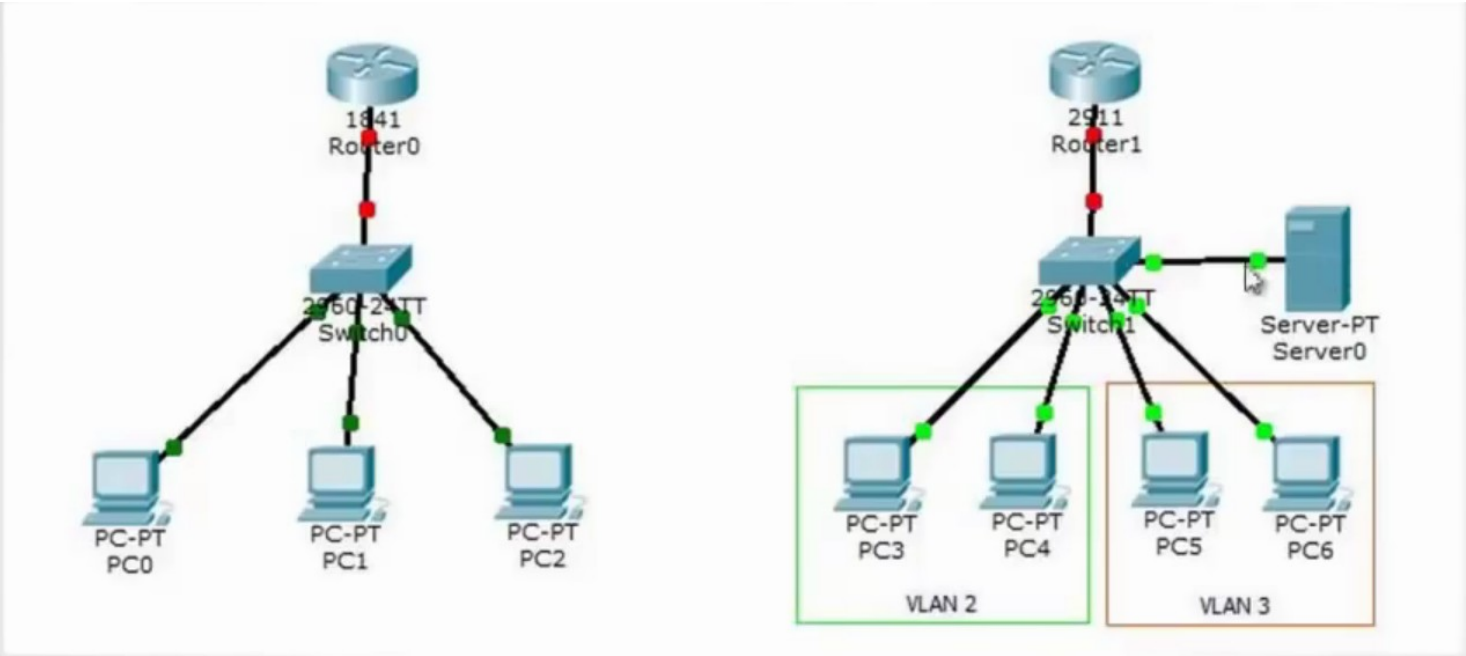
DHCP

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

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

DHCP




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

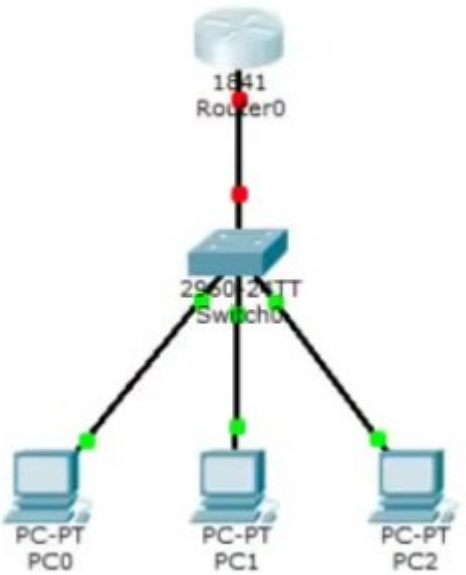
```
ip dhcp excluded-address 192.168.1.100
ip dhcp excluded-address 192.168.1.1
exit
show ip dhcp binding
```

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

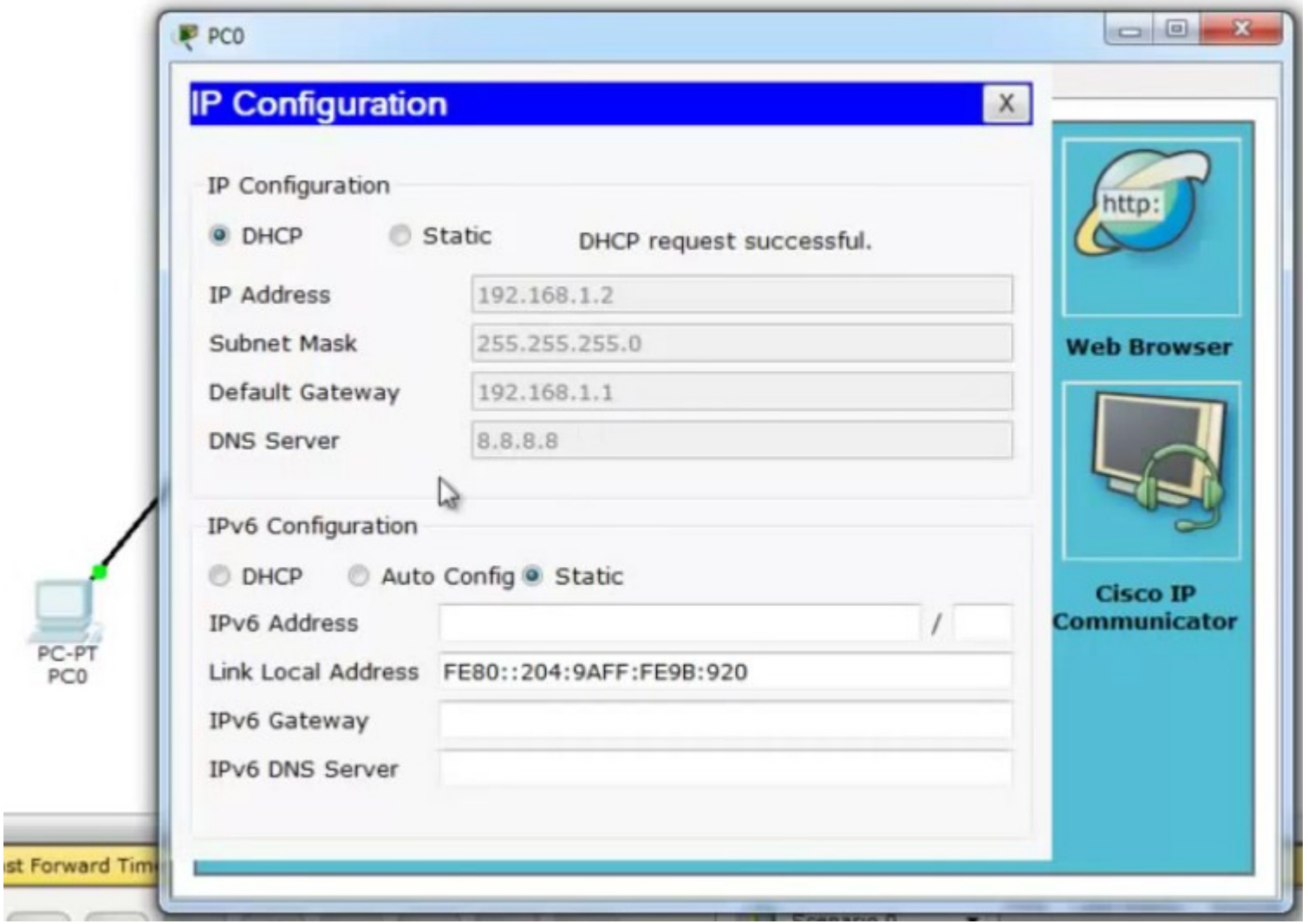
```
exit
interface GigabitEthernet0/1.4
 encapsulation dot1Q 4
 ip address 192.168.4.1 255.255.255.0
```

Настраиваем DHCP-сервер на Router0

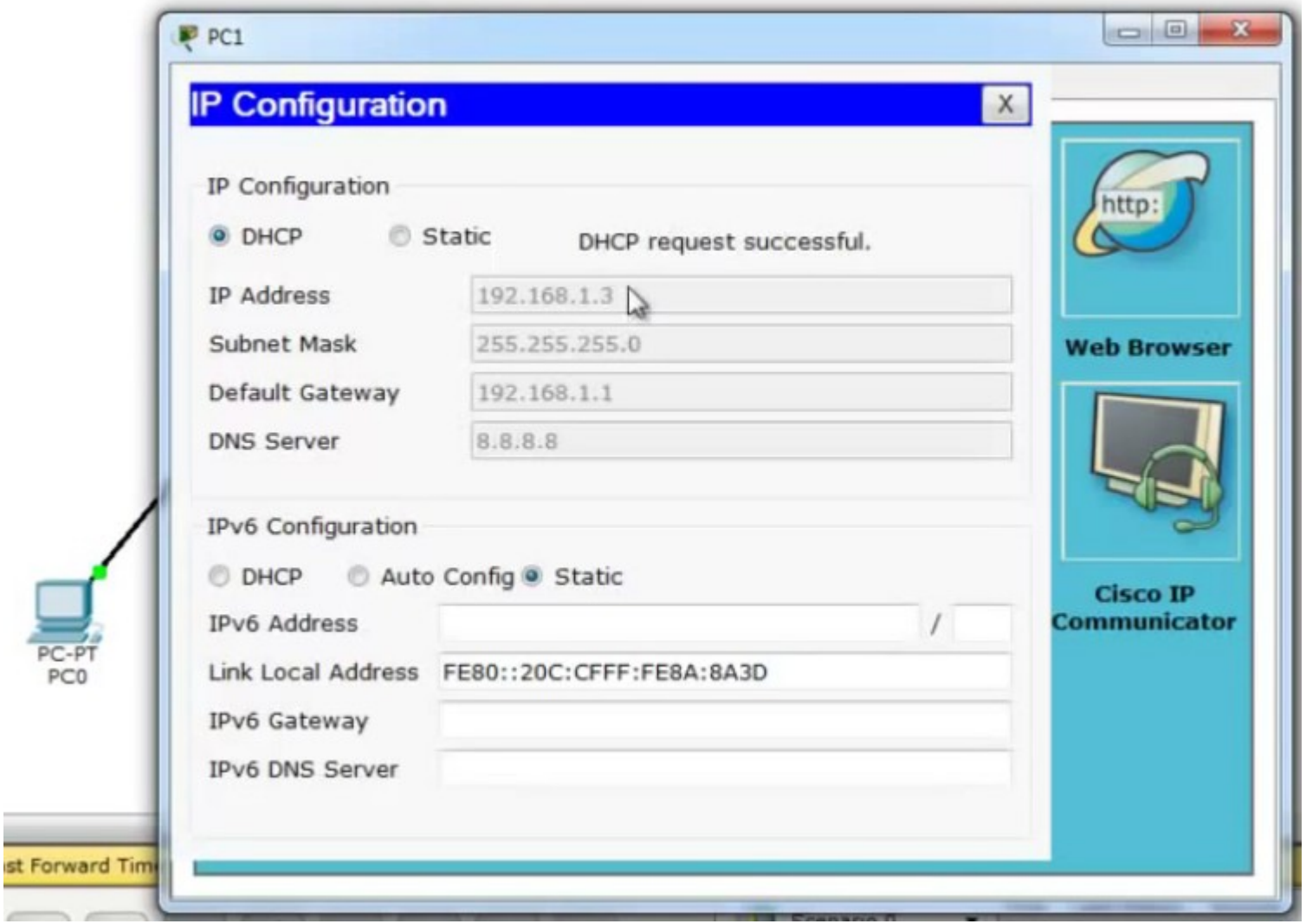
Router0
> no
> en
conf t
(config)# int fa0/0
(config-if)# no shutdown
(config-if)# ip address 192.168.1.1. 255.255.255.0
(config-if)# exit
(config)# ip dhcp pool DHCP
(dhcp-config)# network 192.168.1.0 255.255.255.0
(dhcp-config)# default-router 192.168.1.1
(dhcp-config)# dns-server 8.8.8.8
(dhcp-config)# exit
(config)# ip dhcp excluded-address 192.168.1.100
(config)# ip dhcp excluded-address 192.168.1.1
(config)#exit
wr mem



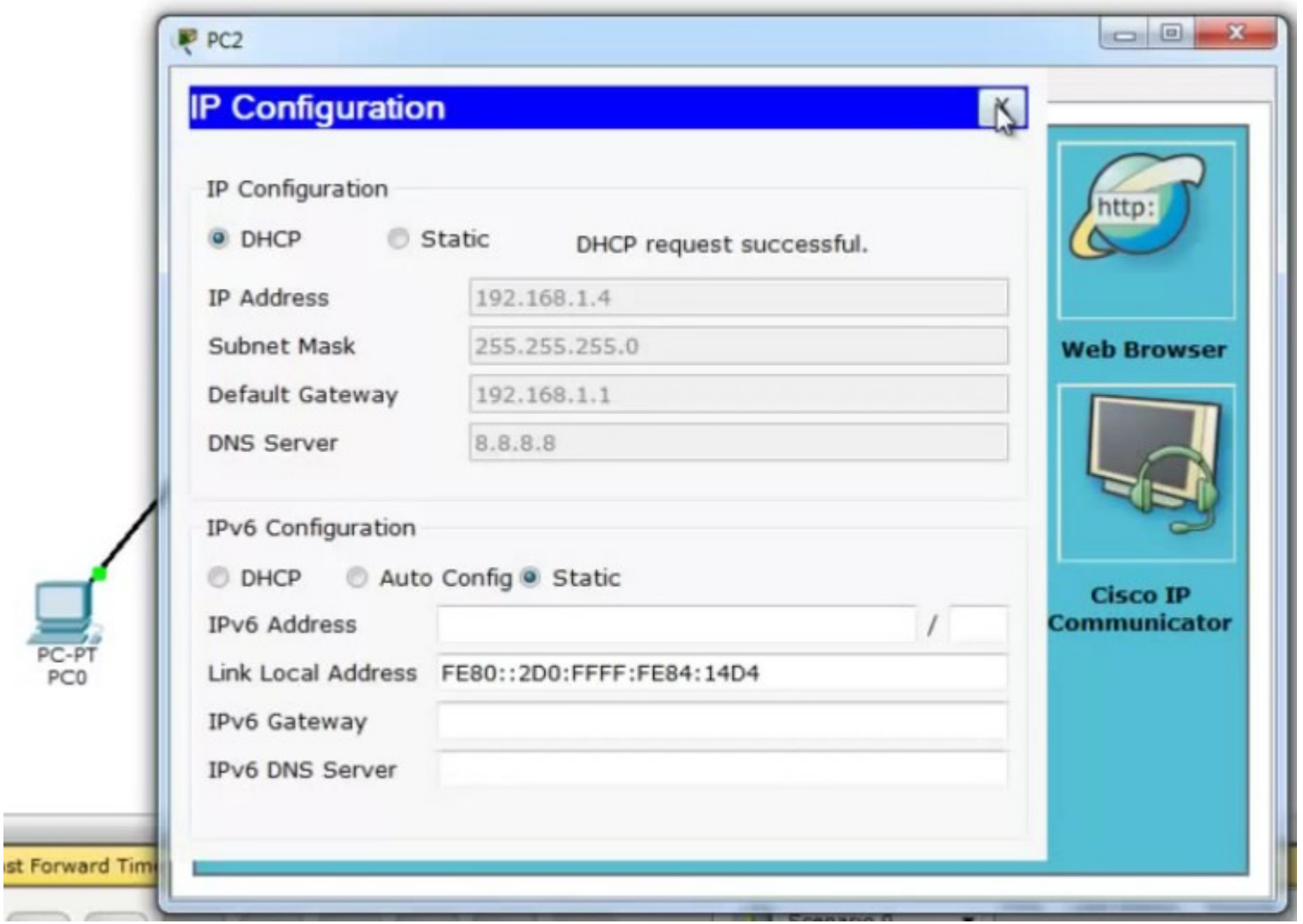
Включаем динамическое получение IP - DHCP на клиенте - PC0



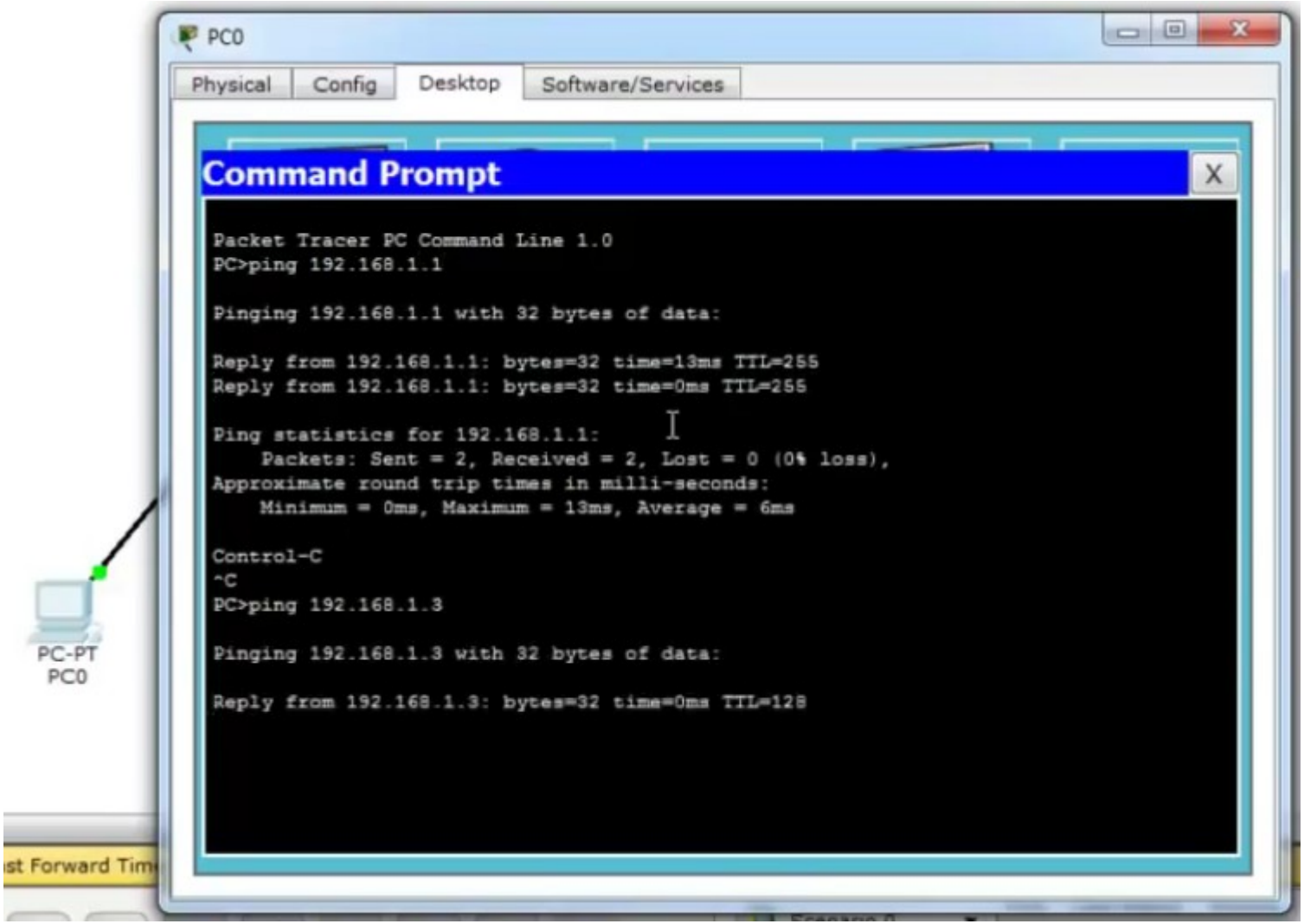
Аналогично поступаем на PC1



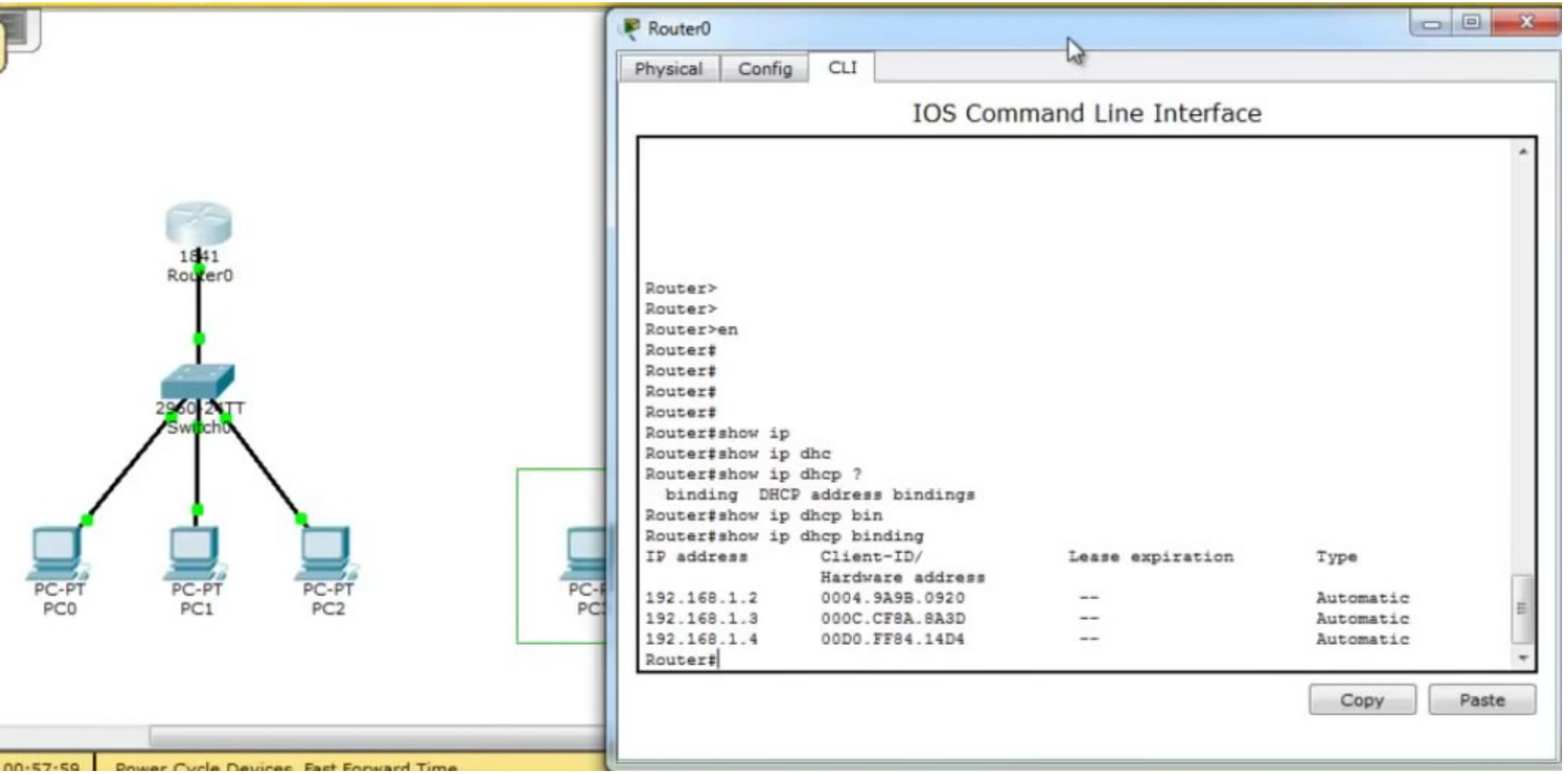
… и на PC2


PC2
IP Configuration
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.1.4
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
8.8.8.8
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2D0:FFFF:FE84:14D4
IPv6 Gateway
IPv6 DNS Server
http:
Web Browser
Cisco IP Communicator
PC-PT
PC0

Проверяем взаимодействие. Готово.

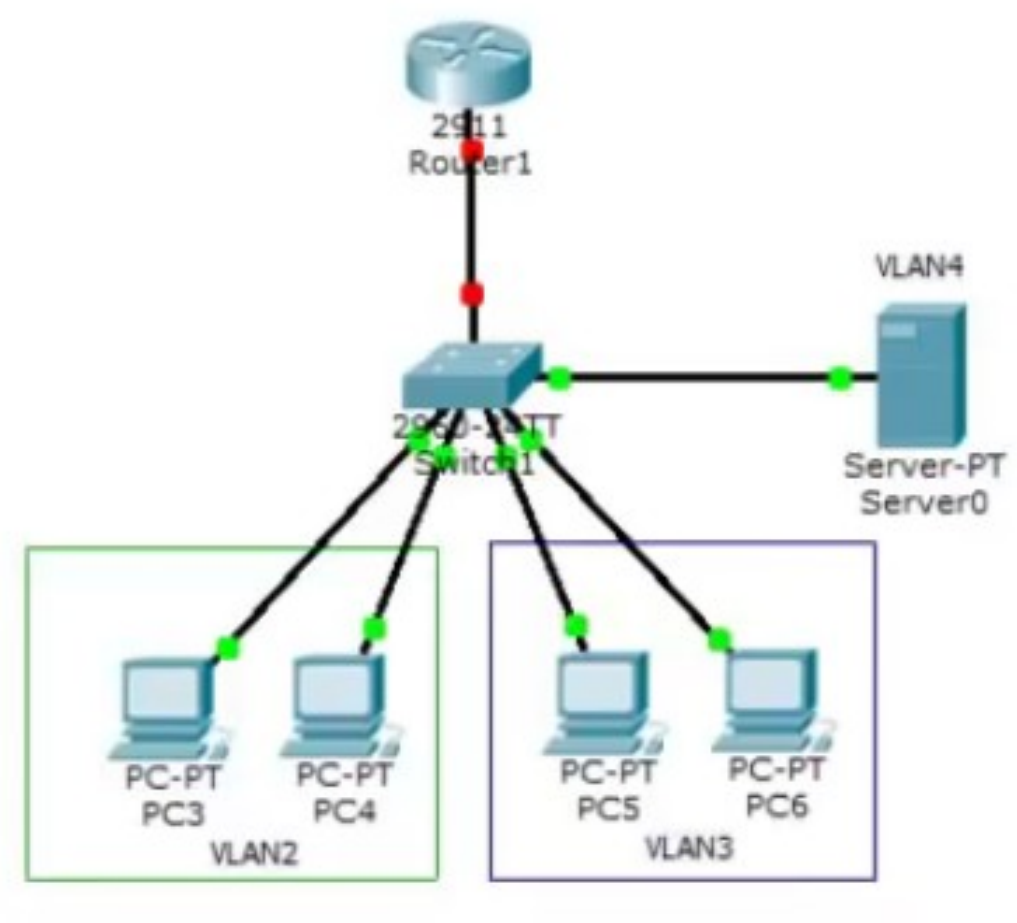


Можно посмотреть какие ip адреса каким узлам выданы.
Командой #show ip dhcp binding



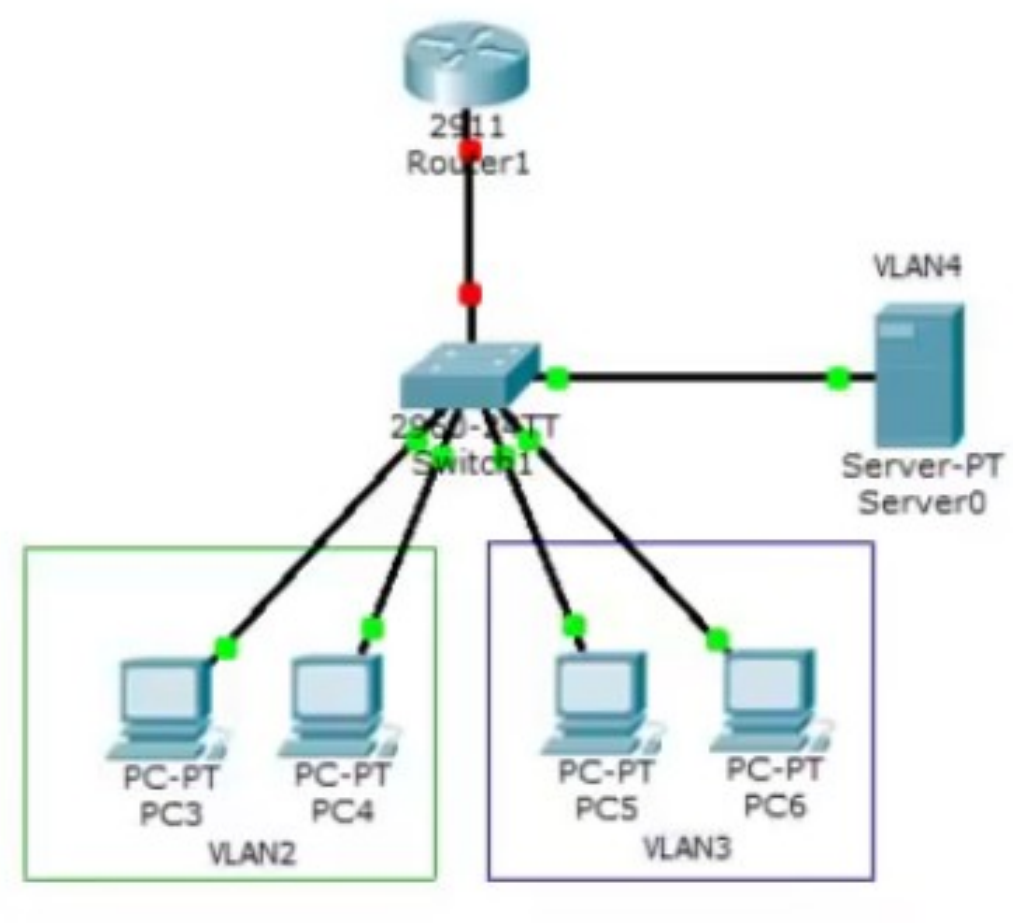
Второй пример.
Уже есть 2 VLAN'a.
(На самом деле Server-PT находится в 3-ем VLAN'e). Настраиваем коммутатор Switch1

```
> 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
```

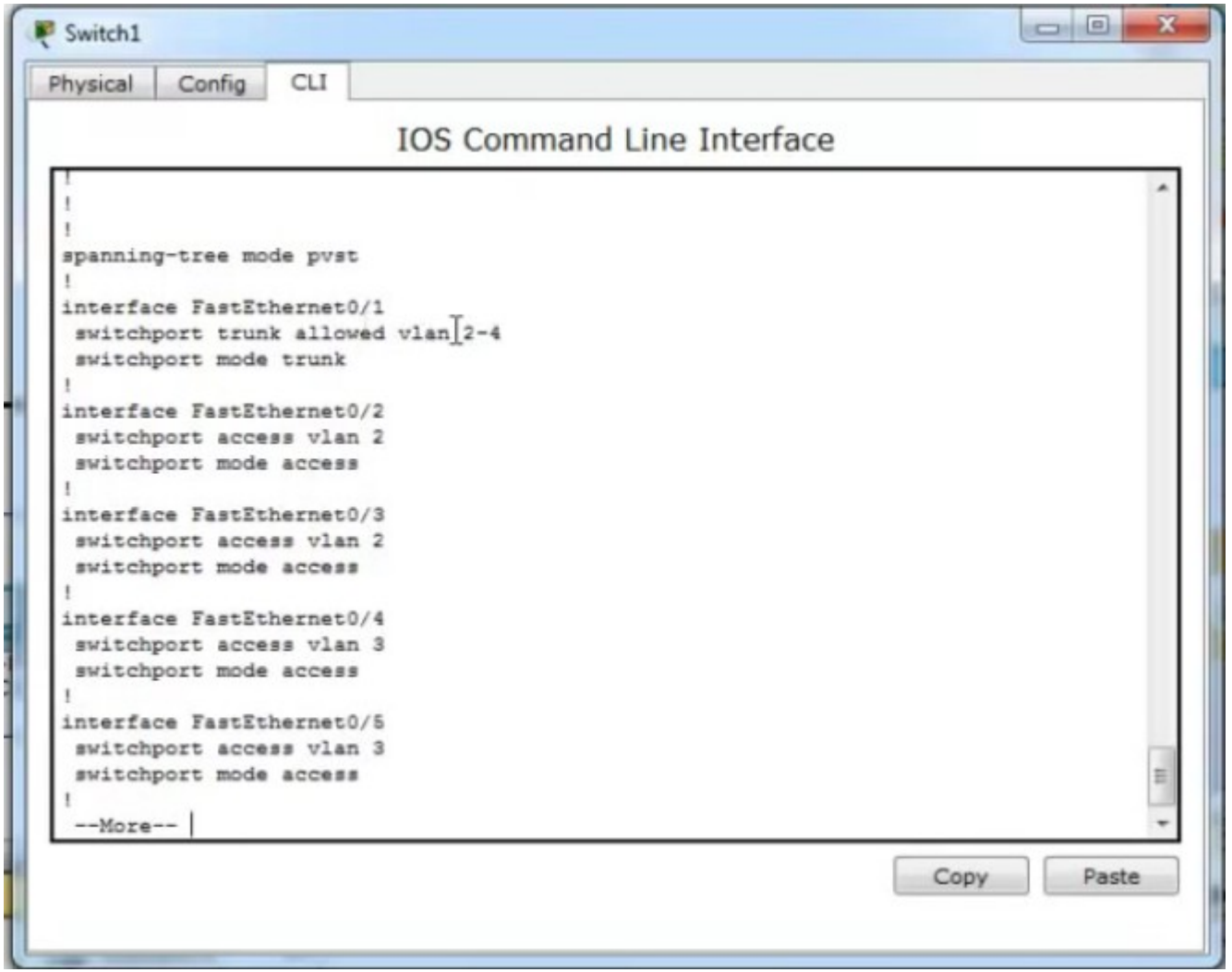


Настраиваем коммутатор Switch1

```
(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
```

