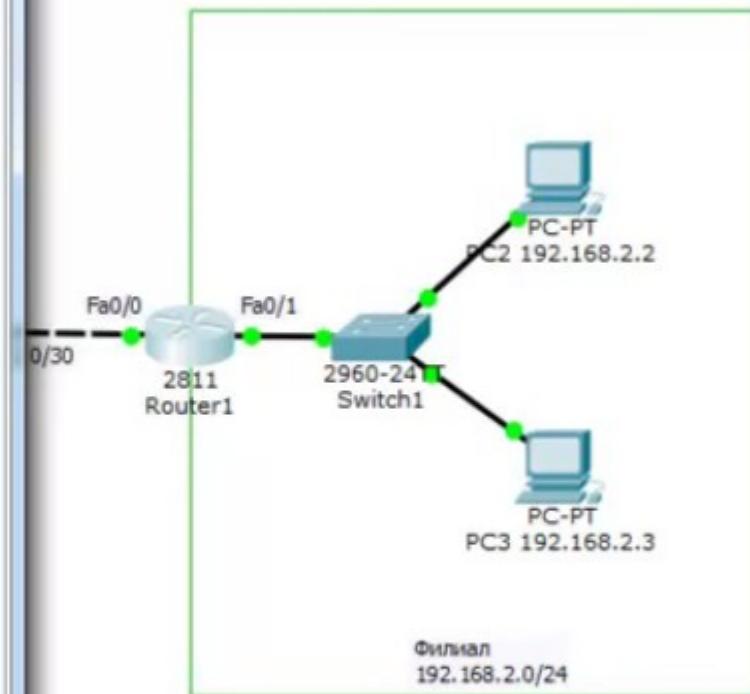
Проверяем доступ роутера провайдера с PC0. Доступно



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



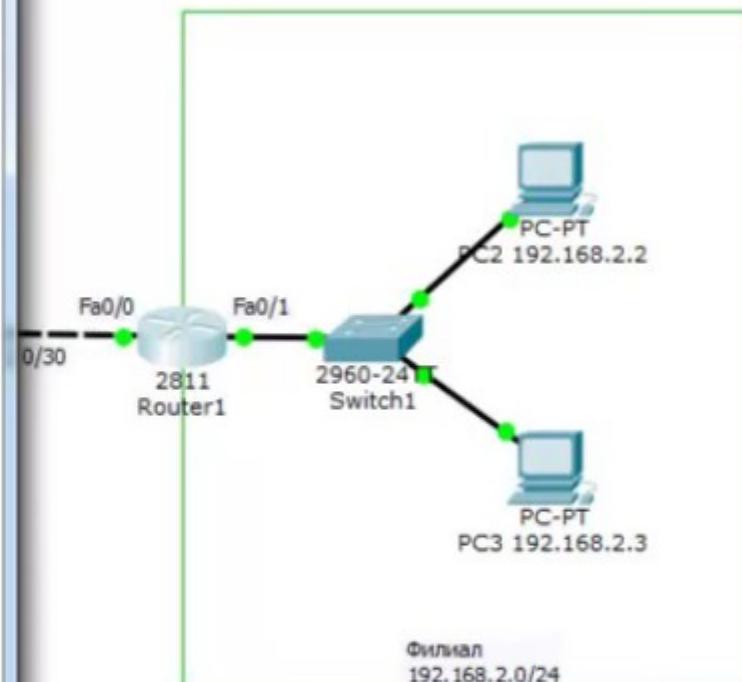
Настраиваем NAT на Router1 филиала, и сохраняем настройки.

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#
```



Филиал
192.168.2.0/24

Проверяем с PC2 доступность интерфейса провайдера

PC2 192.168.2.2

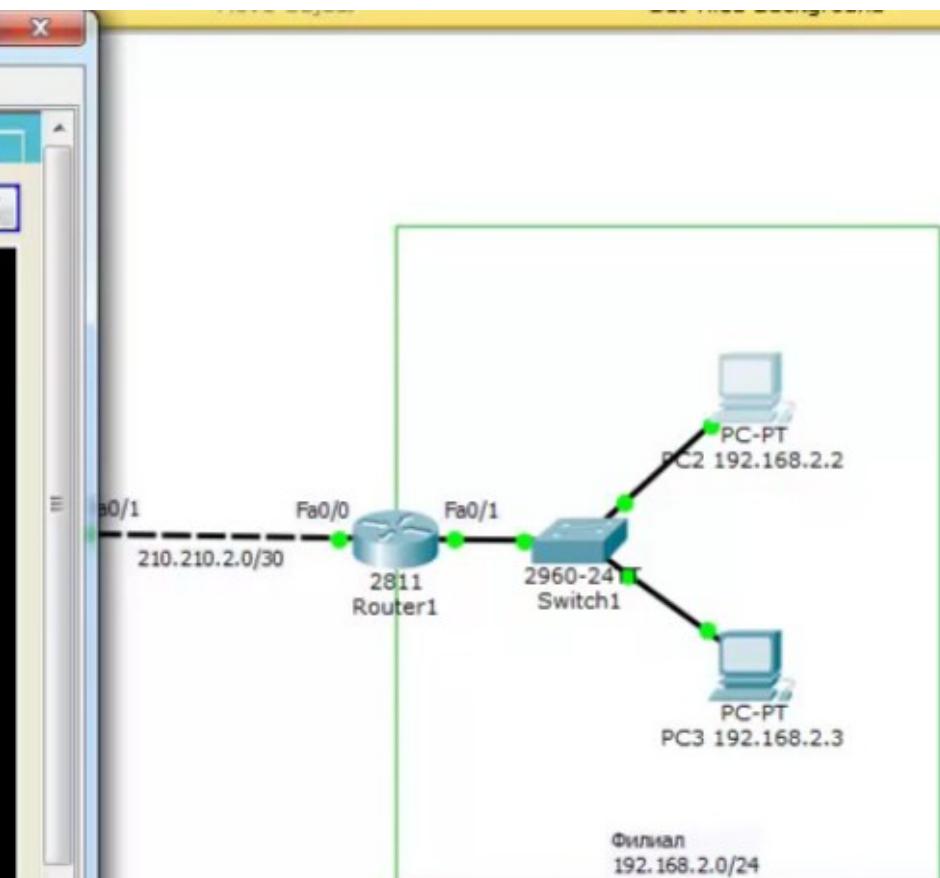
Physical Config Desktop Software/Services

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
```



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
```

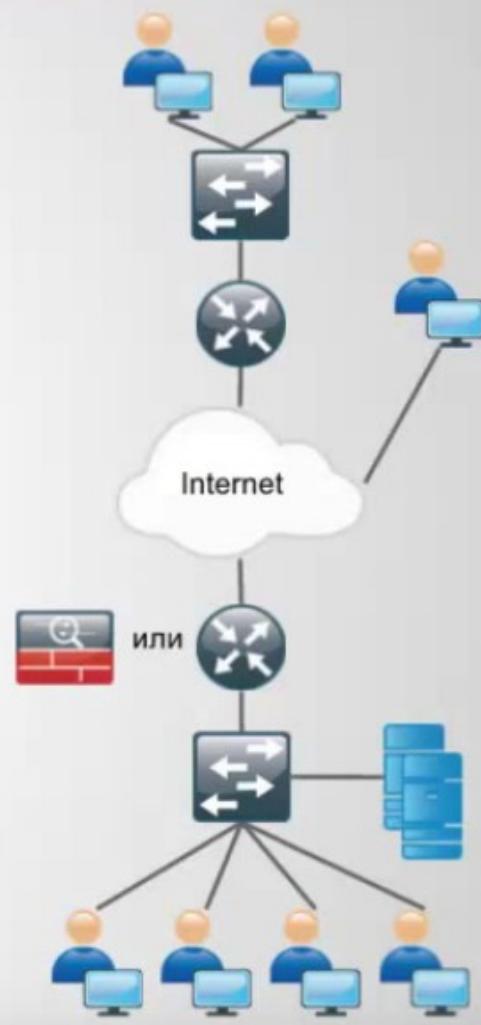
```
crypto map To-Site2 1 set security-association lifetime seconds
```

```
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. Практические

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
```

Router0

Physical Config CLI

IOS Command Line Interface

```
%SYS-5-CONFIG_I: Configured from console by console

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

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

сгурто мар СМАР 10 ipsec-isakmp

set peer 210.210.2.2

set transform-set TS

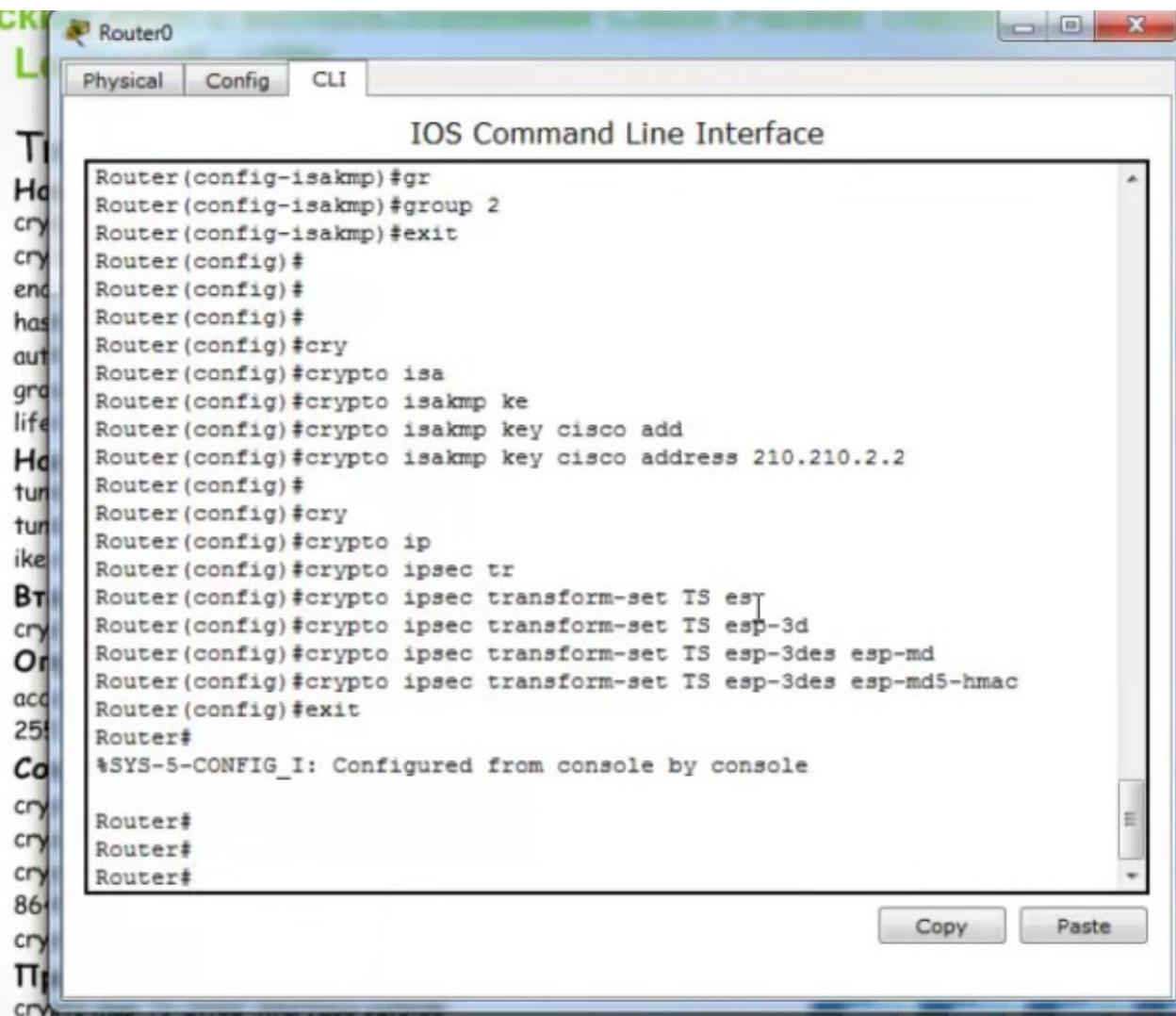
match address EOR-VR

Привязка к интерфейсу

Привязка к интерфейсу interface FastEthernet0/

interface FastEthernet0/0
crypto map CM4B

crypto map CMAP



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

Курс молодого бойца. Практическ

Типовые настройки роутера:

Настройка первой фазы

crypto isakmp policy 1

encr 3des

hash md5

authentication pre-share

group 2

Настройка ключа аутентификации и права

сокращение **isakmp key cisco address 210.210.2.2**

Сергей Захаров

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

hmac

Определяем какой трафик шифровать

ip access-list extended FOR-VPN

permit in 192.168.1.0 0.0.255 192.168.2.0 0.0.255

Создание криптокарты

Создание крипто карт
с помощью SM4R 10 inses-isakmp

crypto map CMAP 10
set peer 310.310.3.3

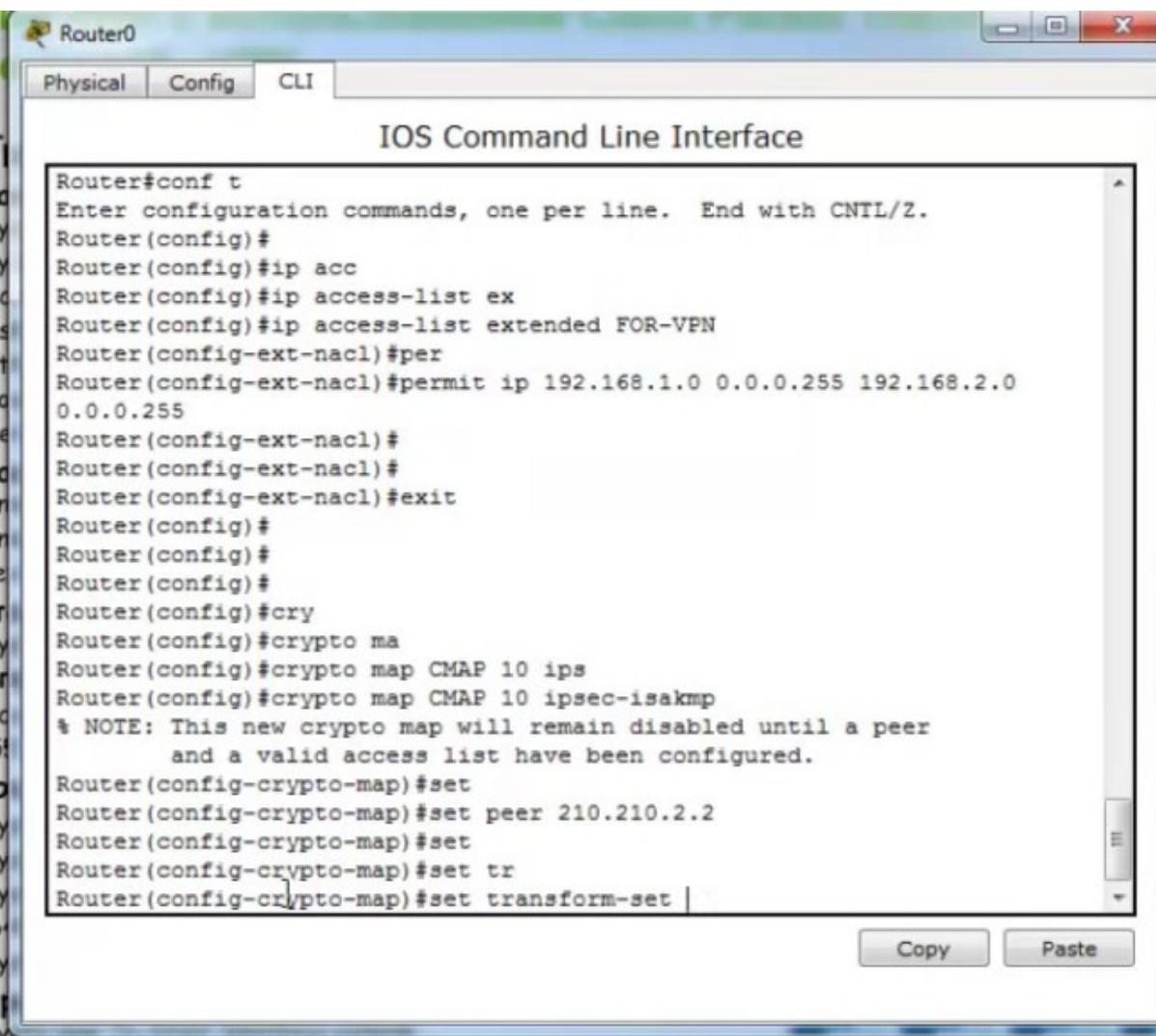
```
set peer 210.210.2.2
```

set transform-set 15

match address FOR-VPN

Привязка к интерфейсу

Interface FastEth



На Router0 создаем крипто-карту с настройками шифрования

КУРС МОЛОДОГО ВОИЦА. ПРАКТИЧЕСКИЙ

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 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

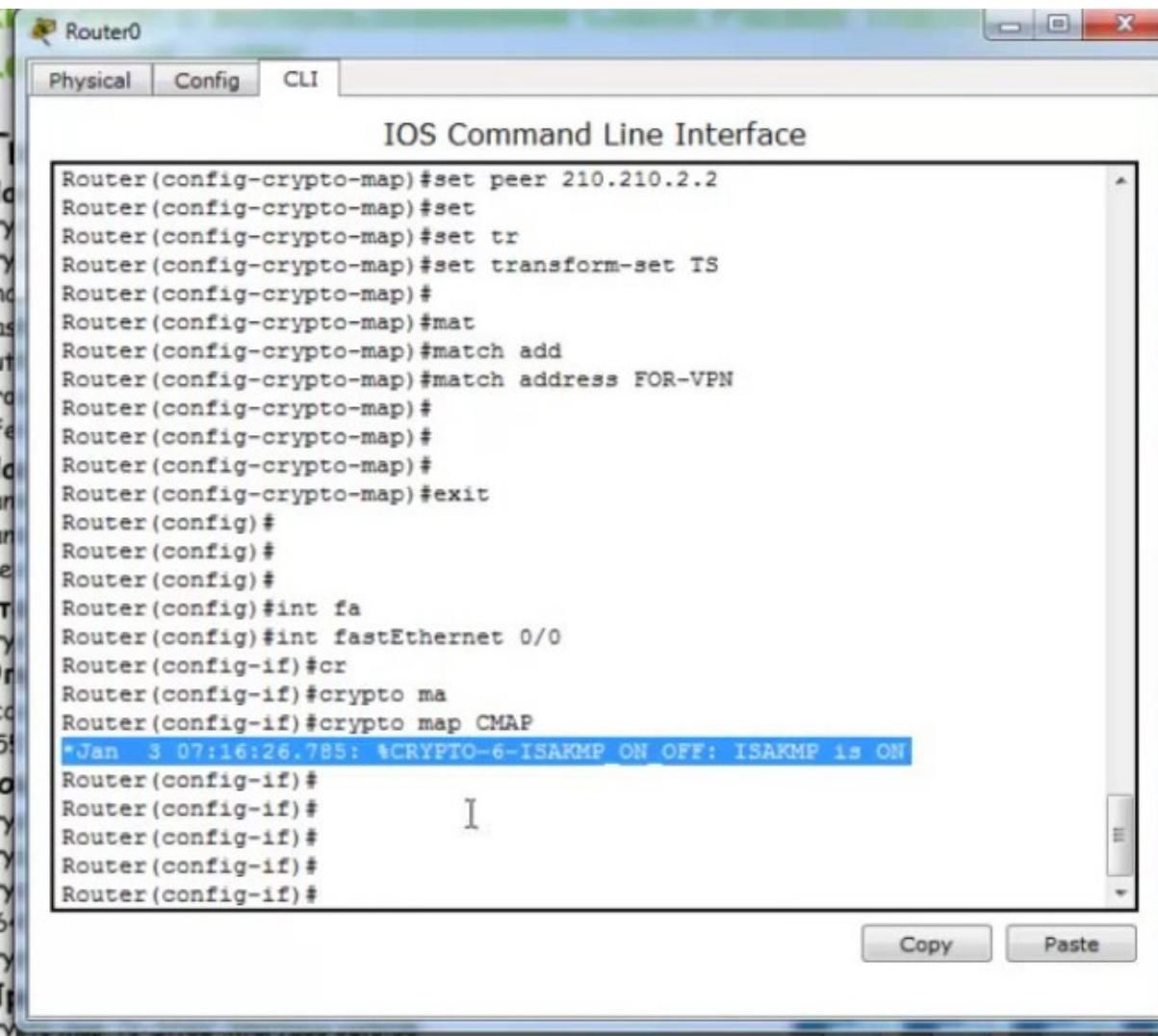
set transform-set TS

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

Router0

Physical Config CLI

IOS Command Line Interface

```
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-crypto-map)#
Router(config)#
Router(config)#
Router(config)#[
```

Copy Paste

Типовые настройки роутера:

Настройка первой фазы

crypto isakmp policy 1

enctr 3des

hash md5

authent

Настройка ключа симметрическими и публичными

Настройка ключа аутентификации и нир crypto isakmp key cisco address 210 210 2 2

Старт изации 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

set peer 210.210.2.2

set transform-set TS

match address FOR-VPN

Привязка к интерфейсу BusCAN

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

Курс молодого бойца. Практический
Lectures

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

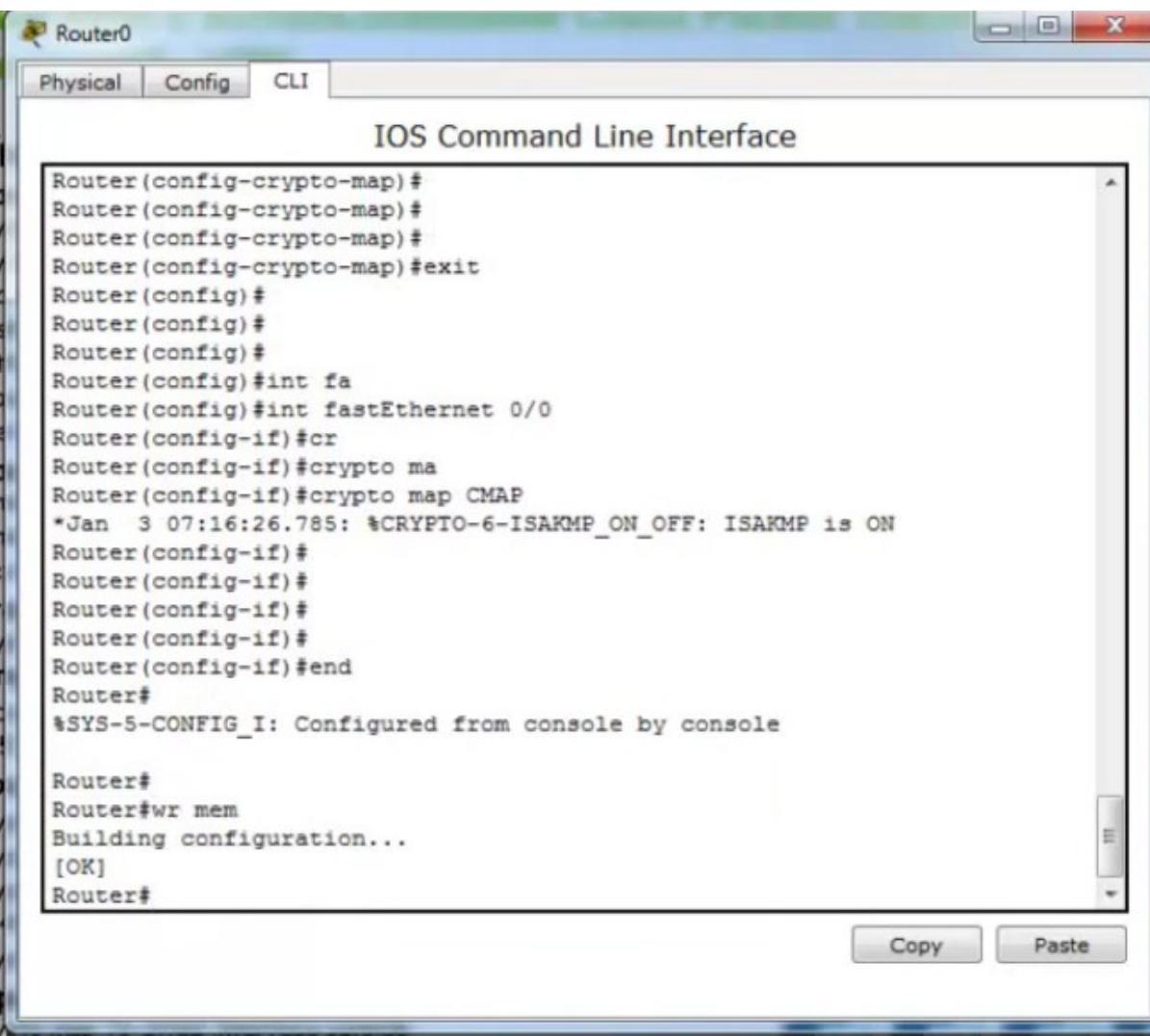
set transform-set TS

match address FOR-VPN

Привязка к интерфейсу

Привязка к интерфейсу interface FastEthernet0/0

interface system 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 пароля

```
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

СУВОРІ МЯР СМАР 10 ірsec-ізакмр

set peer 210.210.2.2

set transform-set TS

set transform-set 75
match address EOR-VPN

match address 1 ok-win

Привязка к интерфейсу FastEth

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#
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 md5
Router(config-isakmp)#aut
Router(config-isakmp)#authentication pre
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#gr
Router(config-isakmp)#group 2
Router(config-isakmp)#
Router(config-isakmp)#
Router(config-isakmp)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#

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 peer
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 0.0.0.255 192.168.2.0 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

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.
```

210.210.2.0/30

2811 Router1

2960-24 Switch1

Филиал 192.168.2.0/24

PC-PT 192.168.2.2

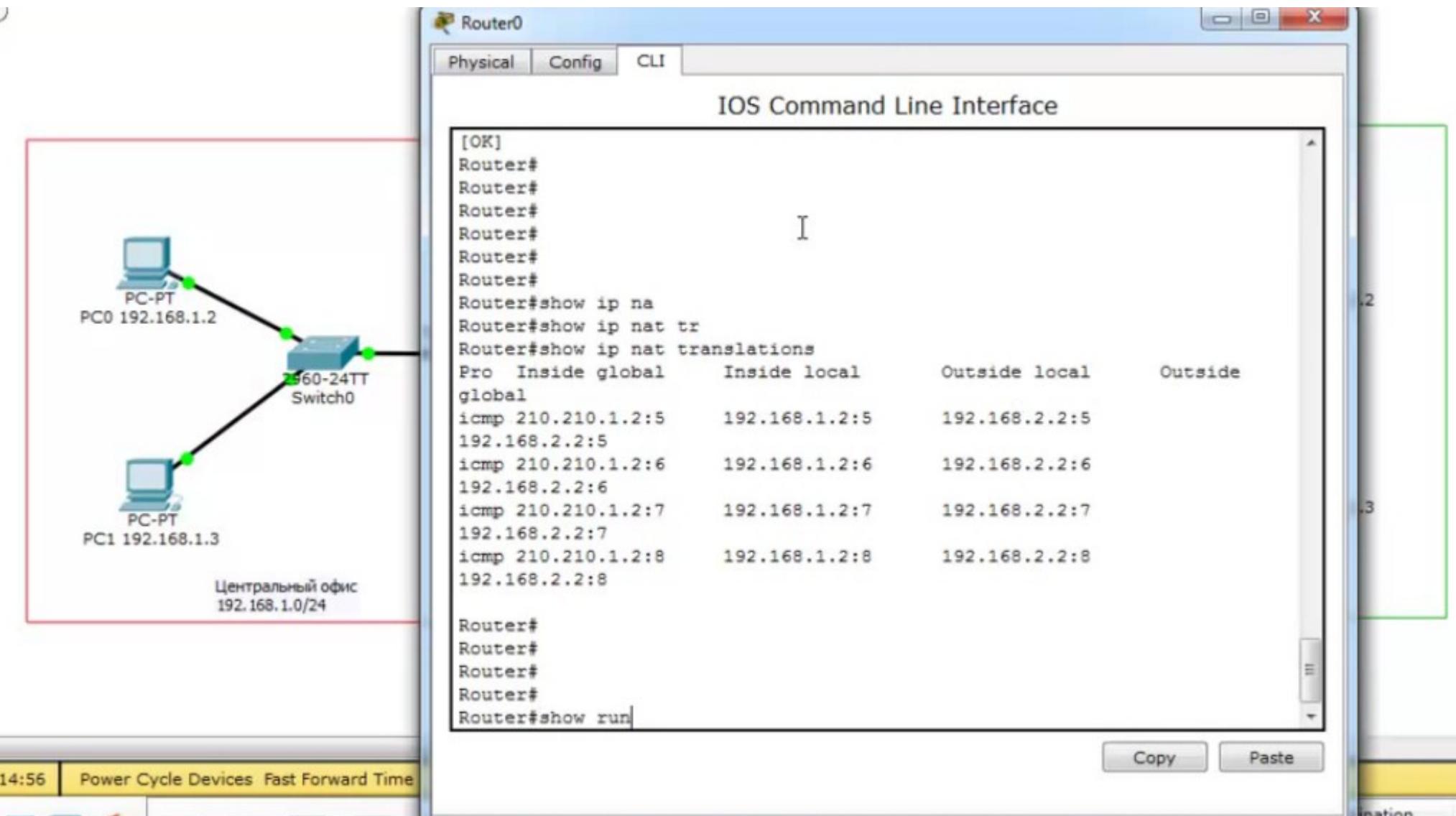
PC-PT 192.168.2.3

PC2 192.168.2.2

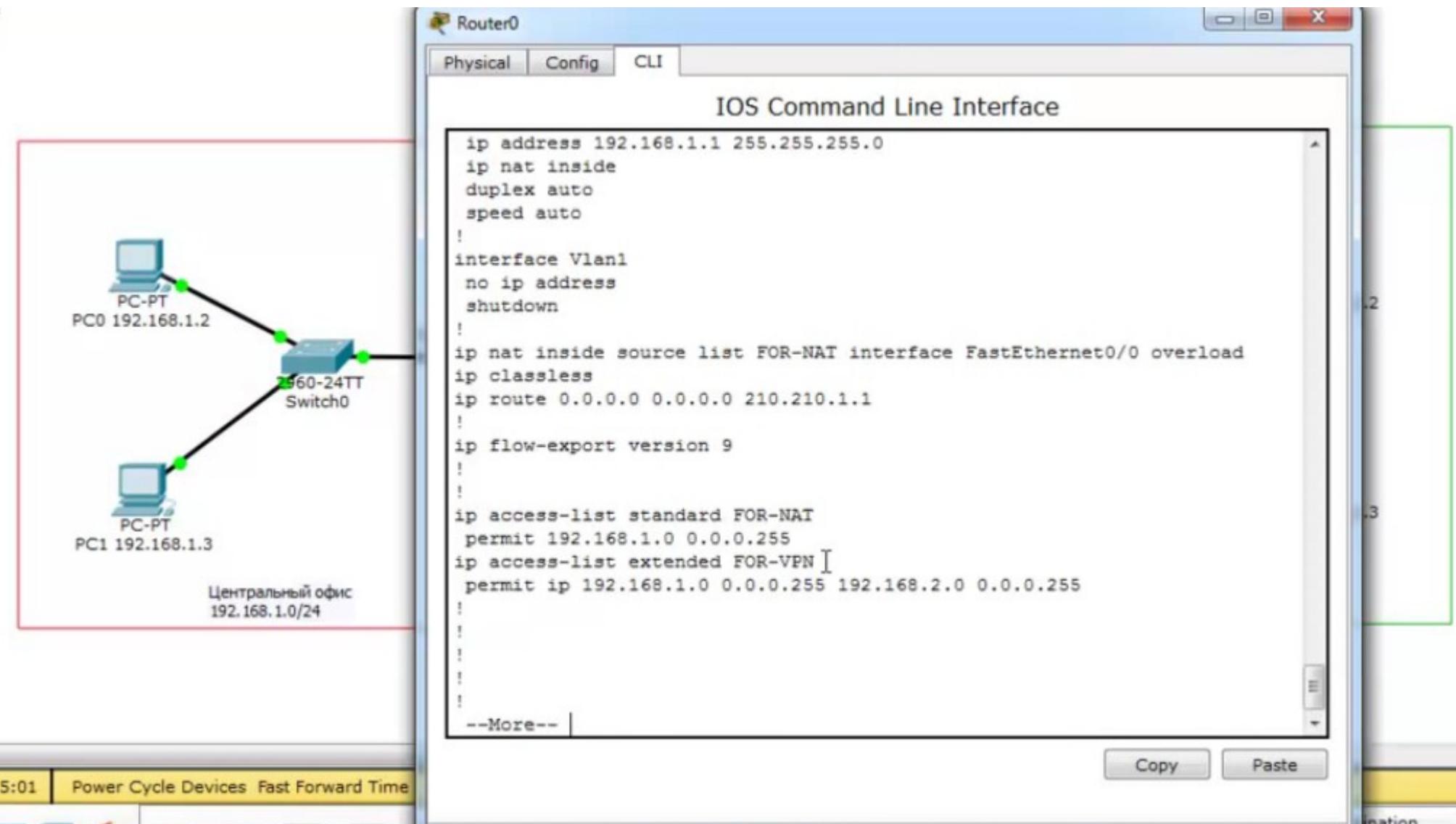
PC3 192.168.2.3

Fire Last Status Source Destination T

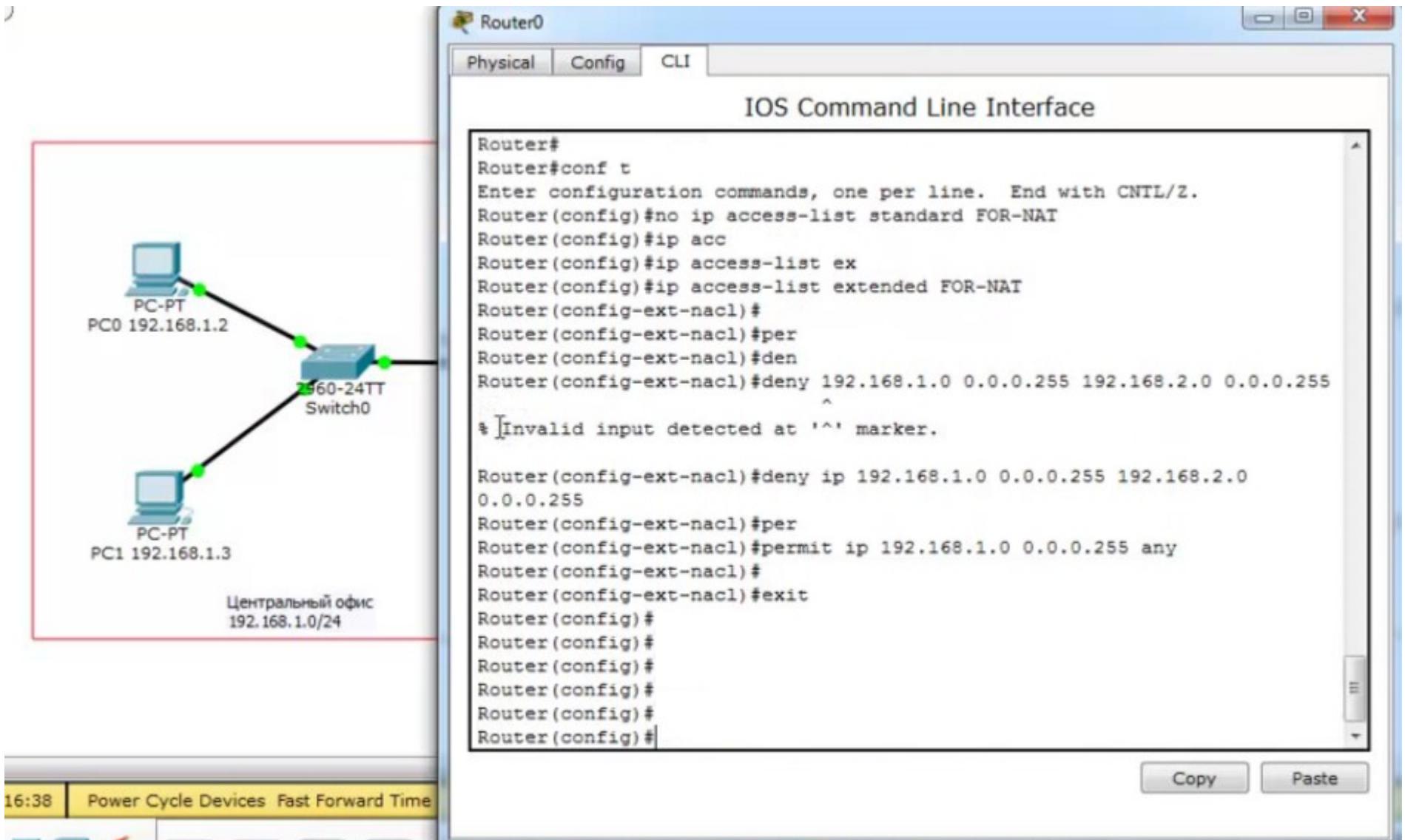
Смотрим настройки NAT на Router0. Траффик, который должен идти в VPN-канал, попадает под преобразования NAT. Посмотрим настройки access-list



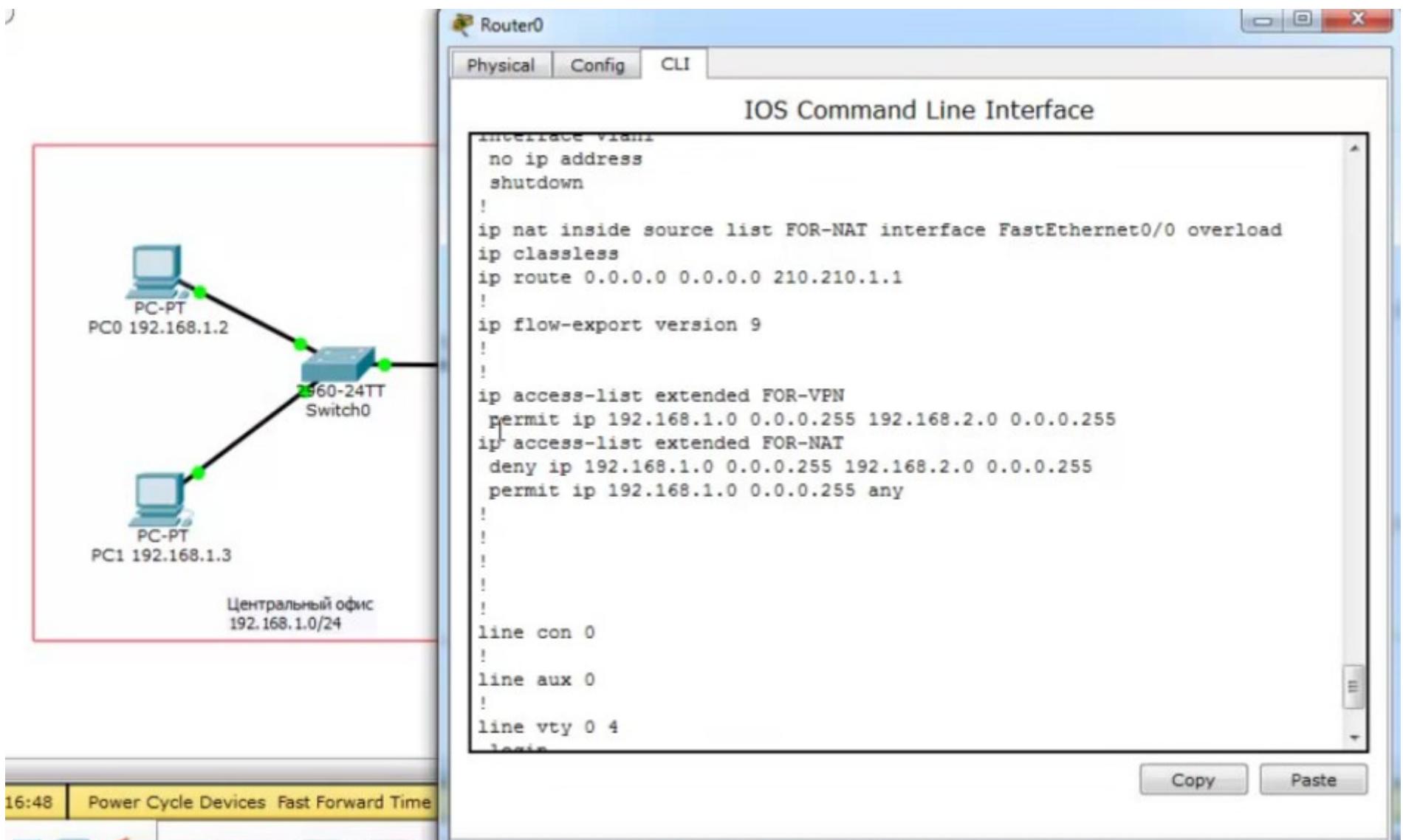
Под действие access-list попадает весь траффик 192.168.1.0, а это не совсем то, что нам нужно