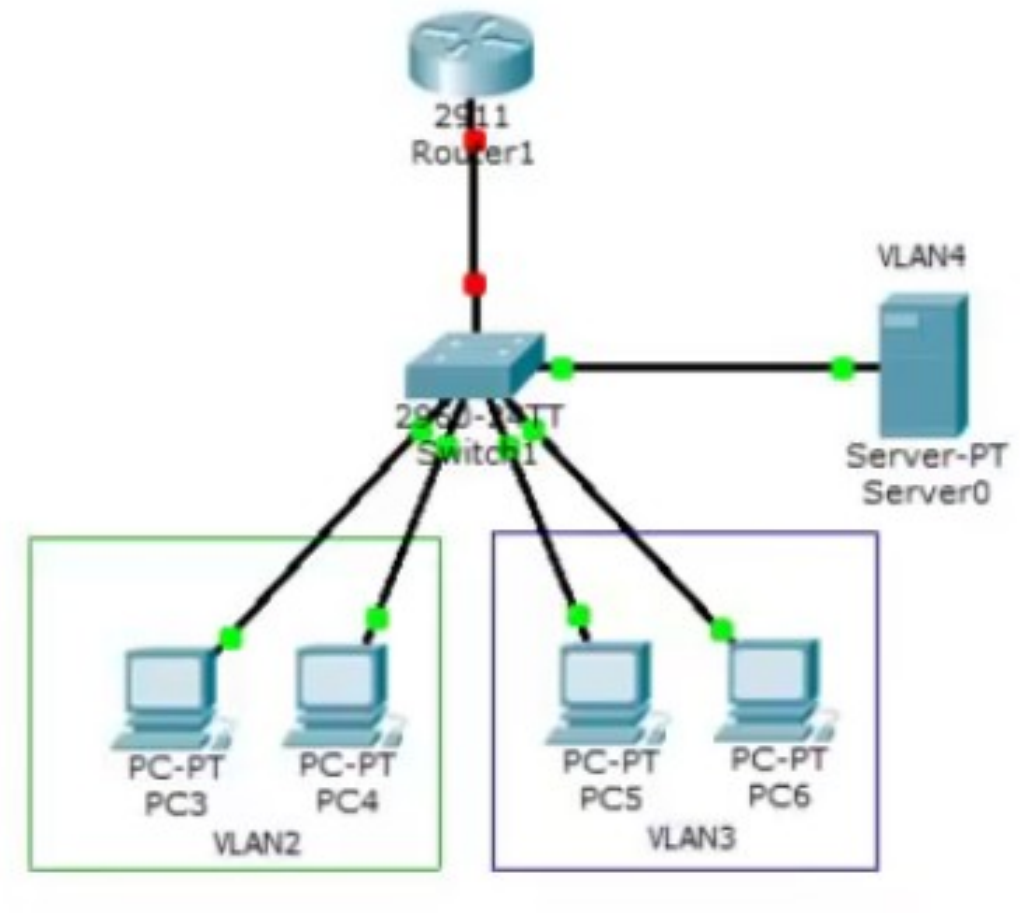


Проверяем конфигурацию Switch1



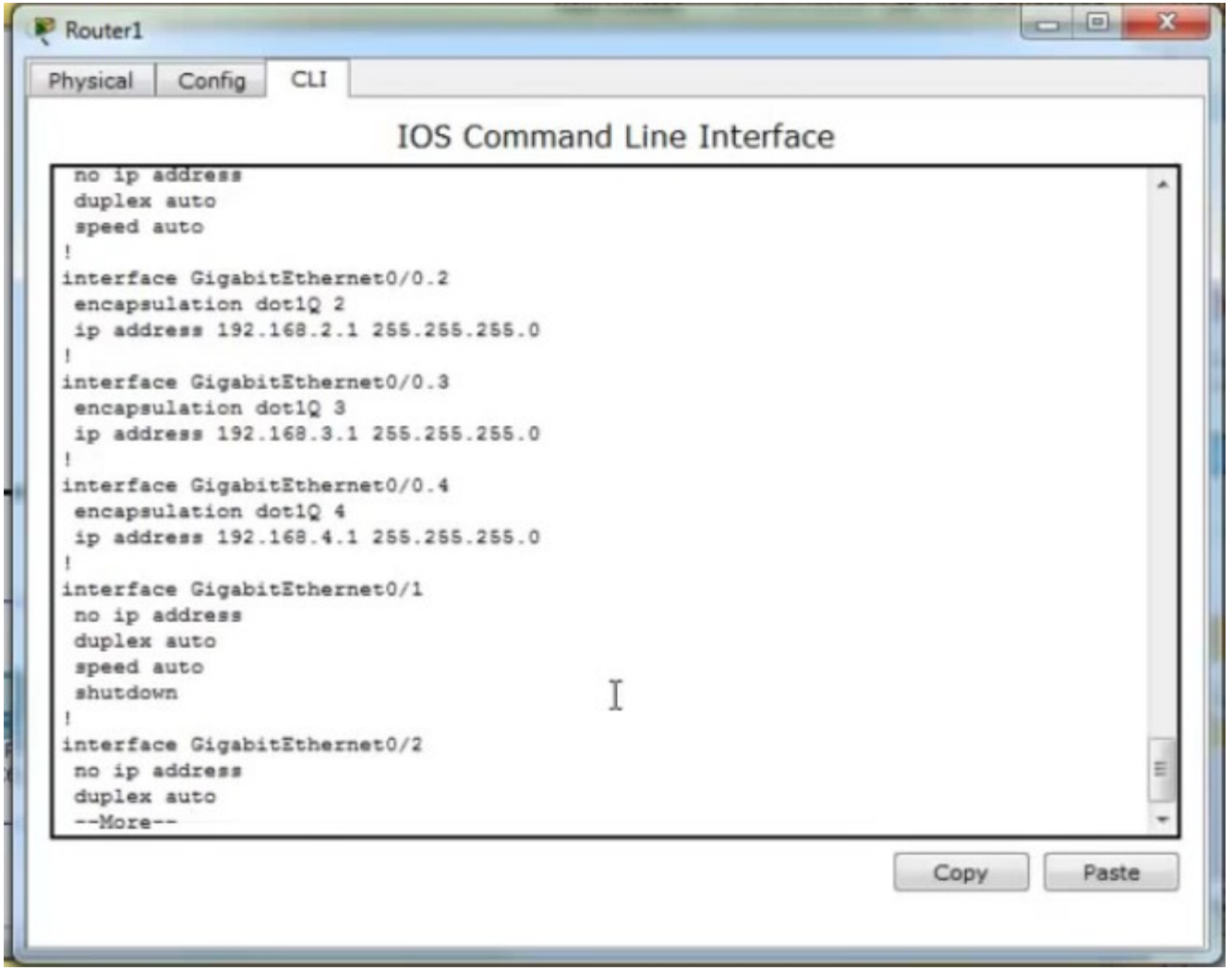
Настраиваем маршрутизатор Router1

```
> 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
```

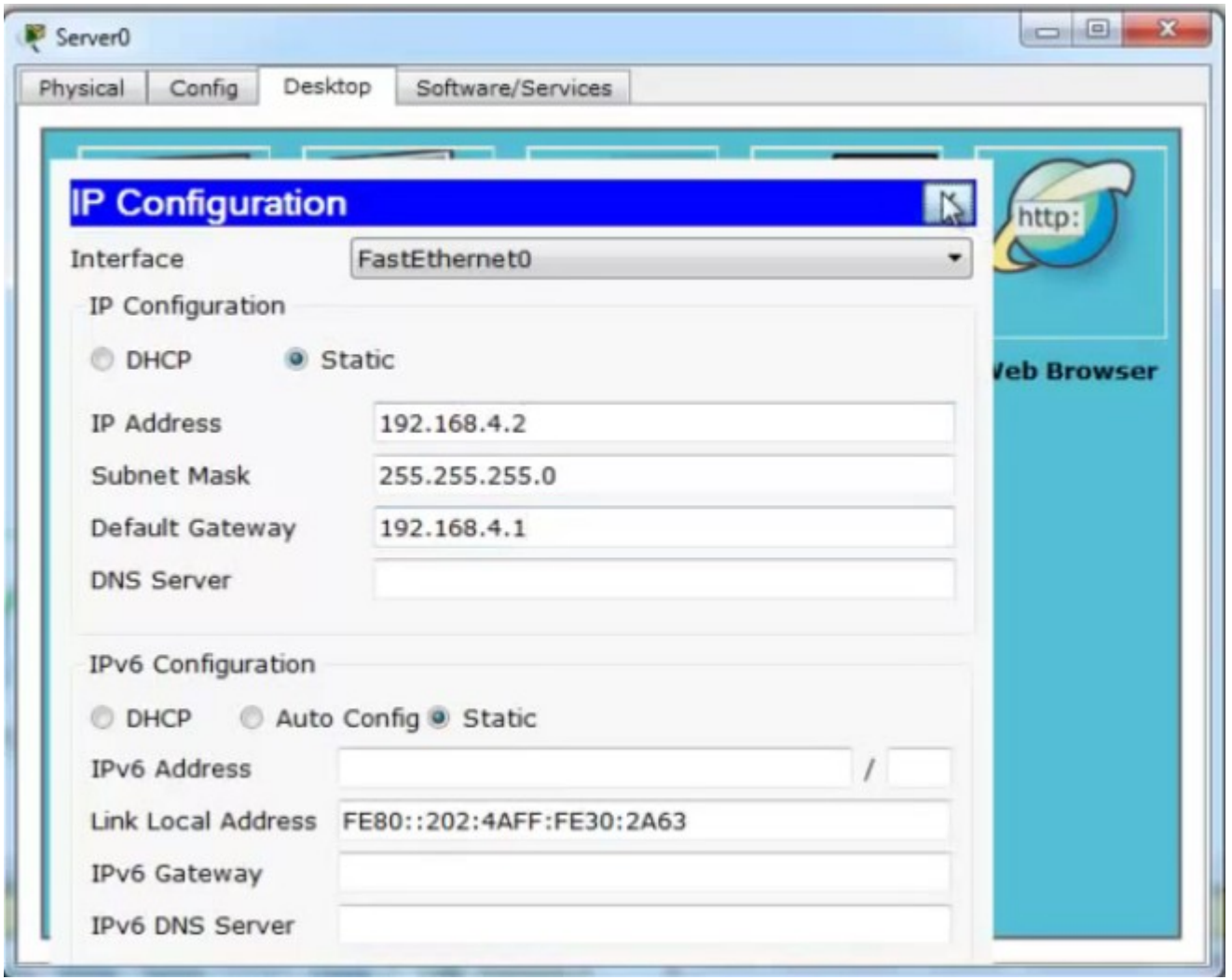


Проверяем настройки маршрутизатора Router1

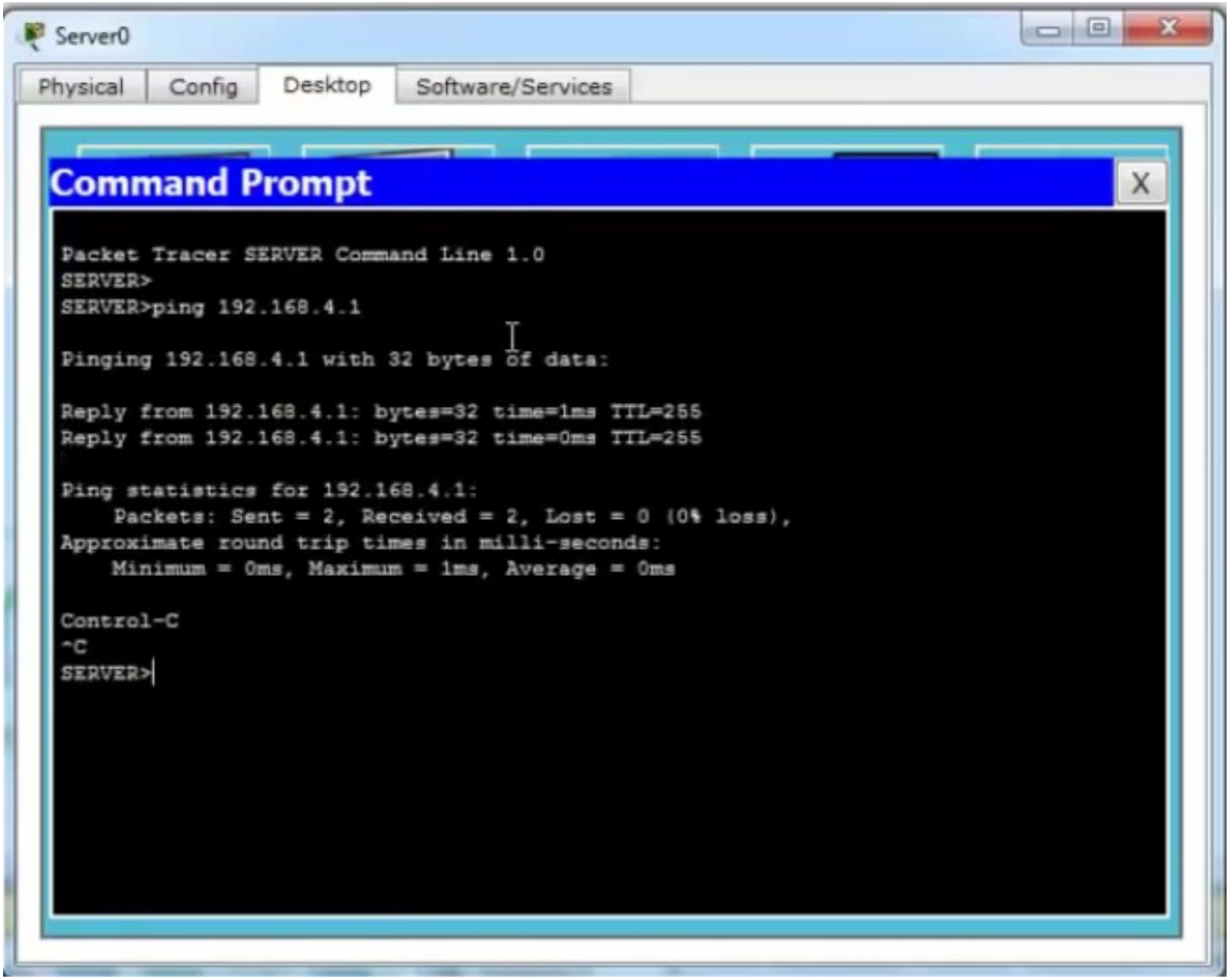
show run



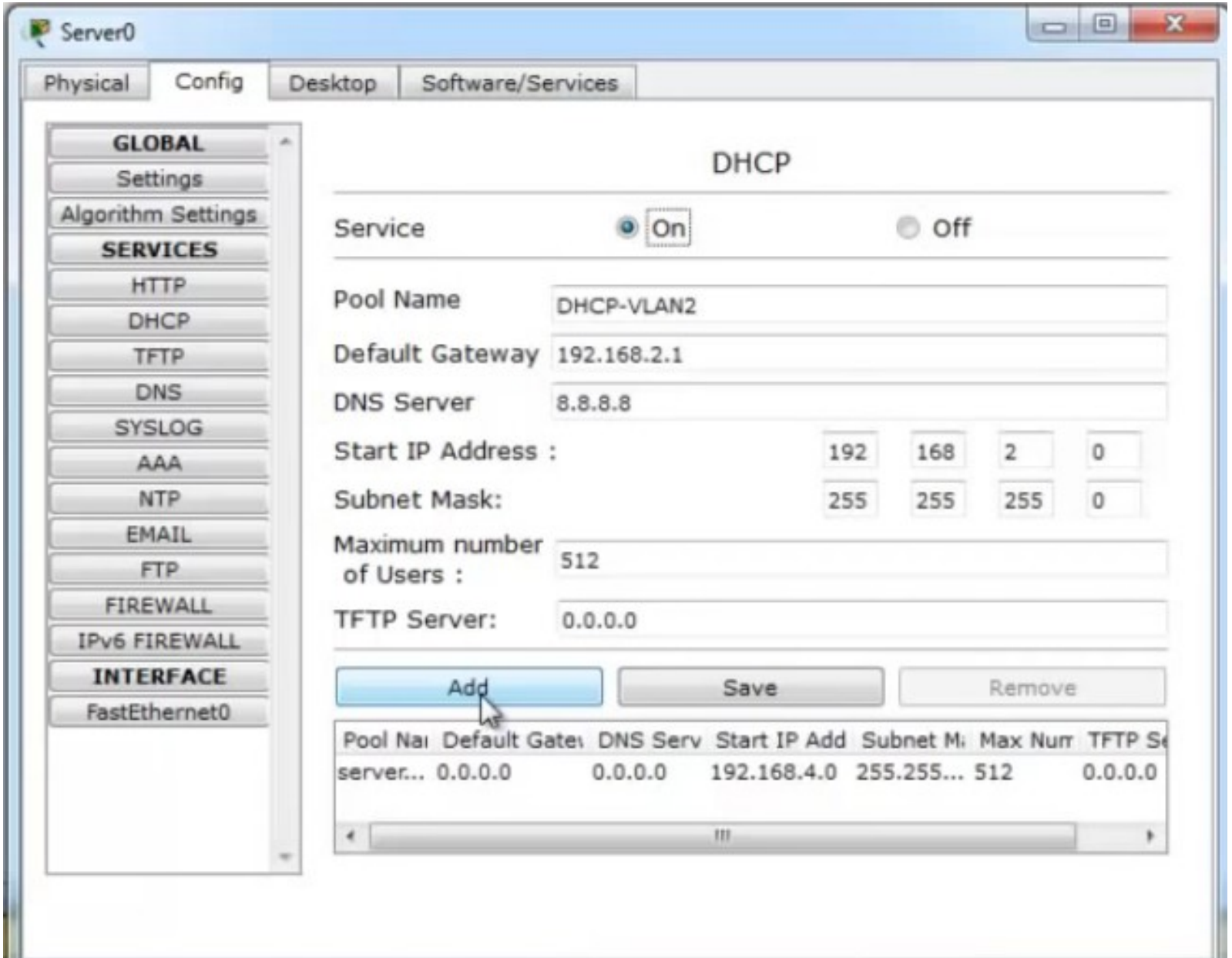
Зададим статический IP для сервера Server0



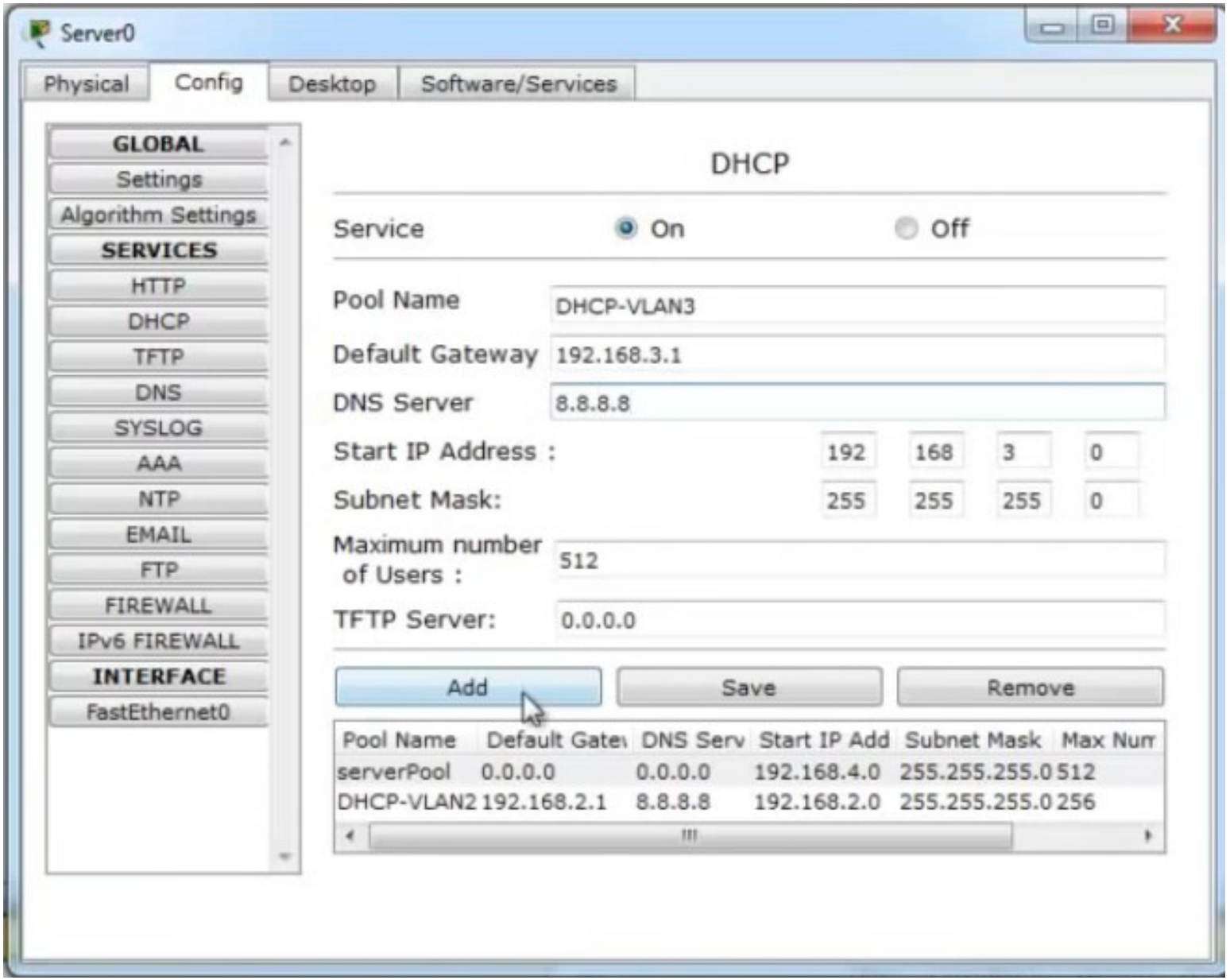
Проверим взаимодействие сервера Server0 и маршрутизатора Router1



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

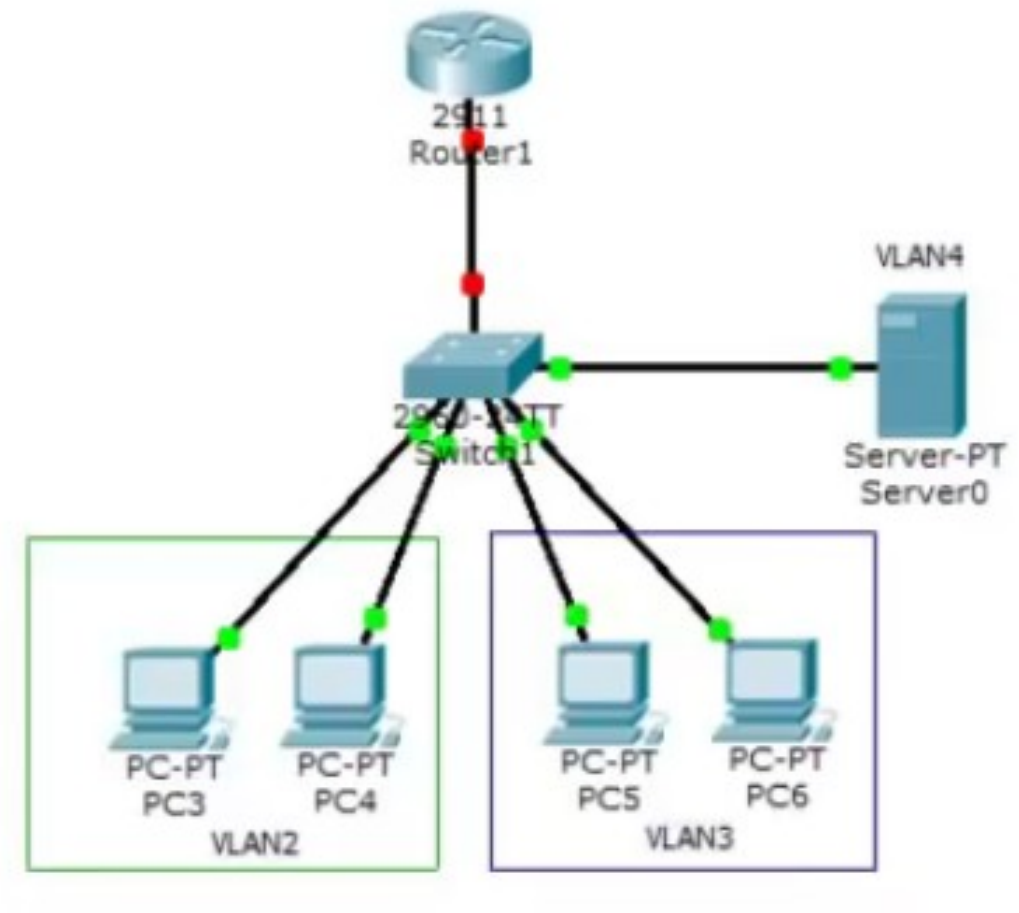


… аналогично добавляем пул для 3-го VLAN ...

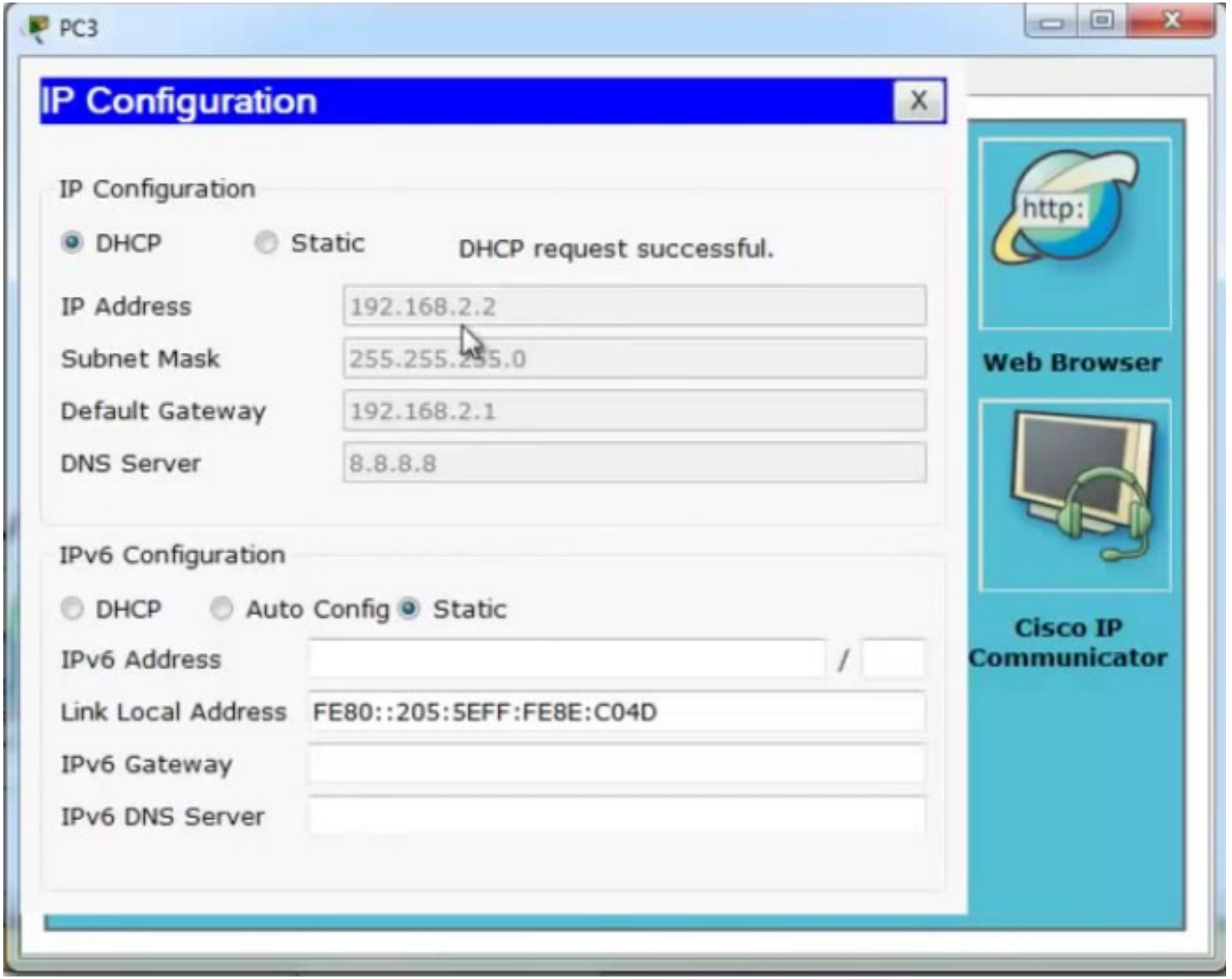


Настраиваем переадресацию DHCP запросов с компьютеров на сервер - на маршрутизаторе Router1

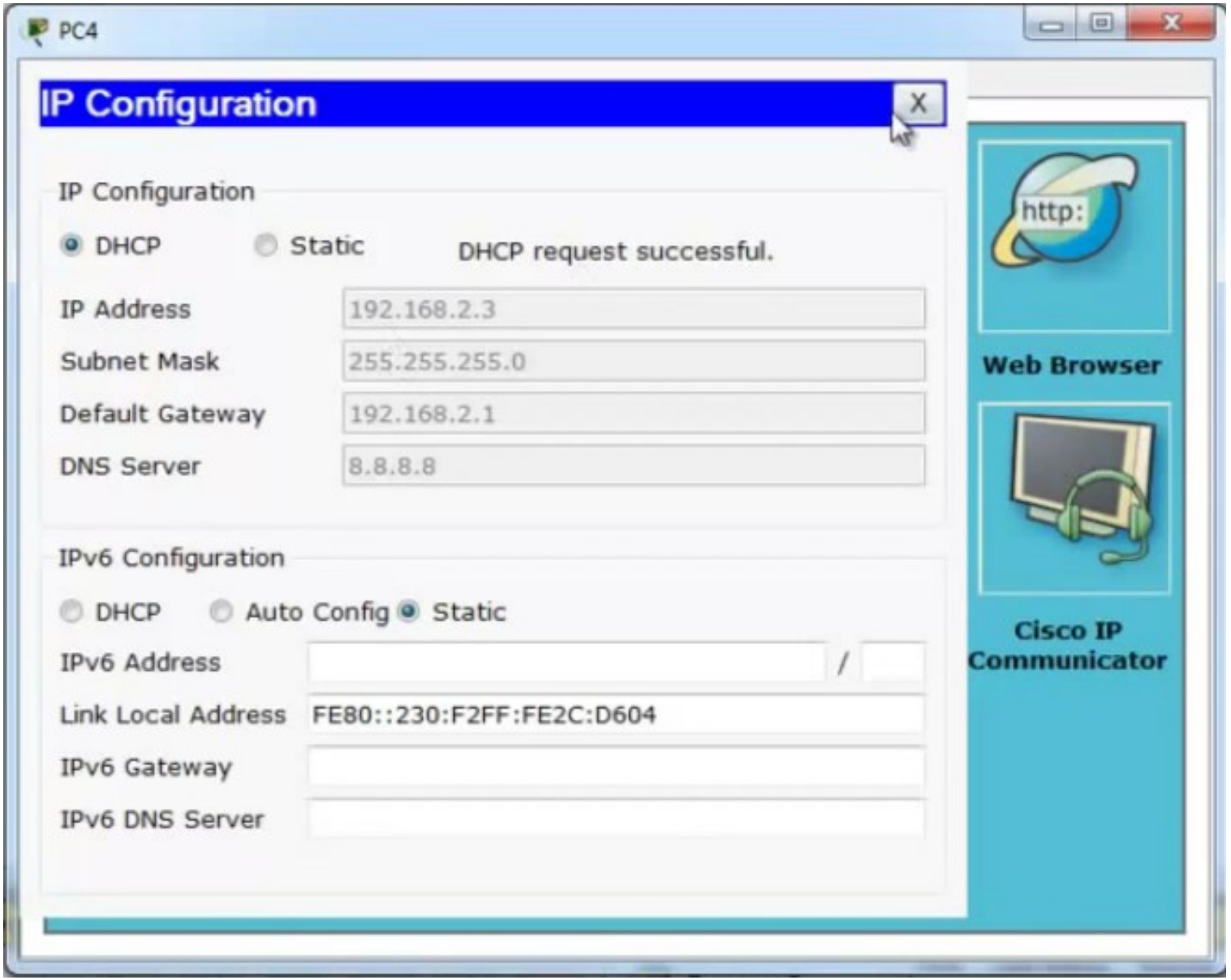
```
#conf t
(config)# int gi 0/0.2
(config-subif)# ip helper-address 192.168.4.2
(config)# exit

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

#wr mem
```



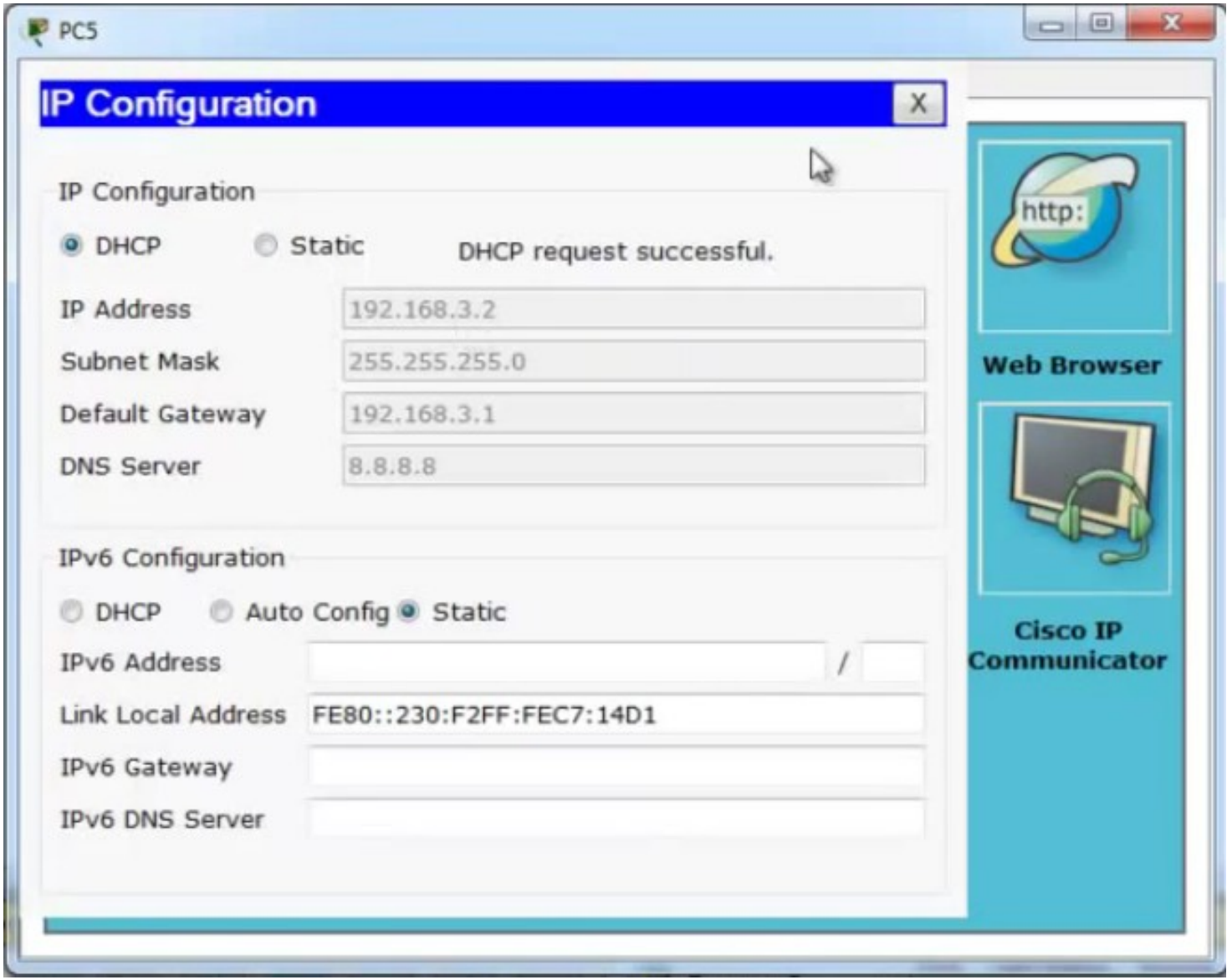
Пробуем получить IP адрес на компьютерах по DHCP



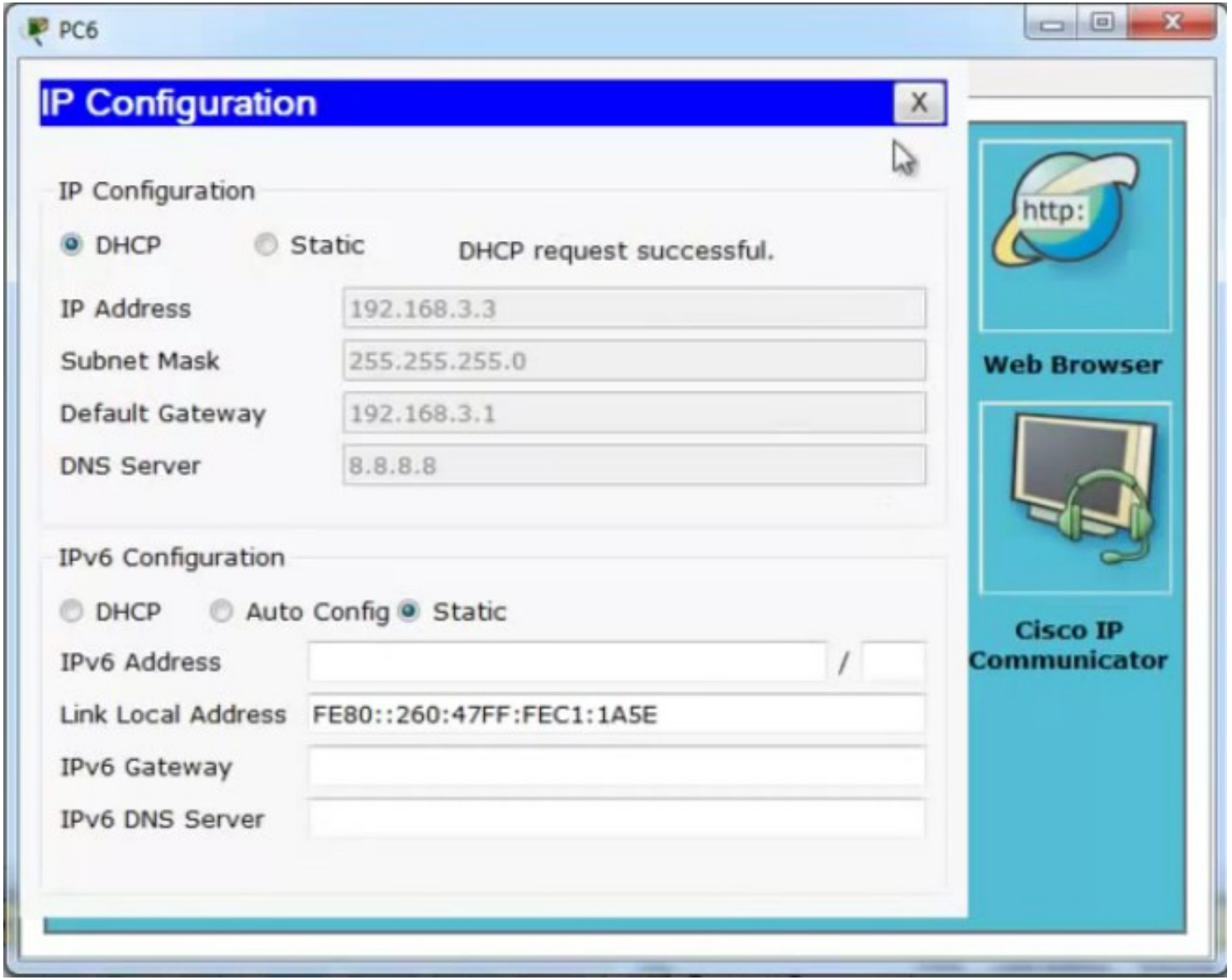
Пробуем получить IP адрес на компьютерах по DHCP



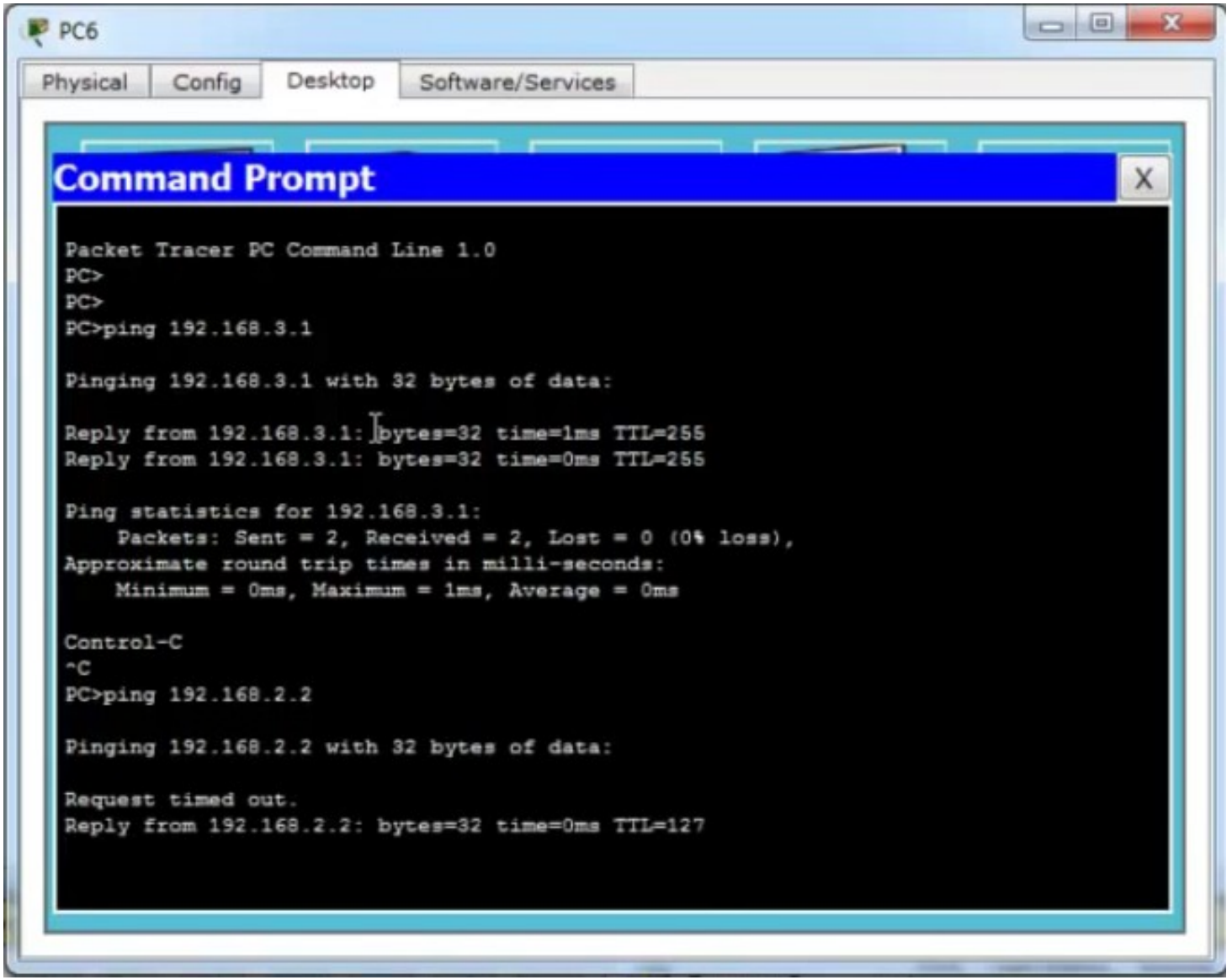
Пробуем получить IP адрес на компьютерах по DHCP



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)

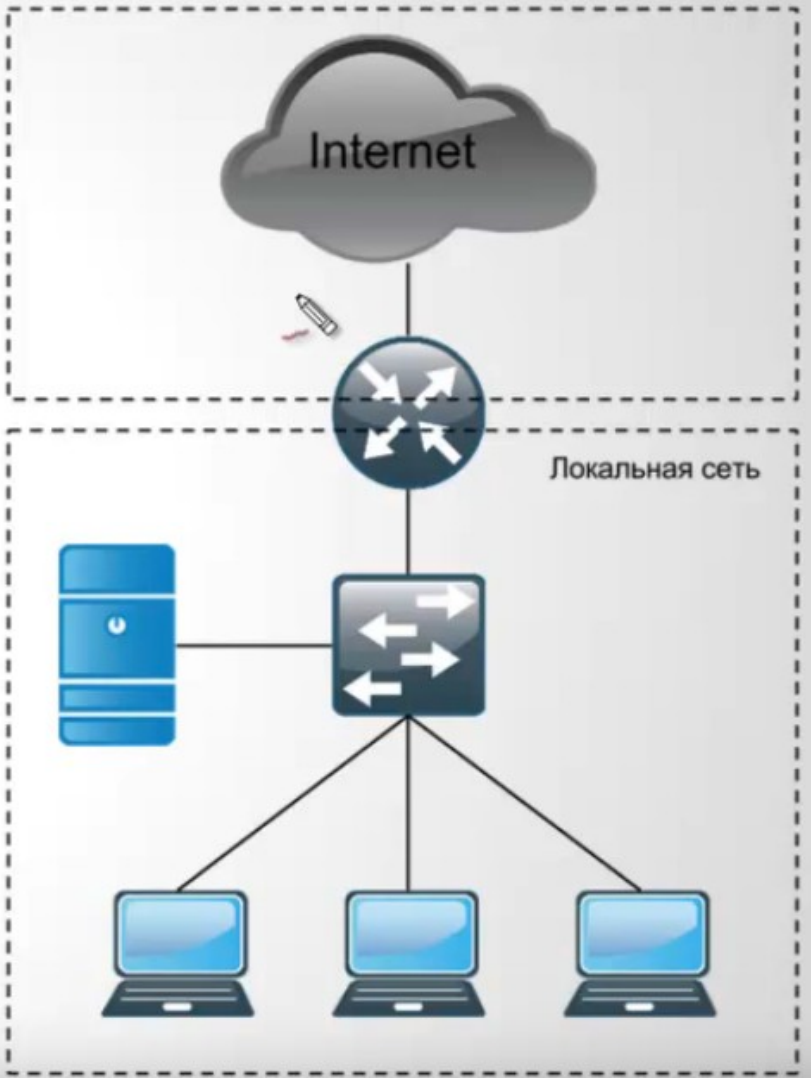
Более подробно читайте здесь

Частный IP адрес (Серый IP)

От 10.0.0.0 до 10.255.255.255 с маской 255.0.0.0.0 (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



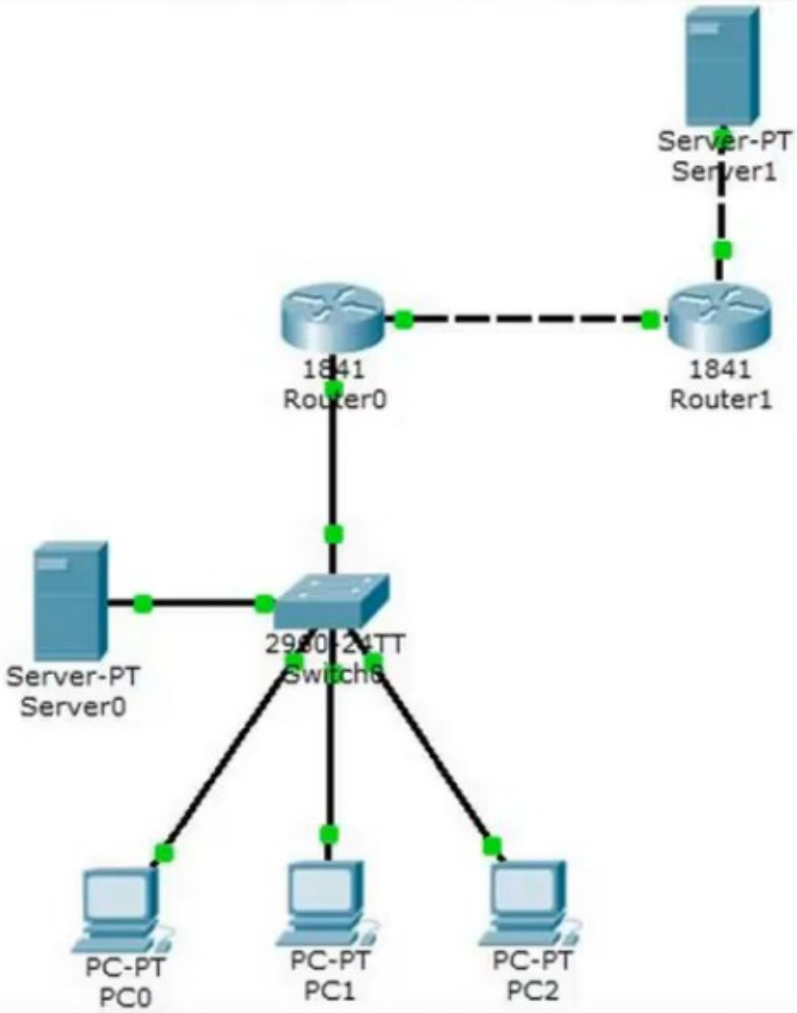
NAT — Network Address Translation

Настройка PAT

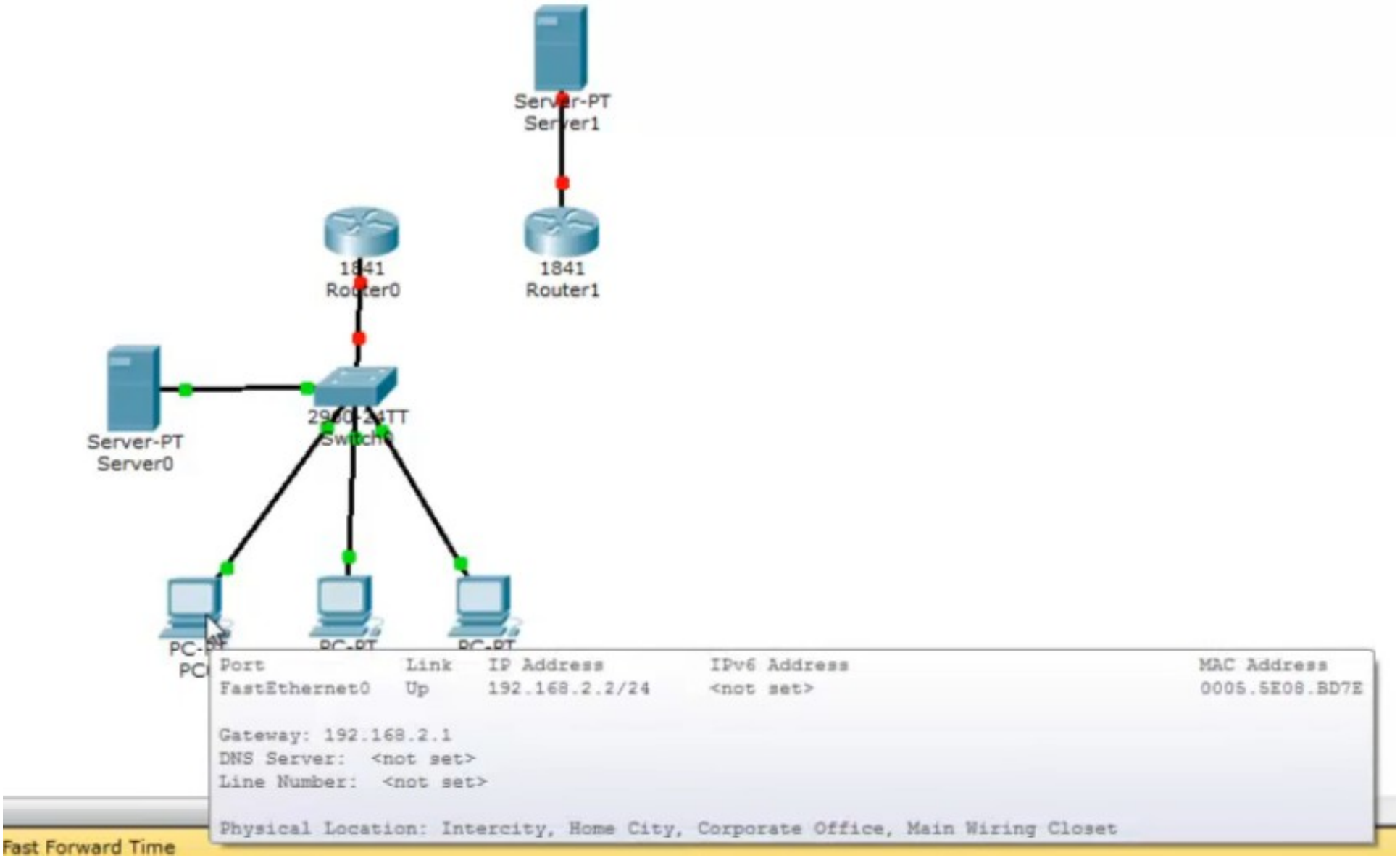
```
interface FastEthernet0/0
 ip nat outside
interface FastEthernet0/1.2
 ip nat inside
interface FastEthernet0/1.3
 ip nat inside

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

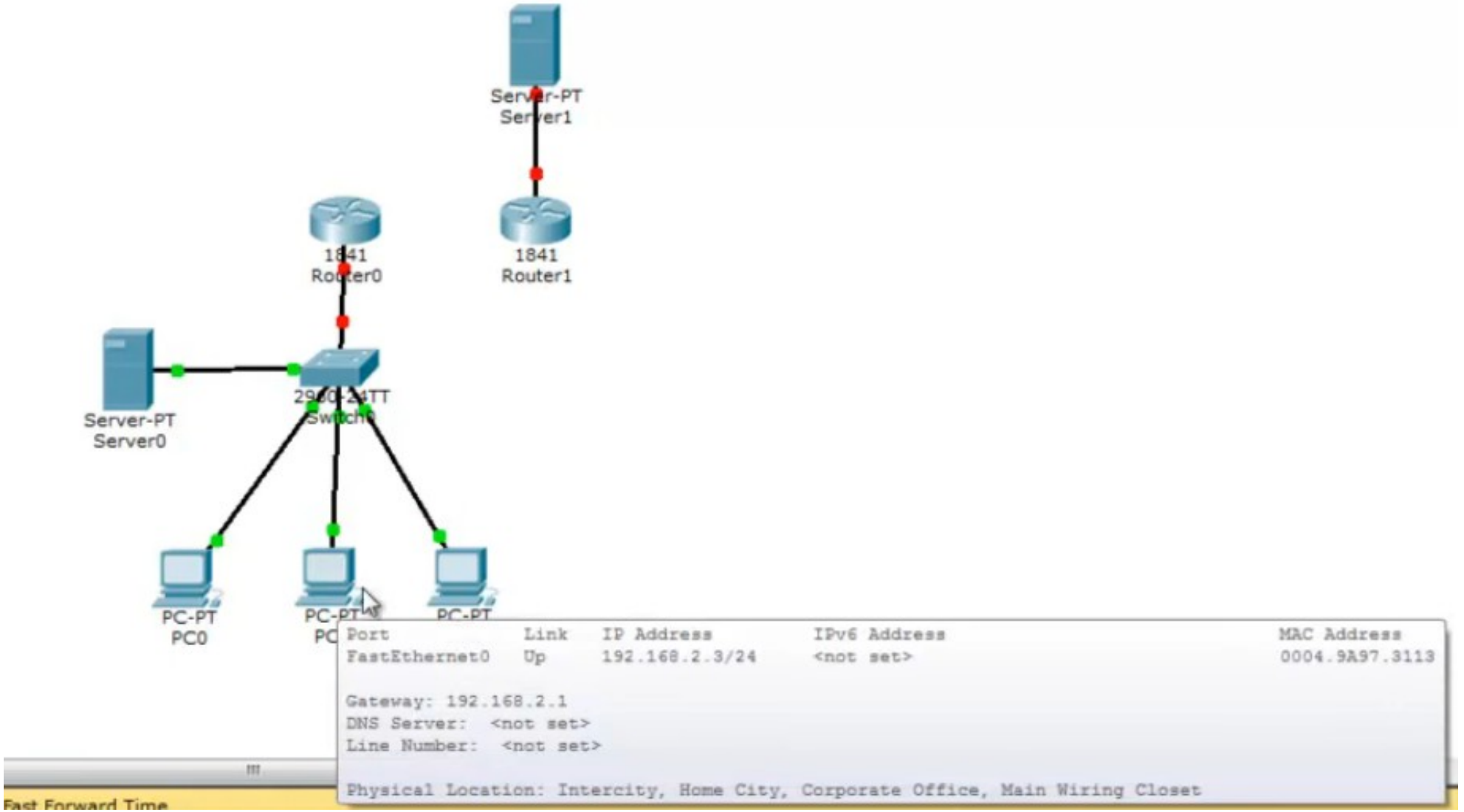
```
ip nat inside source static tcp 192.168.3.2 80 213.234.10.2 80

show ip nat translations
```



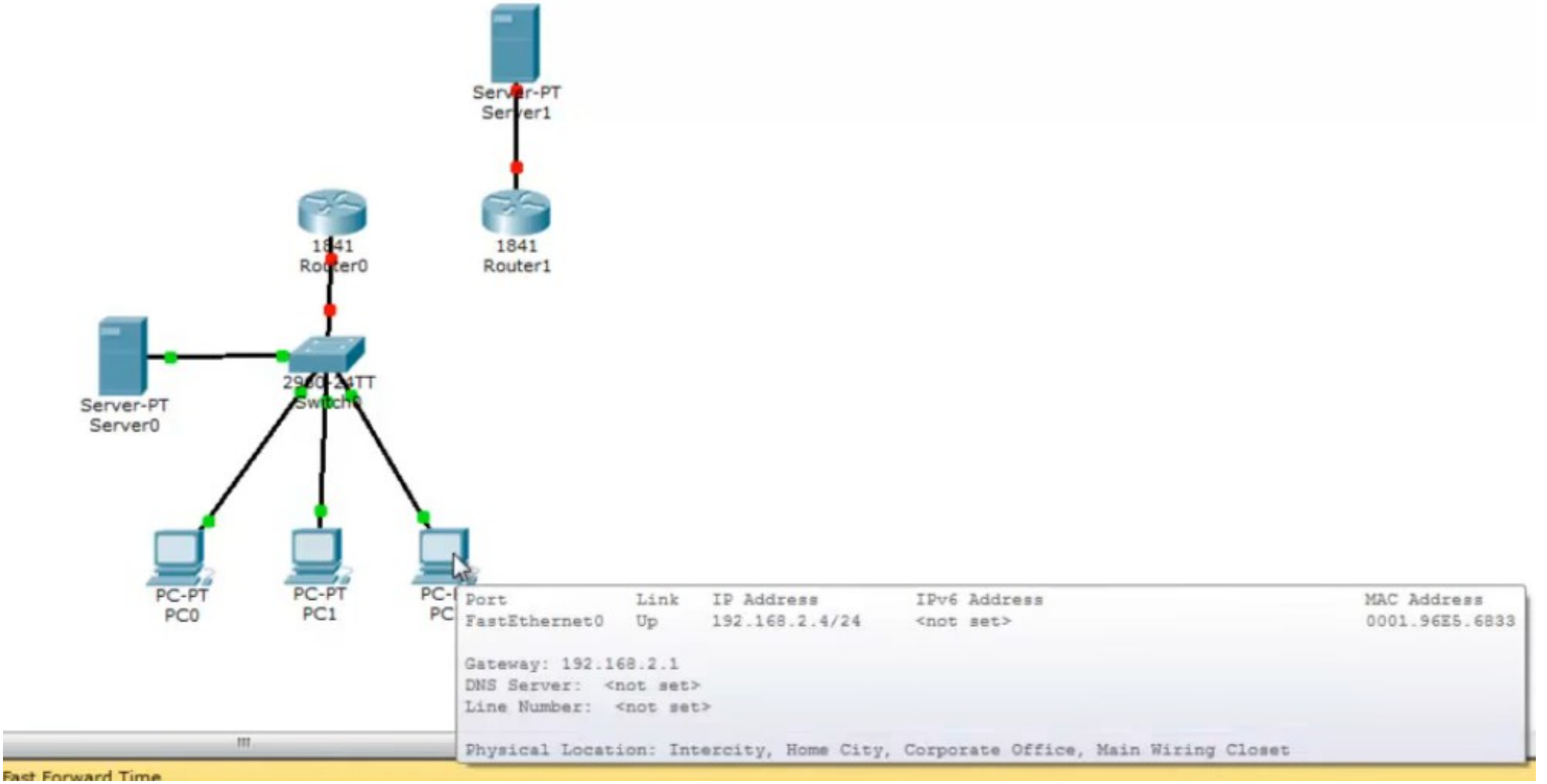
Ip адрес PC0


Server-PT
Server1
1841
Router0
1841
Router1
Server-PT
Server0
Port Link IP Address IPv6 Address MAC Address
FastEthernet0 Up 192.168.2.2/24 <not set> 0005.5E08.BD7E
Gateway: 192.168.2.1
DNS Server: <not set>
Line Number: <not set>
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
Fast Forward Time

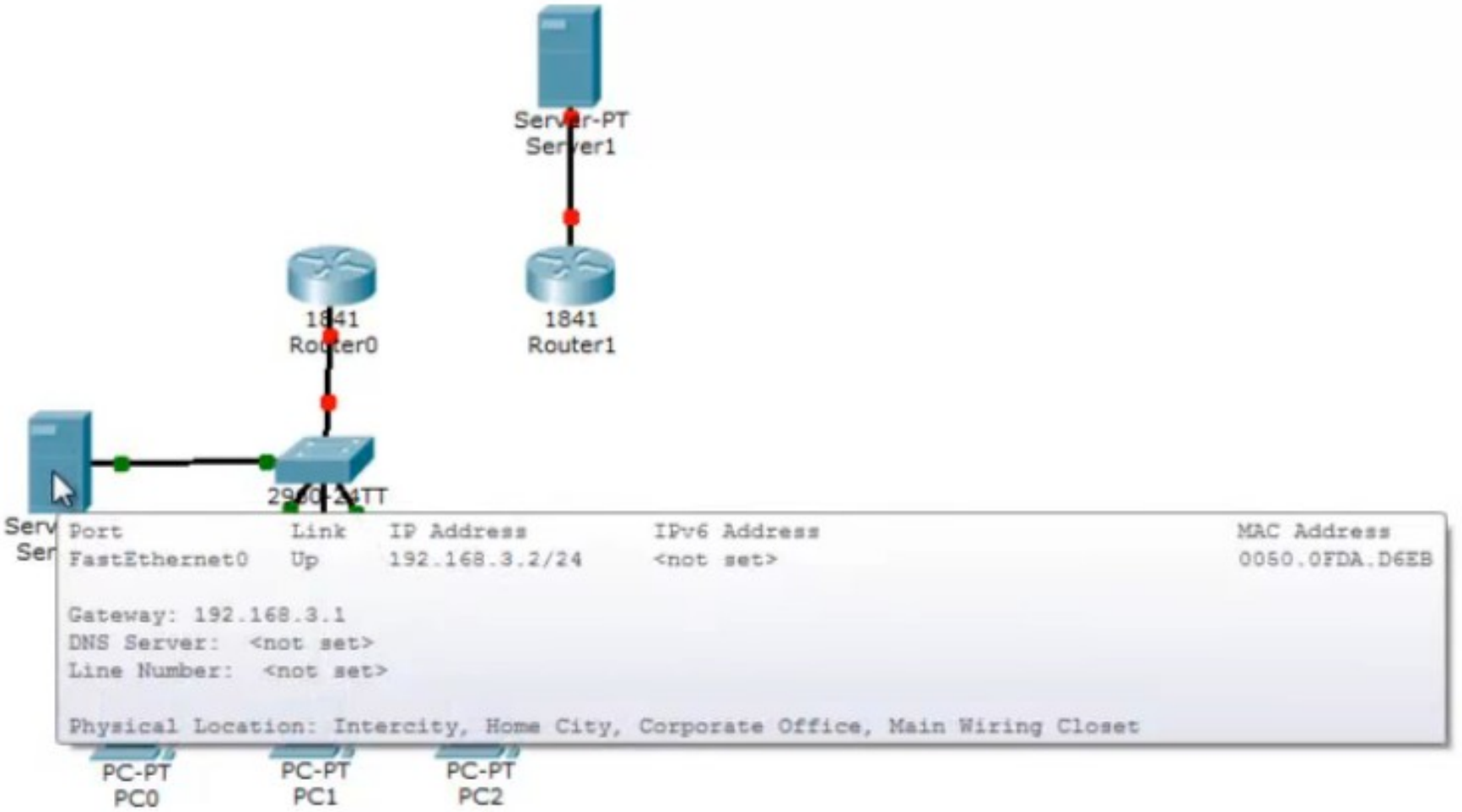
Ip адрес PC1


Server-PT
Server1
1841
Router0
1841
Router1
Server-PT
Server0
PC-PT
PC0
Port Link IP Address IPv6 Address MAC Address
FastEthernet0 Up 192.168.2.3/24 <not set> 0004.9A97.3113
Gateway: 192.168.2.1
DNS Server: <not set>
Line Number: <not set>
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
Fast Forward Time

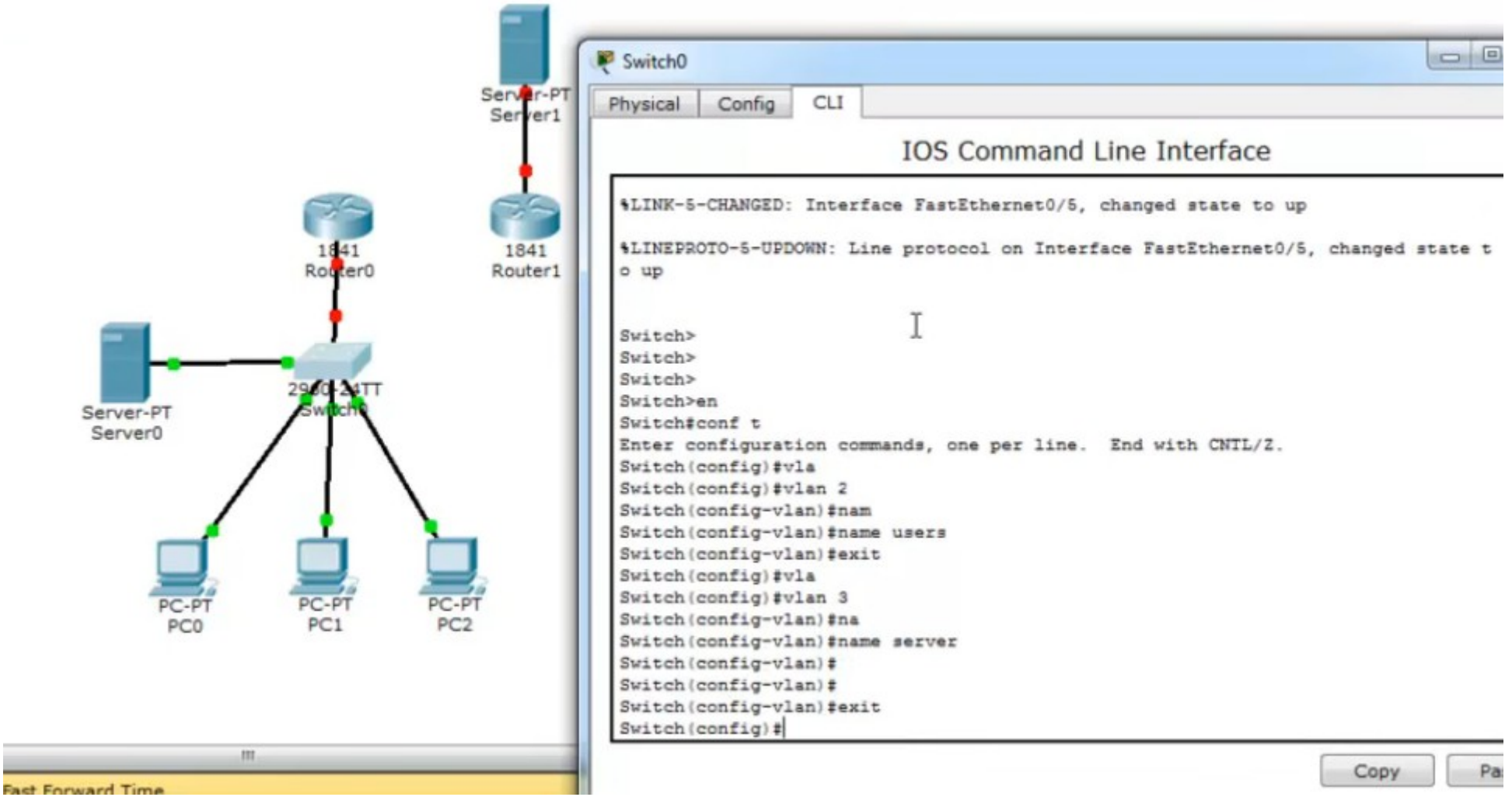
Ip адрес PC2


Server-PT
Server1
1841
Router0
1841
Router1
Server-PT
Server0
PC-PT
PC0
PC-PT
PC1
Port Link IP Address IPv6 Address MAC Address
FastEthernet0 Up 192.168.2.4/24 <not set> 0001.96E5.6833
Gateway: 192.168.2.1
DNS Server: <not set>
Line Number: <not set>
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
Fast Forward Time

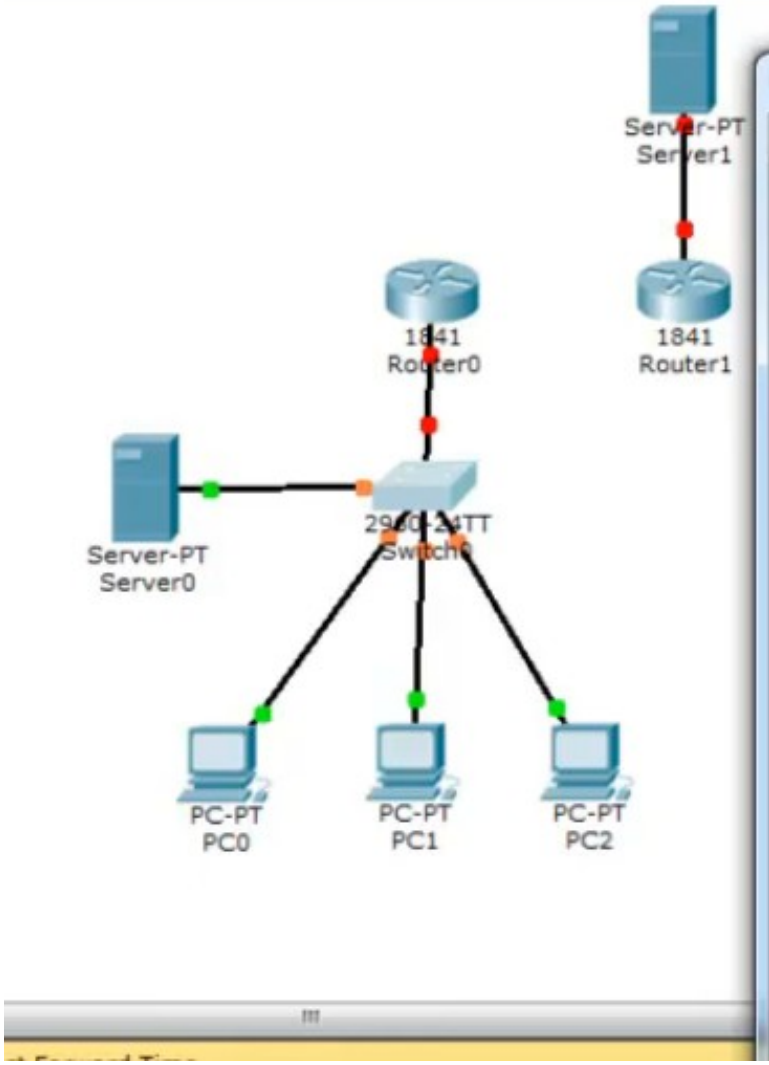
Ip адрес Sever0



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



Назначаем VLAN на порты коммутатора



Switch0

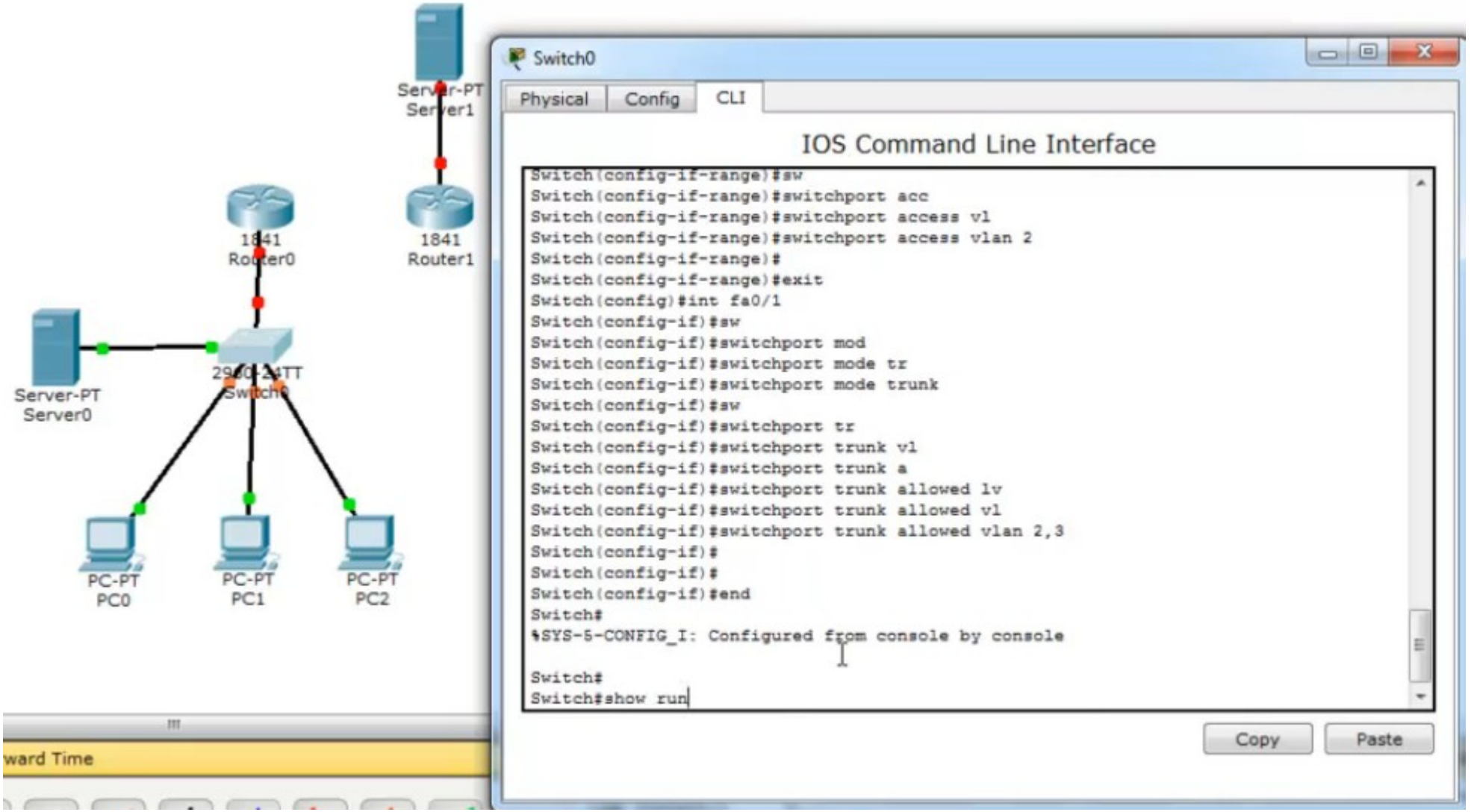
Physical | Config | CLI

IOS Command Line Interface

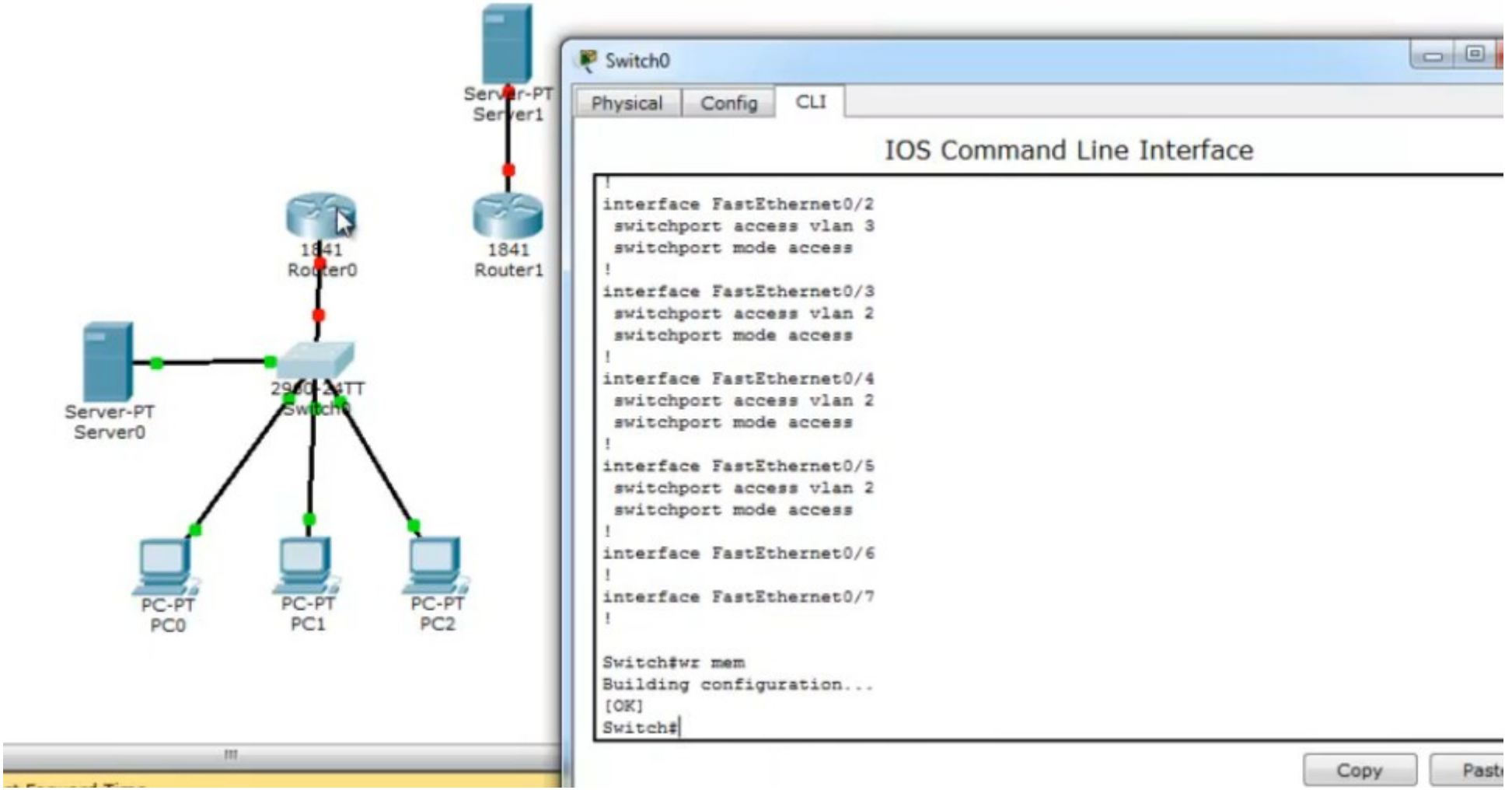
```
Switch(config)#
Switch(config)#int fa0/2
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vl
Switch(config-if)#switchport access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