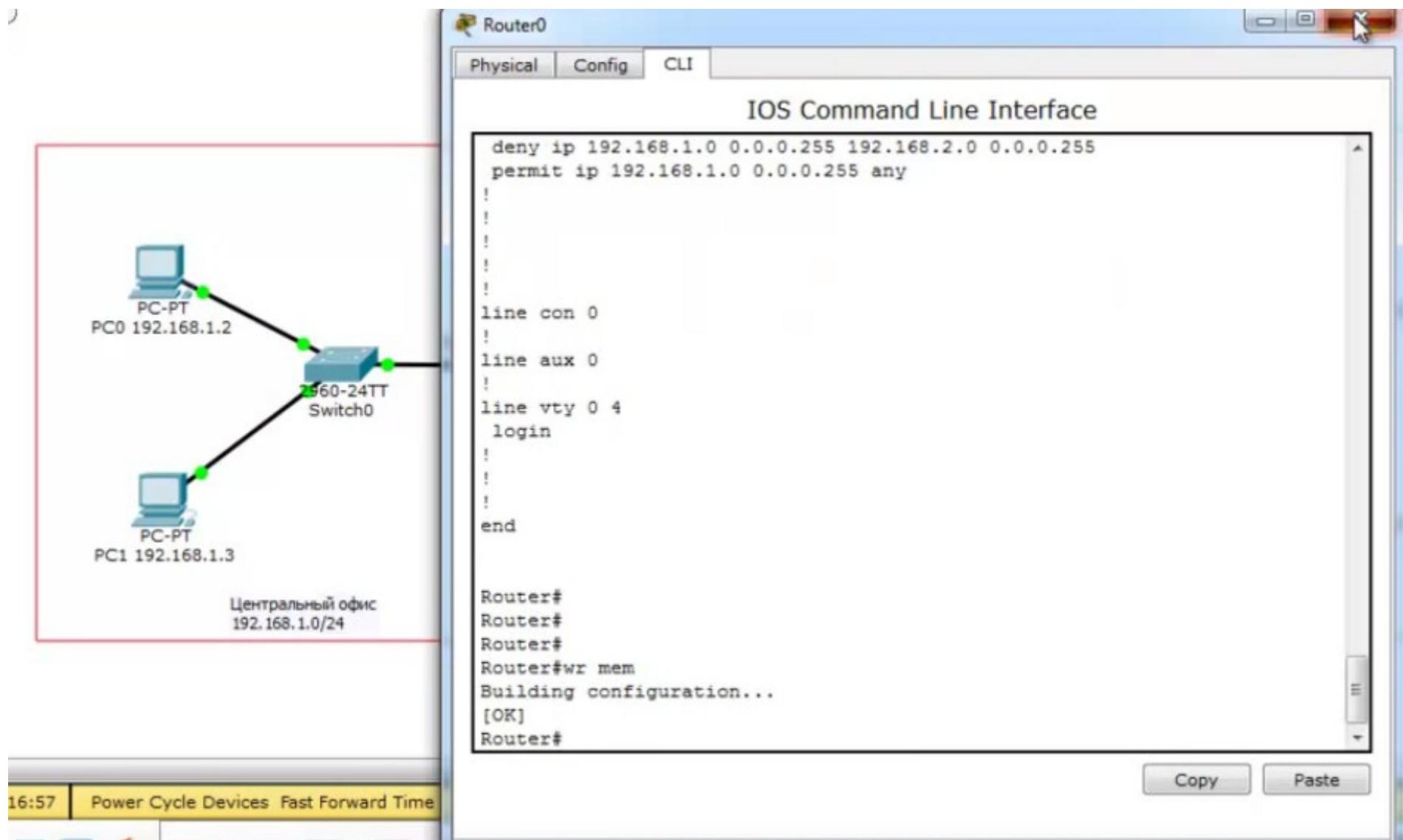
Удалим существующий access-list, добавим исправленный



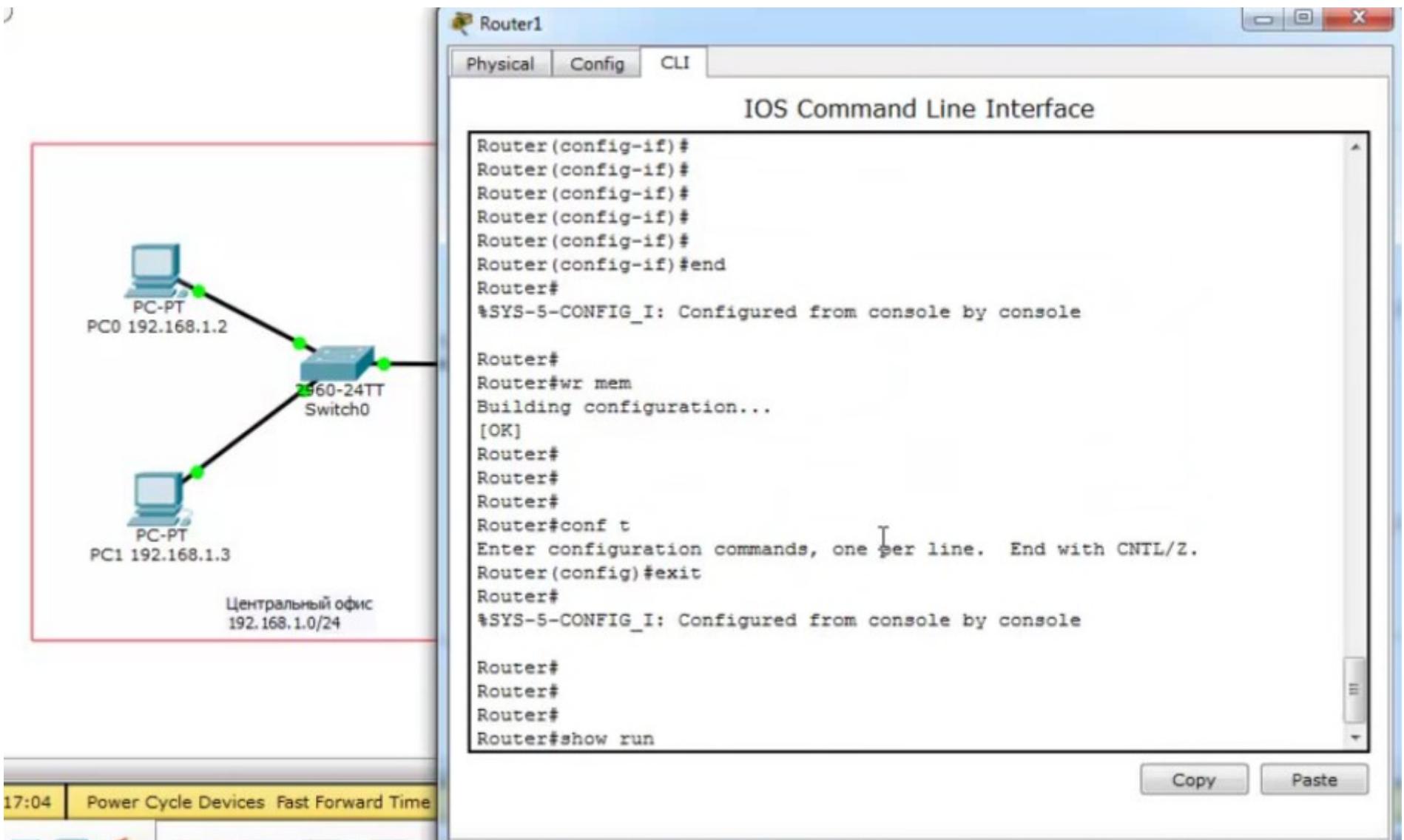
Проверим получившиеся настройки



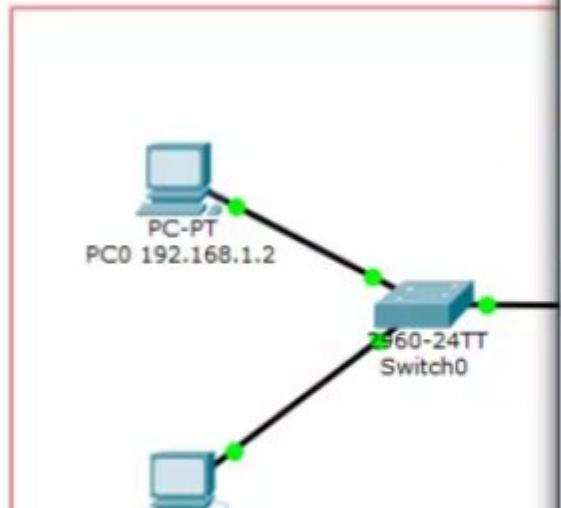
Сохраняем



Зайдем на Router1 филиала, для выполнения тех же операций



Удалим существующий access list



The diagram illustrates a network topology. On the left, a red box represents the 'Центральный офис' (Central Office) with an IP address of 192.168.1.0/24. Inside the box, two PCs are connected to a '560-24TT Switch0'. One PC is labeled 'PC-PT' with IP 192.168.1.2, and the other is labeled 'PC1' with IP 192.168.1.3. An arrow points from the switch to a 'Router1' device on the right. The Router1 window shows the following configuration:

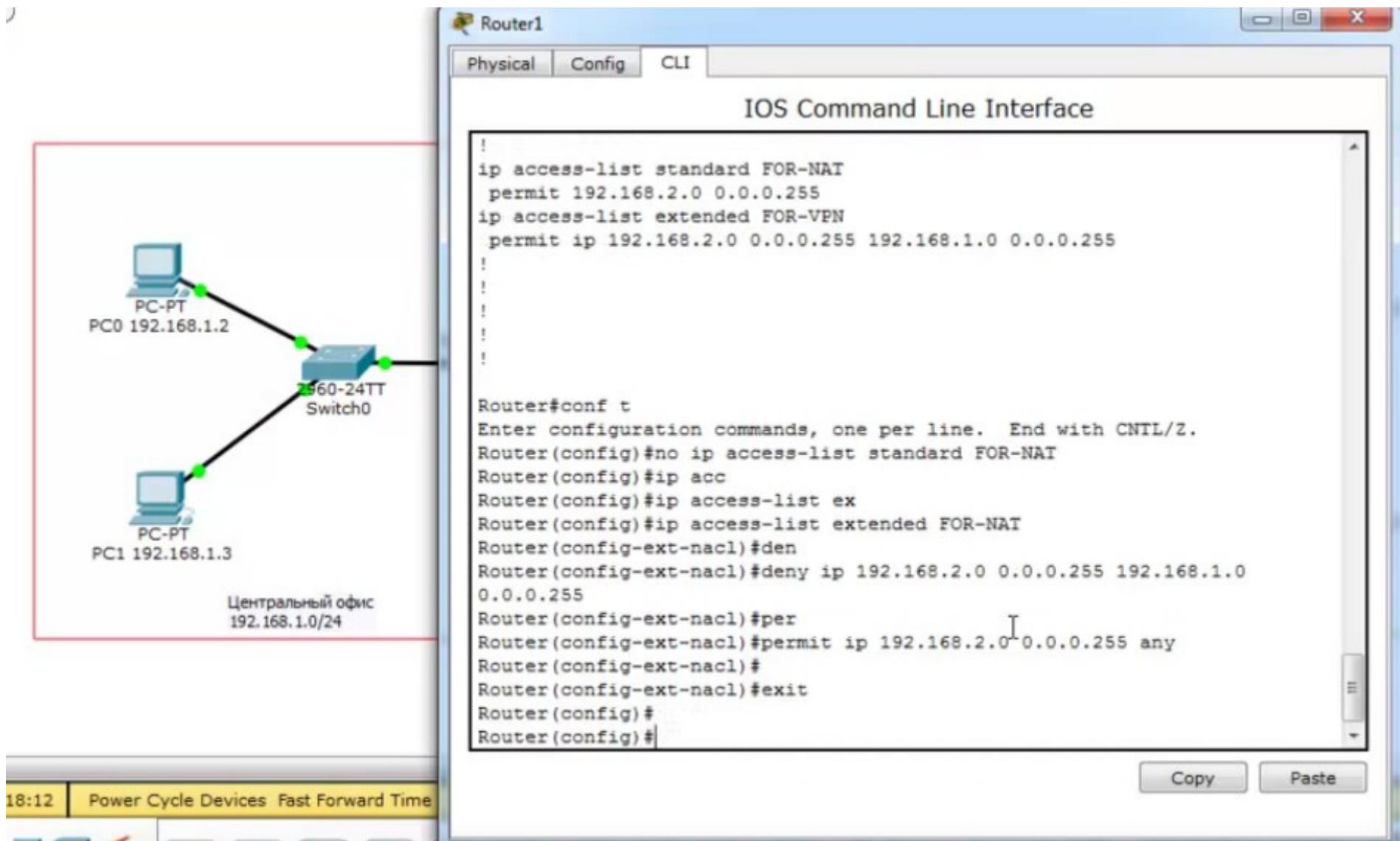
```
Router1
Physical Config CLI
IOS Command Line Interface

!
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)#

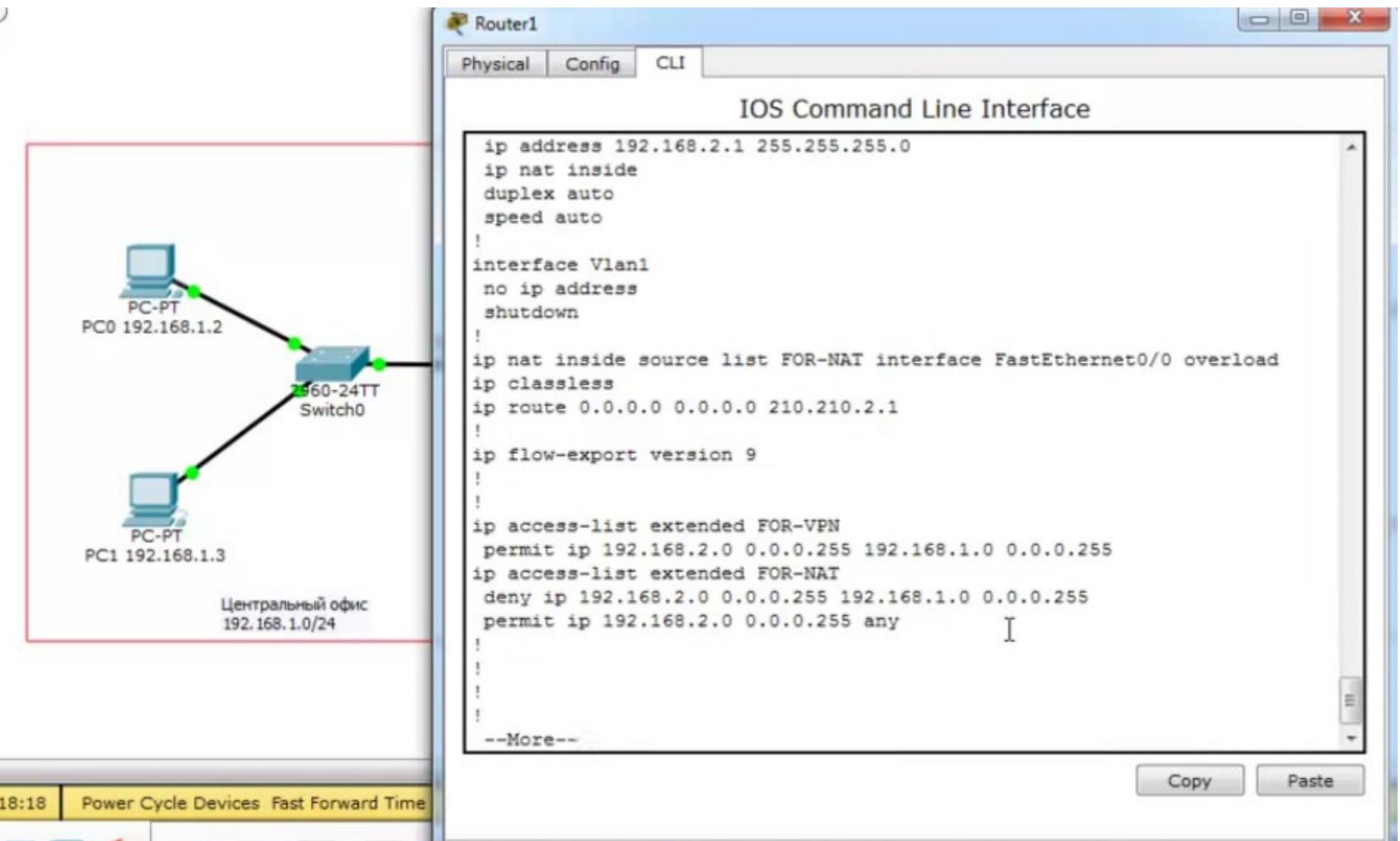
```

At the bottom of the Router1 window, there are 'Copy' and 'Paste' buttons. The status bar at the bottom left shows the time as 17:18 and includes buttons for 'Power Cycle Devices' and 'Fast Forward Time'.

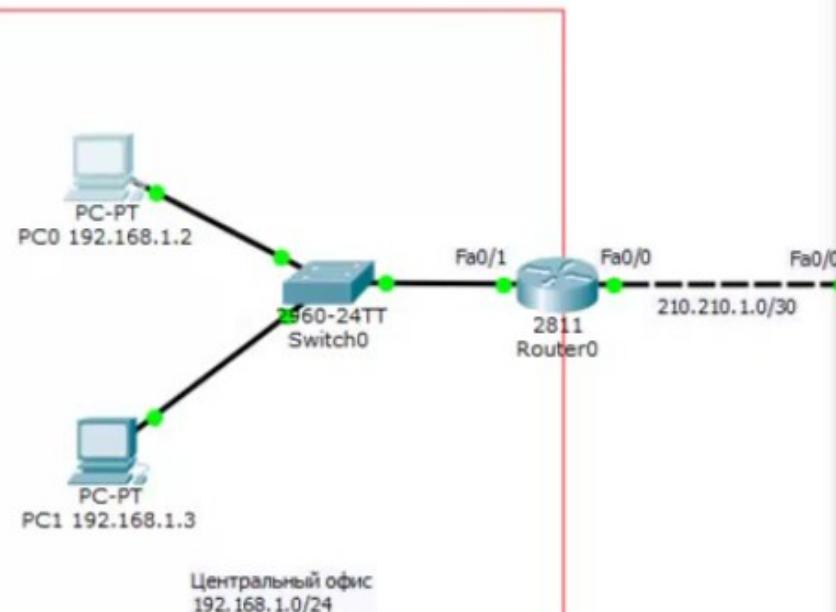
и создадим расширенный



Проверим получившиеся настройки



Проверим ping с PC0 на PC2 - идет



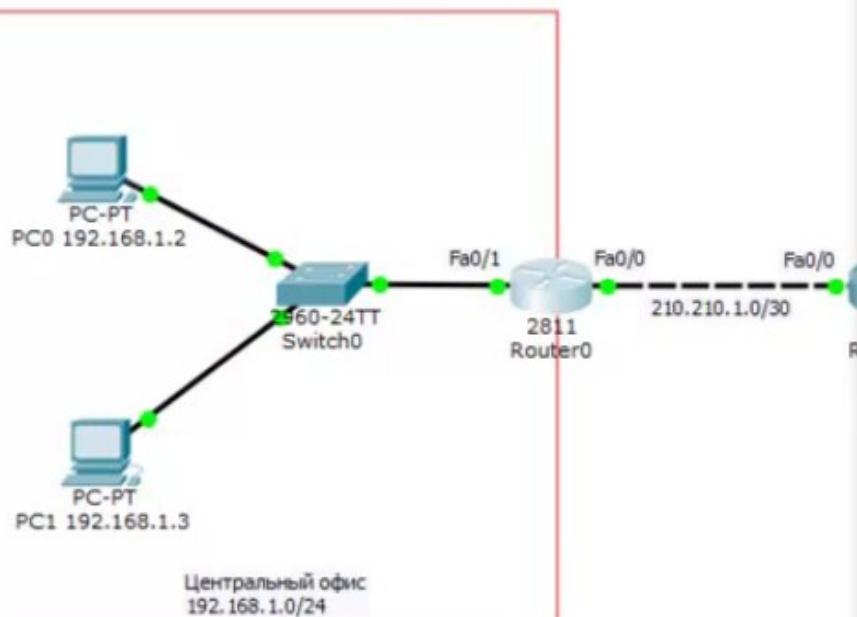
PC0 192.168.1.2

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



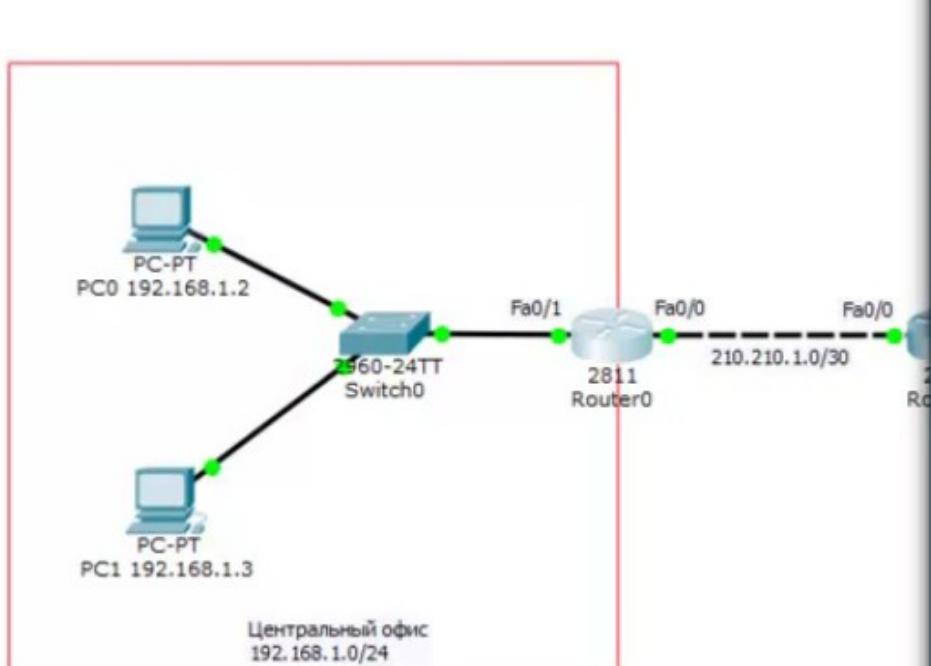
Router#
Router#
Router#
Router#wr mem
Building configuration...
[OK]
Router#
Router#
Router#
Router#
Router#
Router#show isa
Router#show cry
Router#show crypto isa
Router#show crypto isakmp sa
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id slot status
210.210.2.2 210.210.1.2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

IPv6 Crypto ISAKMP SA

Router#

Copy Paste

и наличие ipsec VPN тоннеля



Router0

Physical Config CLI

IOS Command Line Interface

```
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)

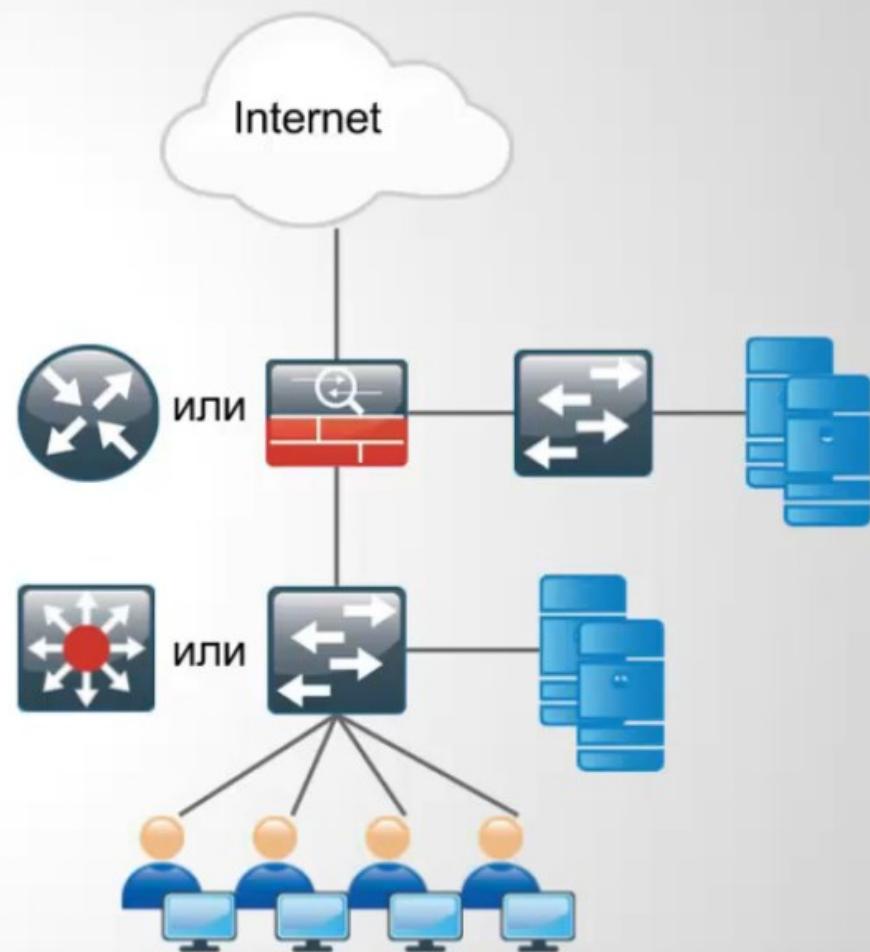
Как правило выделяют минимум три зоны:

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

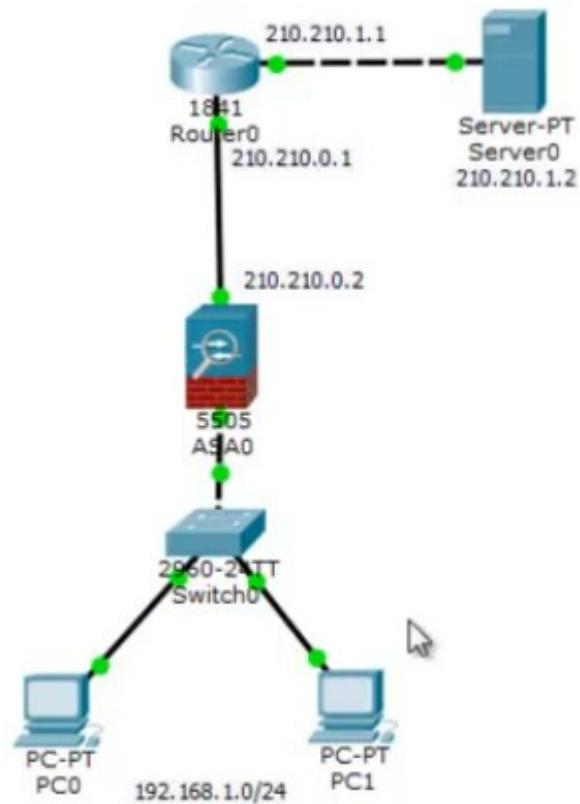
И три основные политики взаимодействия зон:

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

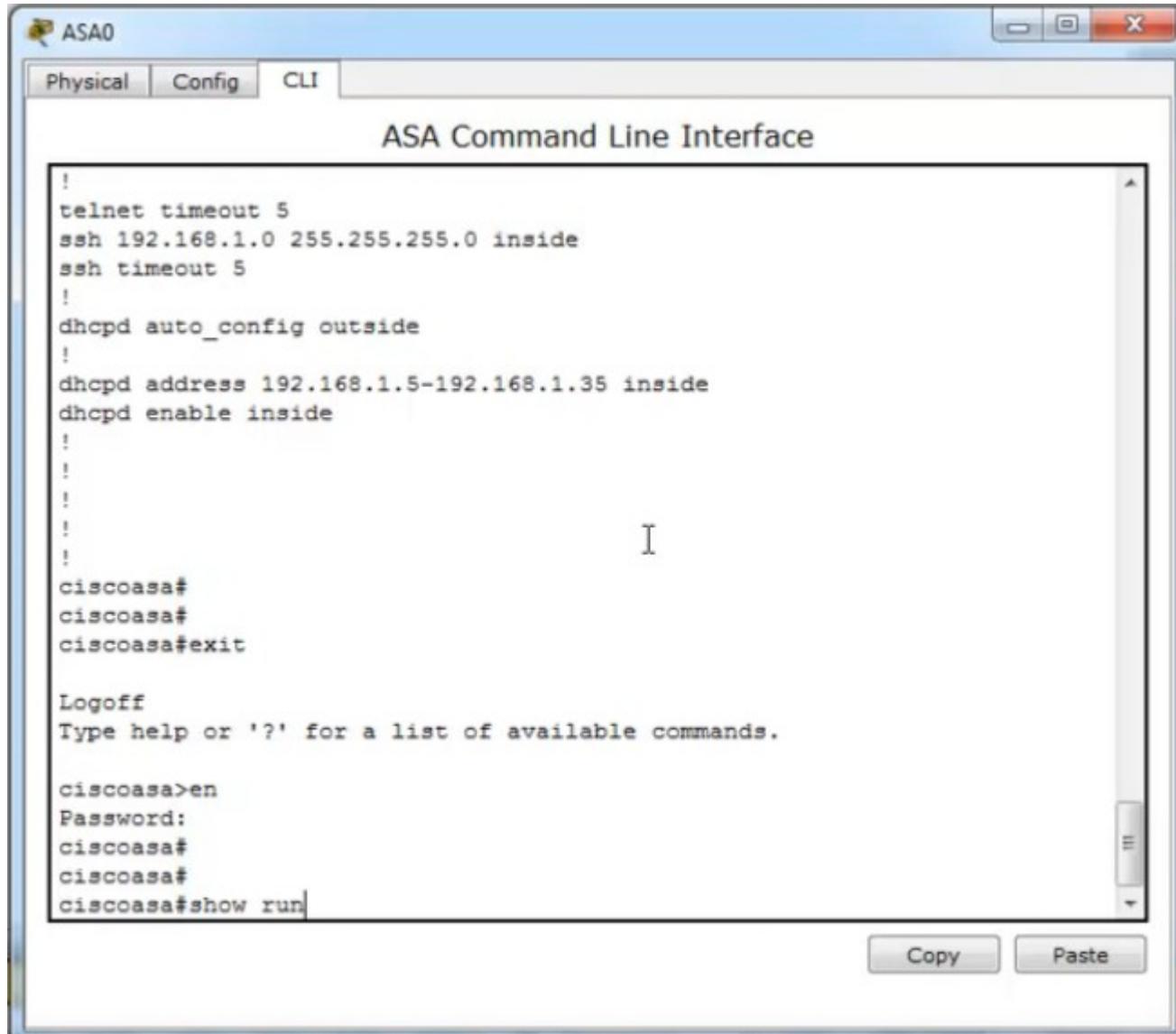
Более подробно о приведенных технологиях можно почитать [здесь](#), [здесь](#), [здесь](#) и [здесь](#)



Изначально используется схема Cisco ASA



На asa0 настроен пароль cisco



ASA Command Line Interface

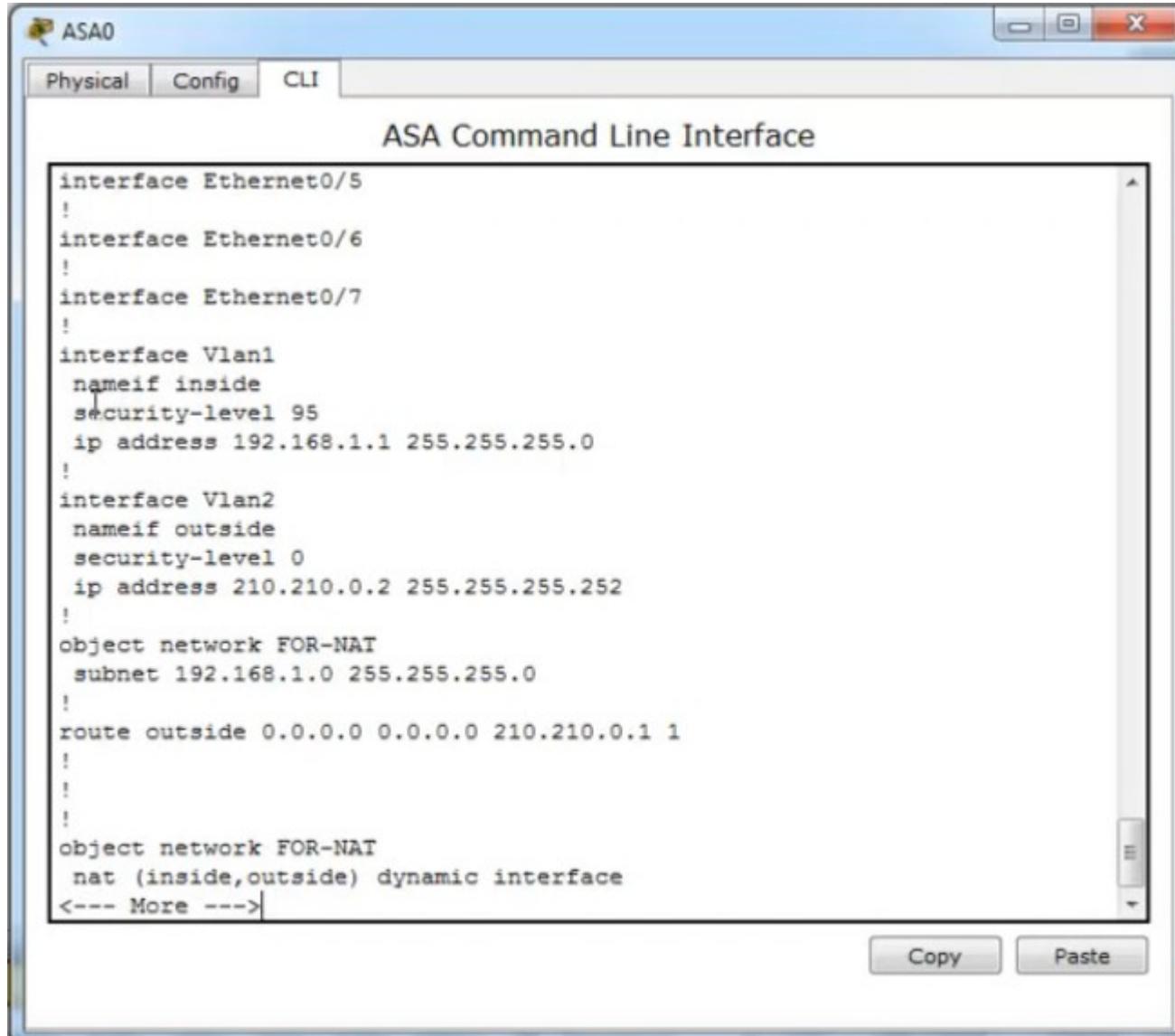
```
!
telnet timeout 5
ssh 192.168.1.0 255.255.255.0 inside
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.35 inside
dhcpd enable inside
!
!
!
!
!
!
ciscoasa#
ciscoasa#
ciscoasa#exit

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

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

Copy Paste

На asa0 настроен NAT

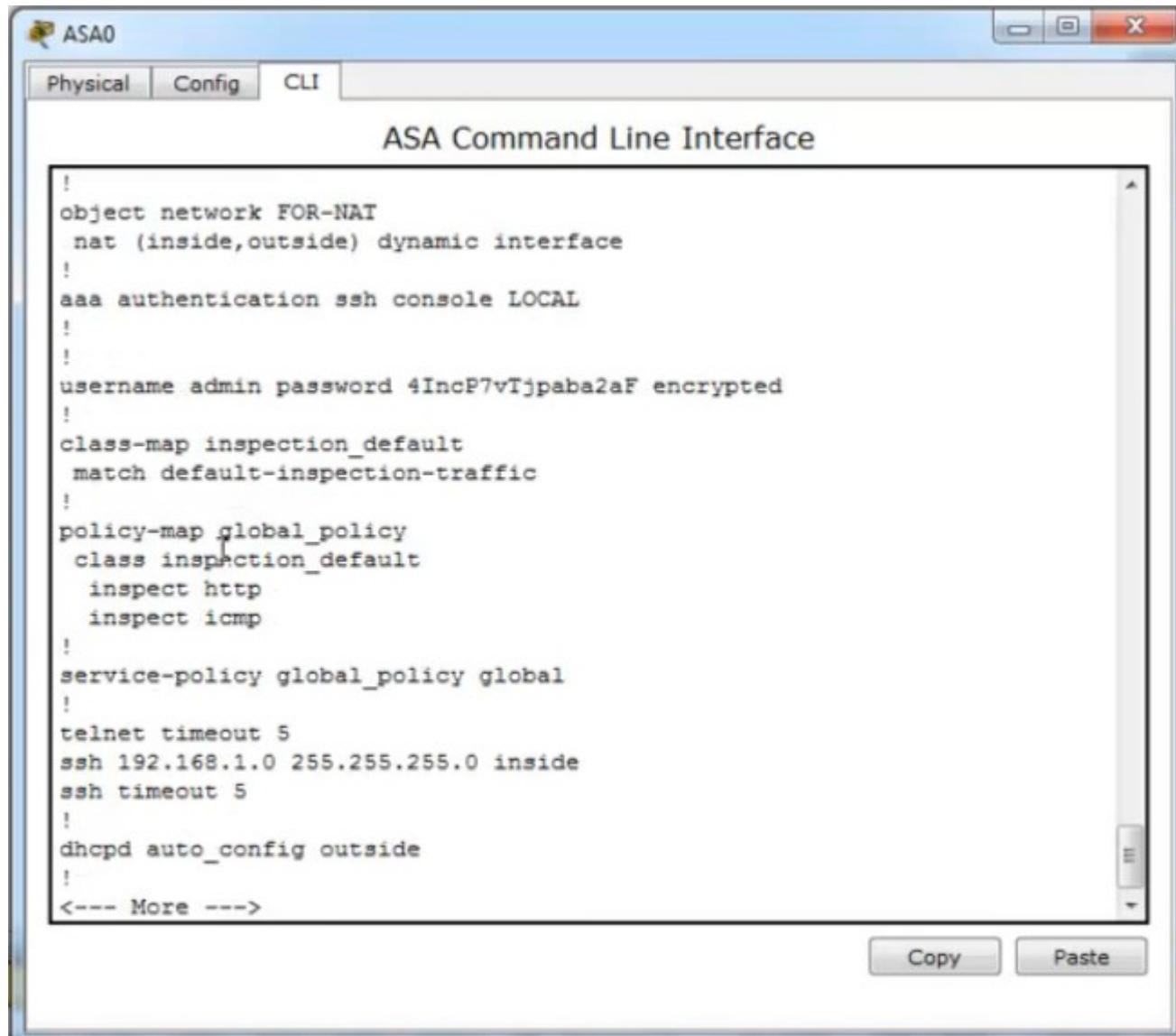


The image shows a screenshot of the ASA Command Line Interface (CLI) window for ASA0. The window title is "ASA0". The tab bar at the top has "Physical", "Config", and "CLI" tabs, with "CLI" being the active tab. The main area is titled "ASA Command Line Interface". The configuration text is as follows:

```
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 CLI window, there are "Copy" and "Paste" buttons.

На asa0 настроено инспектирование трафика

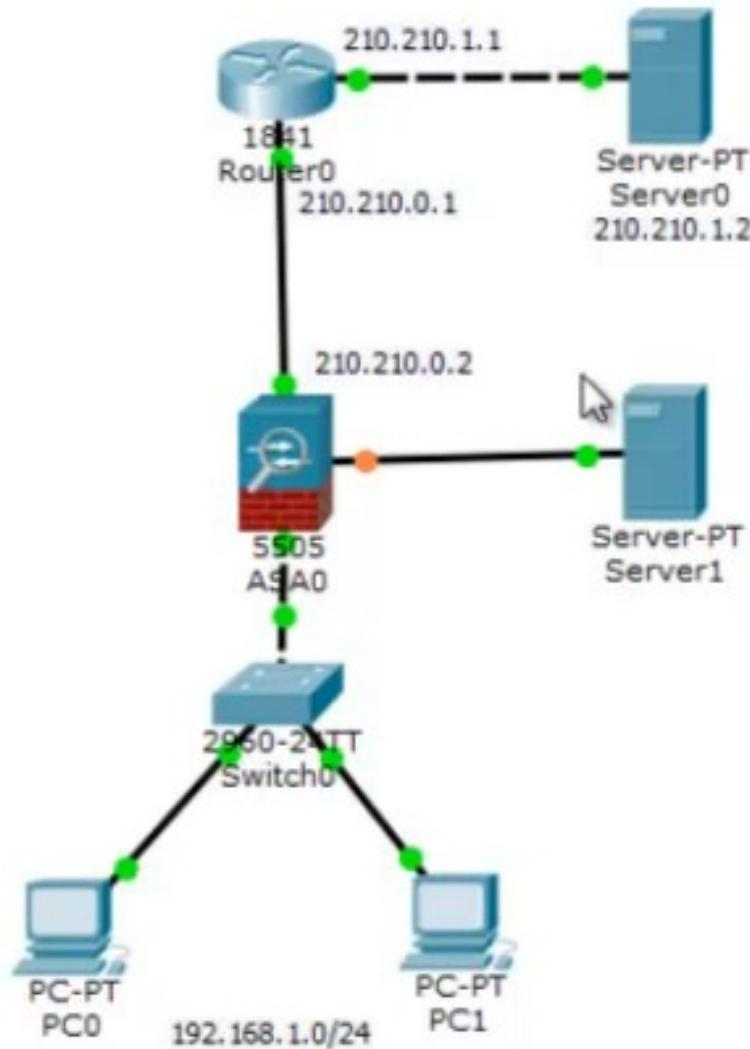


The image shows a screenshot of the ASA Command Line Interface (CLI) window. The window title is "ASA0" and the tab selected is "CLI". The main area displays the following configuration script:

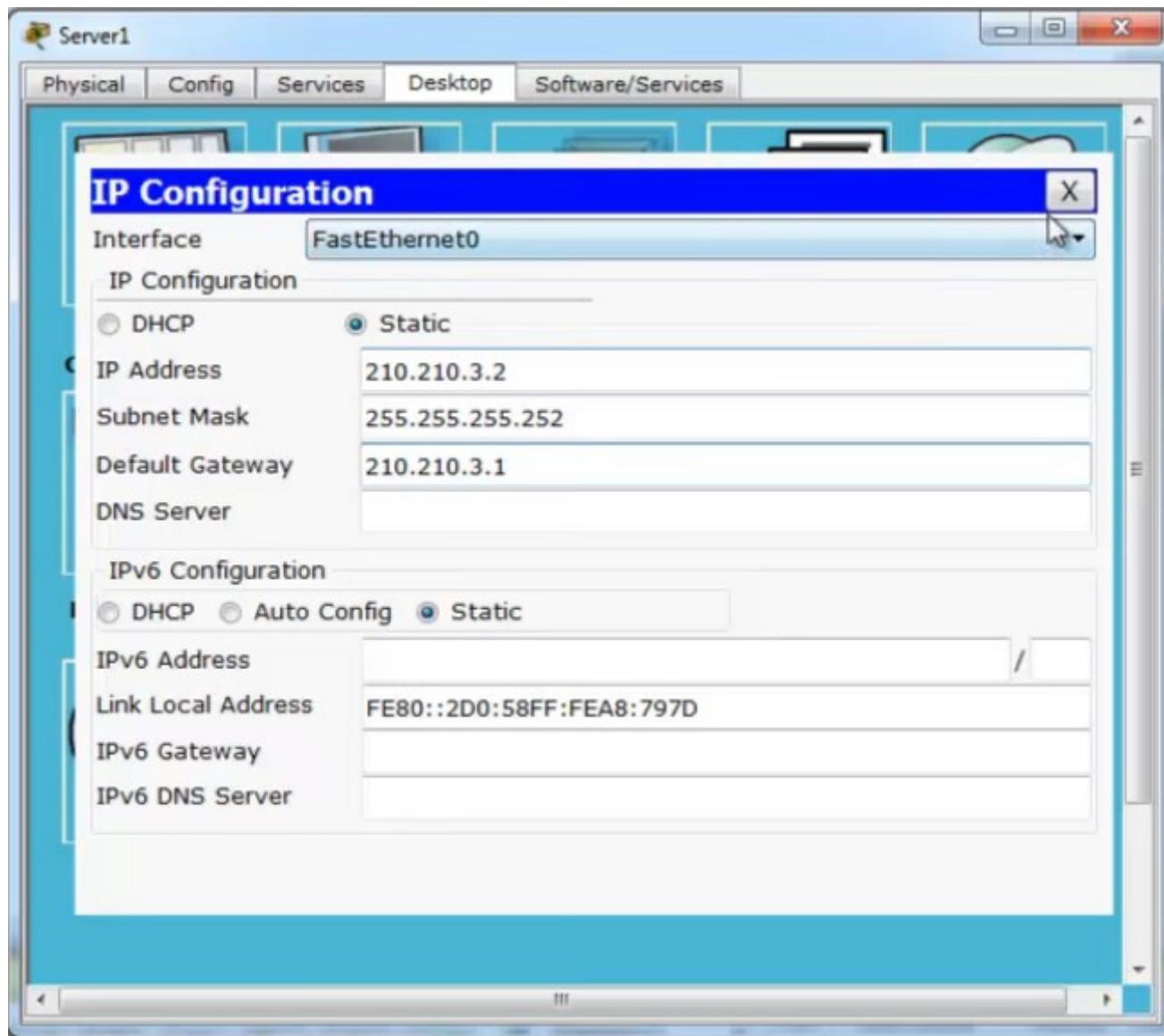
```
!
object network FOR-NAT
    nat (inside,outside) dynamic interface
!
aaa authentication ssh console LOCAL
!
!
username admin password 4Incp7vTjpaba2af encrypted
!
class-map inspection_default
    match default-inspection-traffic
!
policy-map global_policy
    class inspection_default
        inspect 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 of the window, there are "Copy" and "Paste" buttons.