Copy | Past

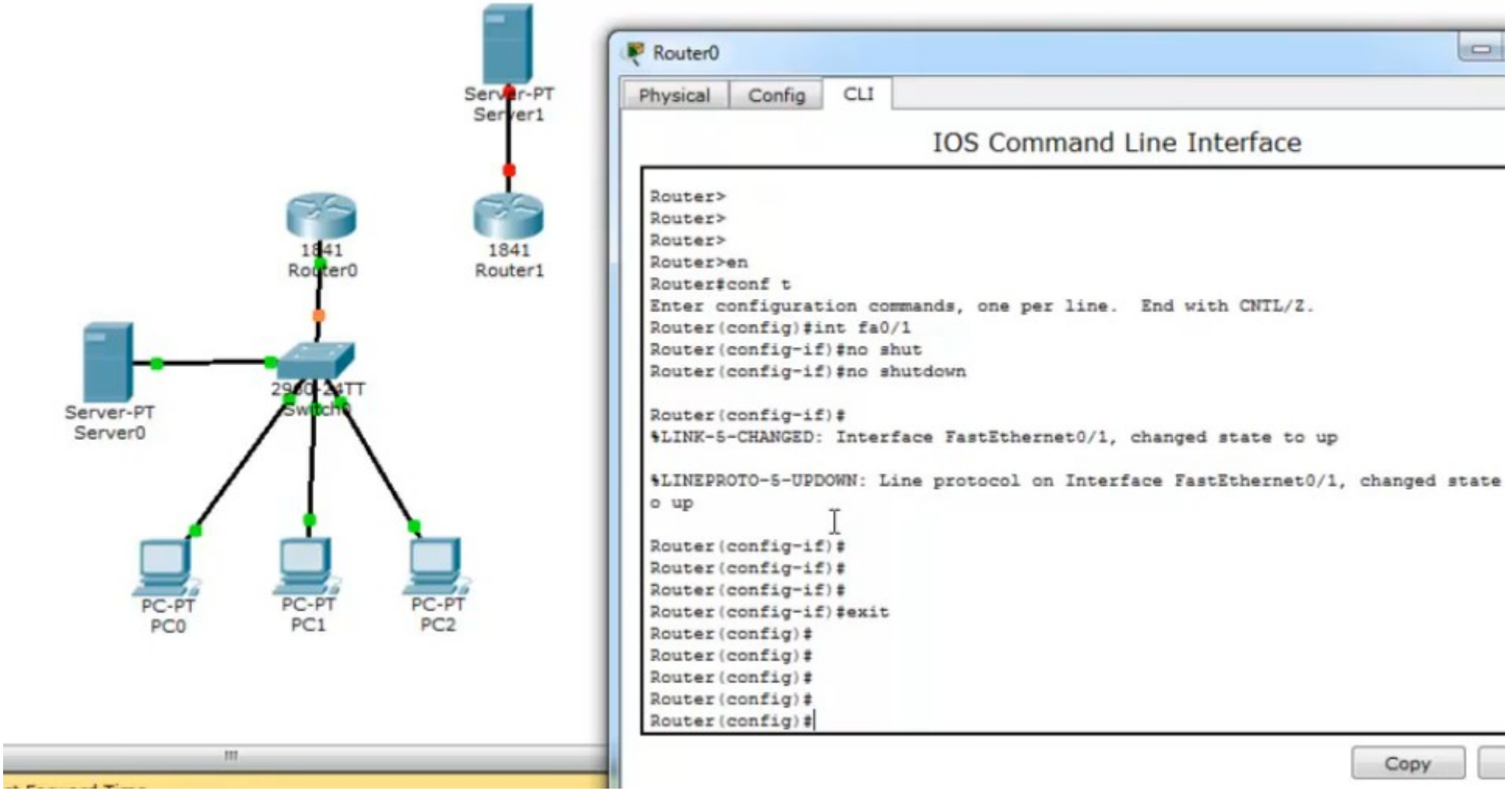
Назначаем trunk порт, проверяем конфигурацию



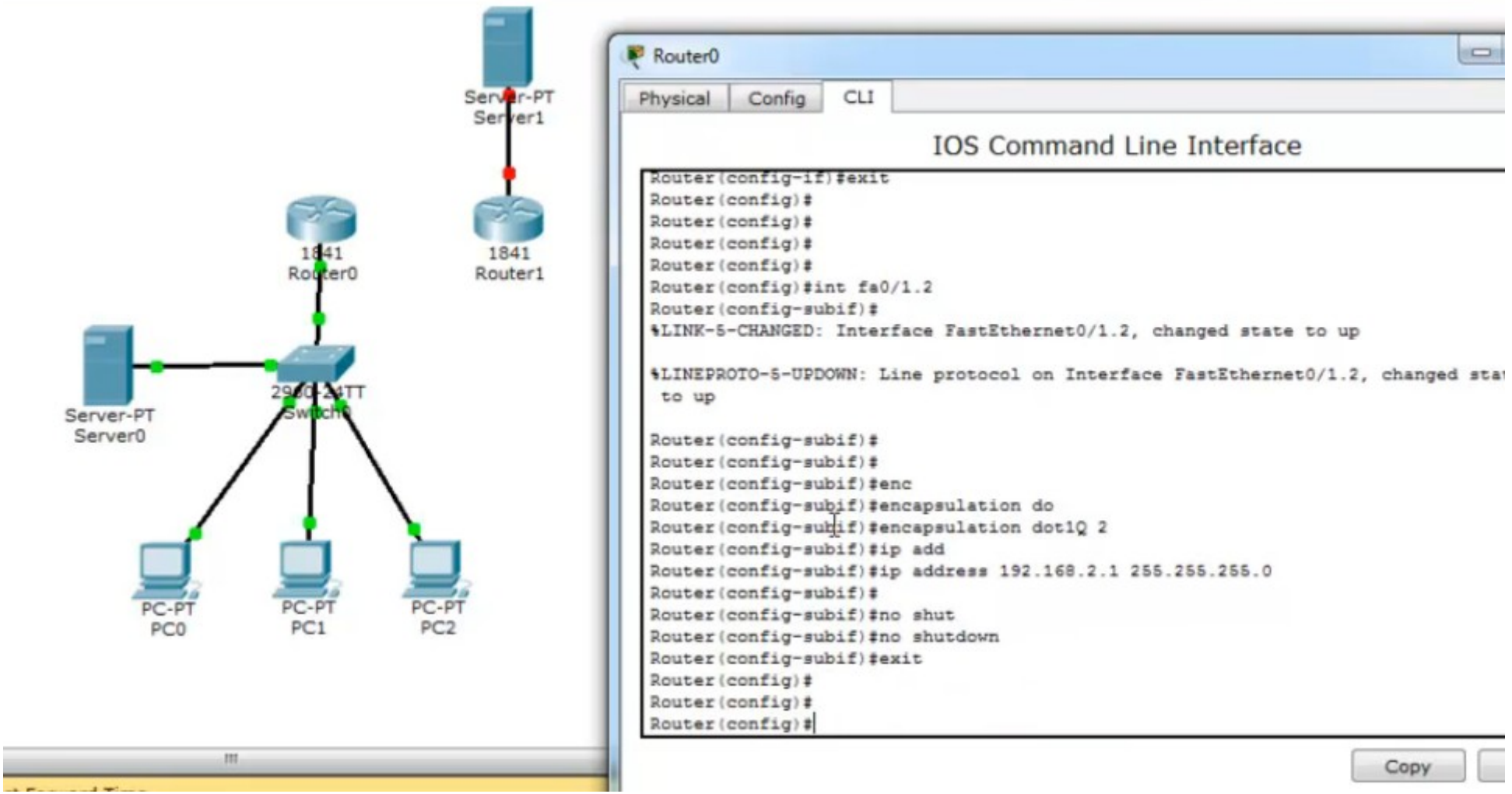
Проверяем конфигурацию, сохраняем



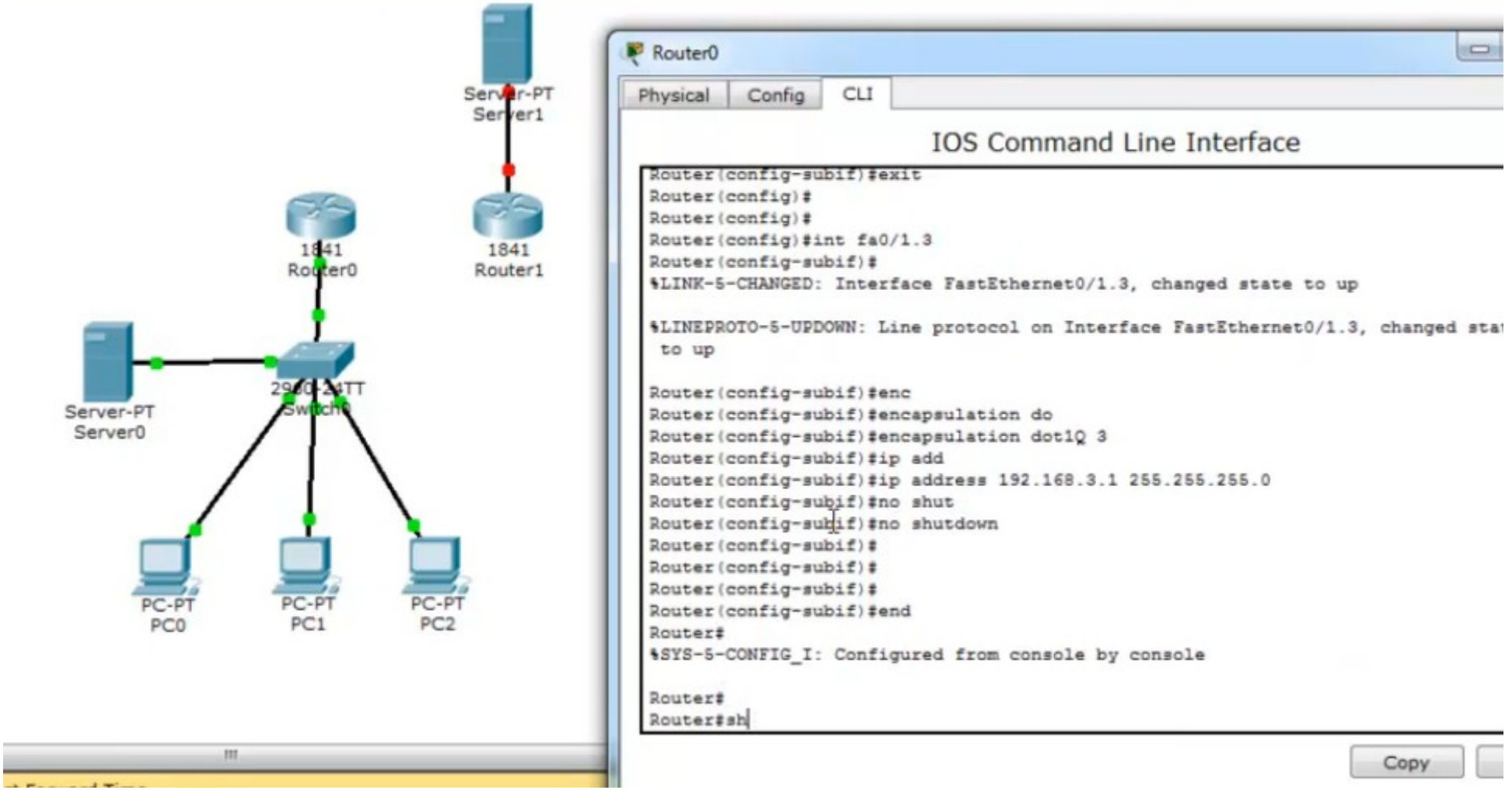
Настраиваем Router0, активируем интерфейс fa0/1



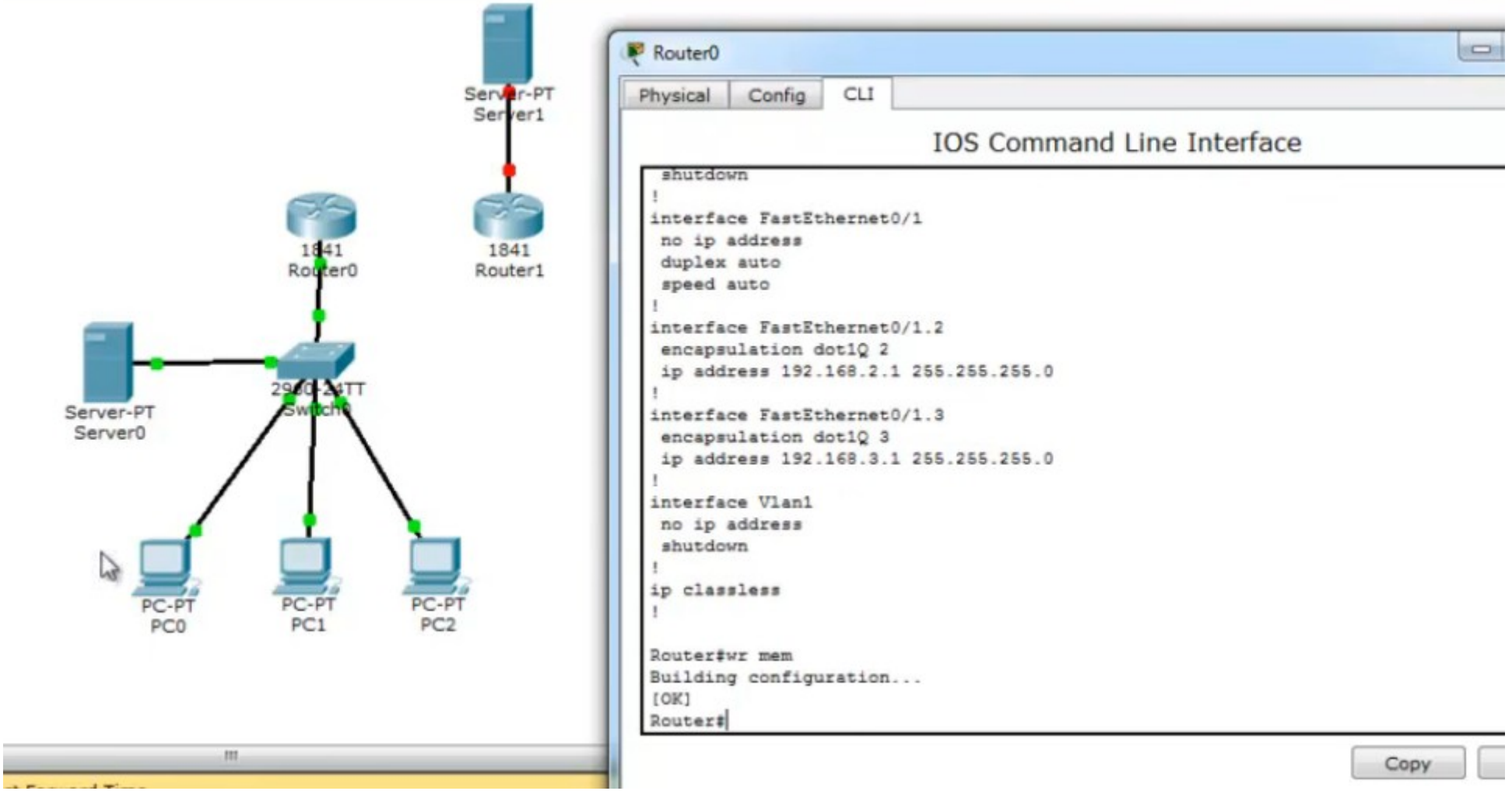
Создадим субинтерфейс для VLAN 2, назначим ip



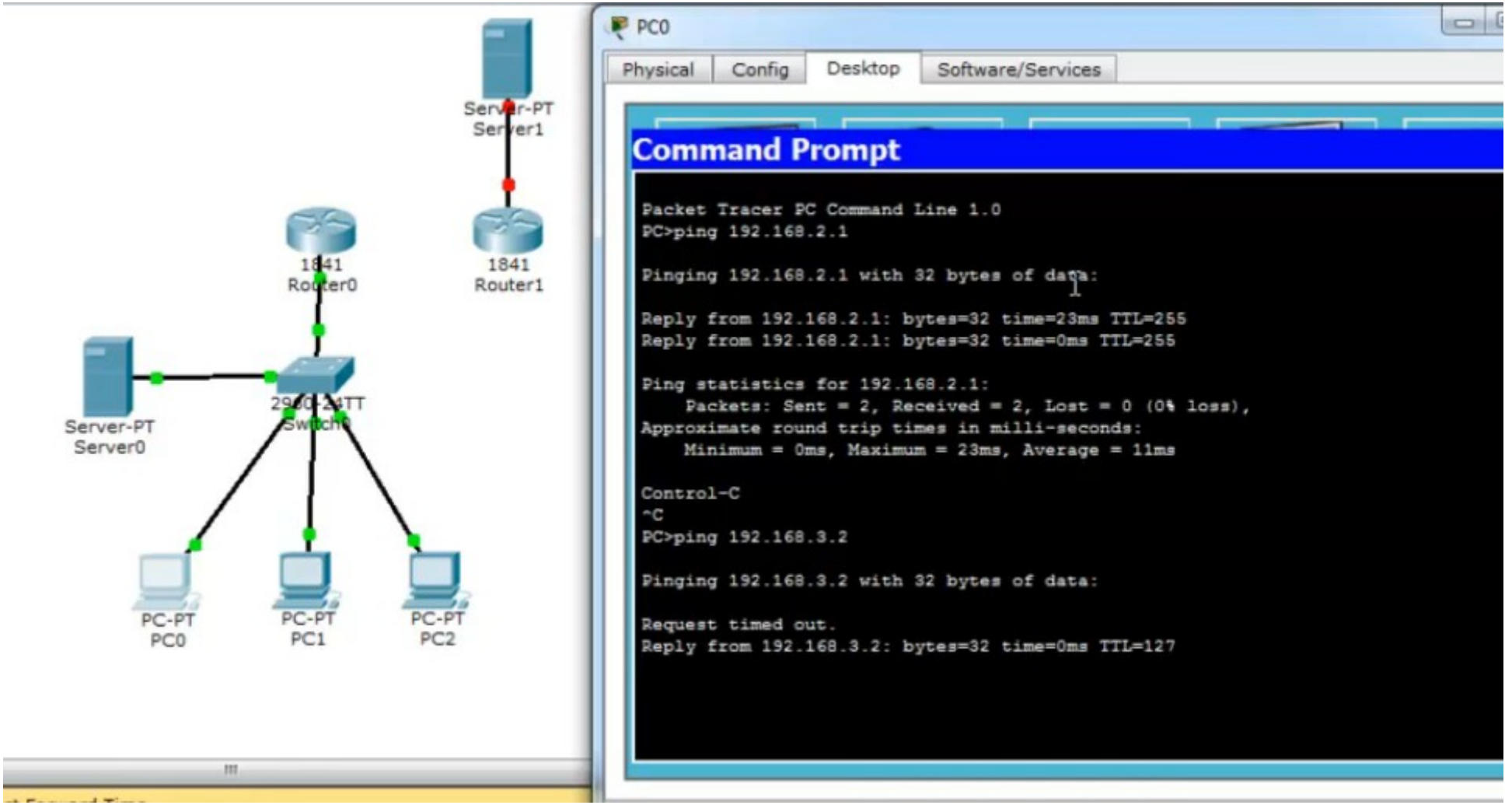
Создадим еще один субинтерфейс для VLAN3, назначим ip



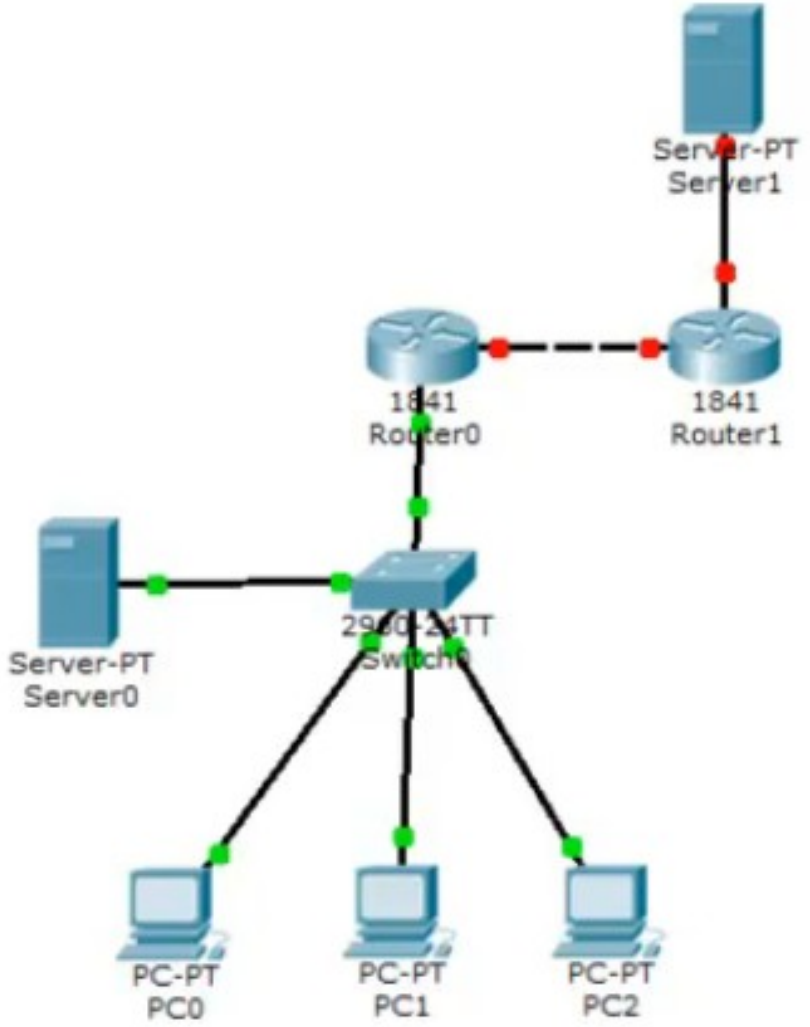
Проверяем, что созданы два субинтерфейса, записываем конфигурацию



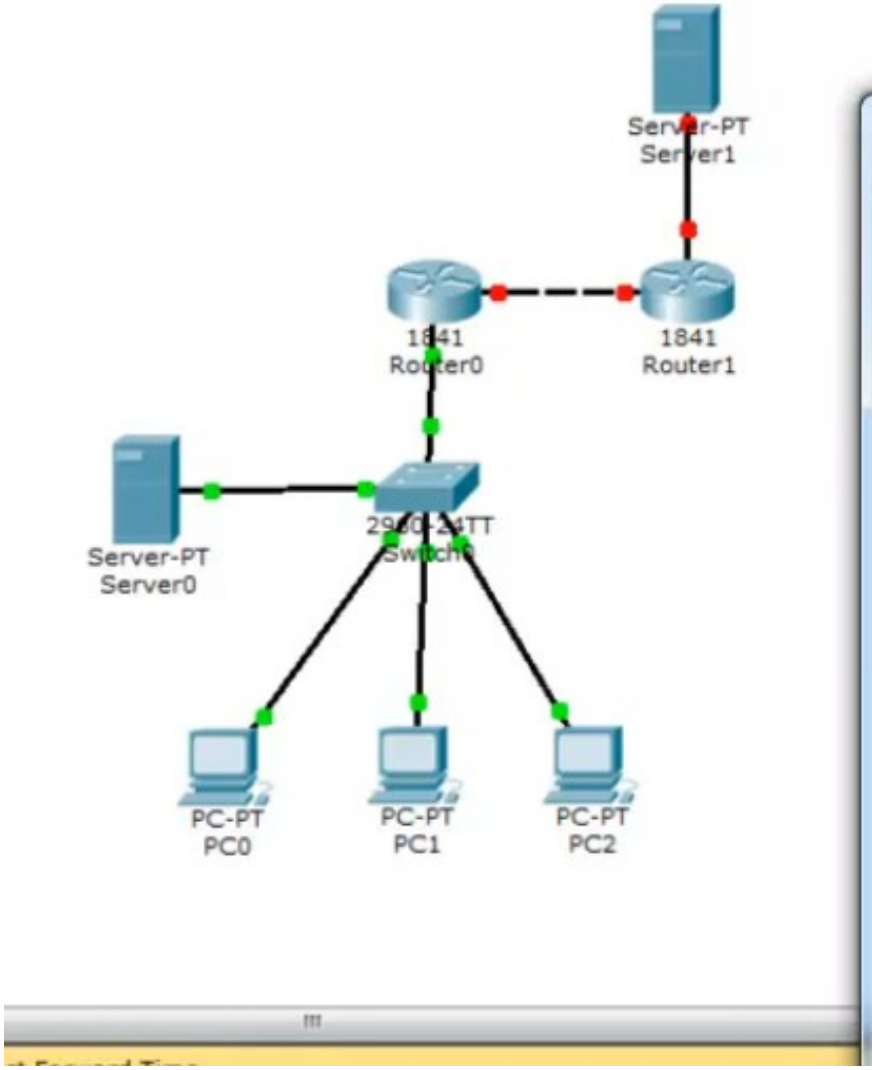
Проверяем, что шлюз и сервер доступны с PC0