Добавим Server1, который мы будем выделять в DMZ



Зададим серверу Server1 статический ip адрес



Добавим маршрут к Server1 на Router0

Router0

Physical Config CLI

IOS Command Line Interface

```
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up

Router>
Router>
Router>
Router>en
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 210.210.3.0 255.255.255.252 210.210.0.2
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#
```

Copy Paste

The network diagram illustrates a topology with the following components and connections:

- Router0** (labeled 1841) is connected to **Switch0** (labeled 2960-24TT) and to **Server-PT Server0** (IP 210.210.1.1).
- Switch0** is connected to **PC-PT PC0** (IP 192.168.1.1) and **PC-PT PC1** (IP 192.168.1.2).
- Server-PT Server1** (IP 210.210.1.2) is connected to **Switch0**.
- Server-PT Server0** (IP 210.210.1.1) is connected to **Router0**.

A path from Router0 to Server1 is highlighted in red, indicating the route being configured.

Посмотрим конфигурацию ASA

ASA0

Physical Config CLI

ASA Command Line Interface

```
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
!
dhcpd address 192.168.1.5-192.168.1.35 inside
dhcpd enable inside
!
!
!
!
!
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#show ver
```

Copy Paste

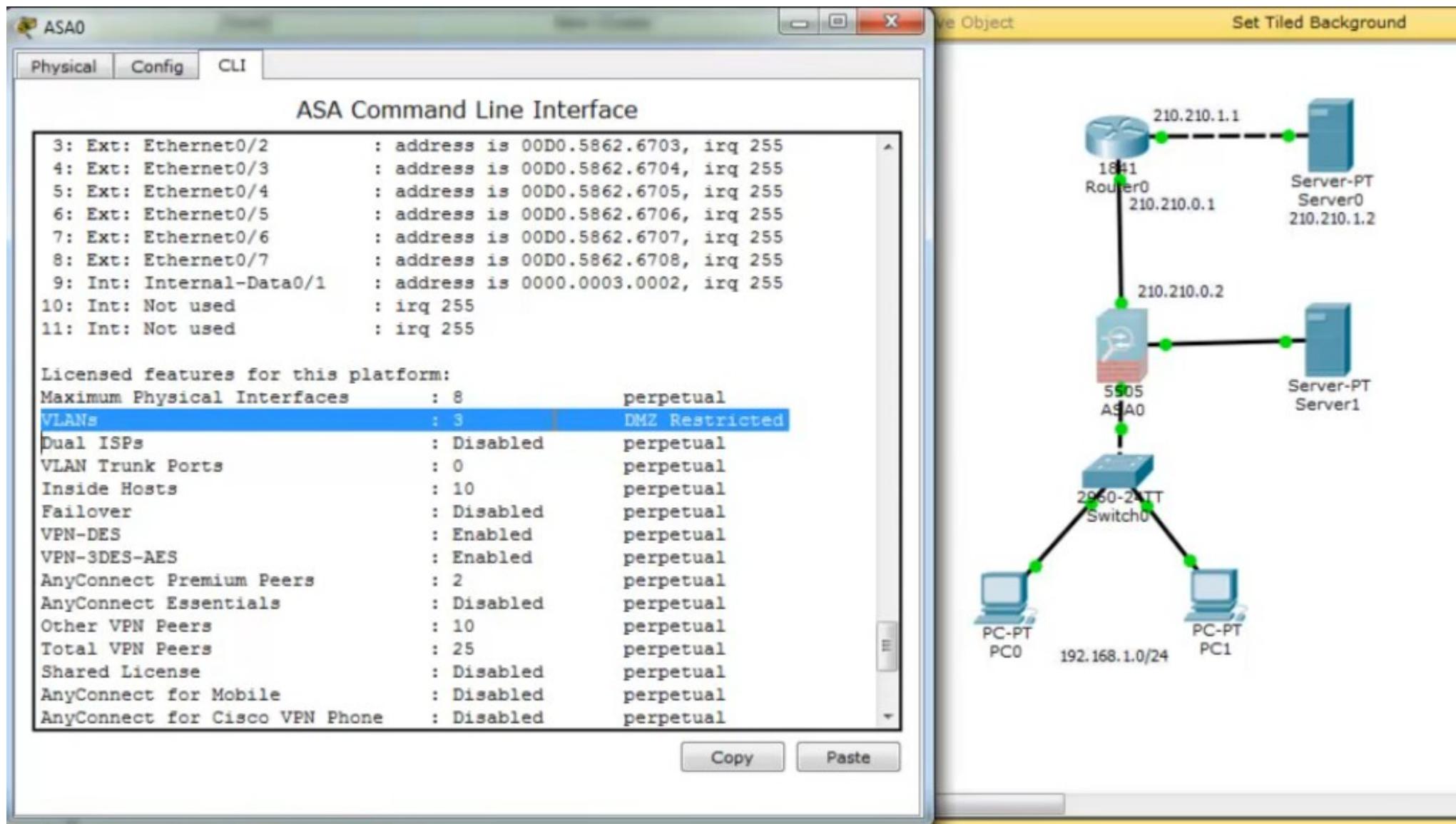
Live Object Set Tiled Background

The network diagram illustrates a topology with the following components and connections:

- Router0** (18.41.210.1.1) is connected to **ASA0** (5.05.210.210.0.1) and **Switch0** (20.60-24.TT.210.210.0.2).
- ASA0** (5.05.210.210.0.1) is connected to **Switch0** (20.60-24.TT.210.210.0.2) and **PC-PT PC0**.
- Switch0** (20.60-24.TT.210.210.0.2) is connected to **PC-PT PC1** and **Server-PT Server1**.
- Server-PT Server0** (210.210.1.2) is connected to **Router0** (18.41.210.1.1).
- Server-PT Server1** (210.210.1.2) is connected to **Switch0** (20.60-24.TT.210.210.0.2).

IP address 192.168.1.0/24 is assigned to the interface connecting ASA0 to the switch.

У нас доступно только 3 VLAN и ограниченный DMZ



Определим новый VLAN3, и получаем ошибку, что на ASA нельзя использовать больше 2 интерфейсов без no forward из-за ограничений лицензии оборудования

ASA0

Physical Config CLI

ASA Command Line Interface

```
ciscoasa#  
ciscoasa#  
ciscoasa#  
ciscoasa#conf t  
ciscoasa(config)#  
ciscoasa(config)#  
ciscoasa(config)#  
ciscoasa(config)#eth  
ciscoasa(config)#int eth0/2  
ciscoasa(config-if)#  
ciscoasa(config-if)#  
ciscoasa(config-if)#sw  
ciscoasa(config-if)#switchport acc  
ciscoasa(config-if)#switchport access vl  
ciscoasa(config-if)#switchport access vlan 3  
ciscoasa(config-if)#  
ciscoasa(config-if)#exit  
ciscoasa(config)#int vla  
ciscoasa(config)#int vlan 3  
ciscoasa(config-if)#  
ciscoasa(config-if)#name  
ciscoasa(config-if)#nameif dmz  
ERROR: This license does not allow configuring more than 2 interfaces  
with nameif and without a "no forward" command on this interface or on 1  
interface(s) with nameif already configured.  
ciscoasa(config-if)#

```

Copy Paste

Live Object Set Tiled Background

The network diagram illustrates the physical connections between the ASA0, Router0, and Switch0 devices. Router0 is connected to ASA0 and two servers (Server0 and Server1). ASA0 is connected to Switch0 and two PCs (PC0 and PC1). The IP address 192.168.1.0/24 is assigned to the interface connecting ASA0 to the Switch0.

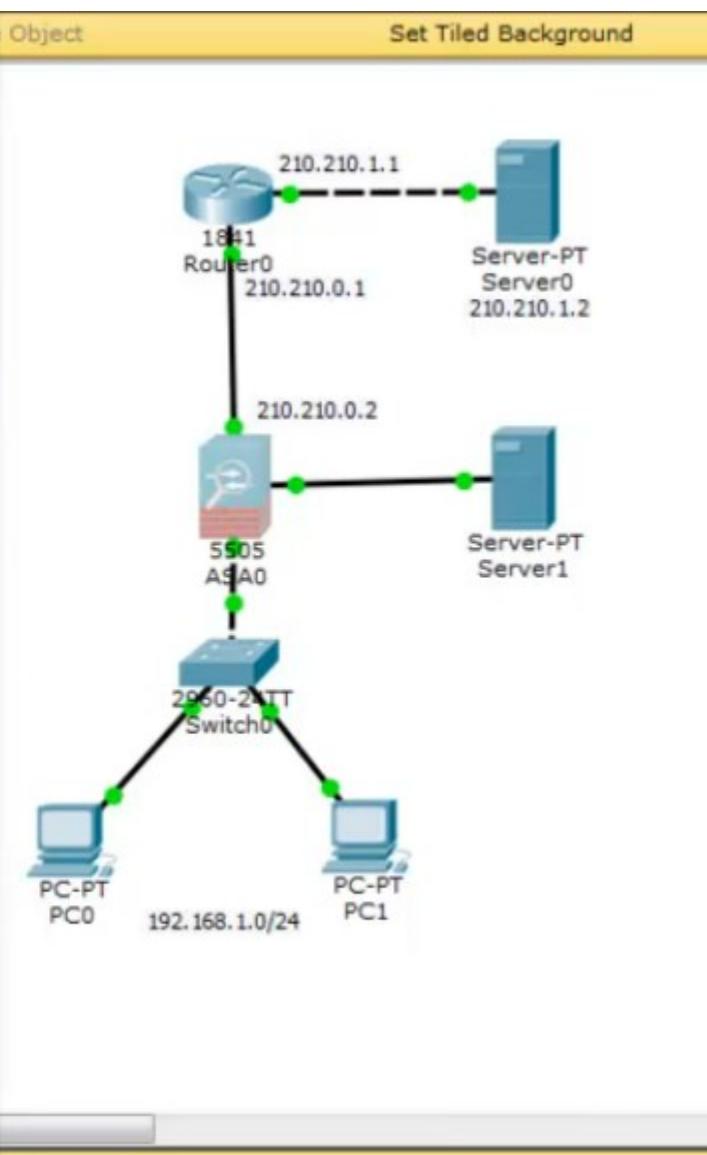
Назначим VLAN1 с указанием «no forward», т. е. с VLAN3 на VLAN1 передача траффика будет невозможна из-за ограничений лицензии

ASA0

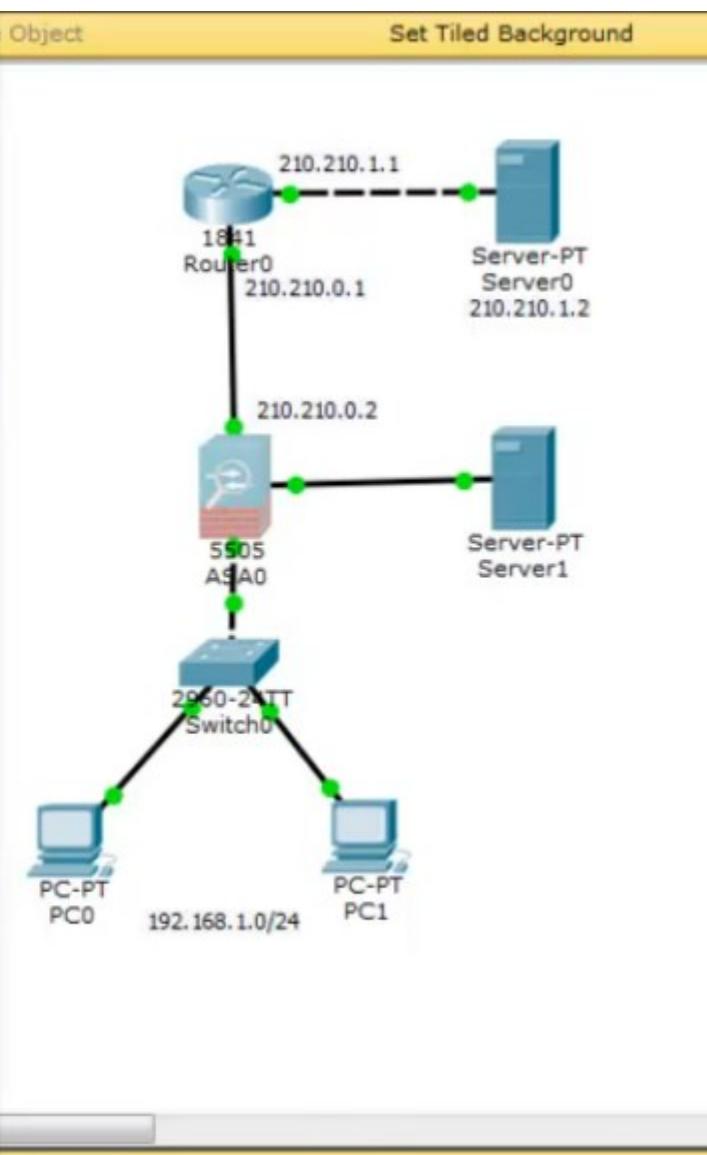
Physical Config CLI

ASA Command Line Interface

```
ciscoasa(config-if)#  
ciscoasa(config-if)#no for  
ciscoasa(config-if)#no forward in  
ciscoasa(config-if)#no forward interface vl  
ciscoasa(config-if)#no forward interface vlan 1  
ciscoasa(config-if)#  
ciscoasa(config-if)#nameif dmz  
INFO: Security level for "dmz" set to 0 by default.  
ciscoasa(config-if)#sec  
ciscoasa(config-if)#security-level 50  
ciscoasa(config-if)#ip add  
ciscoasa(config-if)#ip address 210.210.3.1 255.255.255.252  
ciscoasa(config-if)#no shut  
ciscoasa(config-if)#no shutdown  
ciscoasa(config-if)#  
ciscoasa(config-if)#  
ciscoasa(config-if)#  
ciscoasa(config-if)#  
ciscoasa(config-if)#exit  
ciscoasa(config)#  
ciscoasa(config)#  
ciscoasa(config)#ping 210.210.3.2  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 210.210.3.2, timeout is 2 seconds:  
[  
Copy Paste
```



Проверяем доступен ли Server1 с ASA0 - доступен



Пробуем пинговать Server1 с Server0 — не проходит

Server0

Physical Config Services Desktop Software/Services

Command Prompt

```
Packet Tracer SERVER Command Line 1.0
SERVER>
SERVER>
SERVER>
SERVER>ping 210.210.3.2

Pinging 210.210.3.2 with 32 bytes of data:

Request timed out.
Request timed out.
```

Live Object Set Tiled Background

The diagram illustrates a network topology. At the top, a Router0 (1841 model) is connected to a Server-PT Server0 (210.210.1.2) and a Server-PT Server1 (210.210.1.2). Router0 is also connected to a Switch0 (2960-24-T model). The Switch0 is connected to two PCs: PC-PT PC0 (192.168.1.0/24) and PC-PT PC1. The Router0 is connected to the Switch0 via interface 210.210.0.2. The Server1 is connected to the Switch0 via interface 210.210.0.1. The Router0 has an external IP of 210.210.1.1 and an internal IP of 210.210.0.1.

Чтобы устранить проблему — добавим access list на ASA0

ASA0

Physical Config CLI

ASA Command Line Interface

```
WORD Access list identifier
ciscoasa(config)#access-list FROM-OUTSIDE ex
ciscoasa(config)#access-list FROM-OUTSIDE extended ic
ciscoasa(config)#access-list FROM-OUTSIDE extended ic
ciscoasa(config)#access-list FROM-OUTSIDE extended ?
configure mode commands/options:
  deny   Specify packets to reject
  permit  Specify packets to forward
ciscoasa(config)#access-list FROM-OUTSIDE extended per
ciscoasa(config)#access-list FROM-OUTSIDE extended permit ?
configure mode commands/options:
  icmp
  icmp6
  object-group  Specify a service or protocol object-group after this
keyword
  tcp        Transmission Control Protocol
  udp        User Datagram Protocol
ciscoasa(config)#access-list FROM-OUTSIDE extended permit uc
ciscoasa(config)#access-list FROM-OUTSIDE extended permit ic
ciscoasa(config)#access-list FROM-OUTSIDE extended permit icmp
ciscoasa(config)#access-list FROM-OUTSIDE extended permit icmp any host
ciscoasa(config)#access-list FROM-OUTSIDE extended permit icmp any host
210.210.3.2
ciscoasa(config)#

```

Copy Paste

```
graph TD
    Router0[Router0 18.41] --- ASA0[ASA0 5.9.0.5]
    Router0 --- Switch0[Switch0 2950-24TT]
    ASA0 --- Server0[Server-PT Server0 210.210.1.2]
    ASA0 --- Server1[Server-PT Server1 210.210.1.2]
    ASA0 --- PC0[PC-PT PC0]
    ASA0 --- PC1[PC-PT PC1]
    Router0 --- Host[210.210.1.1]
    Switch0 --- Subnet[192.168.1.0/24]
```

Добавим правило для www траффика

ASA

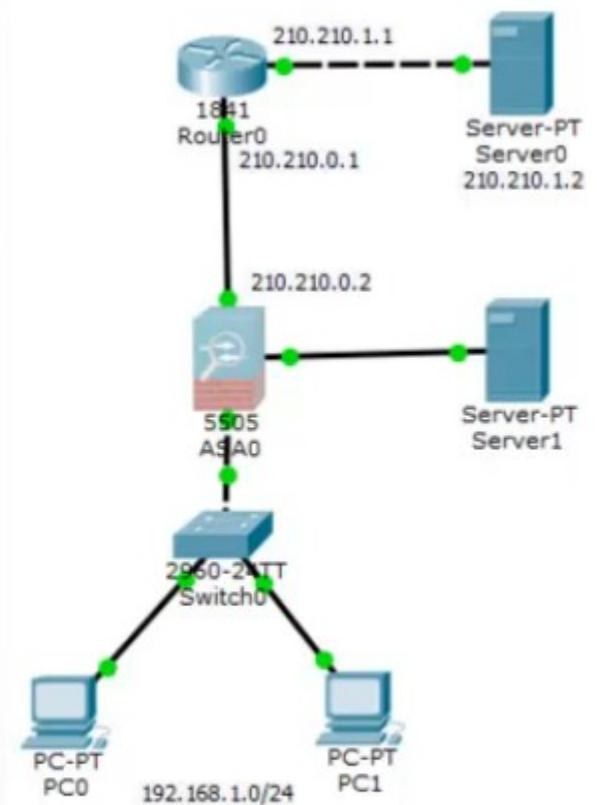
Physical Config CLI

ASA Command Line Interface

```
210.210.3.2
ciscoasa(config)#access-list FROM-OUTSIDE extended permit tcp any host
210.210.3.2 eq ?

configure mode commands/options:
<0-65535>  Port number
domain      Domain Name Service (DNS, 53)
ftp         File Transfer Protocol (21)
pop3        Post Office Protocol v3 (110)
smtp        Simple Mail Transport Protocol (25)
telnet      Telnet (23)
www         World Wide Web (HTTP, 80)
ciscoasa(config)#access-list FROM-OUTSIDE extended permit tcp any host
210.210.3.2 eq www
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#acc
ciscoasa(config)#acces
ciscoasa(config)#access-g
ciscoasa(config)#access-group ?

configure mode commands/options:
WORD  Specify the name of an access-list
ciscoasa(config)#access-group FROM-OUTSIDE
```



Добавим access group

ASA0

Physical Config CLI

ASA Command Line Interface

```
configure mode commands/options:
  in  For input traffic
  out For output traffic
ciscoasa(config)#access-group FROM-OUTSIDE in in
ciscoasa(config)#access-group FROM-OUTSIDE in interface ?

configure mode commands/options:
  inside  Name of interface Vlan1
  outside Name of interface Vlan2
  dmz    Name of interface Vlan3
ciscoasa(config)#access-group FROM-OUTSIDE in interface out
ciscoasa(config)#access-group FROM-OUTSIDE in interface outside
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#end
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 0a0f5a30 12234c1c 543976b6 354c475c

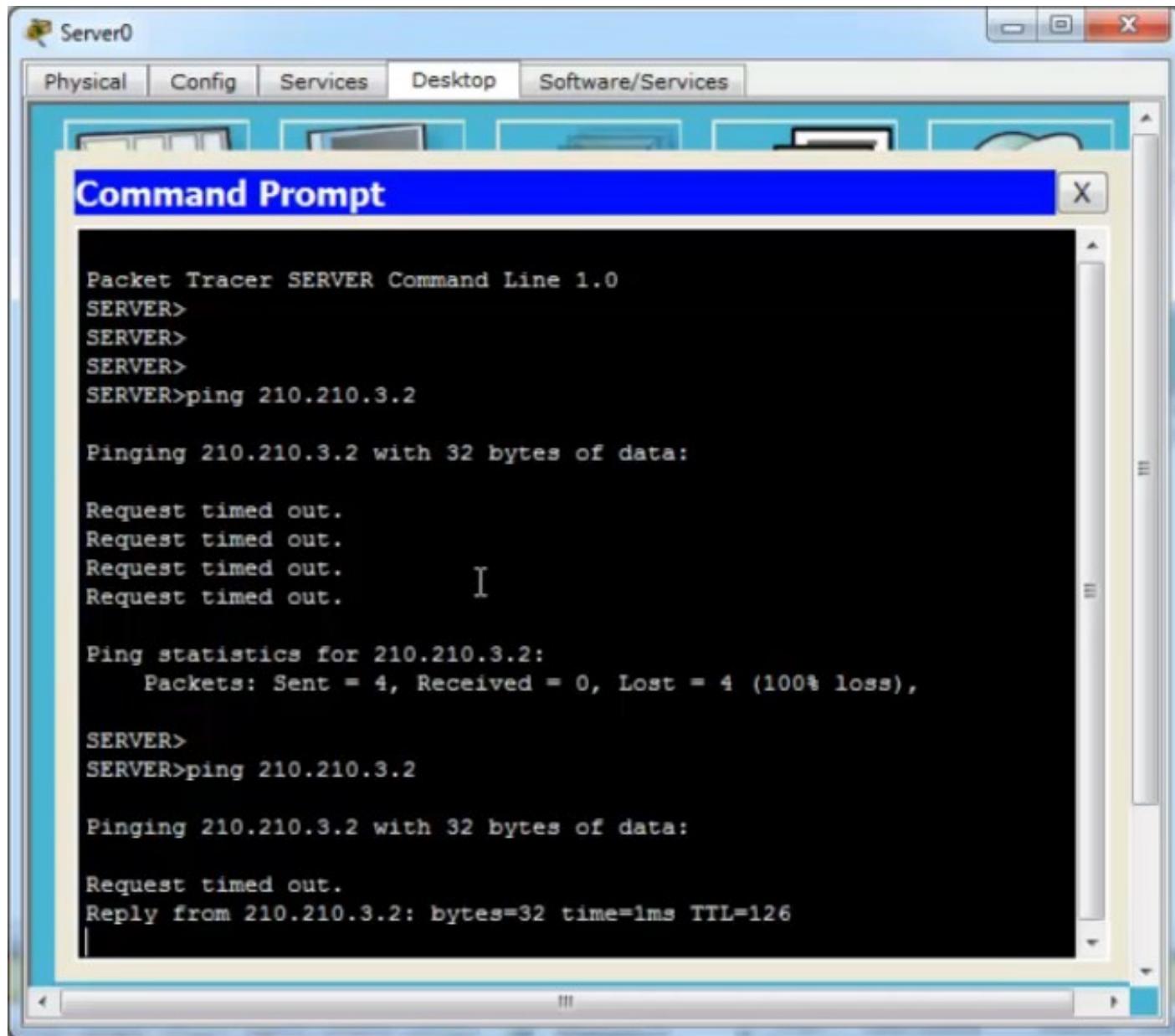
1527 bytes copied in 1.636 secs (933 bytes/sec)
[OK]
ciscoasa#
```

Copy Paste

Live Object Set Tiled Background

```
graph TD
    Router0[Router0 1841] --- ASA0[ASA0 5505]
    Router0 --- Server0[Server-PT Server0 210.210.1.2]
    Router0 --- Server1[Server-PT Server1 210.210.1.2]
    ASA0 --- Switch0[Switch0 2950-24TT]
    Switch0 --- PC0[PC-PT PC0]
    Switch0 --- PC1[PC-PT PC1]
    style Router0 fill:#ccc,stroke:#000
    style ASA0 fill:#ccc,stroke:#000
    style Switch0 fill:#ccc,stroke:#000
    style PC0 fill:#ccc,stroke:#000
    style PC1 fill:#ccc,stroke:#000
    style Server0 fill:#ccc,stroke:#000
    style Server1 fill:#ccc,stroke:#000
```

Снова проверим доступ с Server0 на Server1 — работает



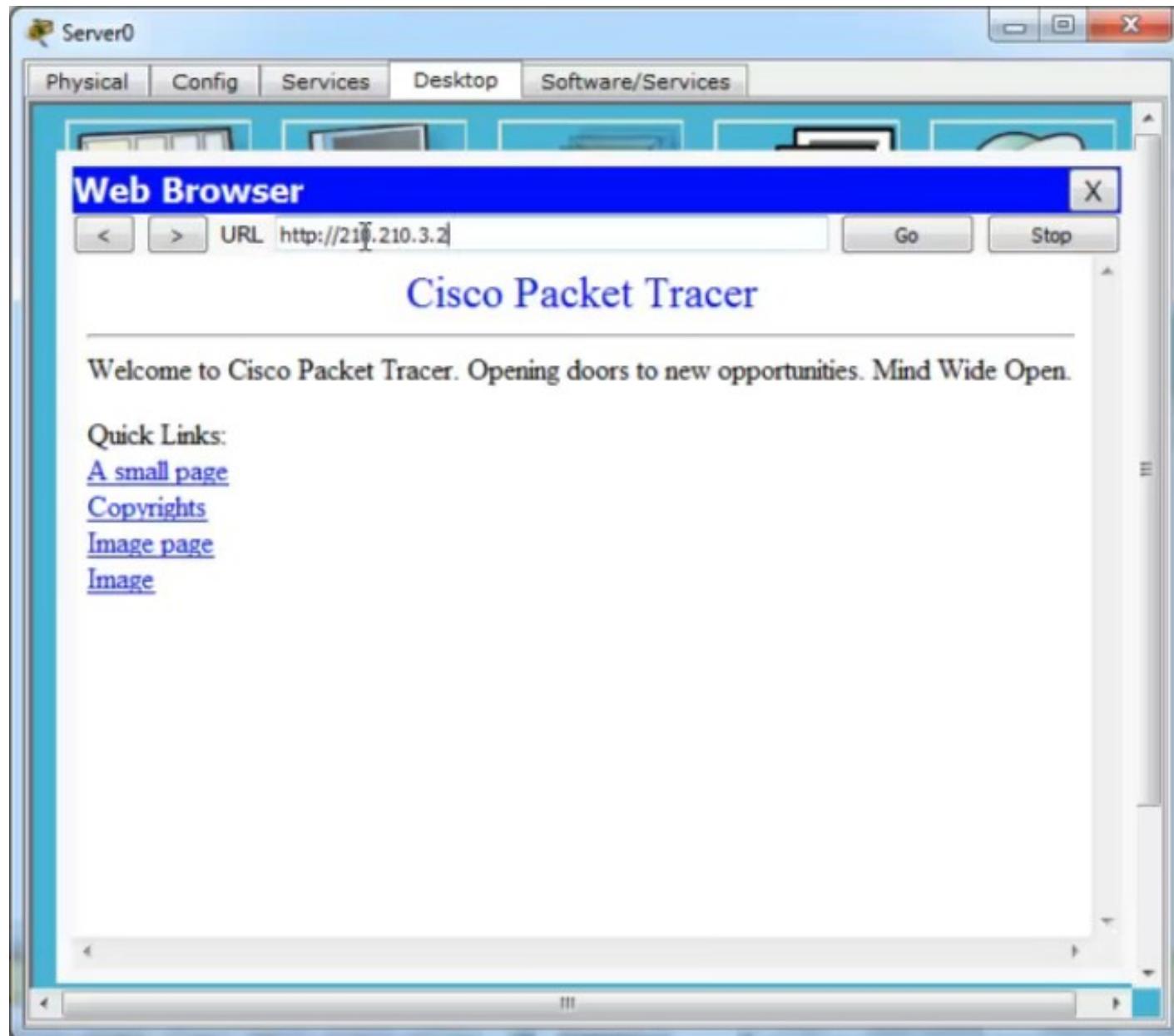
```
Packet Tracer SERVER Command Line 1.0
SERVER>
SERVER>
SERVER>
SERVER>ping 210.210.3.2

Pinging 210.210.3.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

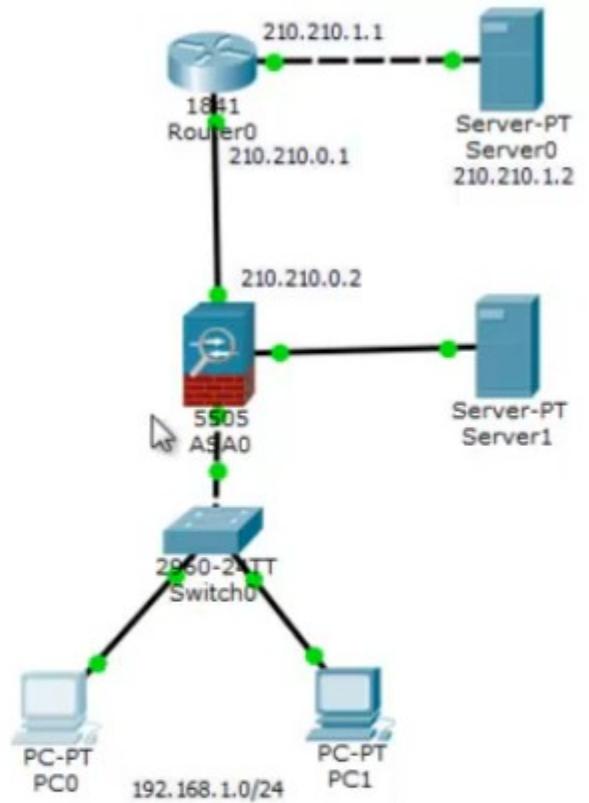
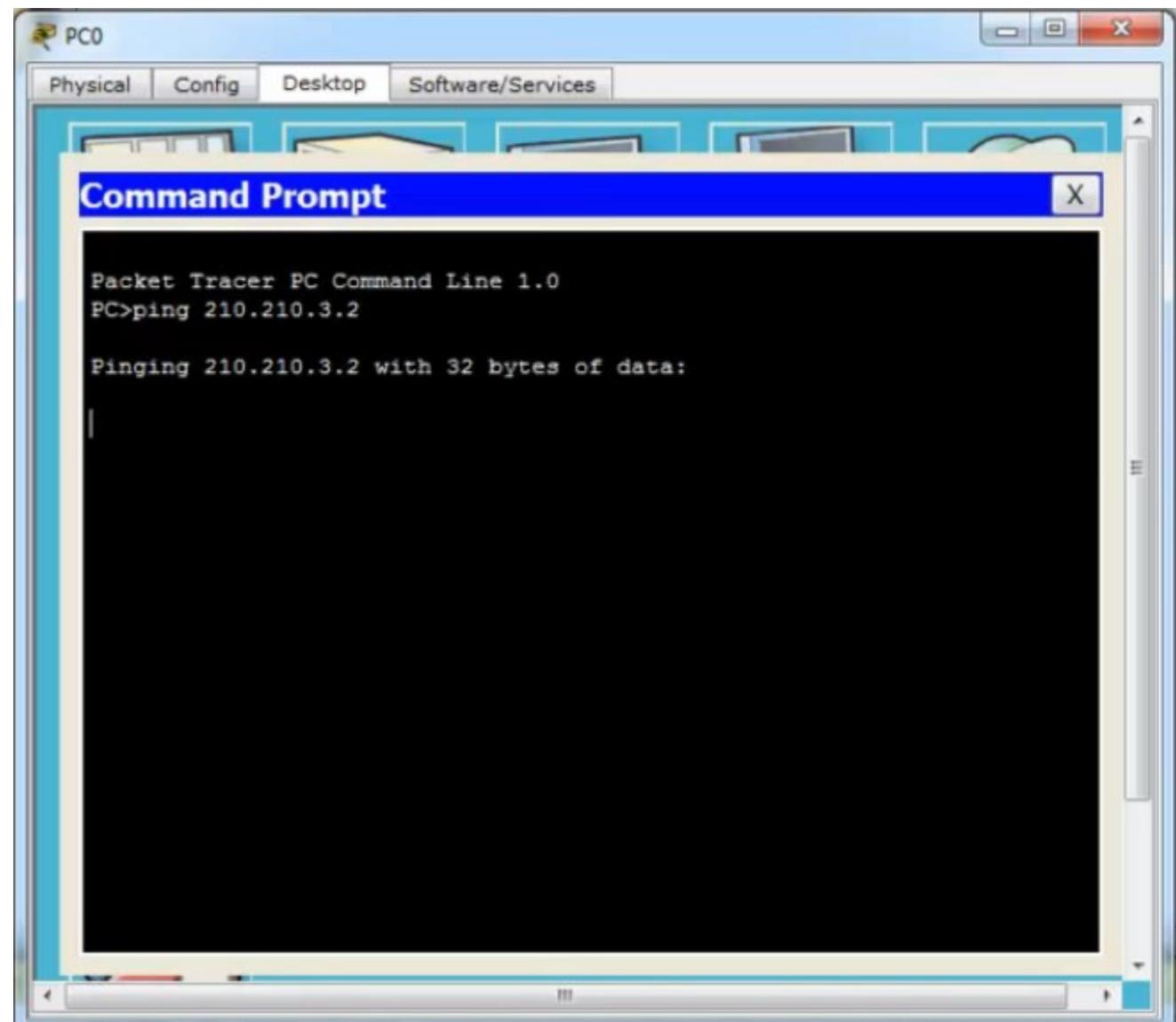
Ping statistics for 210.210.3.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    SERVER>
    SERVER>ping 210.210.3.2

Pinging 210.210.3.2 with 32 bytes of data:
Request timed out.
Reply from 210.210.3.2: bytes=32 time=1ms TTL=126
```

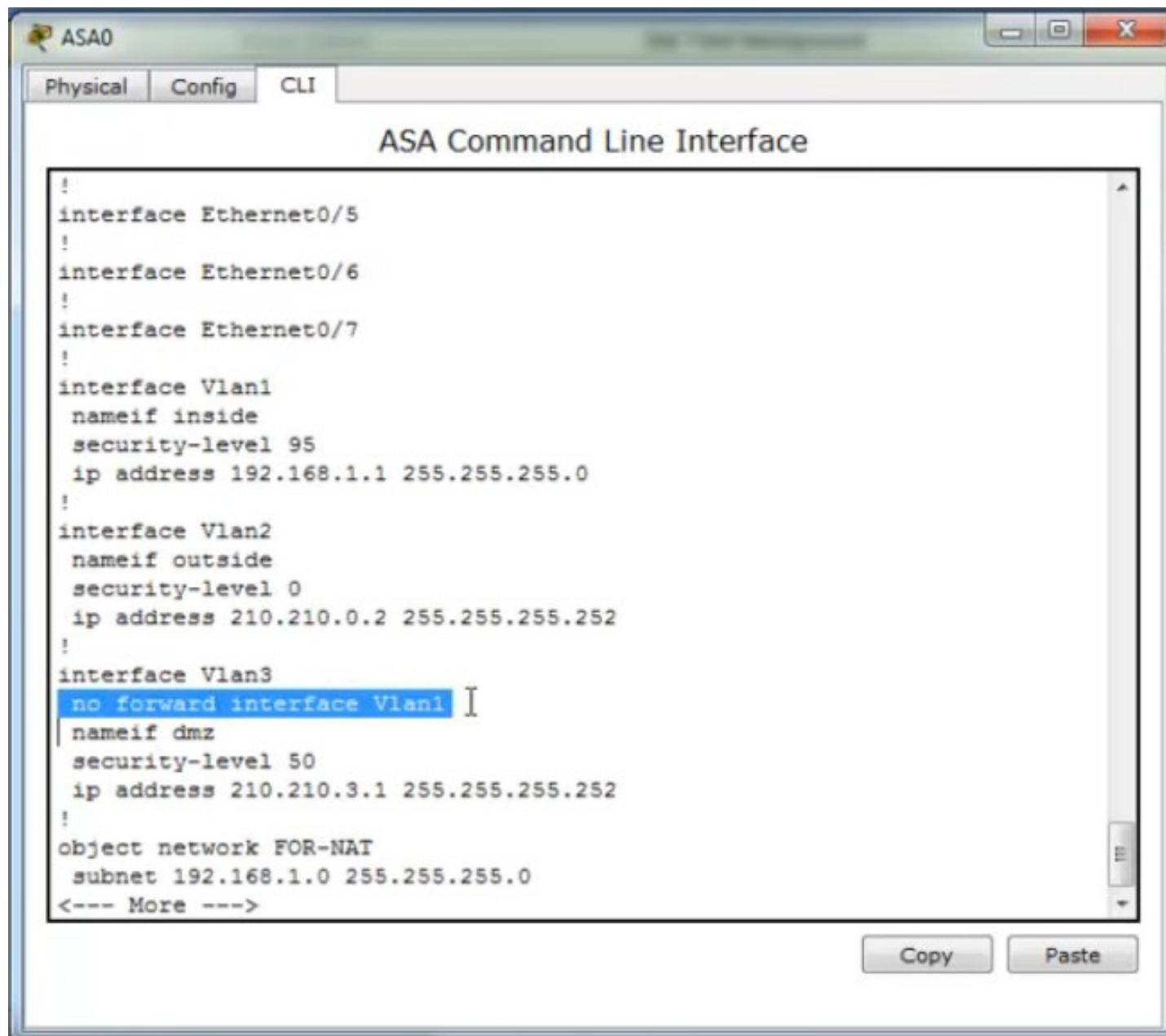
Снова проверим доступность веб-сервера на Server1 — работает



При этом доступ на Server1 с PC0 — не работает



не работает из-за no forward между VLAN3 и VLAN1

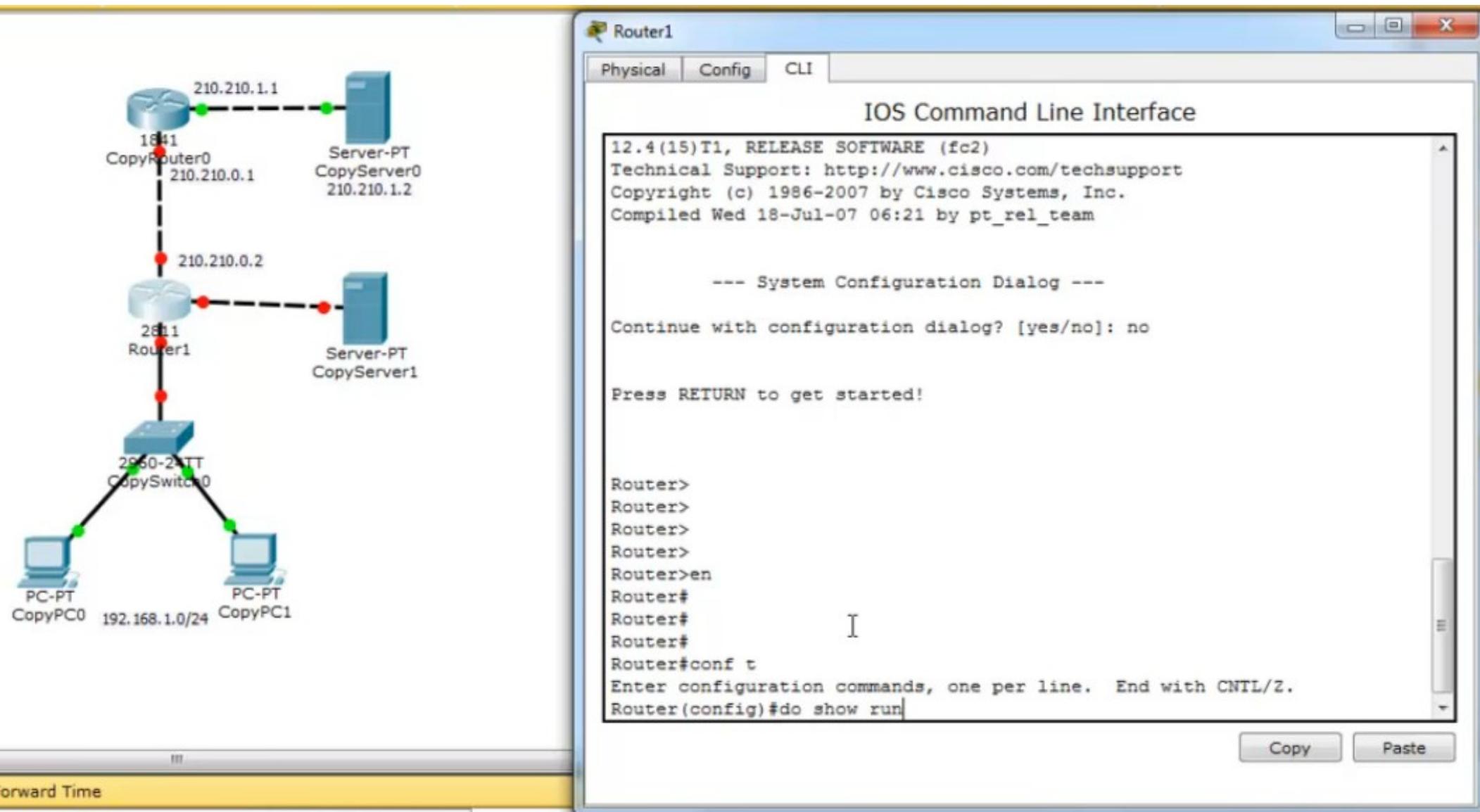


The image shows a window titled "ASA0" with a tab bar containing "Physical", "Config", and "CLI". The "CLI" tab is selected, and the title bar says "ASA Command Line Interface". The main area of the window displays the following ASA configuration code:

```
!
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
!
interface Vlan3
  no forward interface Vlan1
  nameif dmz
  security-level 50
  ip address 210.210.3.1 255.255.255.252
!
object network FOR-NAT
  subnet 192.168.1.0 255.255.255.0
<--- More --->
```

The line "no forward interface Vlan1" is highlighted with a blue selection bar. At the bottom of the window, there are "Copy" and "Paste" buttons.