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



Зададим ip адрес на интерфейсе Router1, обращенного к Router0



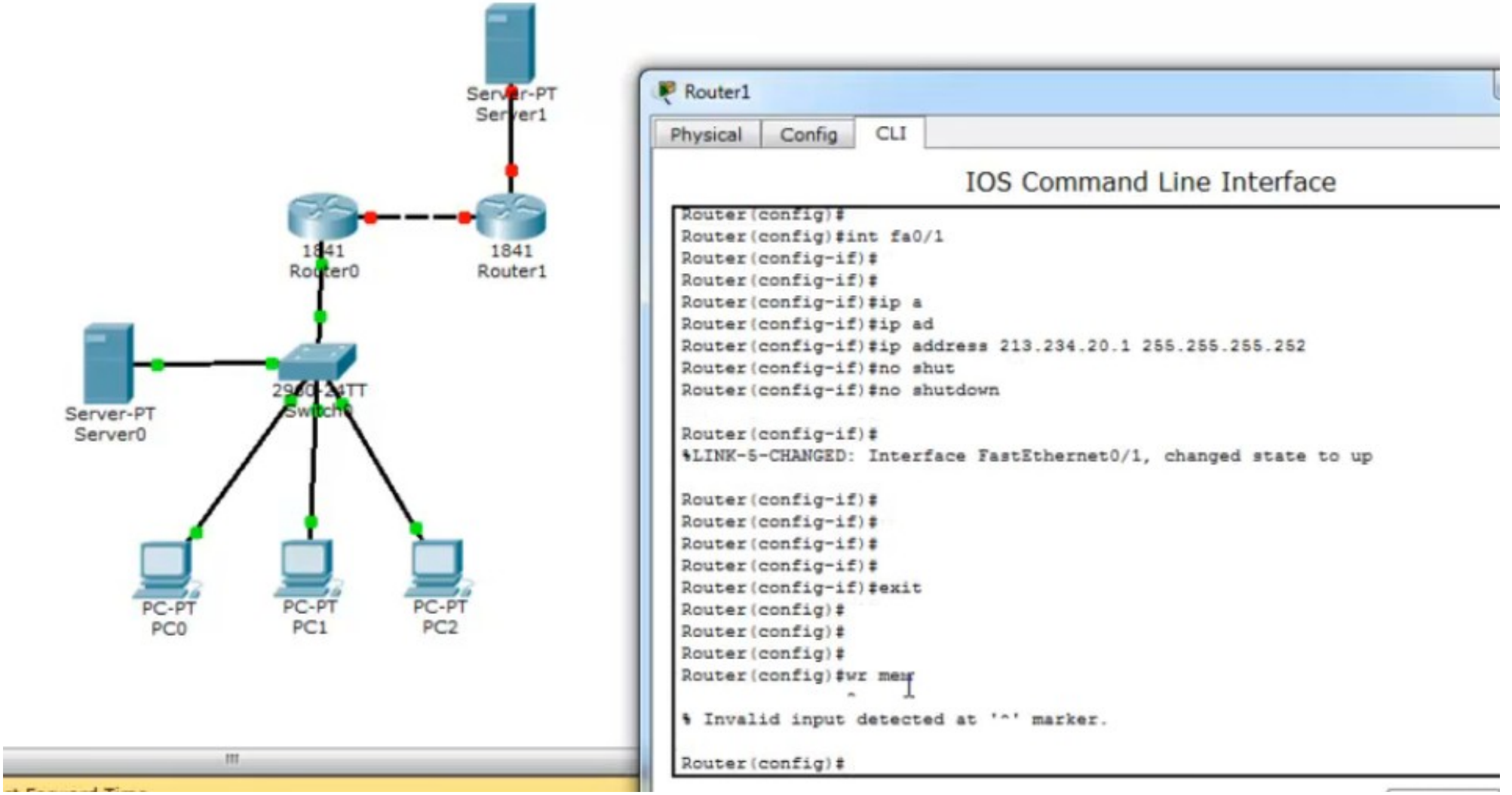
Router1

Physical | Config | CLI

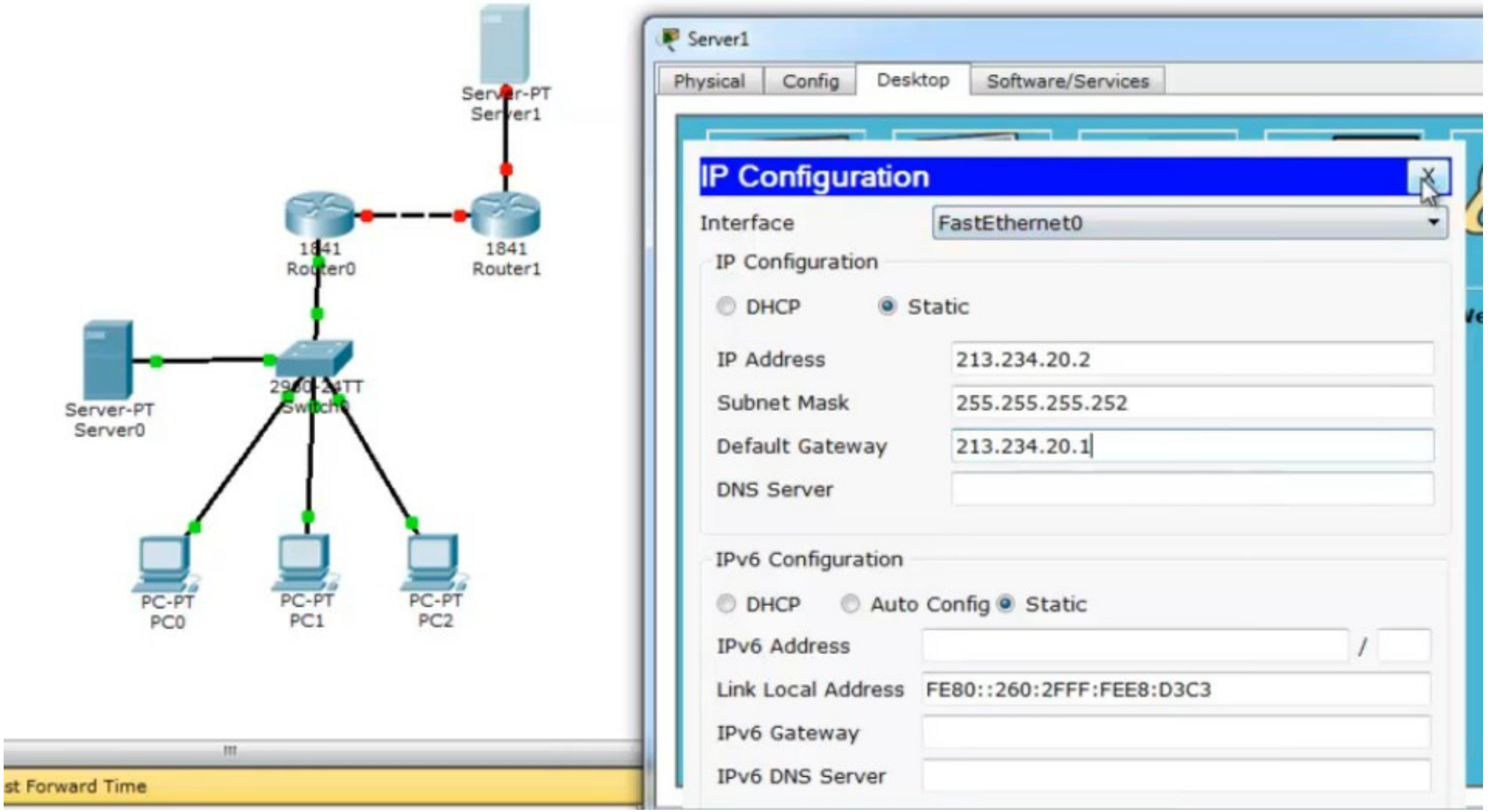
IOS Command Line Interface

```
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)#
```

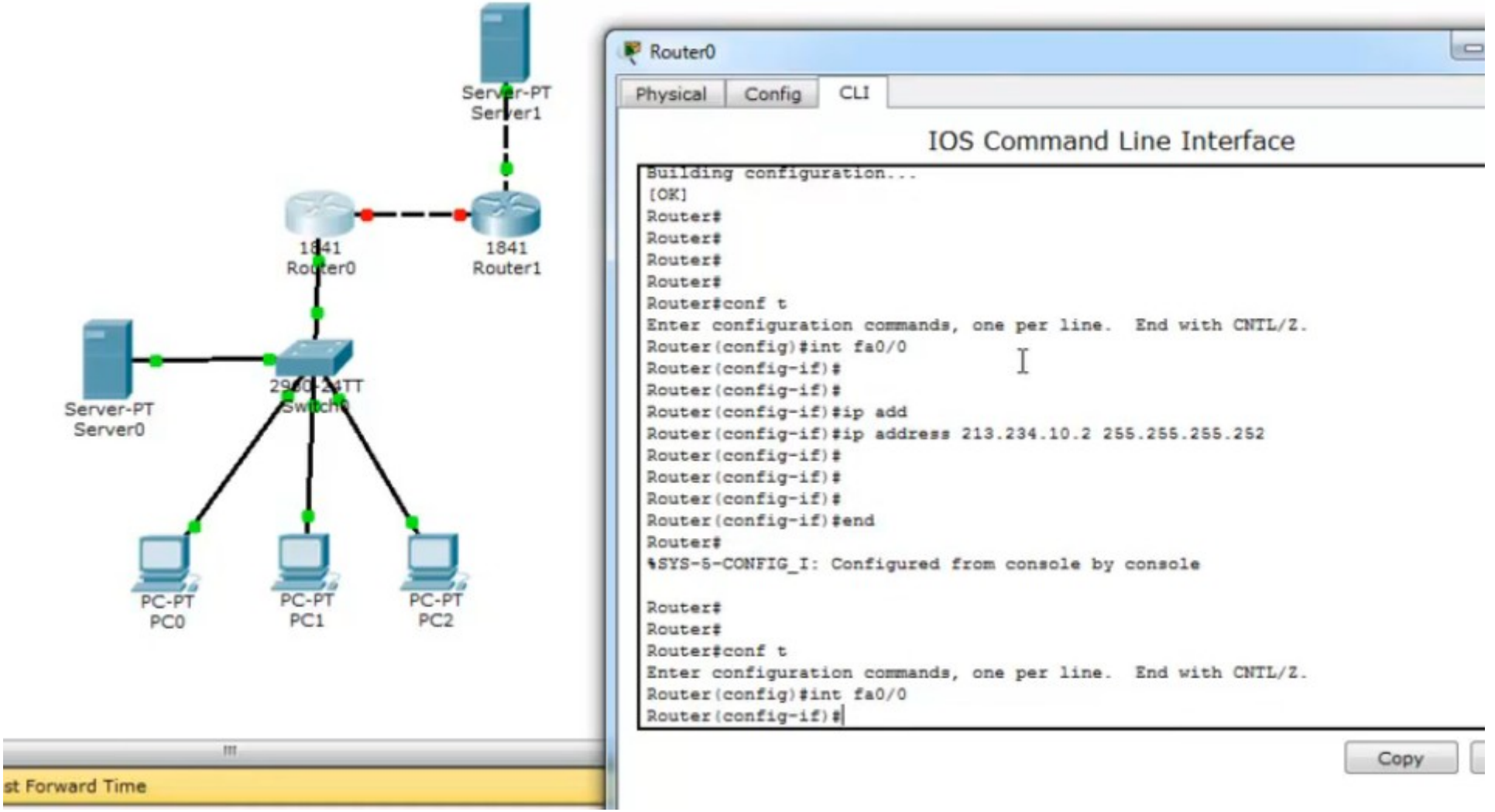
Зададим ip адрес на интерфейсе Router1, обращенного к Server1



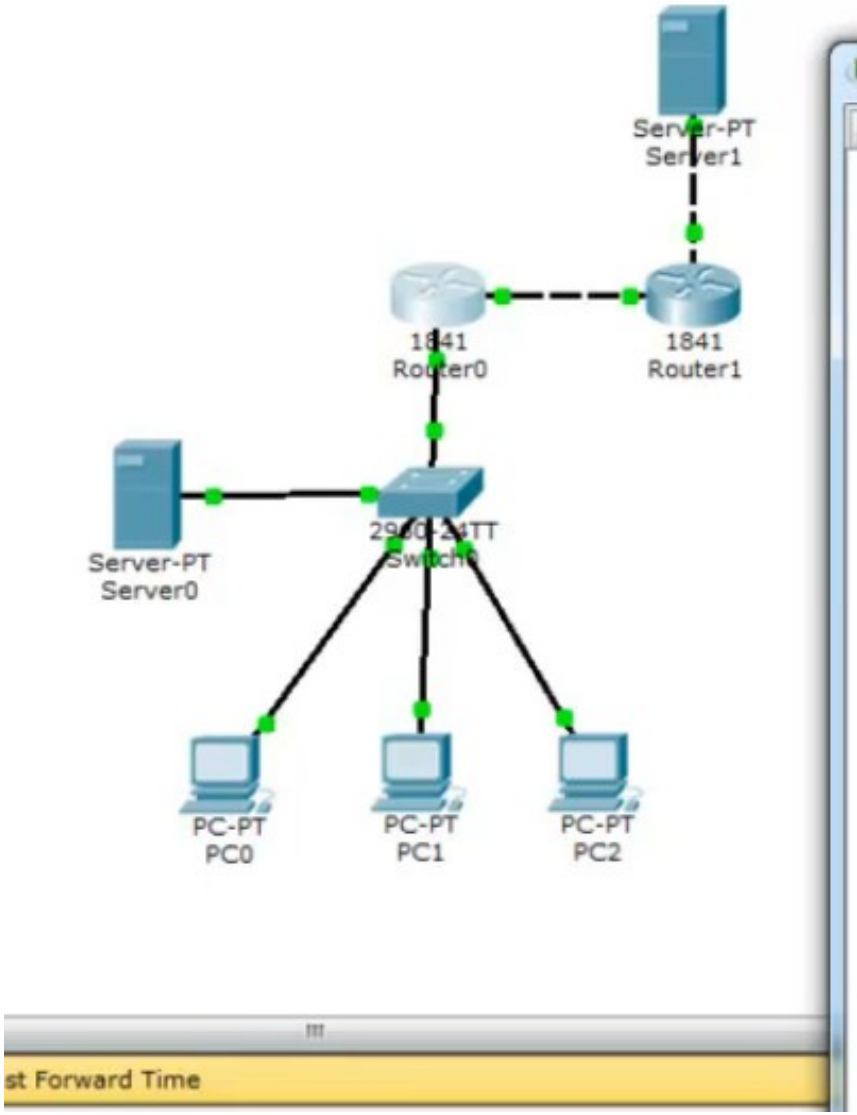
Зададим ip адрес для Server1

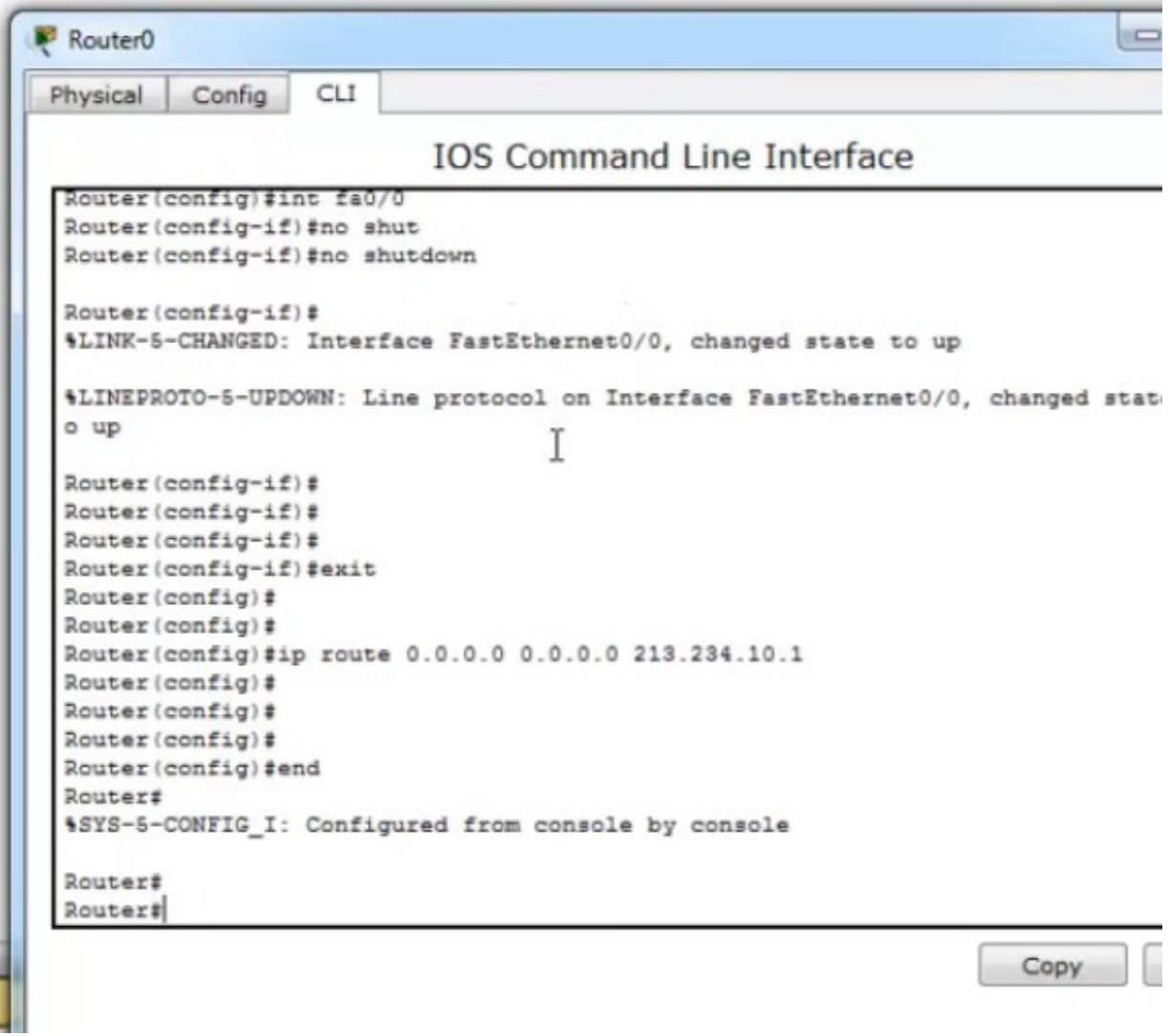


Заменим тип кабеля между Server1 и Router1. Зададим ip на Router0.

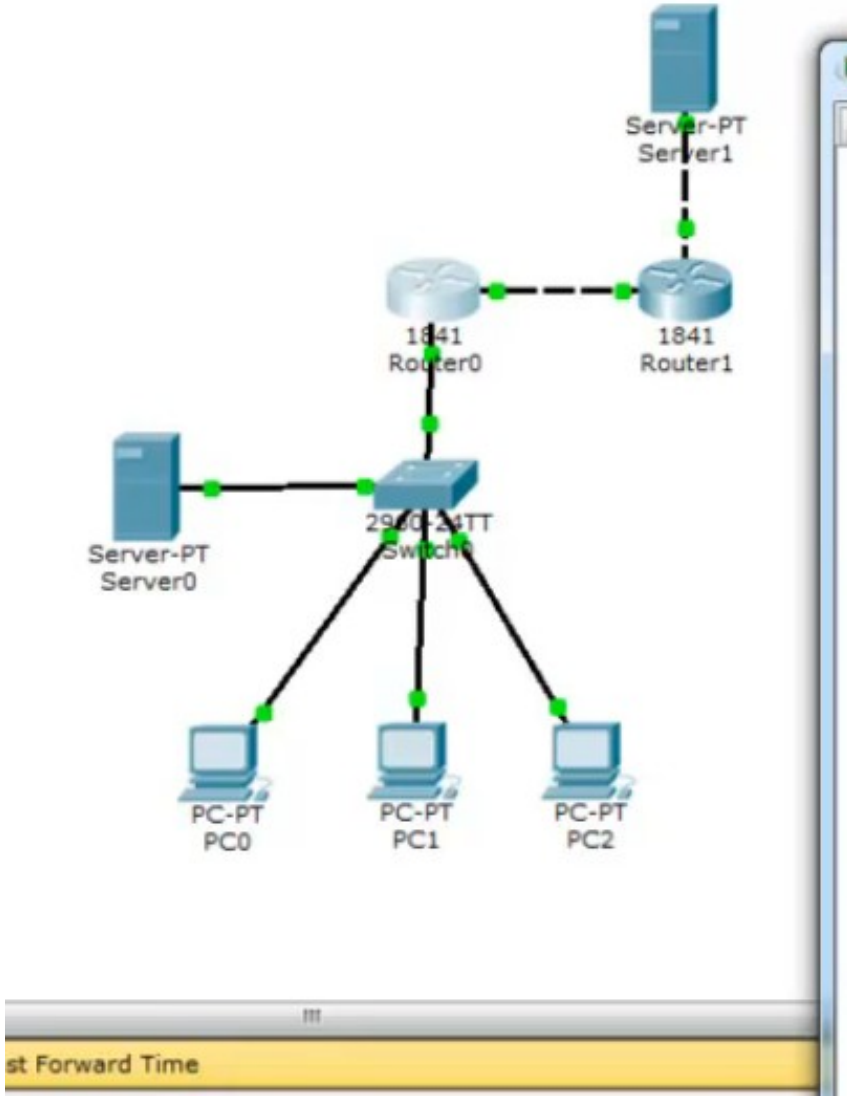


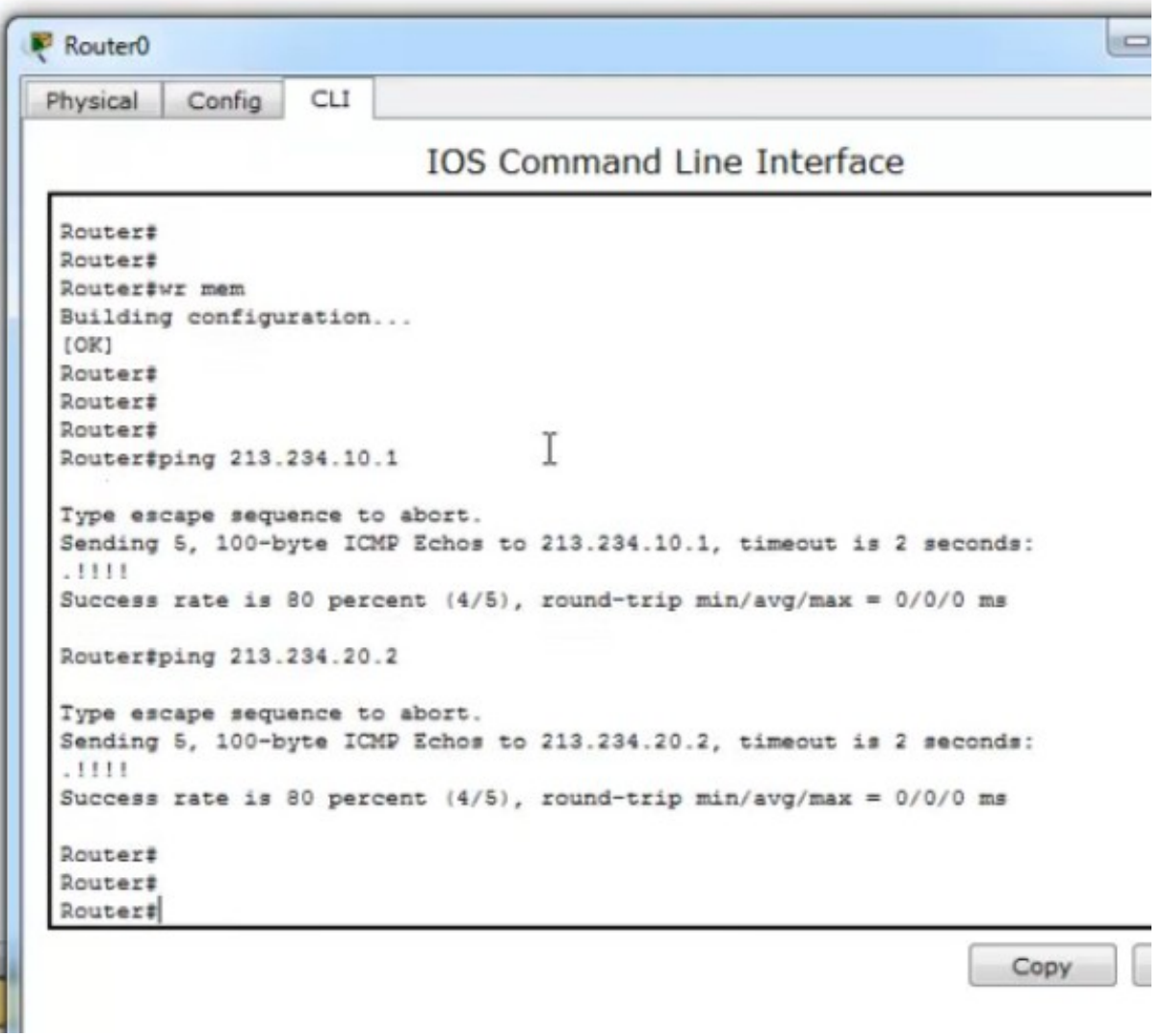
Зададим шлюз по умолчанию на Router0



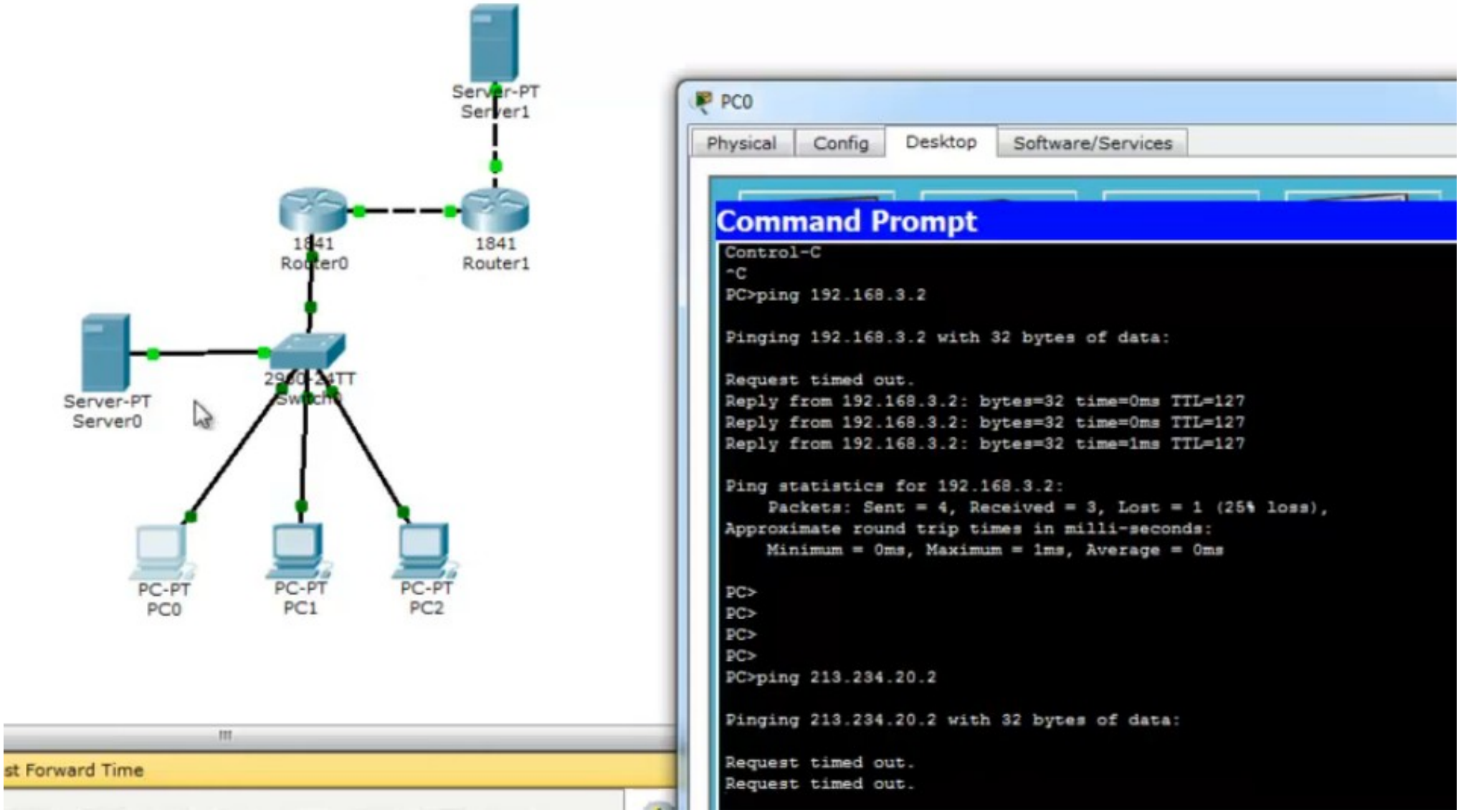


Сохраняем. Проверяем связанность с Server1, Router1

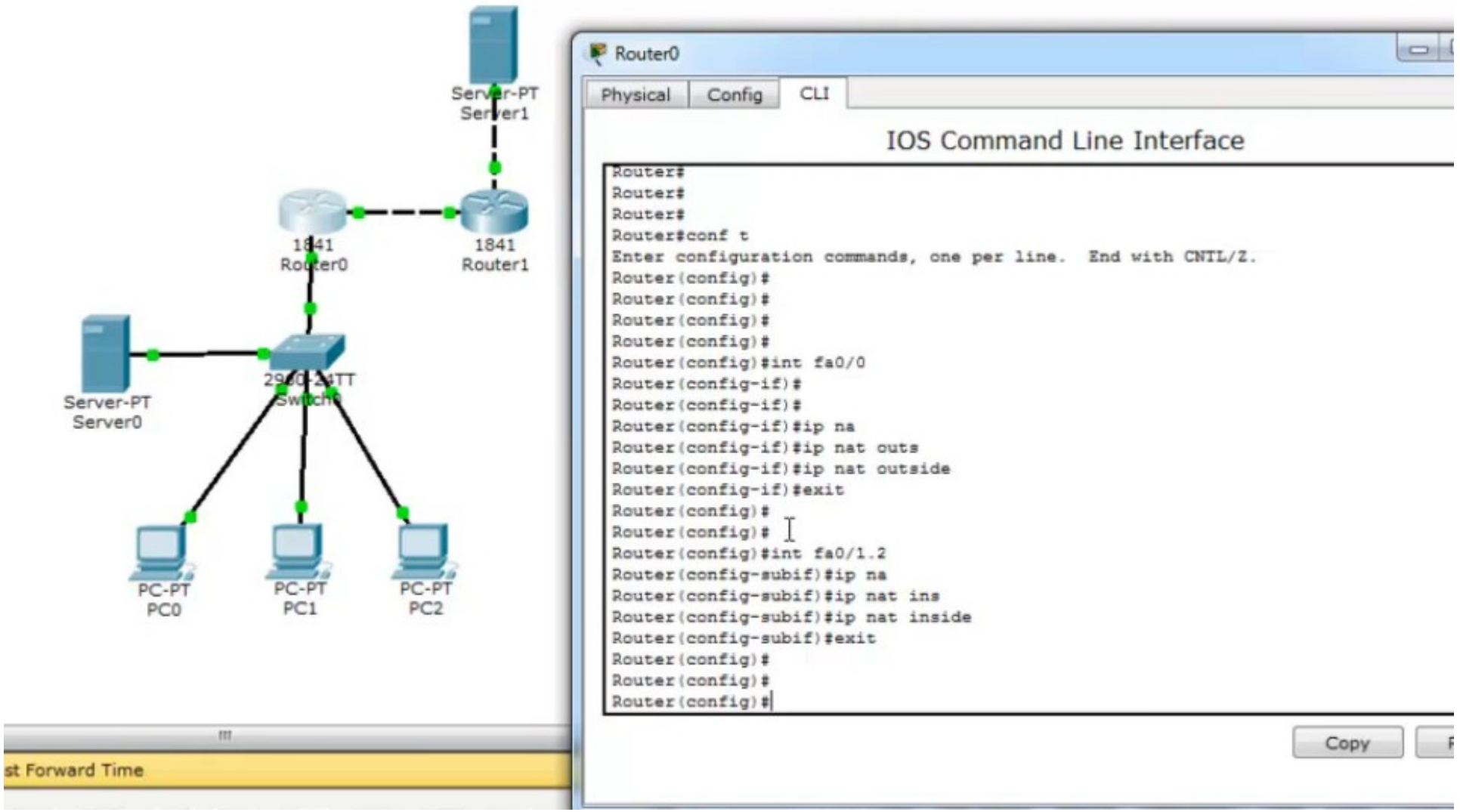




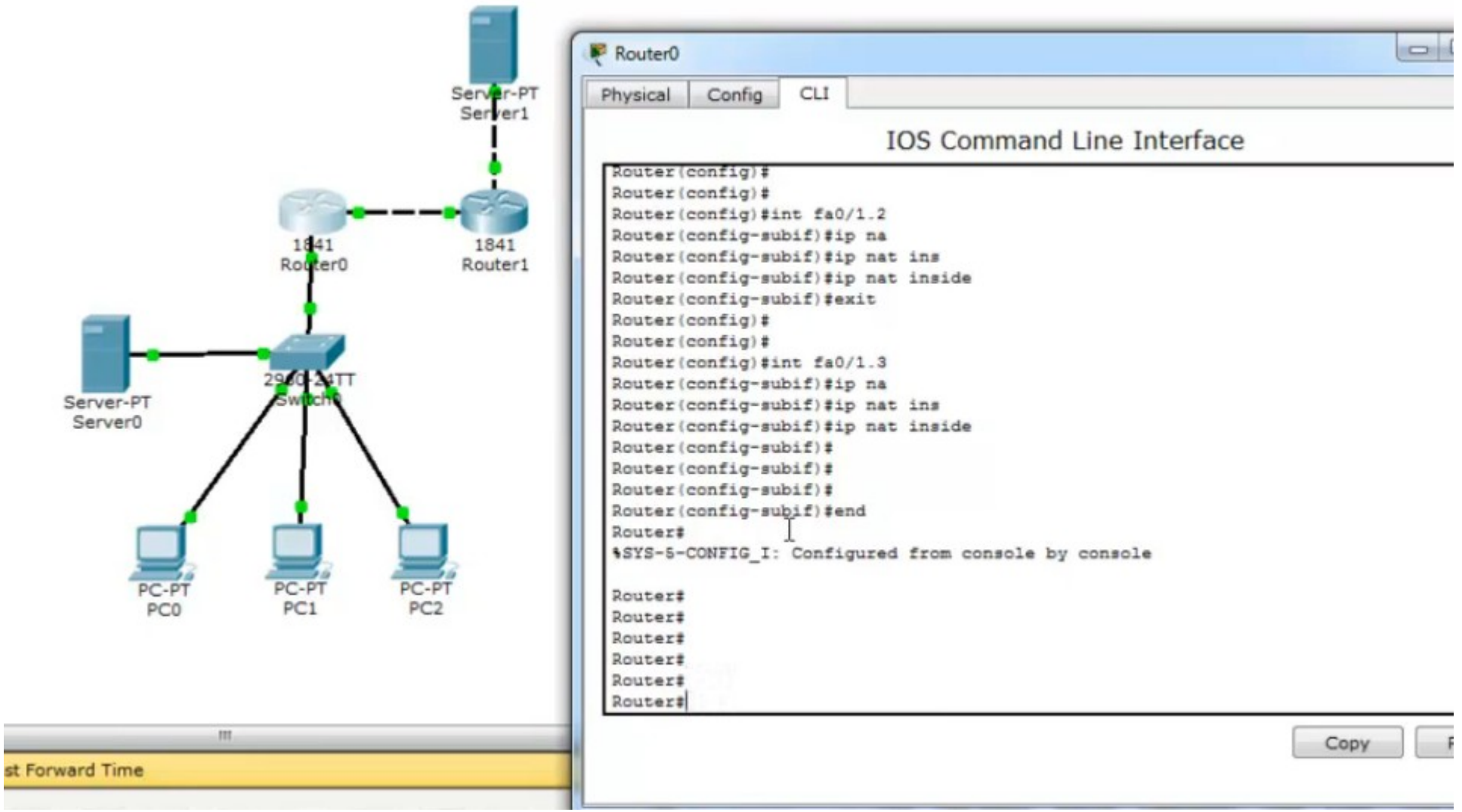
Пингуем Server1 с PC0 — не проходит. Router1 не знает как работать с «серыми» ip адресами PC0, PC1, PC2



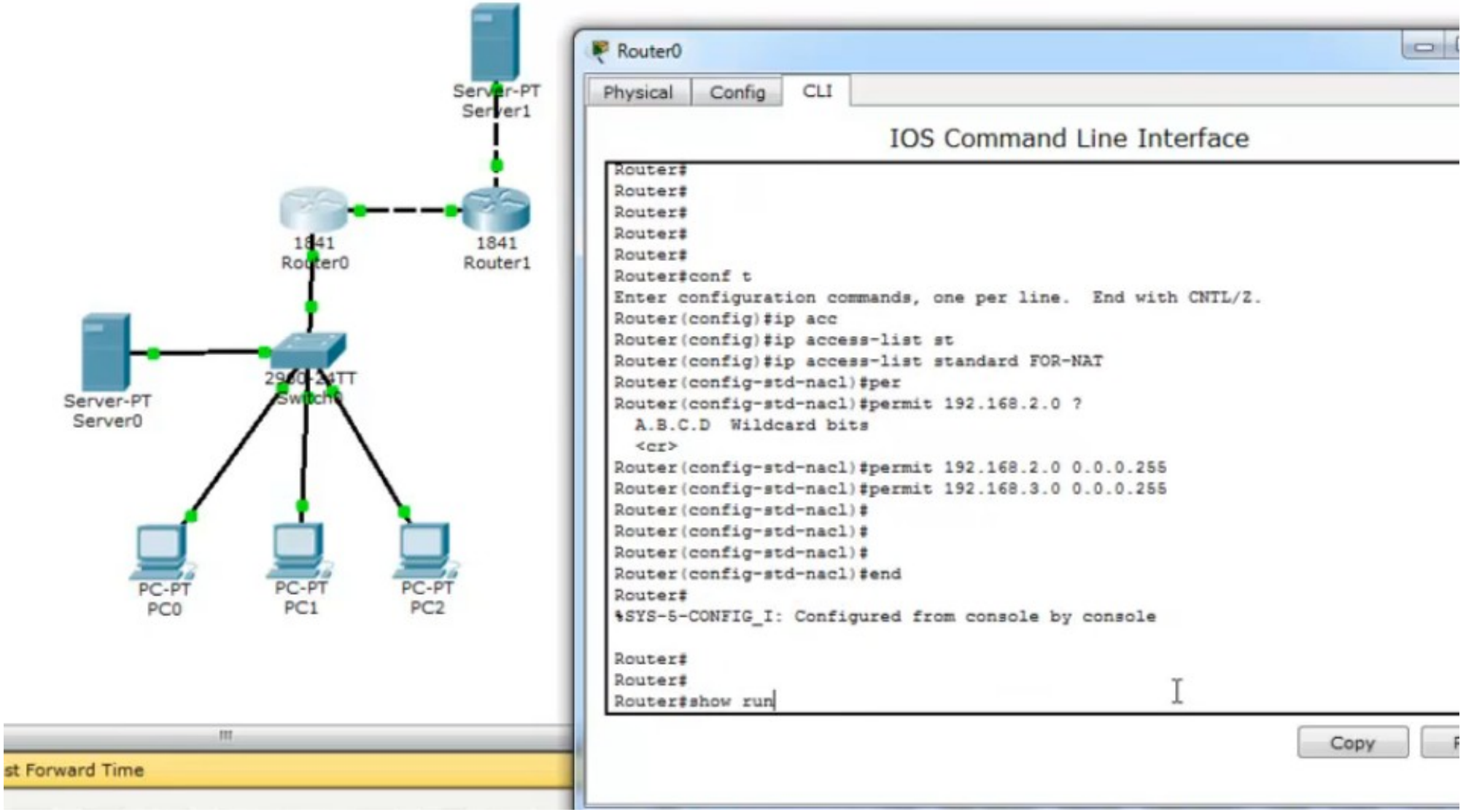
На Router0 определяем fa0/0 как внешний, fa0/1.2 как внутренний интерфейс



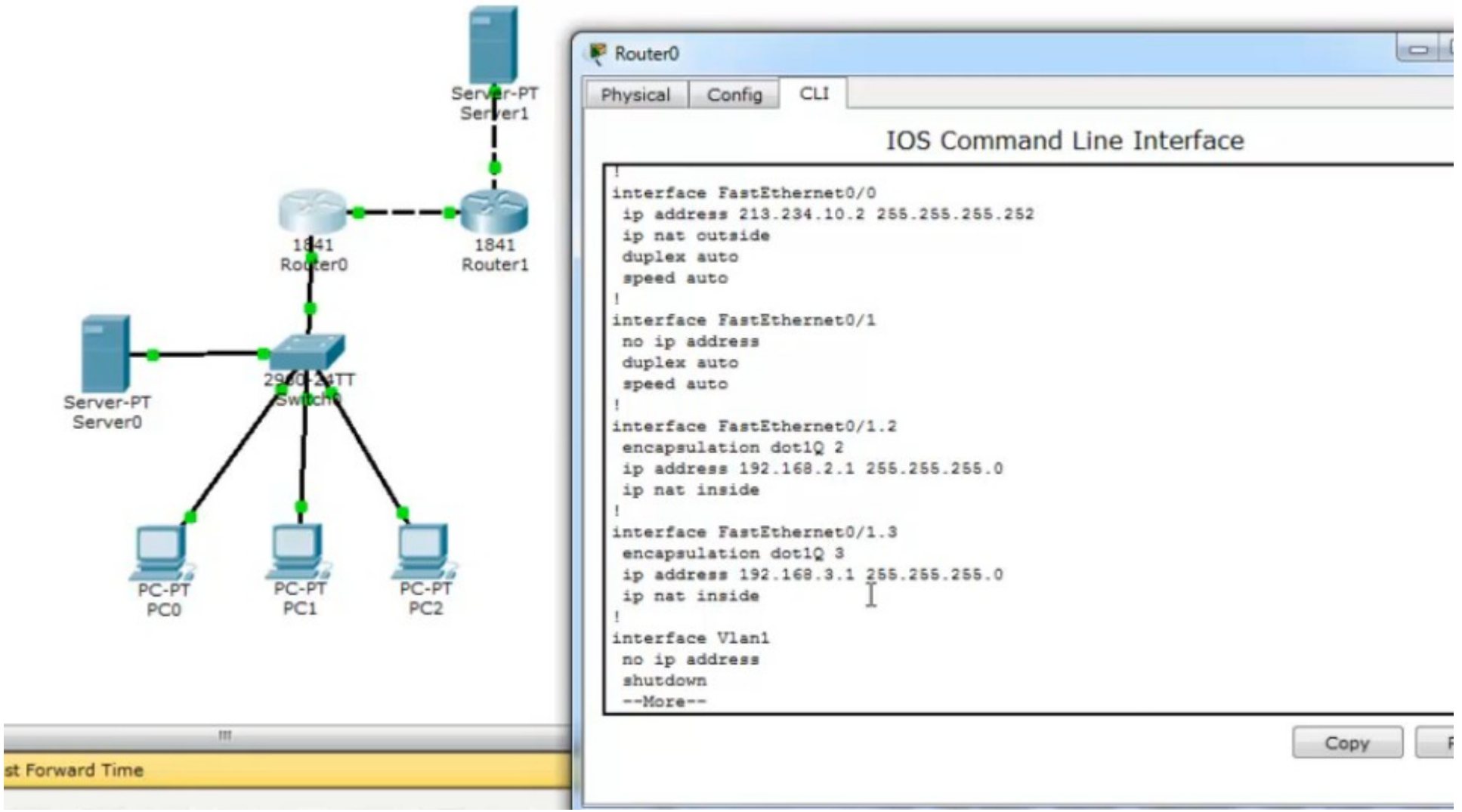
определяем fa0/1.3 тоже как внутренний



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



В конфигурации — какие интерфейсы inside, какие outside.



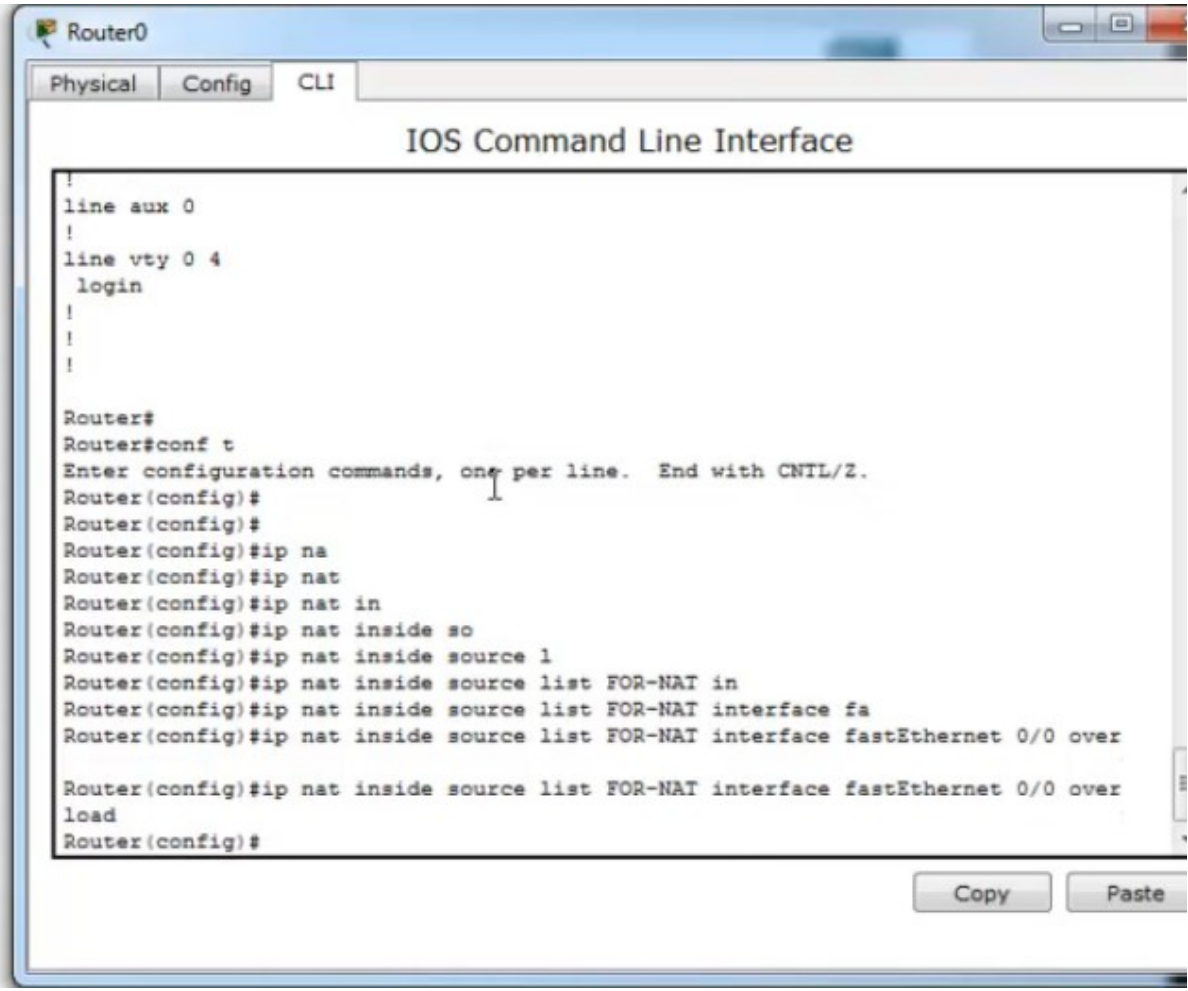
Настраиваем Port-Address-Translation

Настройка PAT

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

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

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

Настройка Static NAT

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


show ip nat translations
```



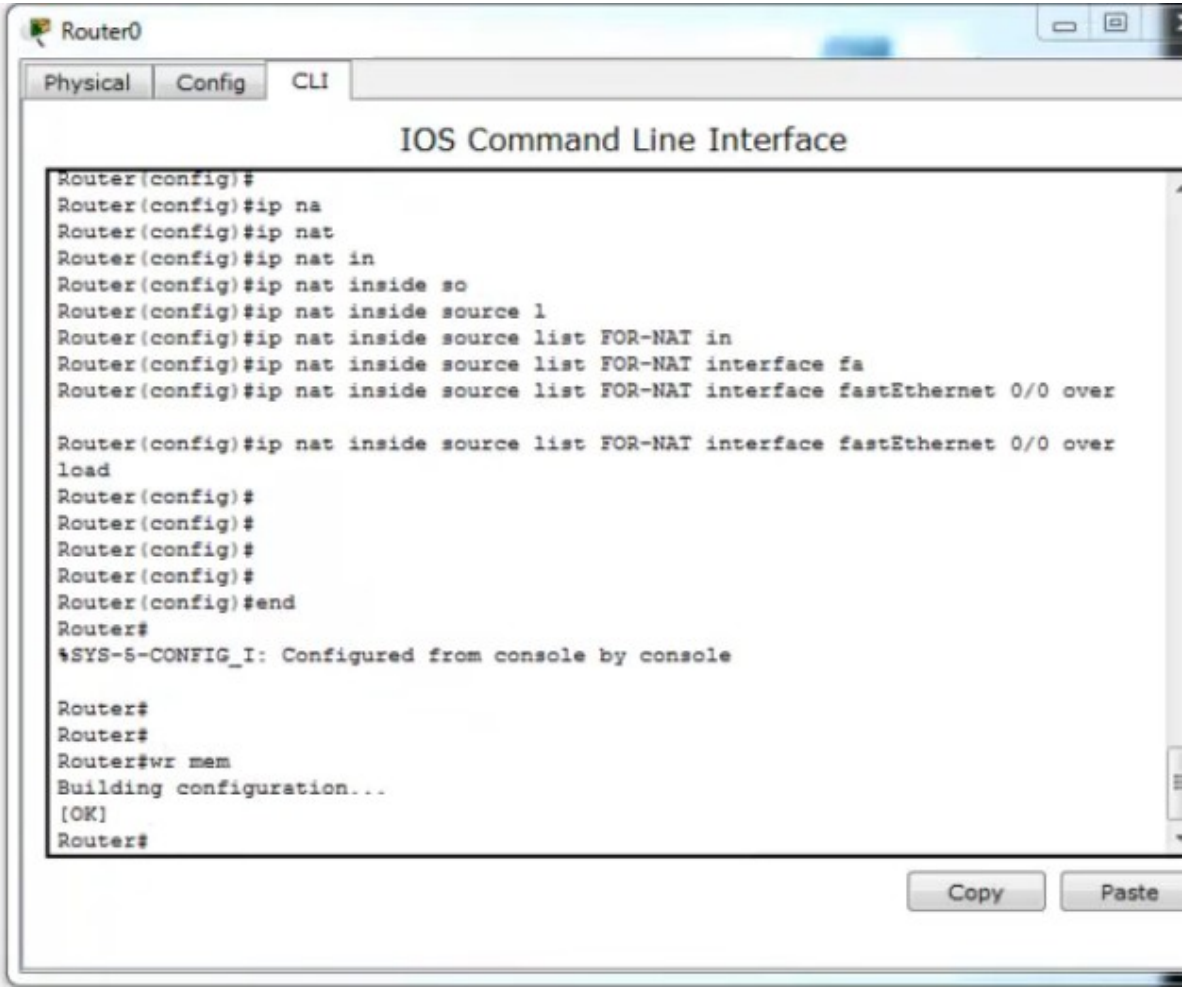
Сохраняем

Настройка PAT

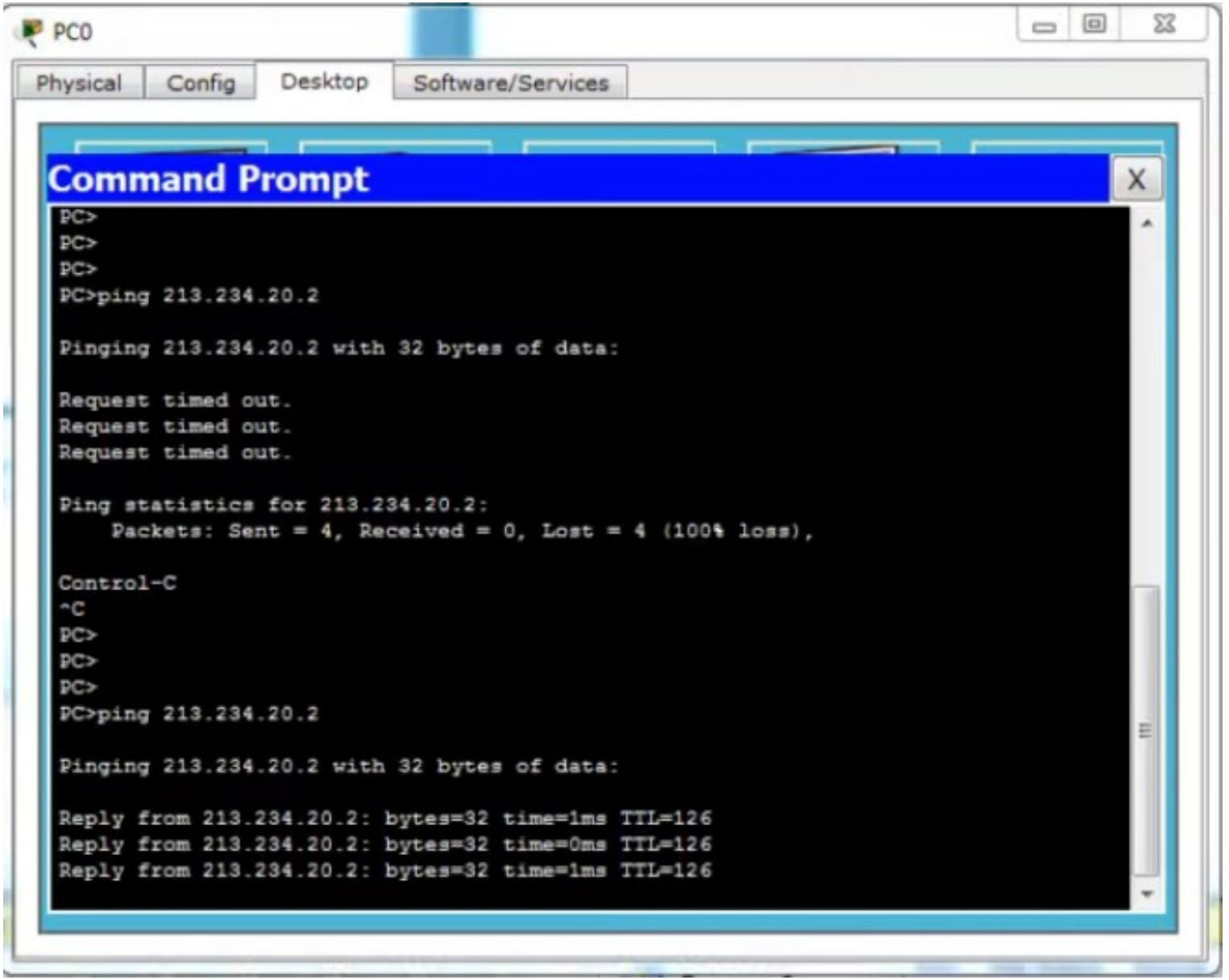
```
interface FastEthernet0/0
 ip nat outside
interface FastEthernet0/1.2
 ip nat inside
interface FastEthernet0/1.3
 ip nat inside

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

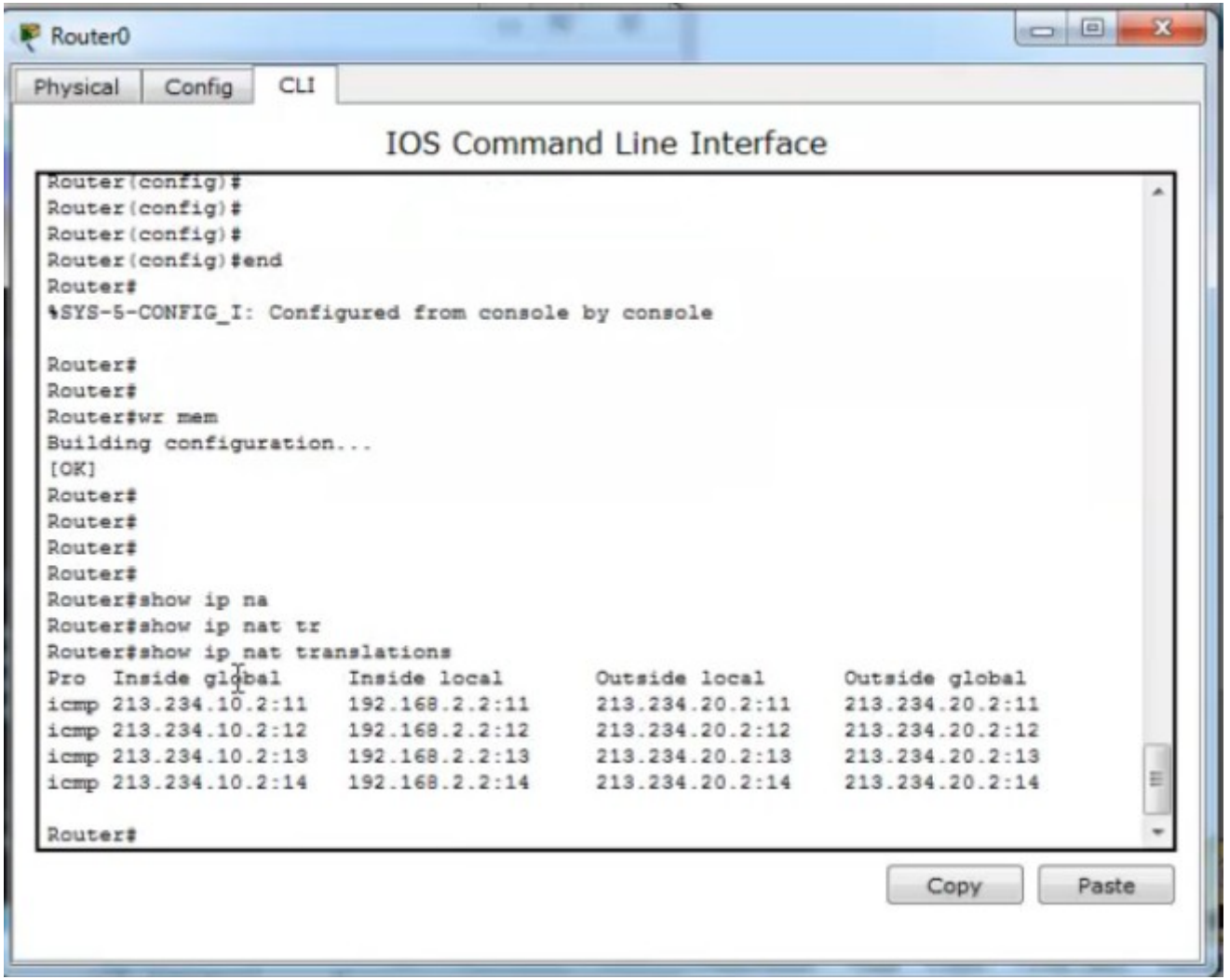
```
ip nat inside source static tcp 192.168.3.2 80 213.234.10.2 80


show ip nat translations
```



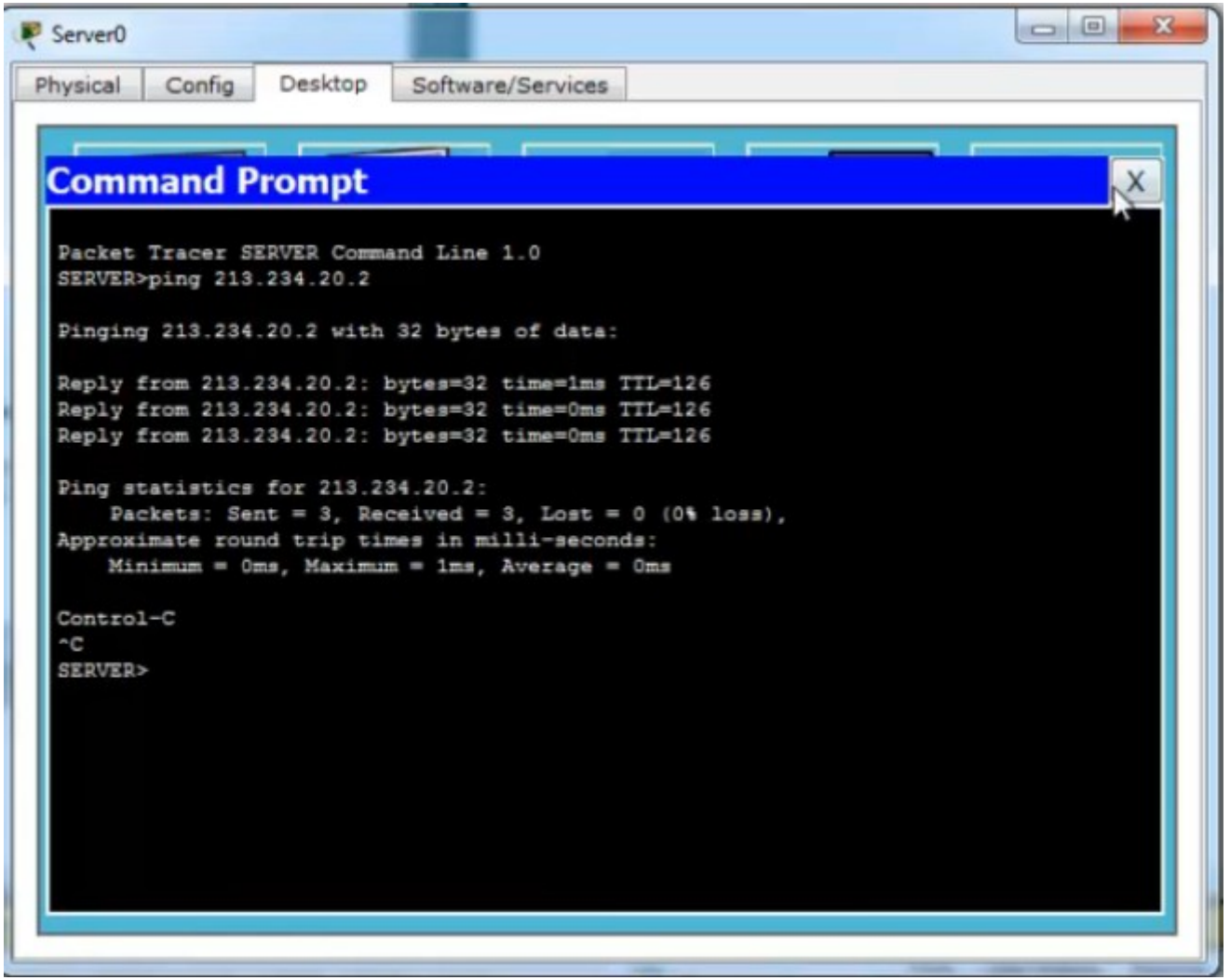
Проверяем доступность Sever1 с PC0 — пинг проходит.



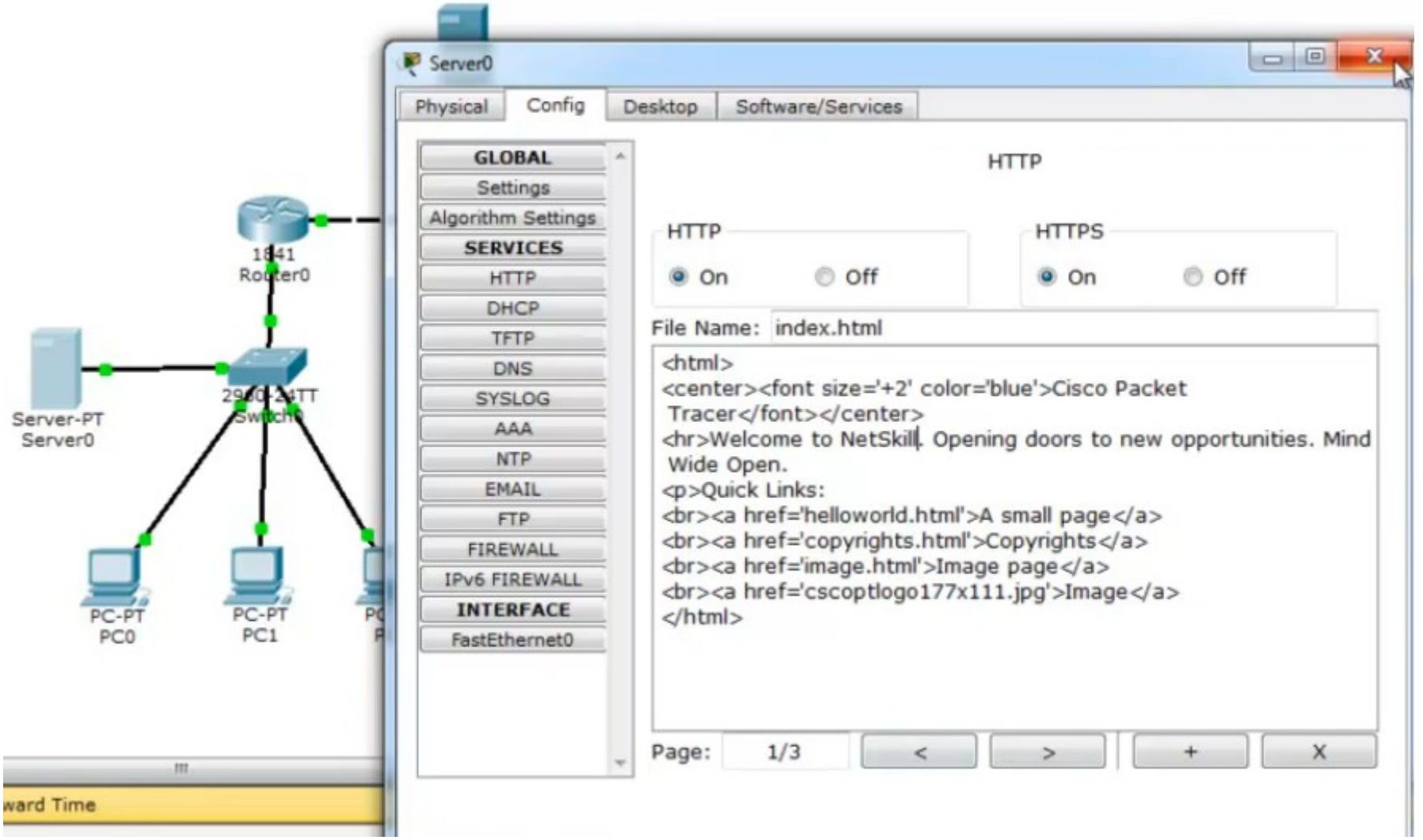
На Router0 видим настройки NAT



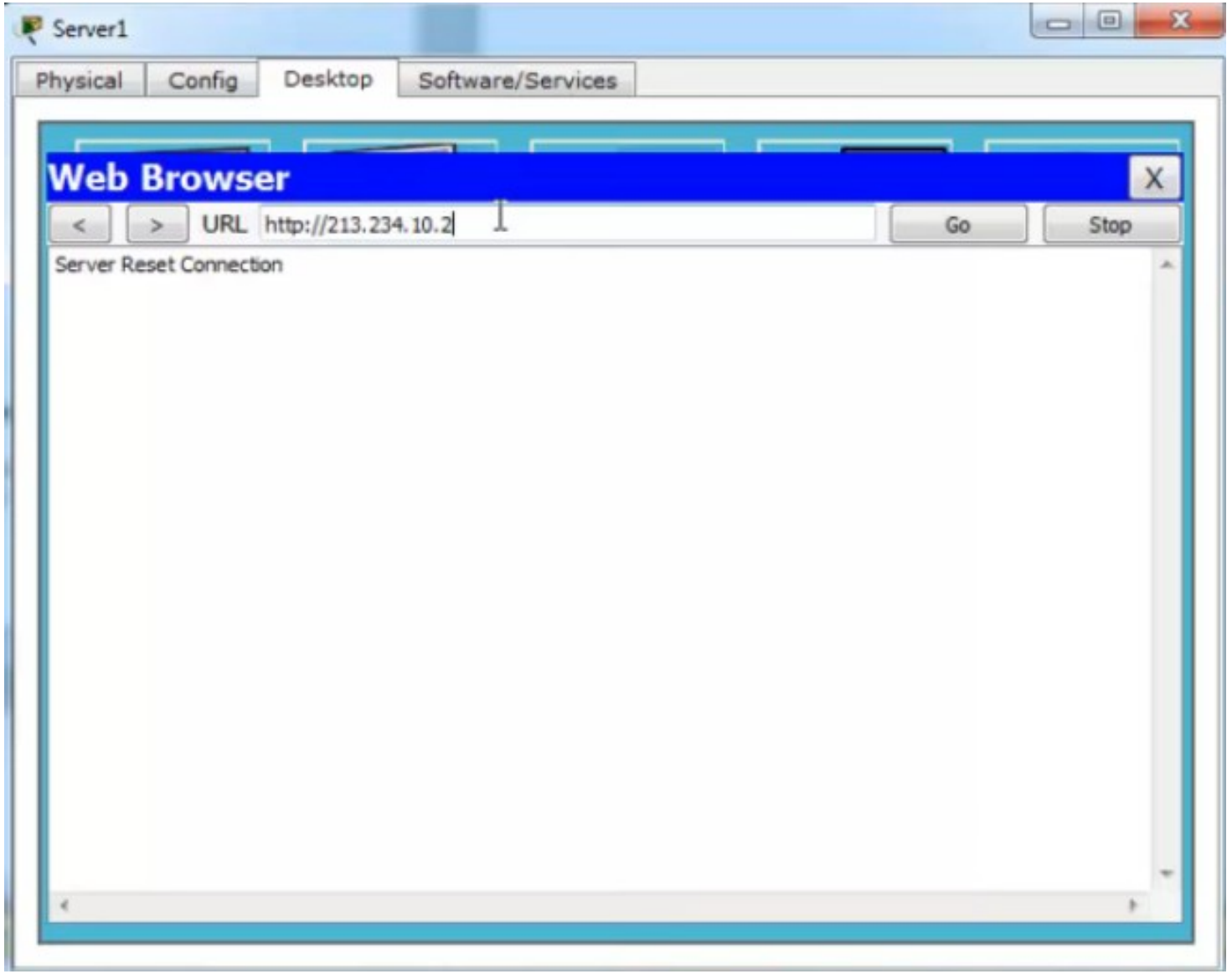
Проверяем, что с Server1 доступен PC0



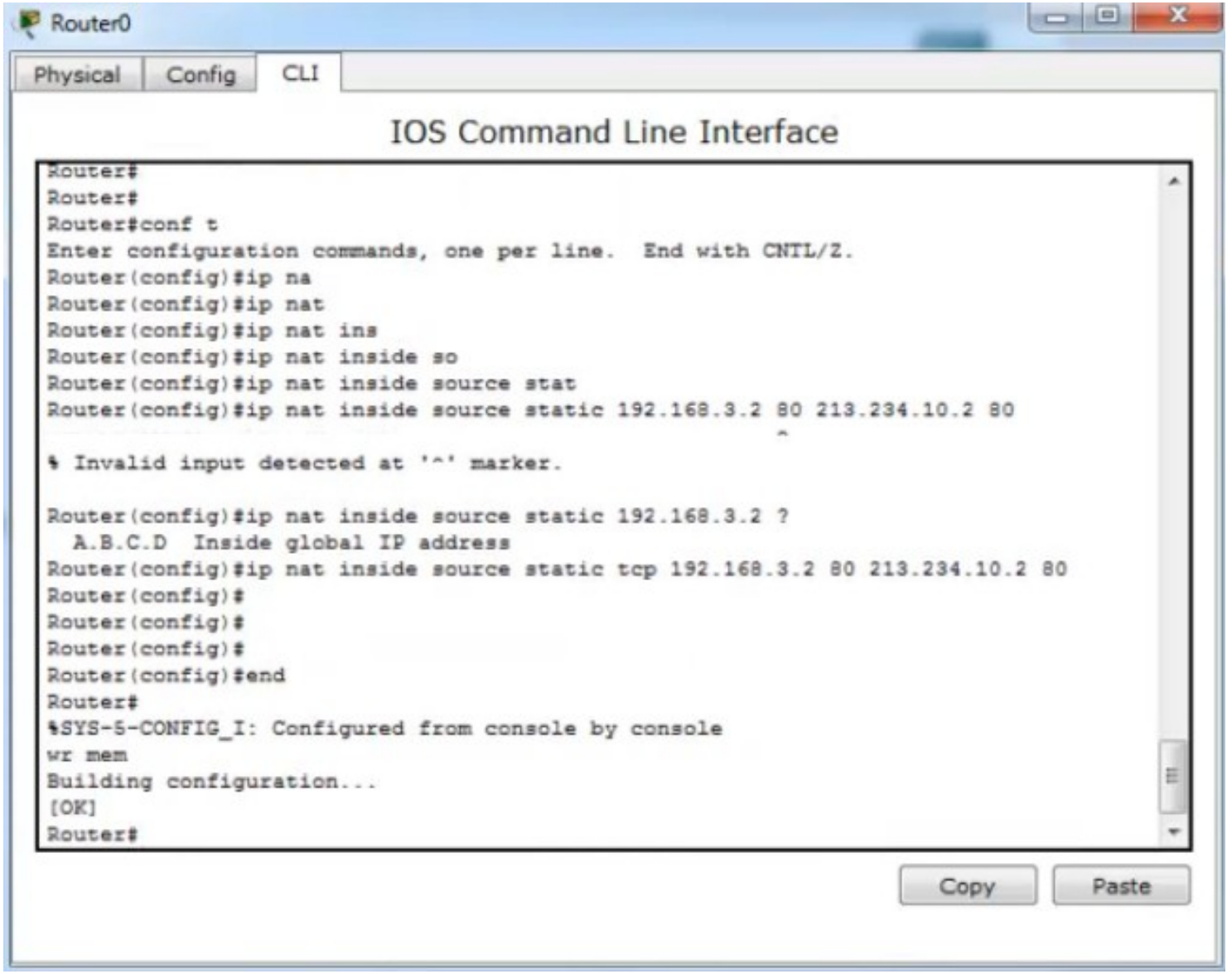
Далее настроим статический NAT для доступа к Server0 из внешней сети. Изменим содержание index.html в Config > HTTP у Server0