Скопируем сеть зажав Ctrl и заменим ASA на Router 2811



The image shows a network diagram on the left and a Router1 CLI window on the right.

Network Diagram:

- Top segment: A router (CopyRouter0) with IP 210.210.1.1 is connected to a server (Server-PT CopyServer0) with IP 210.210.1.2.
- Middle segment: A router (Router1) with IP 210.210.0.2 is connected to a server (Server-PT CopyServer1) with IP 210.210.0.1.
- Bottom segment: A switch (CopySwitch0) with IP 2060-24-PT is connected to two PCs (PC-PT CopyPC0 and PC-PT CopyPC1) on a network with IP 192.168.1.0/24.

Router1 CLI Window:

- Physical Tab:** Shows the physical interface configuration.
- Config Tab:** Shows the configuration dialog:
 - 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
- CLI Tab:** Shows the IOS Command Line Interface:

```
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

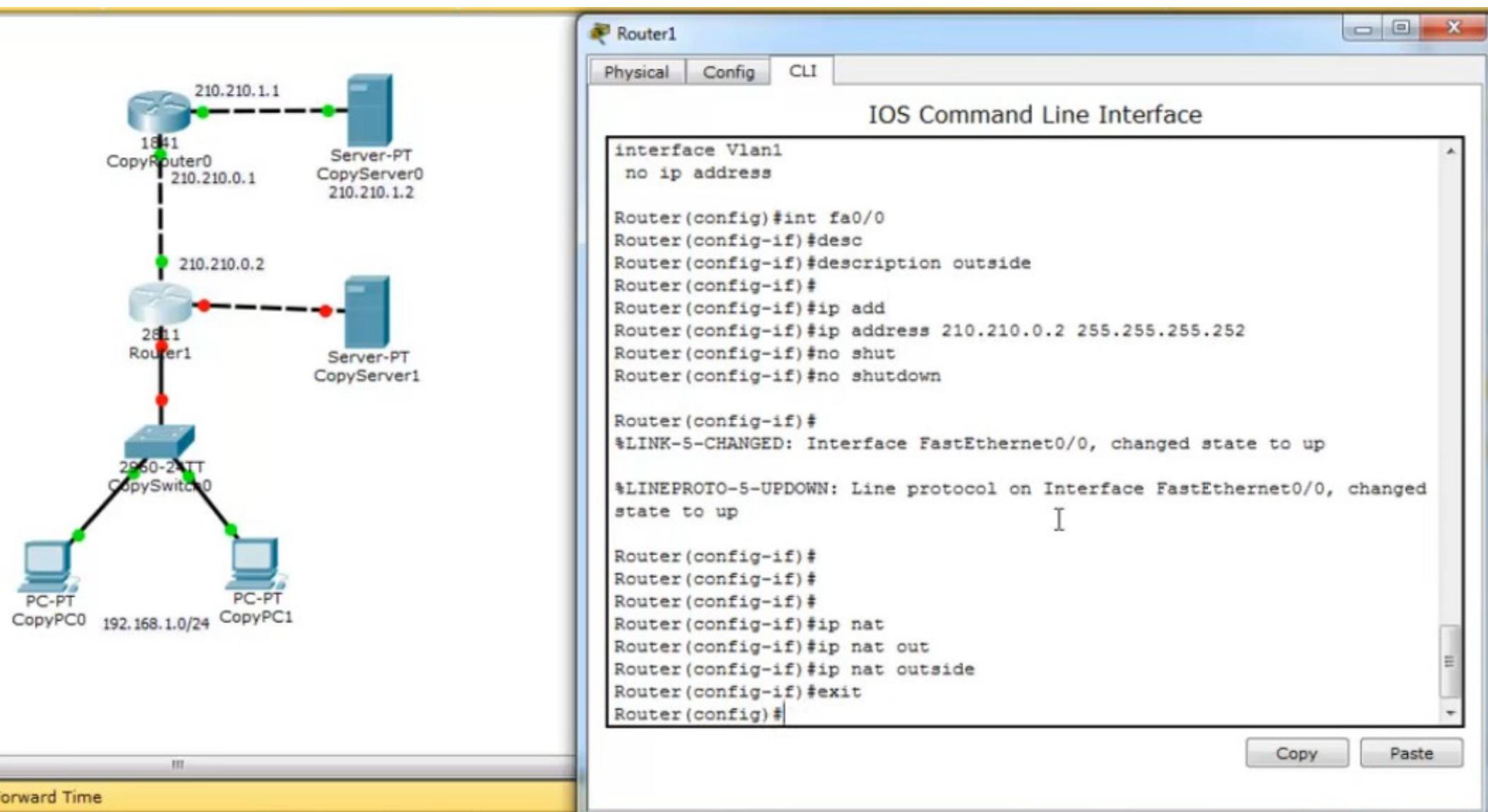
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>
Router>
Router>
Router>
Router>en
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#do show run|
```

На новом Router1 запустим интерфейсы и настроим NAT



The image shows a network diagram on the left and a Router1 configuration window on the right.

Network Diagram:

- Router0:** IP 210.210.1.1, MAC 18:41. It has an interface **CopyRouter0** with IP 210.210.0.1.
- Router1:** IP 210.210.0.2, MAC 28:11. It has an interface **CopyRouter1** with IP 210.210.0.1.
- Switch0:** IP 2060-24TT, MAC 20:60. It has two interfaces: **CopySwitch0** (IP 192.168.1.0/24) and **CopySwitch1**.
- Server-PT:** IP 210.210.1.2, MAC 00:00. It is connected to Router0 and Router1.
- PC-PT:** IP 192.168.1.1, MAC 00:00. It is connected to Switch0.

Router1 Configuration (CLI window):

```
Router1
Physical Config CLI
IOS Command Line Interface

interface Vlan1
no ip address

Router(config)#int fa0/0
Router(config-if)#desc
Router(config-if)#description outside
Router(config-if)#
Router(config-if)#ip add
Router(config-if)#ip address 210.210.0.2 255.255.255.252
Router(config-if)#no shut
Router(config-if)#no shutdown

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

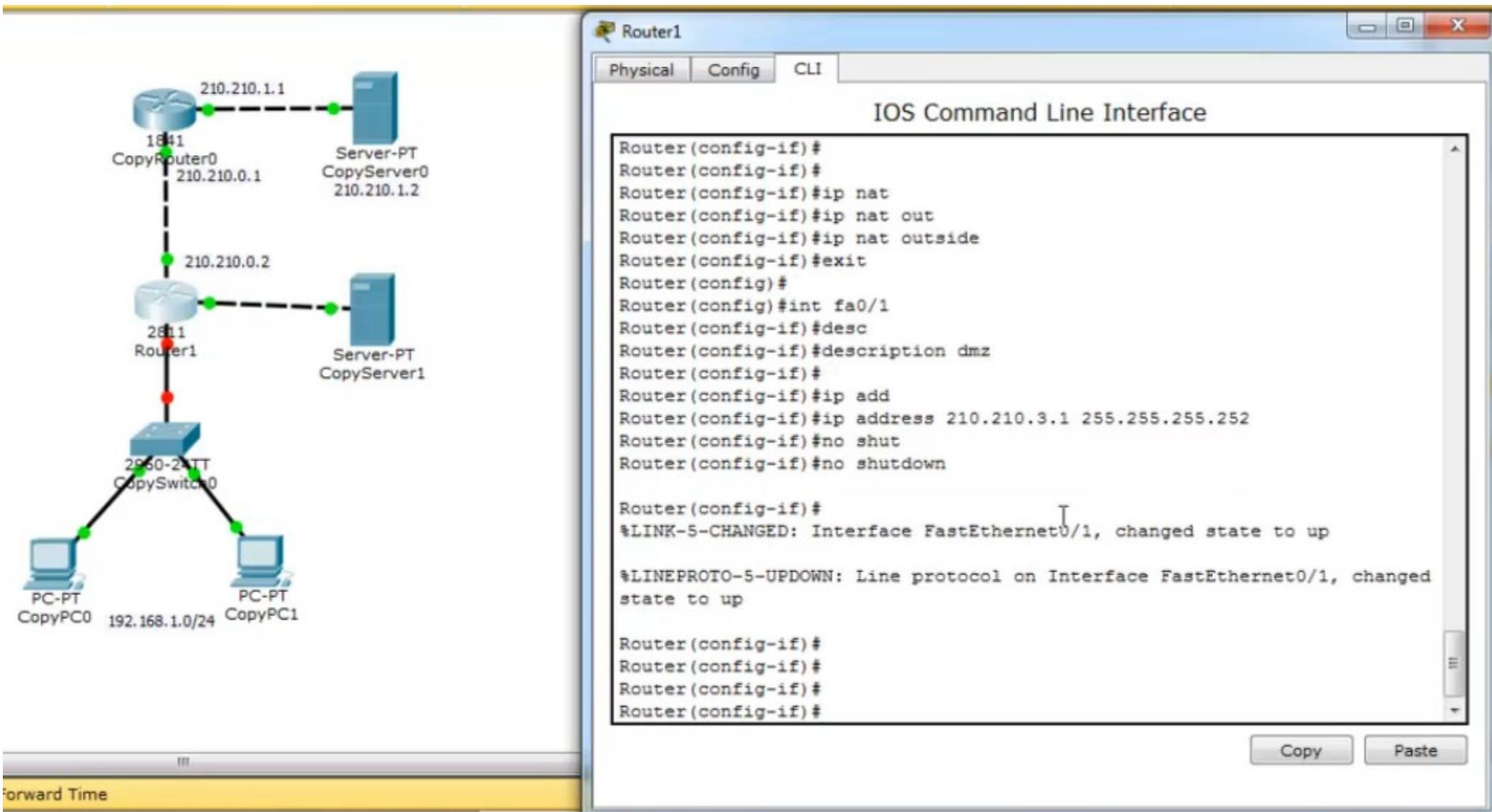
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#ip nat
Router(config-if)#ip nat out
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#

```

Buttons at the bottom of the CLI window: **Copy** and **Paste**.

Зададим ip адрес на fa 0/1, обращенного к DMZ и Server1



The image shows a network diagram on the left and a configuration window for Router1 on the right.

Network Diagram:

- Router0:** IP 210.210.1.1, connected to a server (IP 210.210.1.2) and a switch (IP 210.210.0.2).
- Router1:** IP 210.210.0.1, connected to a server (IP 210.210.1.2) and a switch (IP 210.210.0.2).
- Switch0:** IP 210.210.0.2, connected to two PCs (IPs 192.168.1.0/24 and 192.168.1.1/24).

Router1 Configuration (IOS CLI):

```
Router(config-if)#
Router(config-if)#
Router(config-if)#ip nat
Router(config-if)#ip nat out
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
Router(config)#int fa0/1
Router(config-if)#desc
Router(config-if)#description dmz
Router(config-if)#
Router(config-if)#ip add
Router(config-if)#ip address 210.210.3.1 255.255.255.252
Router(config-if)#no shut
Router(config-if)#no shutdown

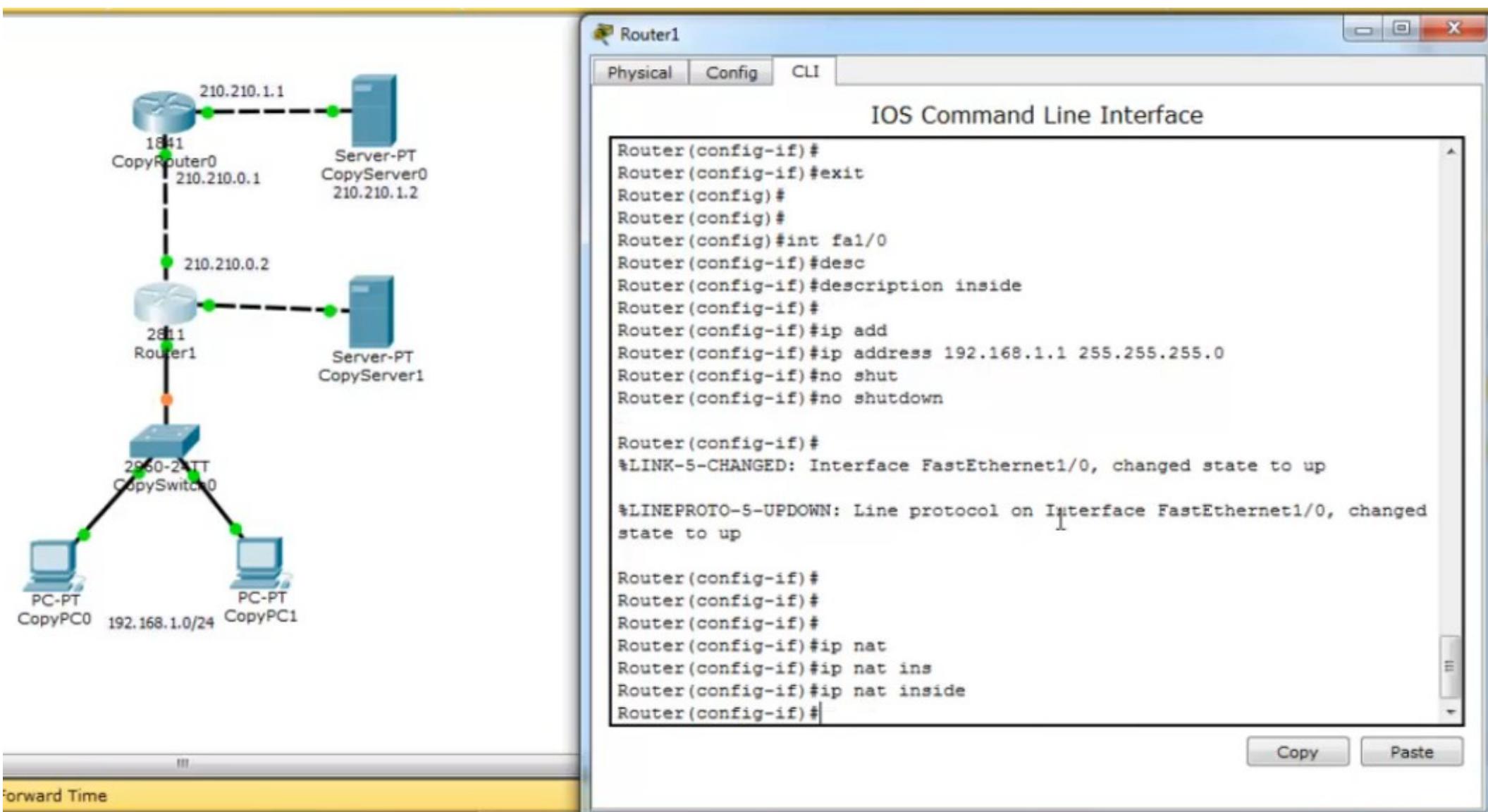
Router(config-if)#
*LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up

Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
```

Forward Time: (This text is located at the bottom left of the diagram area.)

Зададим ip адрес на fa1/0, внутреннем



The image shows a network diagram on the left and a Router1 CLI window on the right.

Network Diagram:

- Router0:** IP 210.210.1.1, Serial 1841, connected to a **Server-PT** (IP 210.210.1.2).
- Router0:** IP 210.210.0.1, connected to **Router1**.
- Router1:** IP 210.210.0.2, connected to a **Server-PT** (IP 210.210.1.2) and a **Switch0**.
- Switch0:** IP 2850-2-ATT, connected to two **PC-PT** hosts: **CopyPC0** (IP 192.168.1.0/24) and **CopyPC1**.

Router1 CLI Window:

IOS Command Line Interface

```
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config-if)#
Router(config-if)int fa1/0
Router(config-if)#desc
Router(config-if)#description inside
Router(config-if)#
Router(config-if)ip add
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed
state to up

Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)ip nat
Router(config-if)ip nat ins
Router(config-if)ip nat inside
Router(config-if)#

```

Buttons at the bottom: **Copy** and **Paste**.

Создадим access-list

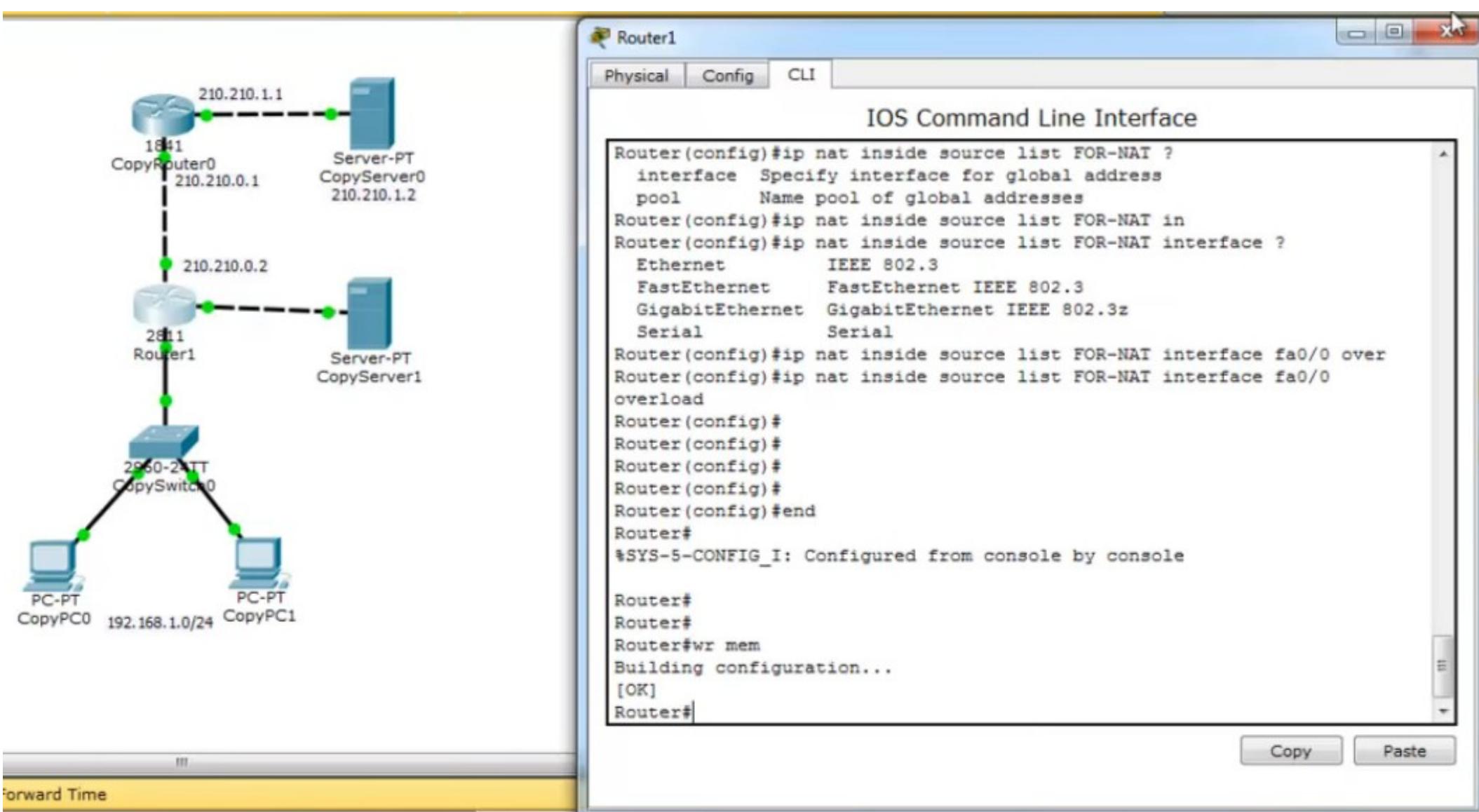
The diagram illustrates a network topology with three routers (CopyRouter0, Router1, CopySwitch0) and two servers (CopyServer0, CopyServer1). Router1 is connected to CopyRouter0 and CopySwitch0. CopyRouter0 is connected to CopyServer0 and a PC (PC-PT). Router1 is connected to CopyServer1 and another PC (PC-PT). The IP addresses shown are 210.210.1.1, 210.210.0.1, 210.210.0.2, 210.210.244, 192.168.1.0/24, and 210.210.1.2.