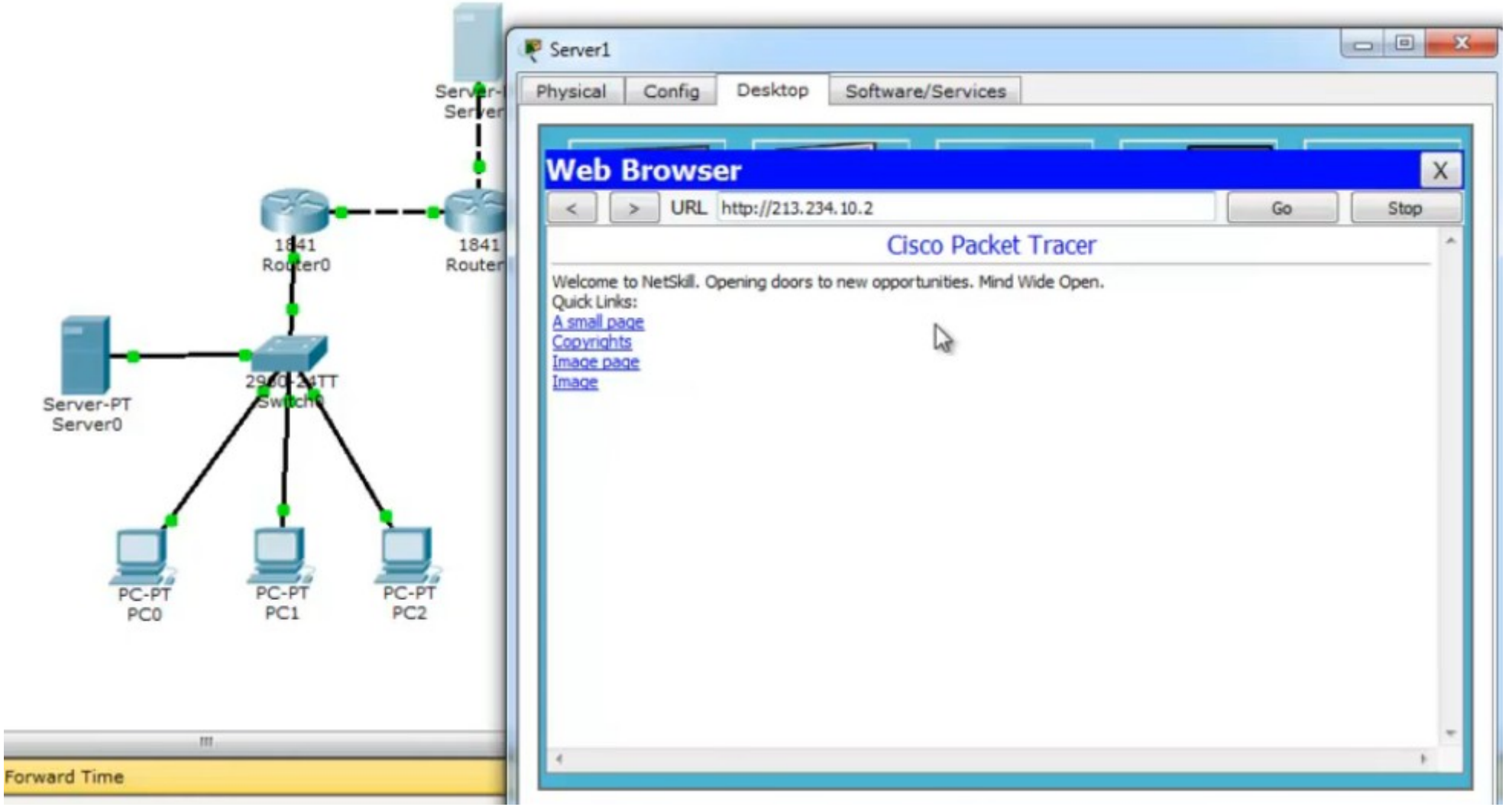
Проверяем доступность веб-сервера на Server0 с Server1 — недоступен.



Настроим static NAT на Router0



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



VPN — Vitrual Private Network

Lesson18 - VPN

Как дать доступ к локальным серверам?

1. Static NAT
2. DMZ
3. VPN

VPN - Virtual Private Network - виртуальная частная сеть

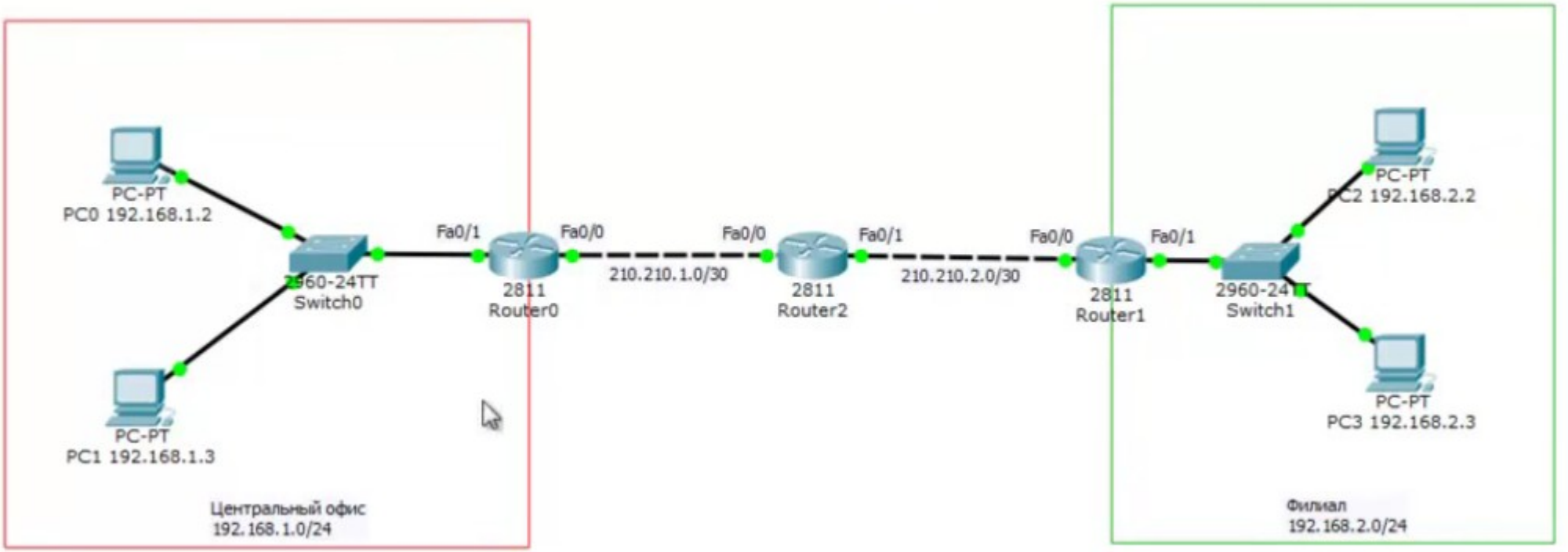
- IPsec Site-to-Site VPN - объединение сетей
- IPsec RA VPN - подключение удаленного пользователя

Построение туннеля в две фазы (IKE)

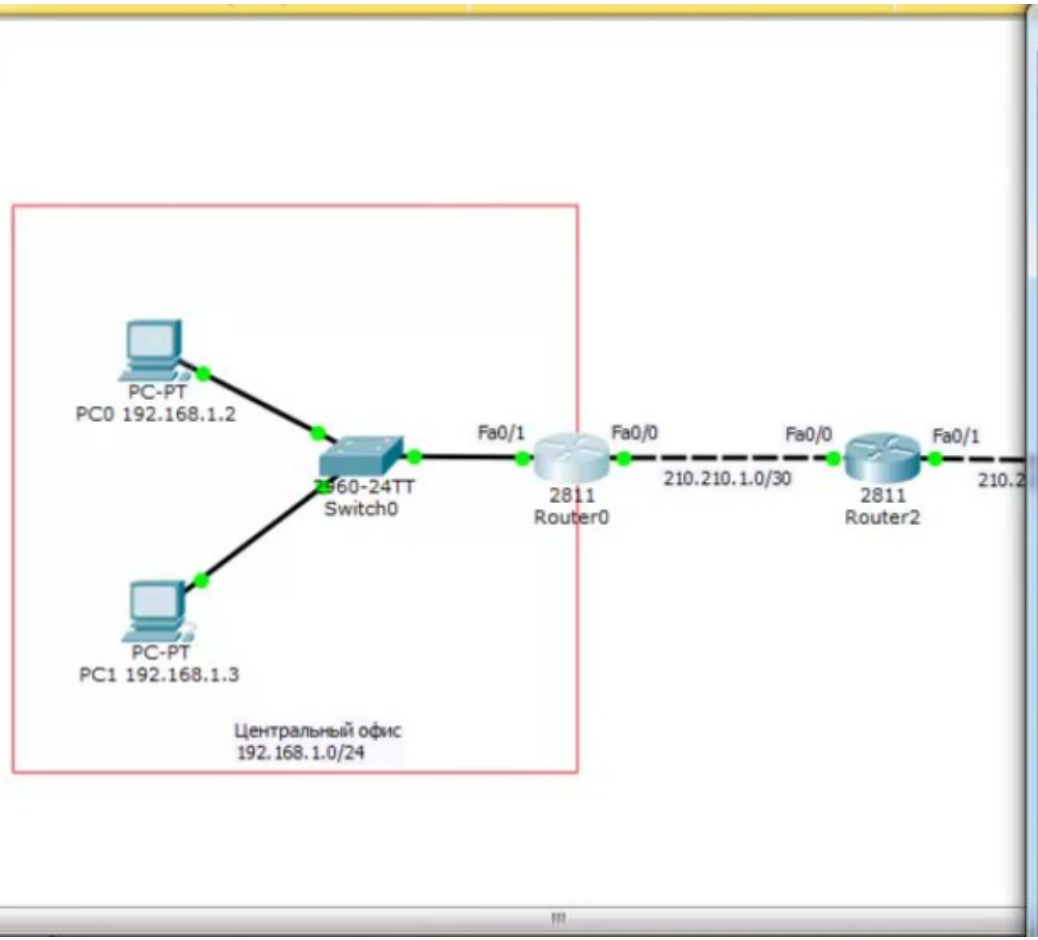
1. Первая фаза (установка SA и ISAKMP Tunnel)
2. Вторая фаза (IPsec Tunnel)

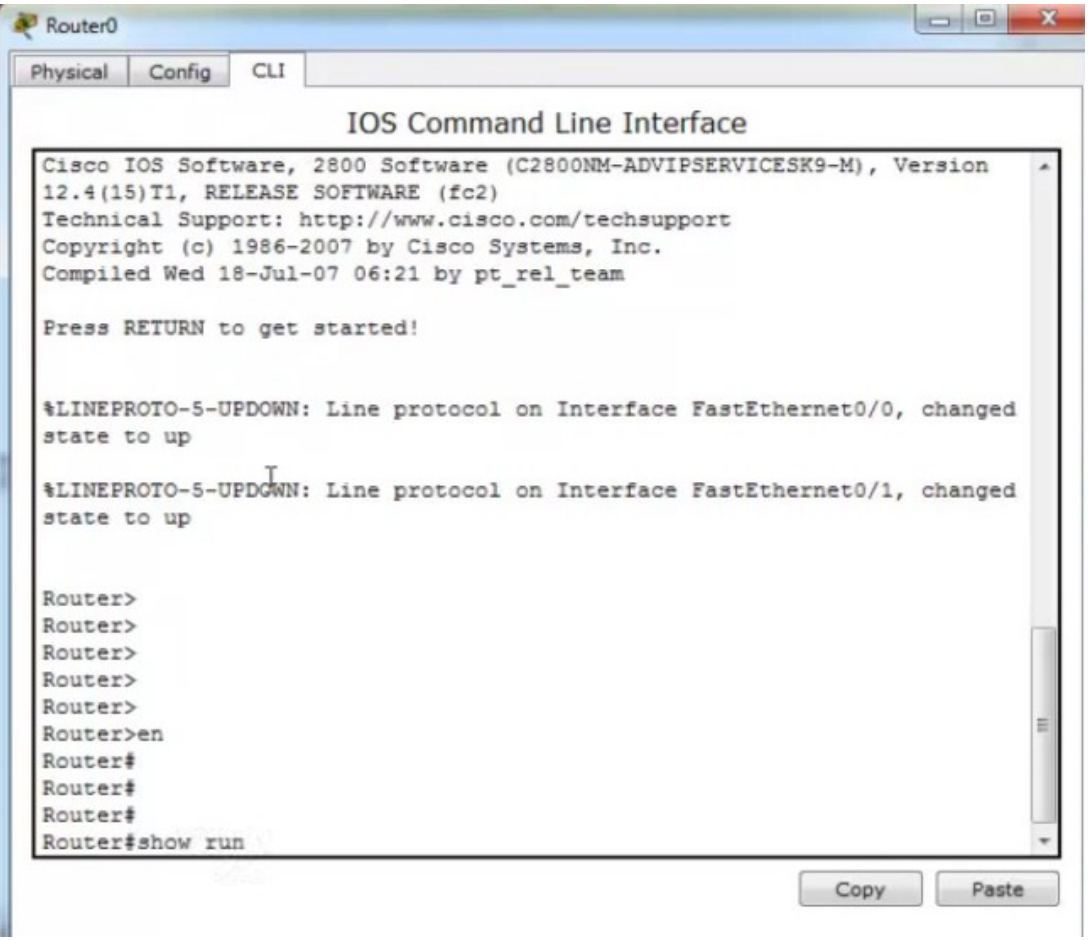
Более подробно о приведенных технологиях можно почитать здесь и здесь

VPN, пример. Есть центральный офис и филиал

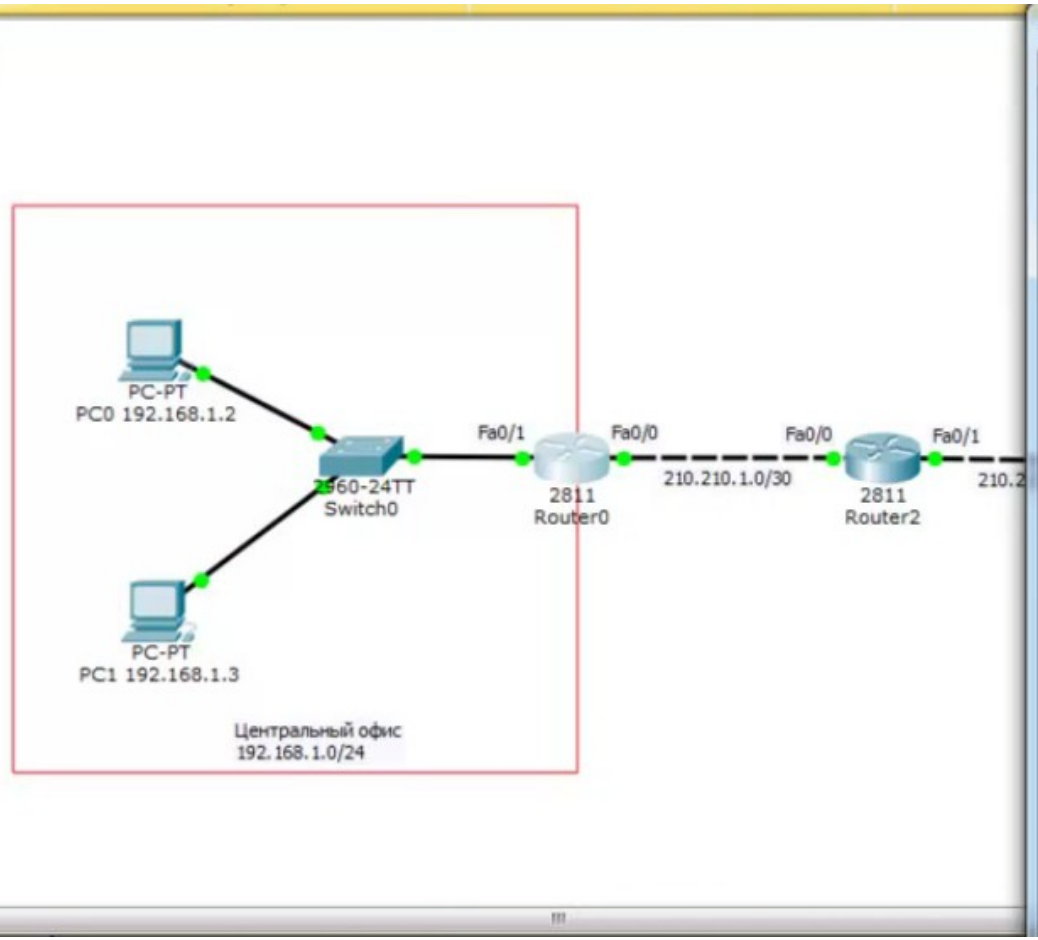


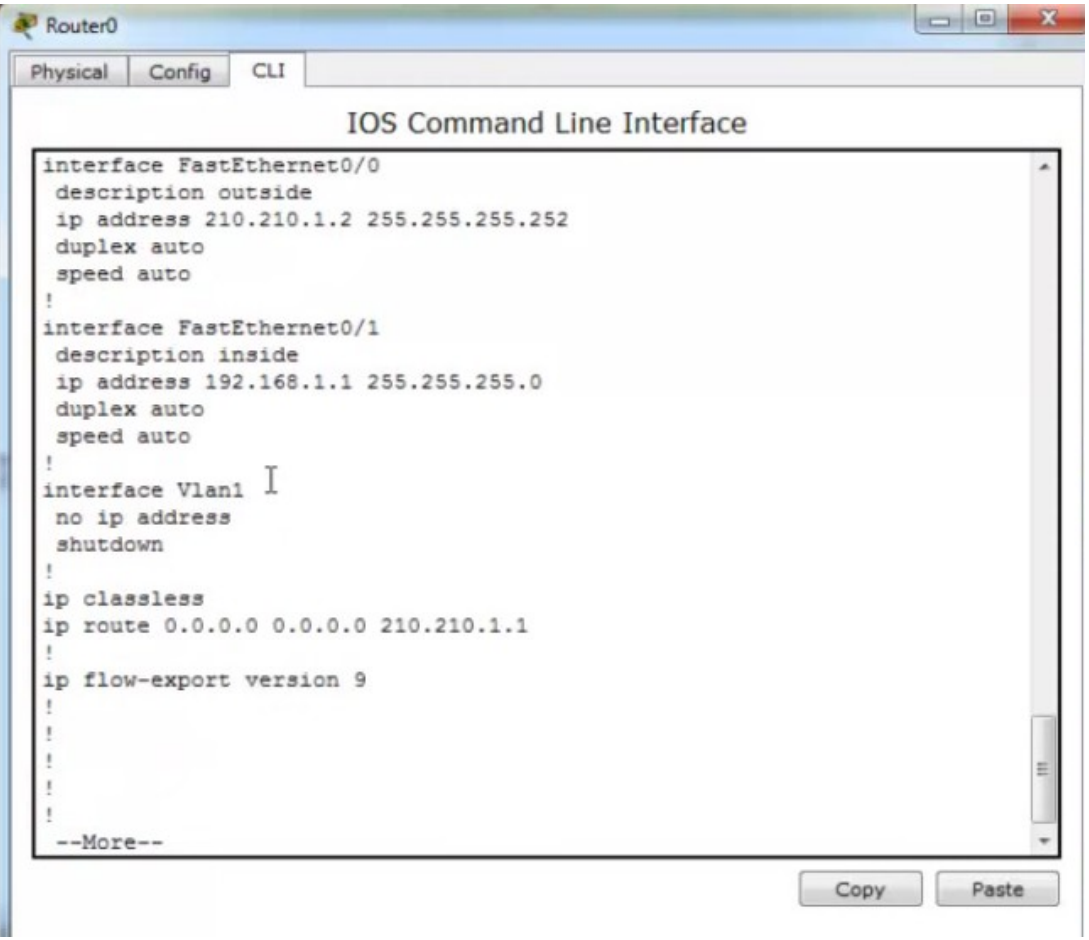
Смотрим настройки на Router0 в центральном офисе



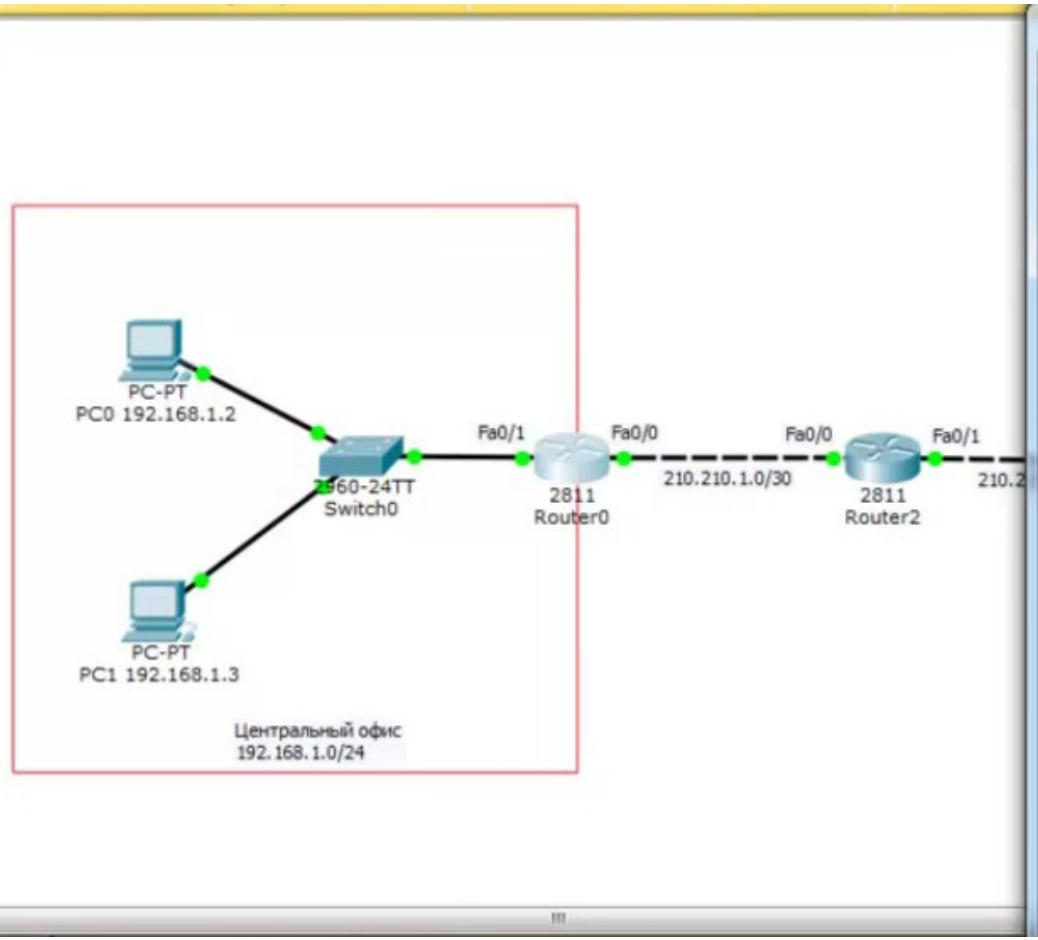


На Router0 настроено 2 ip адреса, маршрут по умолчанию.