The CLI window shows the configuration of an access-list on Router1:

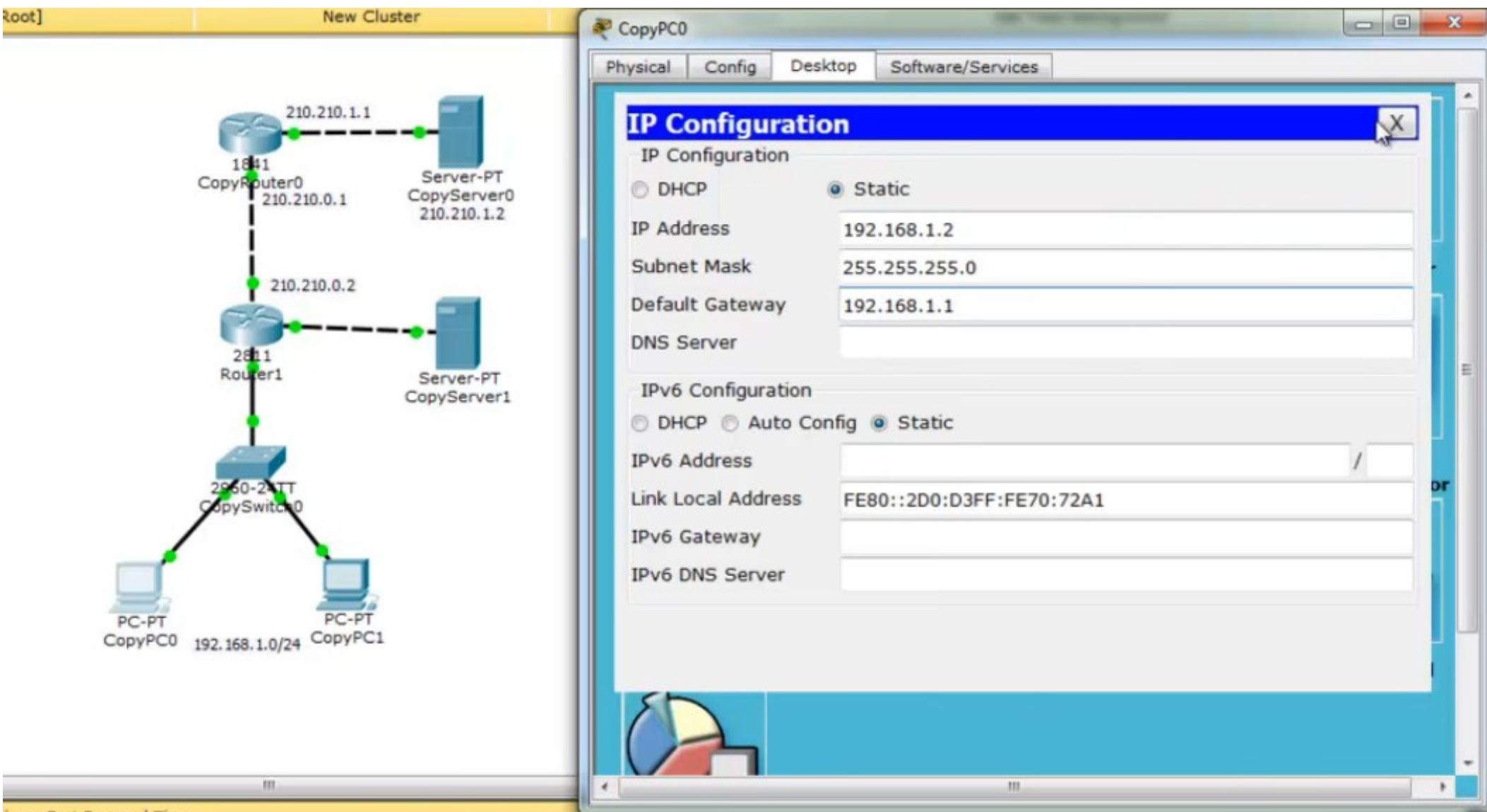
```
Router(config)#ip access-list st
Router(config)#ip access-list standard FOR-NAT
Router(config-std-nacl)#per
Router(config-std-nacl)#permit 192.168.1.0 ?
  A.B.C.D  Wildcard bits
  <cr>
Router(config-std-nacl)#permit 192.168.1.0 0.0.0.255
Router(config-std-nacl)#
Router(config-std-nacl)#exit
Router(config)#
Router(config)#ip nat
Router(config)#ip nat ins
Router(config)#ip nat inside so
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 ?
  Ethernet    IEEE 802.3
  FastEthernet FastEthernet IEEE 802.3
  GigabitEthernet GigabitEthernet IEEE 802.3z
  Serial      Serial
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
```

Buttons at the bottom of the CLI window: Copy and Paste.

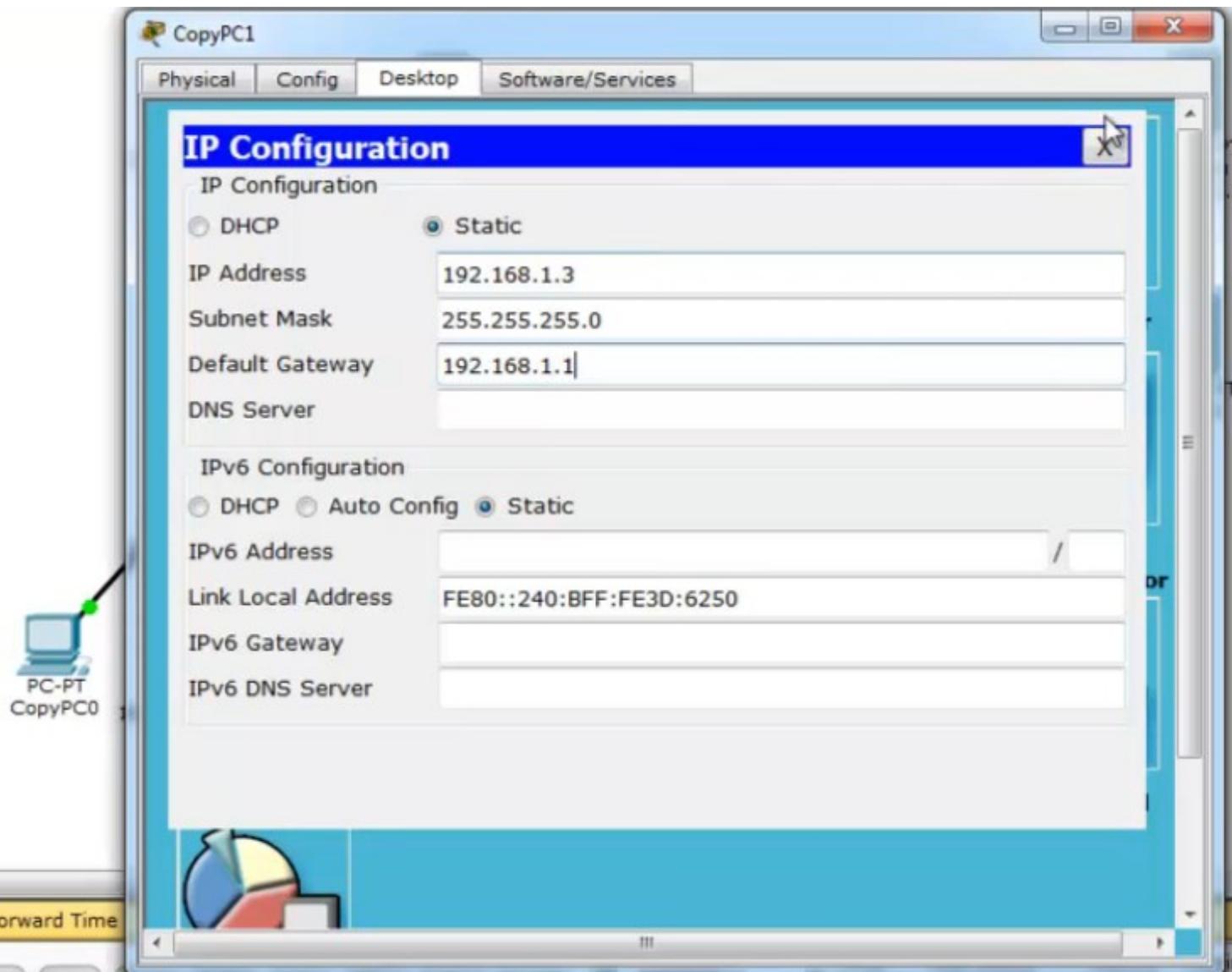
Сохраняем настройки



Зададим ір на PC0, т. к. DHCP сервера у нас нет



Зададим ір на PC1



Проверяем доступ с Router1 к Router0, к Server1, к PC0

The diagram illustrates a network topology with the following components and connections:

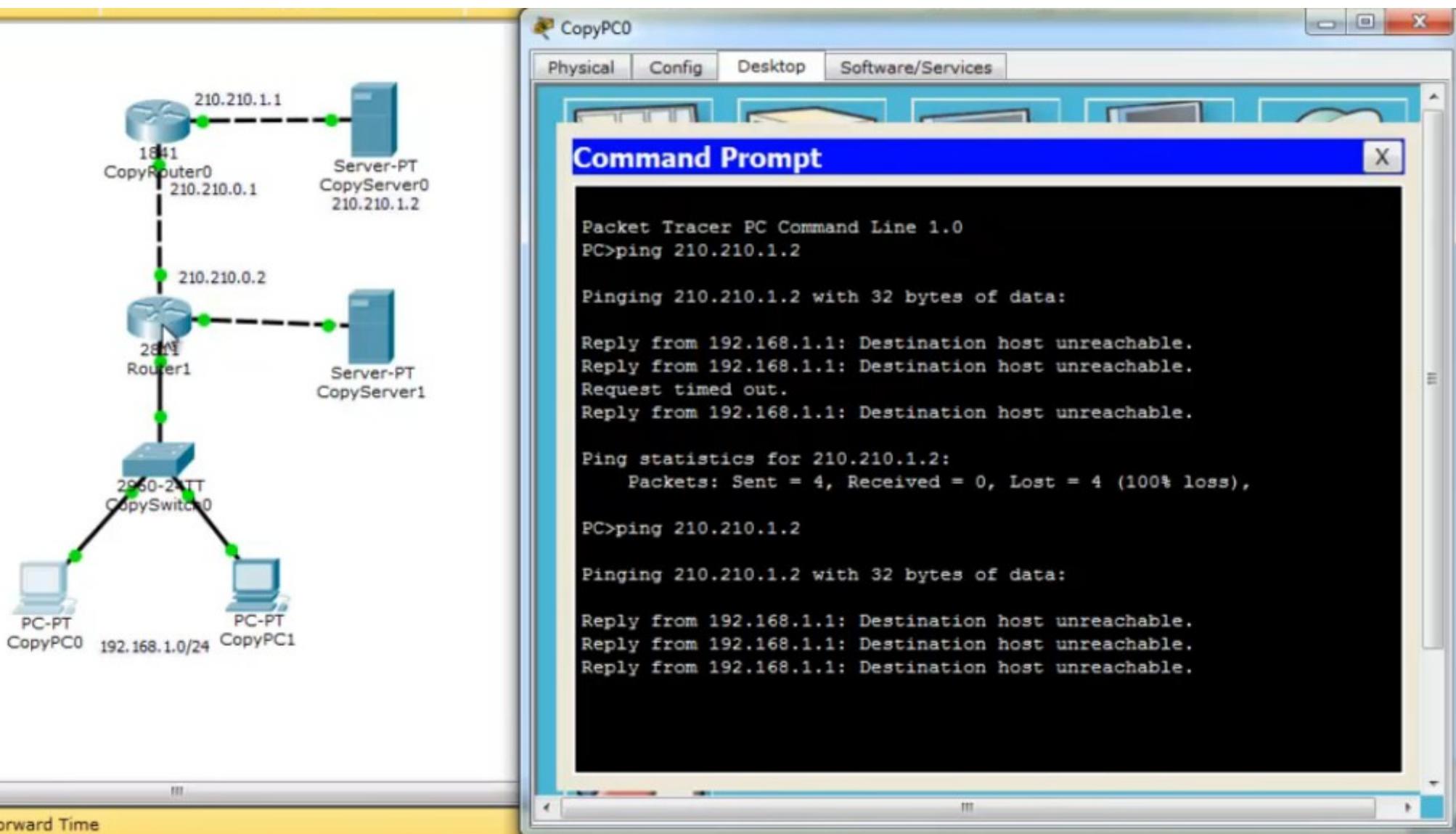
- Router0:** IP 210.210.1.1, Serial port 1841 connected to Router1.
- Router1:** IP 210.210.0.1, Serial port 2811 connected to Router0 and Switch0.
- Switch0:** IP 2850-24TT, connected to Router1 and two PCs (PC0 and PC1).
- Server0:** IP 210.210.1.2, connected to Router0.
- Server1:** IP 210.210.3.2, connected to Router1.
- PC0:** IP 192.168.1.0/24, connected to Switch0.
- PC1:** IP 192.168.1.1/24, connected to Switch0.

The Router1 CLI window displays the following ping results:

```
Router#  
Router#  
Router#ping 210.210.0.1  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 210.210.0.1, timeout is 2 seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms  
  
Router#  
Router#ping 210.210.3.2  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 210.210.3.2, timeout is 2 seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/2 ms  
  
Router#  
Router#ping 192.168.1.2  
[  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/8/17 ms  
  
Router#
```

Buttons at the bottom of the CLI window: **Copy** and **Paste**.

Проверяем доступ с PC0 к Server1 — не проходит



The diagram illustrates a network topology with the following components and connections:

- Router0:** IP 210.210.1.1, connected to the top port of the Switch0 and to the left port of Router1.
- Router1:** IP 210.210.0.2, connected to the bottom port of Router0 and to the left port of the Switch0.
- Switch0:** IP 29.60-24.TT, connected to the left port of Router1, the left port of PC-PT CopyPC0, and the left port of PC-PT CopyPC1.
- PC-PT CopyPC0:** IP 192.168.1.0/24, connected to the right port of the Switch0.
- PC-PT CopyPC1:** IP 192.168.1.1/24, connected to the right port of the Switch0.
- Server-PT CopyServer0:** IP 210.210.1.2, connected to the right port of Router0.
- Server-PT CopyServer1:** IP 210.210.1.2, connected to the right port of Router1.

The Command Prompt window shows the results of two ping attempts from PC-PT CopyPC0 to Server-PT CopyServer1:

```
Packet Tracer PC Command Line 1.0
PC>ping 210.210.1.2

Pinging 210.210.1.2 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Request timed out.
Reply from 192.168.1.1: Destination host unreachable.

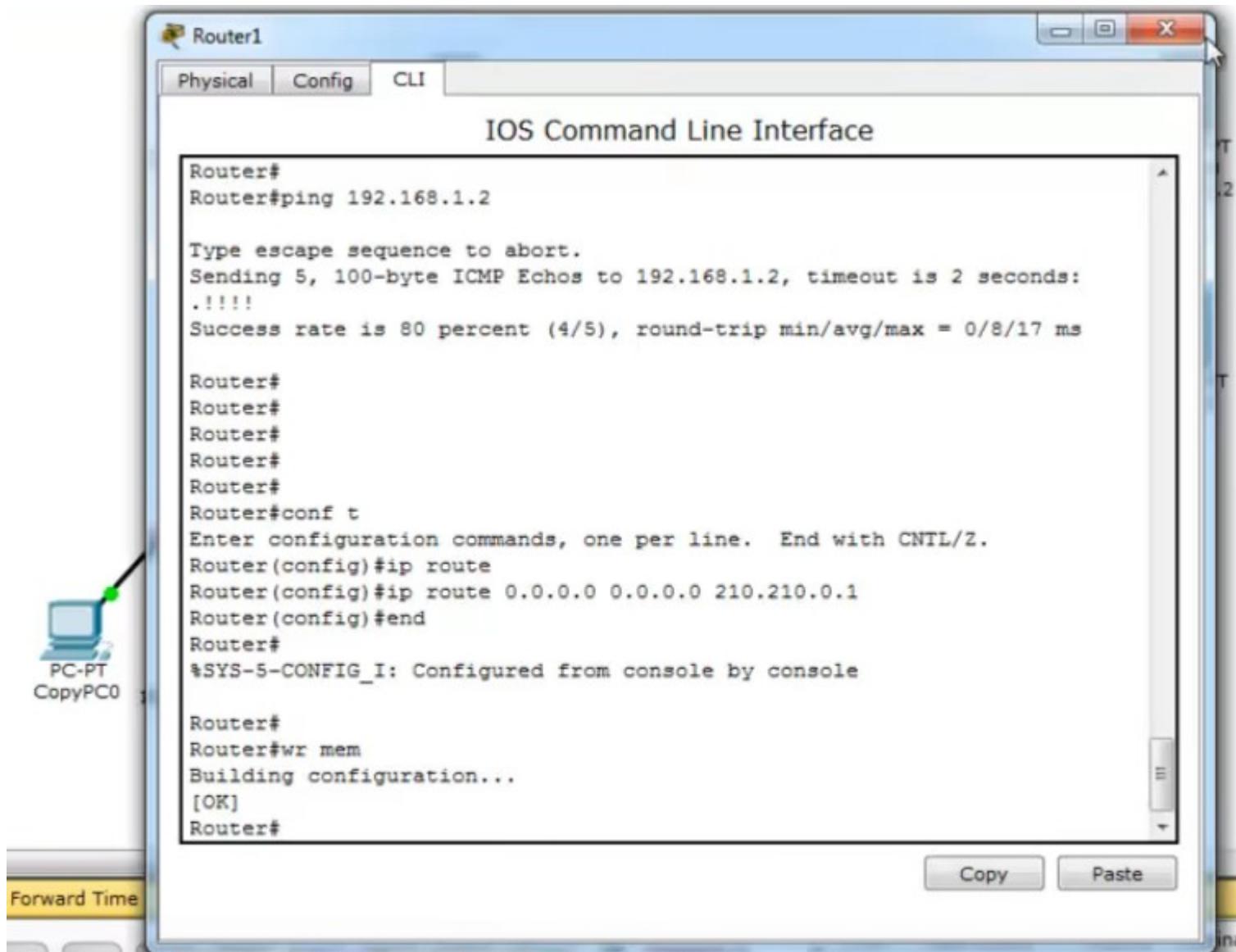
Ping statistics for 210.210.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 210.210.1.2

Pinging 210.210.1.2 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
```

Чтобы исправить добавляем маршрут на Router1



The screenshot shows a Cisco Router configuration interface. The window title is "Router1" and the tab selected is "CLI". The main area displays the "IOS Command Line Interface". The terminal window shows the following command sequence and output:

```
Router#  
Router#ping 192.168.1.2  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:  
!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/8/17 ms  
  
Router#  
Router#  
Router#  
Router#  
Router#  
Router#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#ip route  
Router(config)#ip route 0.0.0.0 0.0.0.0 210.210.0.1  
Router(config)#end  
Router#  
%SYS-5-CONFIG_I: Configured from console by console  
  
Router#  
Router#wr mem  
Building configuration...  
[OK]  
Router#
```

On the left side of the interface, there is a sidebar with a computer icon and the text "PC-PT" and "CopyPC0". At the bottom of the window, there are "Copy" and "Paste" buttons. The bottom left corner of the window has a yellow bar with the text "Forward Time".

Теперь с PC0 доступны Server0, Server1