На Router0 настроим NAT



Router0

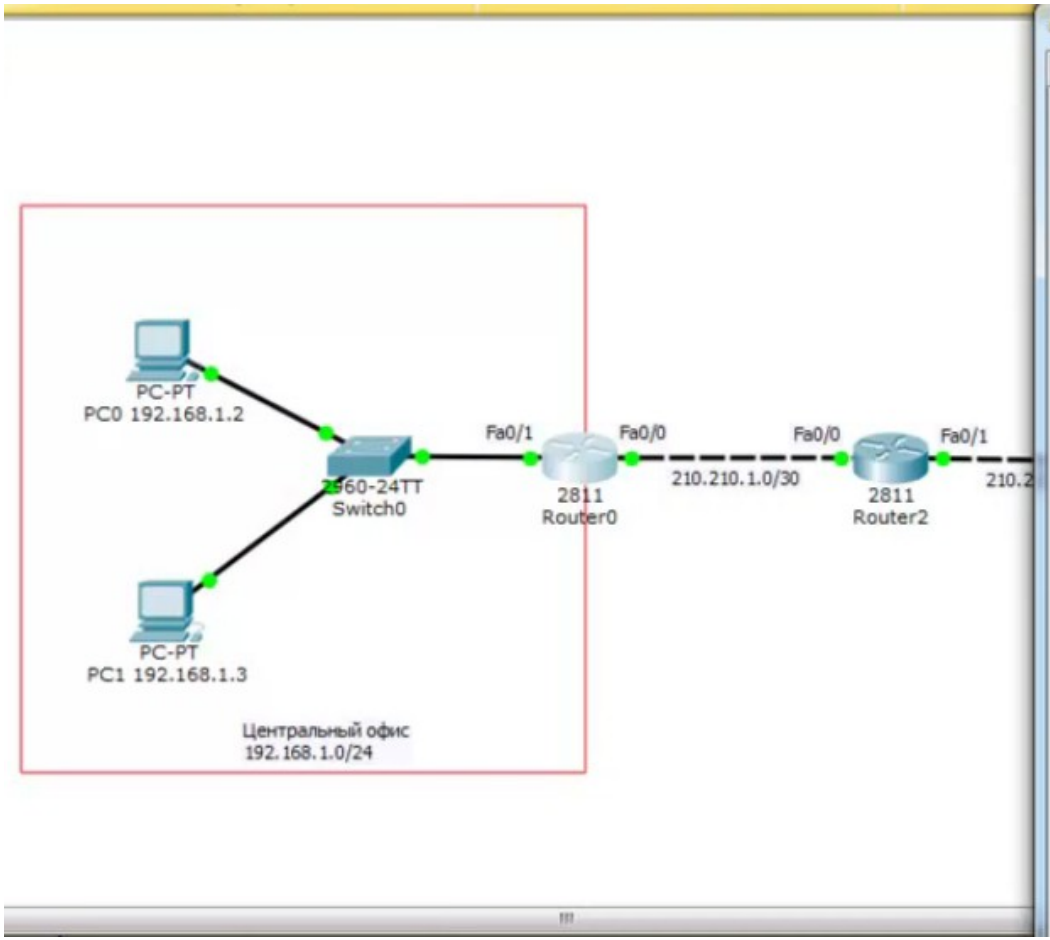
Physical | Config | CLI

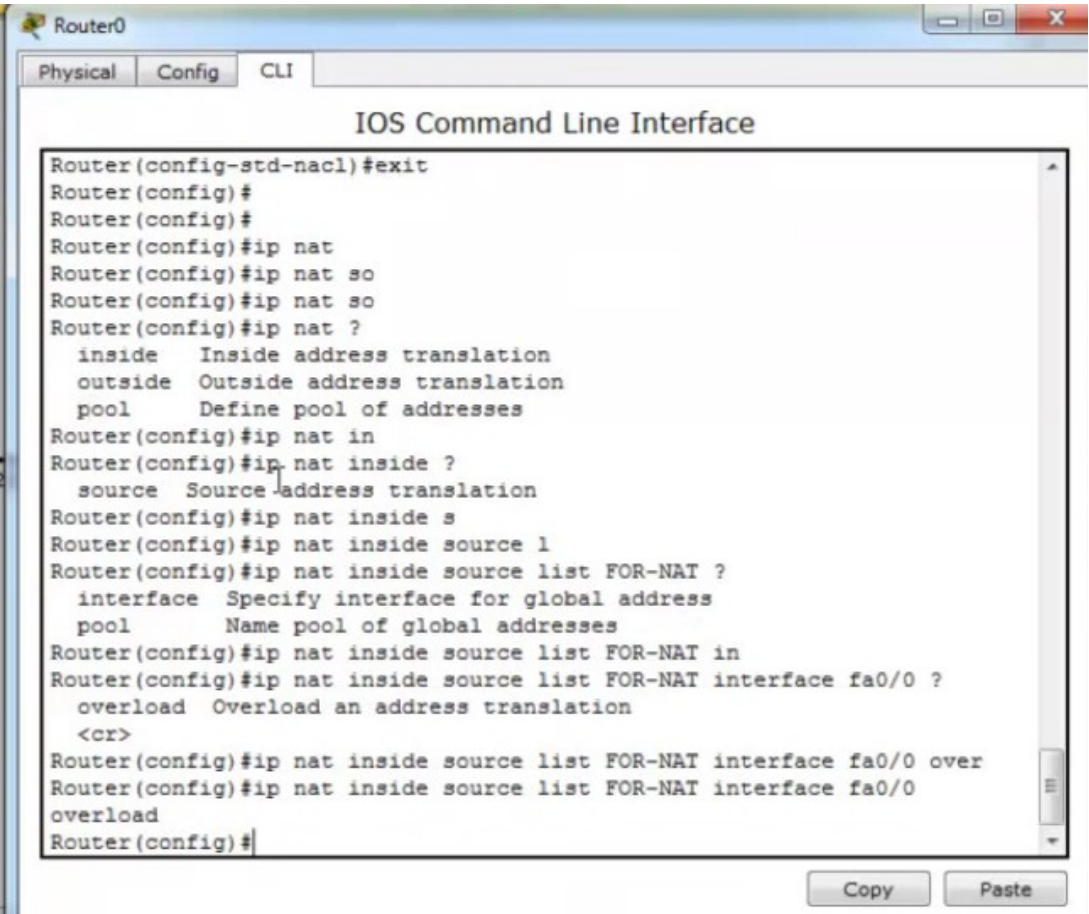
IOS Command Line Interface

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

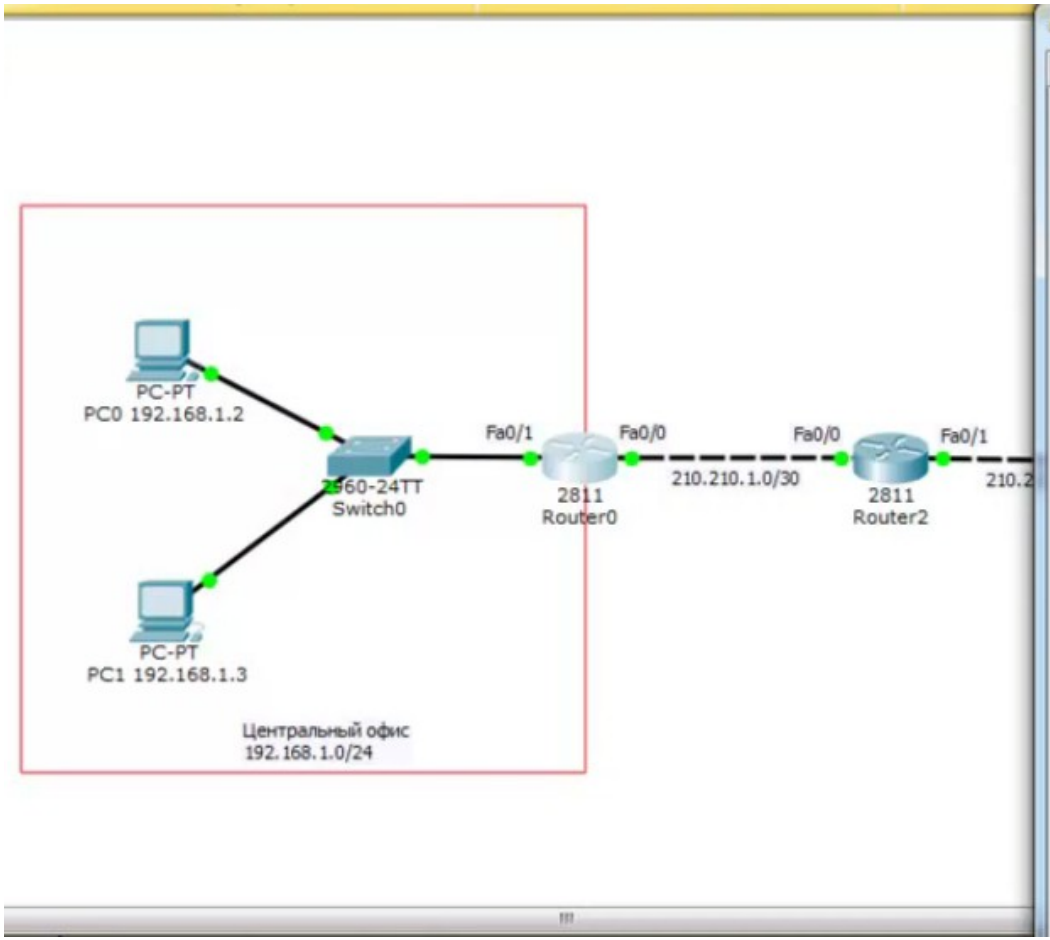
Copy | Paste

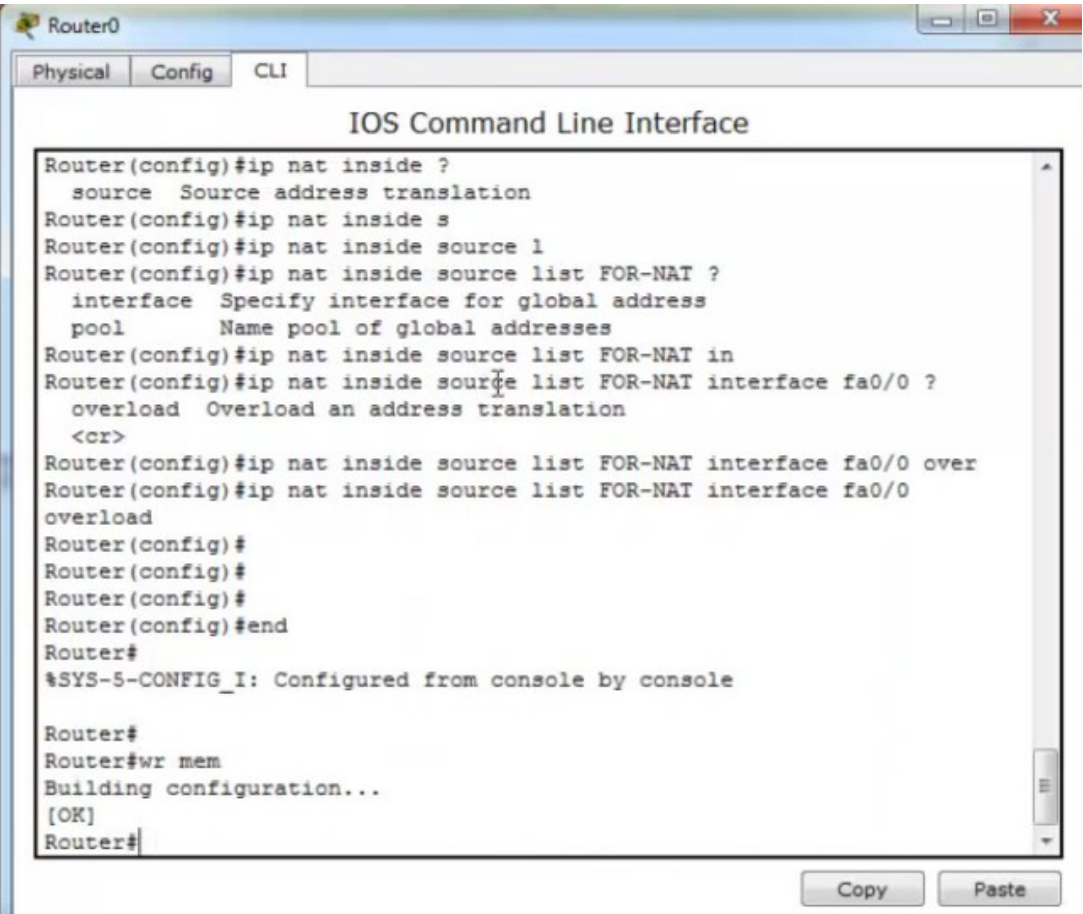
На Router0 настроим NAT



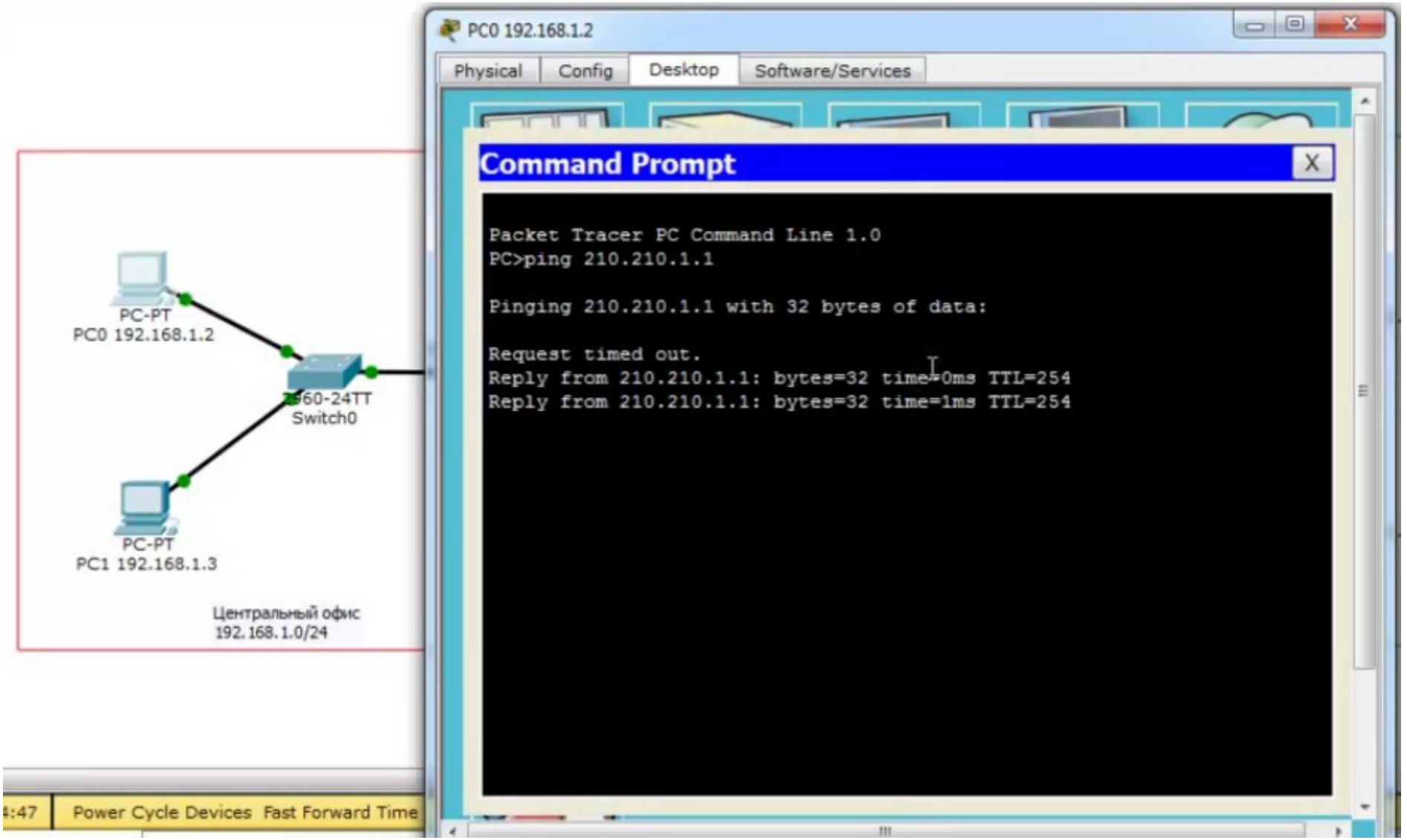


Сохраняем настройки





Проверяем доступ роутера провайдера с PC0. Доступно



Настраиваем NAT на Router1 филиала

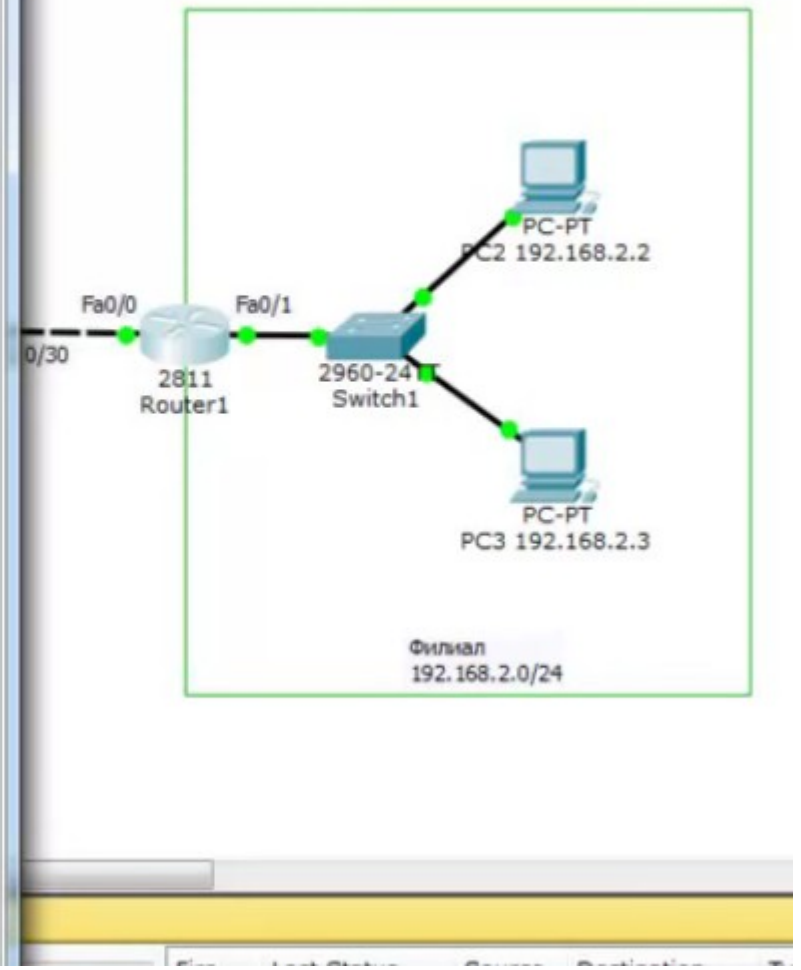
Router1

Physical | Config | CLI

IOS Command Line Interface

```
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.

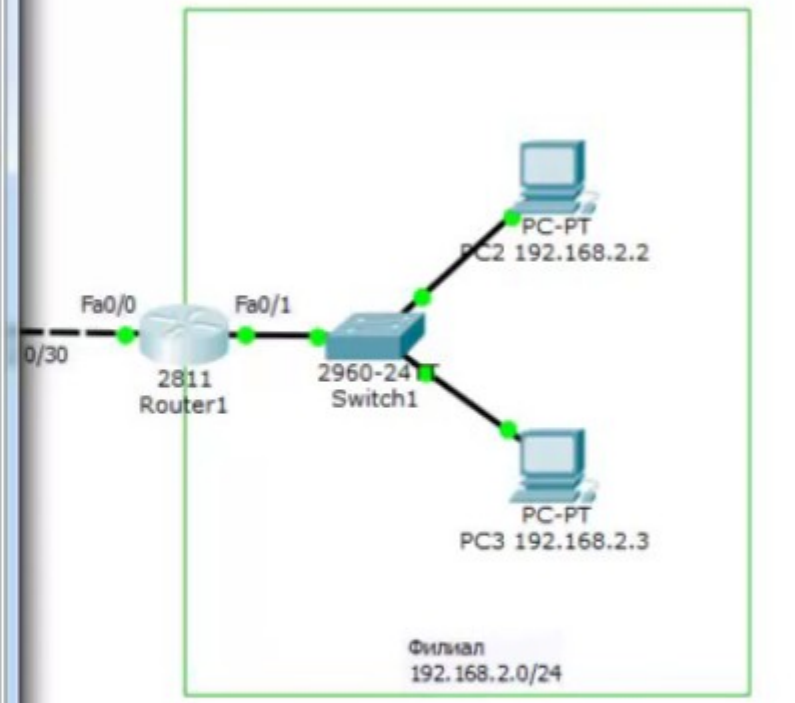
Router1

Physical | Config | CLI

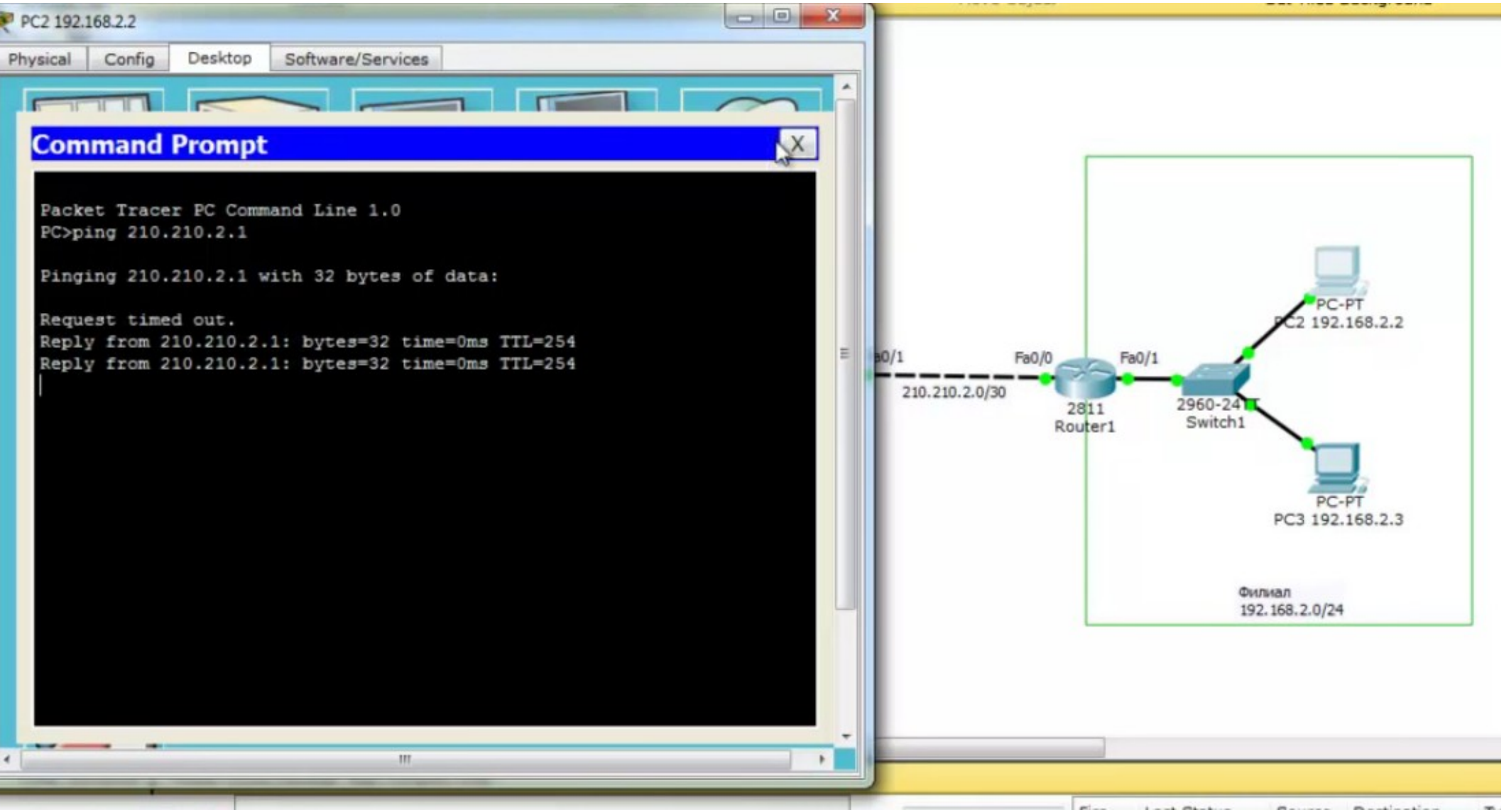
IOS Command Line Interface

```
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#
```

Copy | Paste



Проверяем с PC2 доступность интерфейса провайдера



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»

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

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

```
Router(config-isakmp)#gr
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#
Router(config)#
Router(config)#
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 210.210.2.2
Router(config)#
Router(config)#cry
Router(config)#crypto ip
Router(config)#crypto ipsec tr
Router(config)#crypto ipsec transform-set TS es
Router(config)#crypto ipsec transform-set TS esp-3d
Router(config)#crypto ipsec transform-set TS esp-3des esp-md
Router(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#
Router#
```

Copy | Paste

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

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

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#ip acc
Router(config)#ip access-list ex
Router(config)#ip access-list extended FOR-VPN
Router(config-ext-nacl)#per
Router(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0
0.0.0.255
Router(config-ext-nacl)#
Router(config-ext-nacl)#
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
```

Copy | Paste

На Router0 создаем крипто-карту с настройками шифрования

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

```
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)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#int fa
Router(config)#int fastEthernet 0/0
Router(config-if)#cr
Router(config-if)#crypto ma
Router(config-if)#crypto map CMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
```

Copy | Paste

На Router0 создаем крипто-карту с настройками шифрования

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

```
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)#exit
Router(config)#
Router(config)#
Router(config)#
```

Copy | Paste

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

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

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

```
Router(config-crypto-map)#
Router(config-crypto-map)#
Router(config-crypto-map)#
Router(config-crypto-map)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#int fa
Router(config)#int fastEthernet 0/0
Router(config-if)#cr
Router(config-if)#crypto ma
Router(config-if)#crypto map CMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

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#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)#
```

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

Copy Paste

Выполняем те же действия на Router1 роутере филиала

Типовые настройки роутера:

Настройка первой фазы

```
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
```

Настройка ключа аутентификации и пира

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

Вторая фаза

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

Определяем какой трафик шифровать

```
ip access-list extended FOR-VPN
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Создание криптокарты

```
crypto map CMAP 10 ipsec-isakmp
set peer 210.210.2.2
set transform-set TS
match address FOR-VPN
```

Привязка к интерфейсу

```
interface FastEthernet0/0
crypto map CMAP
```

Router1

Physical | Config | CLI

IOS Command Line Interface

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

Copy | Paste

Сохраняем настройки

Типовые настройки роутера:

Настройка первой фазы

```
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
```

Настройка ключа аутентификации и пира

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

Вторая фаза

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

Определяем какой трафик шифровать

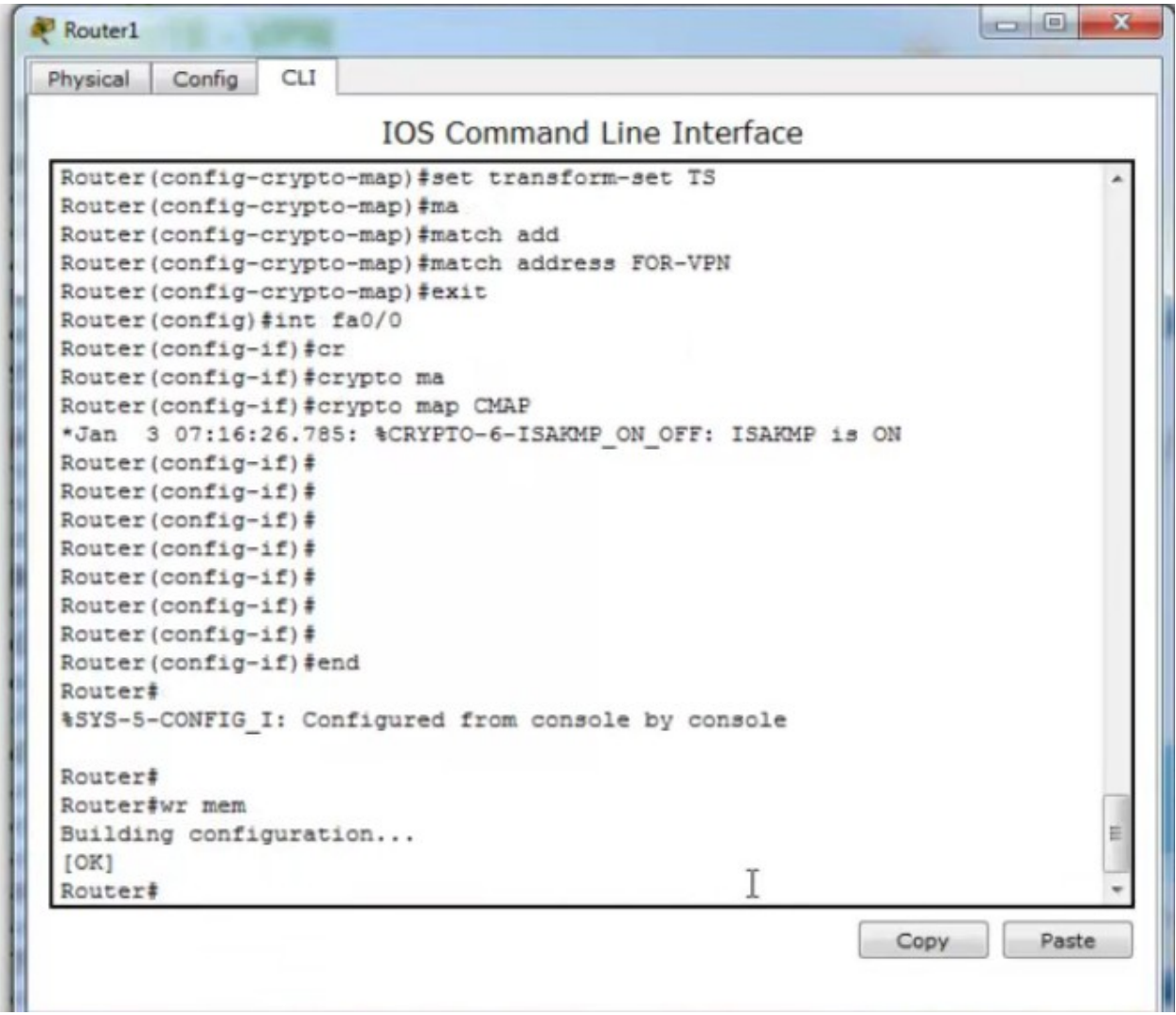
```
ip access-list extended FOR-VPN
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Создание криптокарты

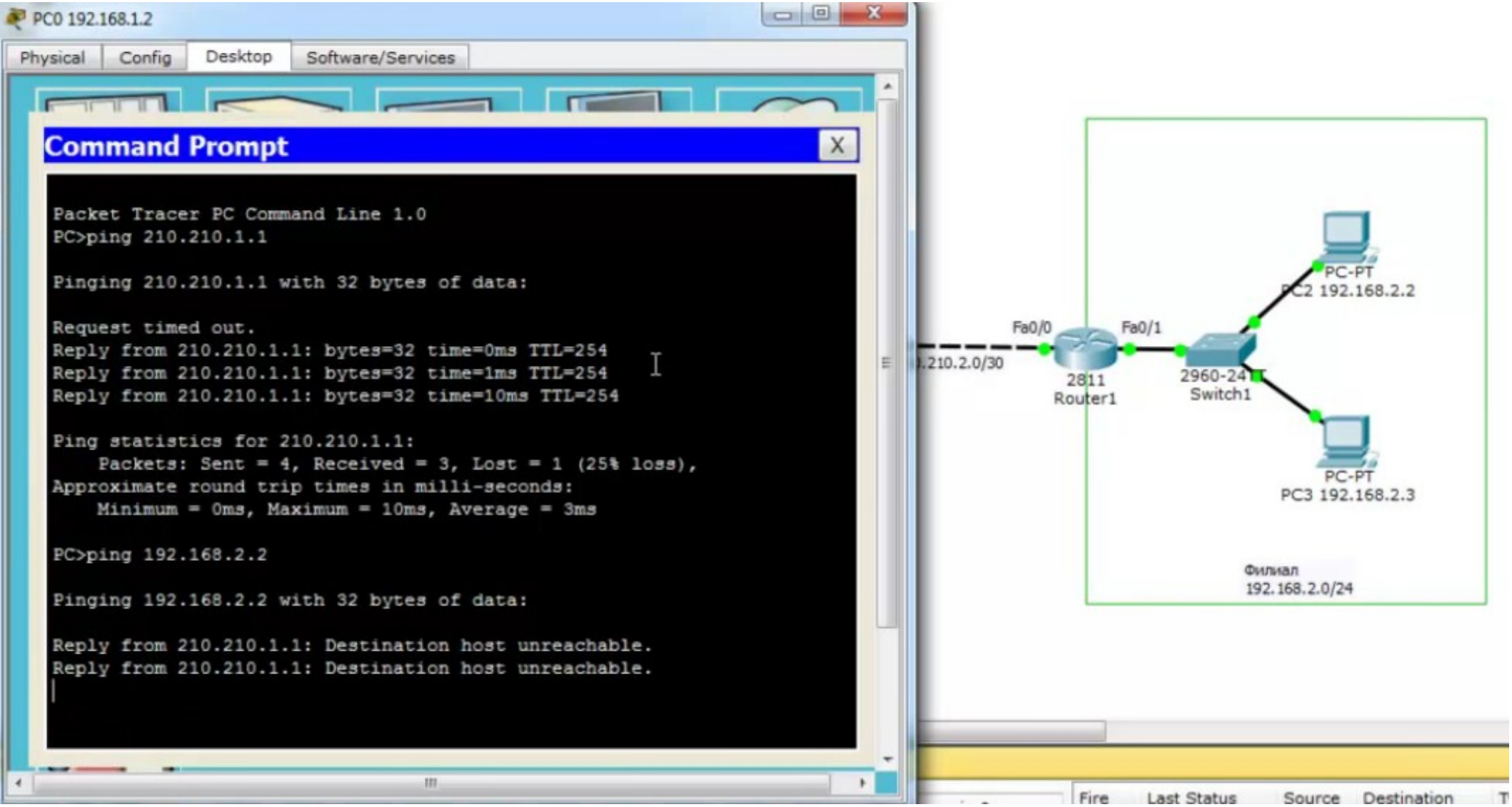
```
crypto map CMAP 10 ipsec-isakmp
set peer 210.210.2.2
set transform-set TS
match address FOR-VPN
```

Привязка к интерфейсу

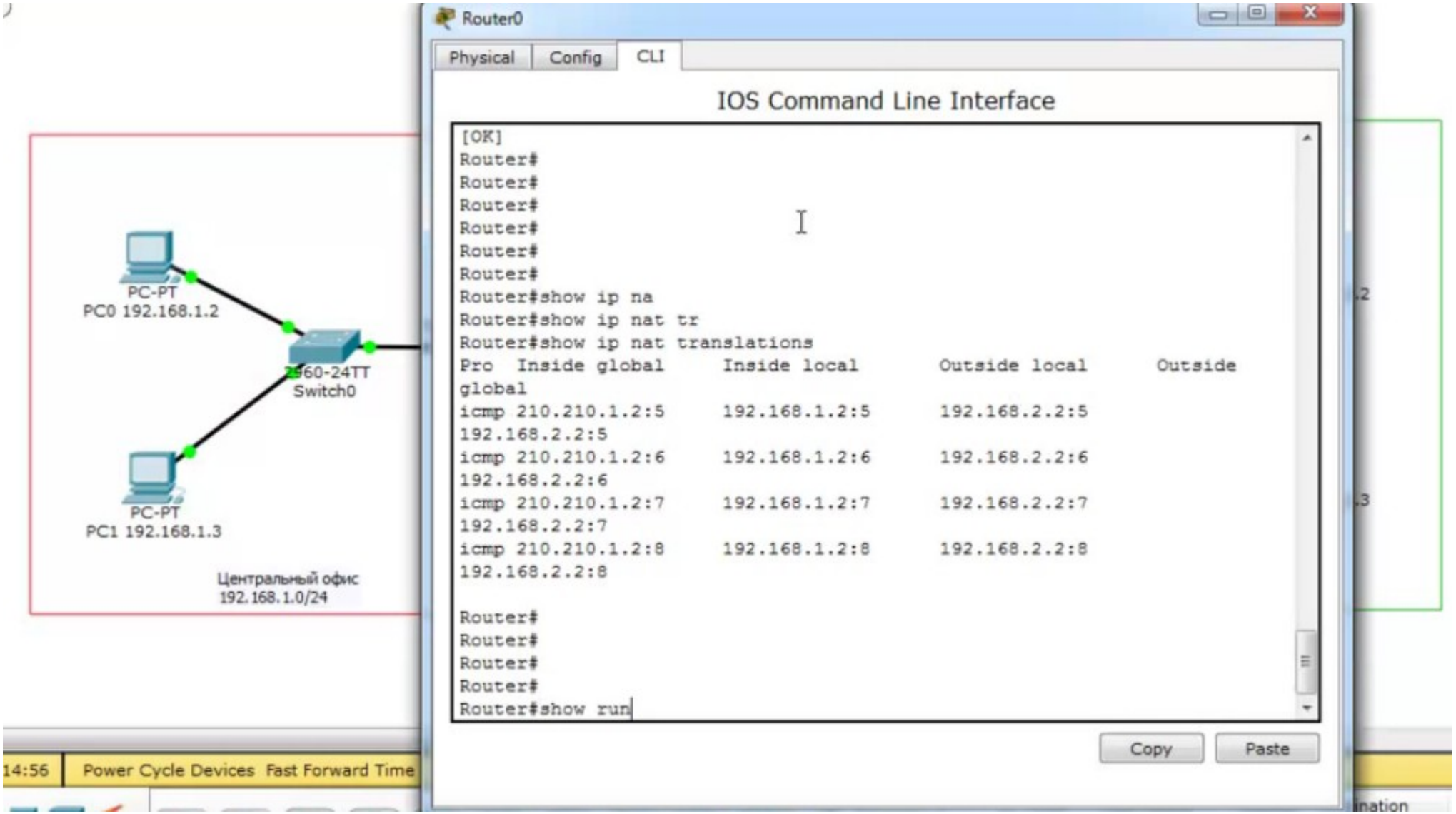
```
interface FastEthernet0/0
crypto map CMAP
```



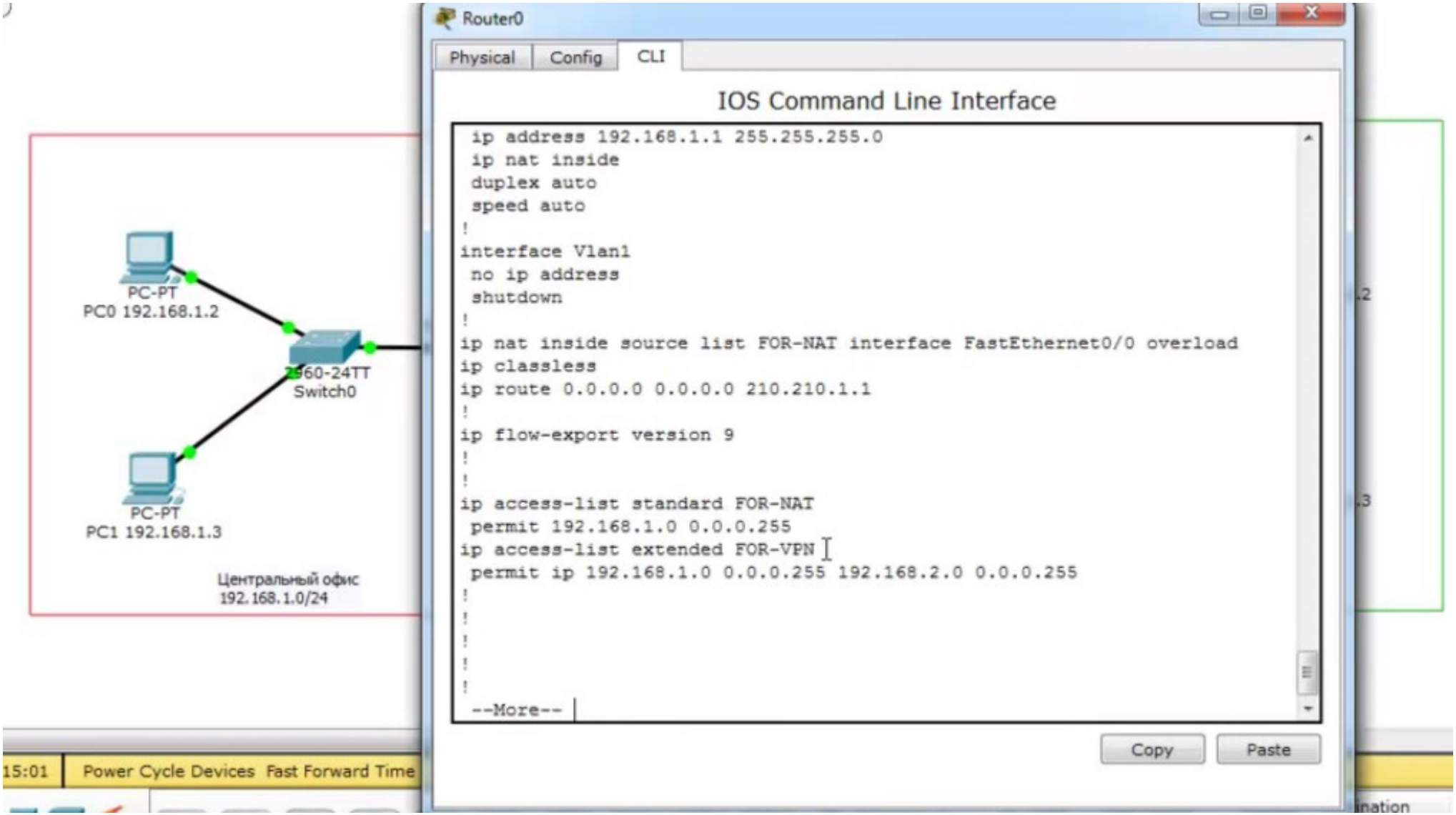
Попробуем с компьютера PC0 центрального офиса пропинговать компьютер PC2 в филиале. Не проходит



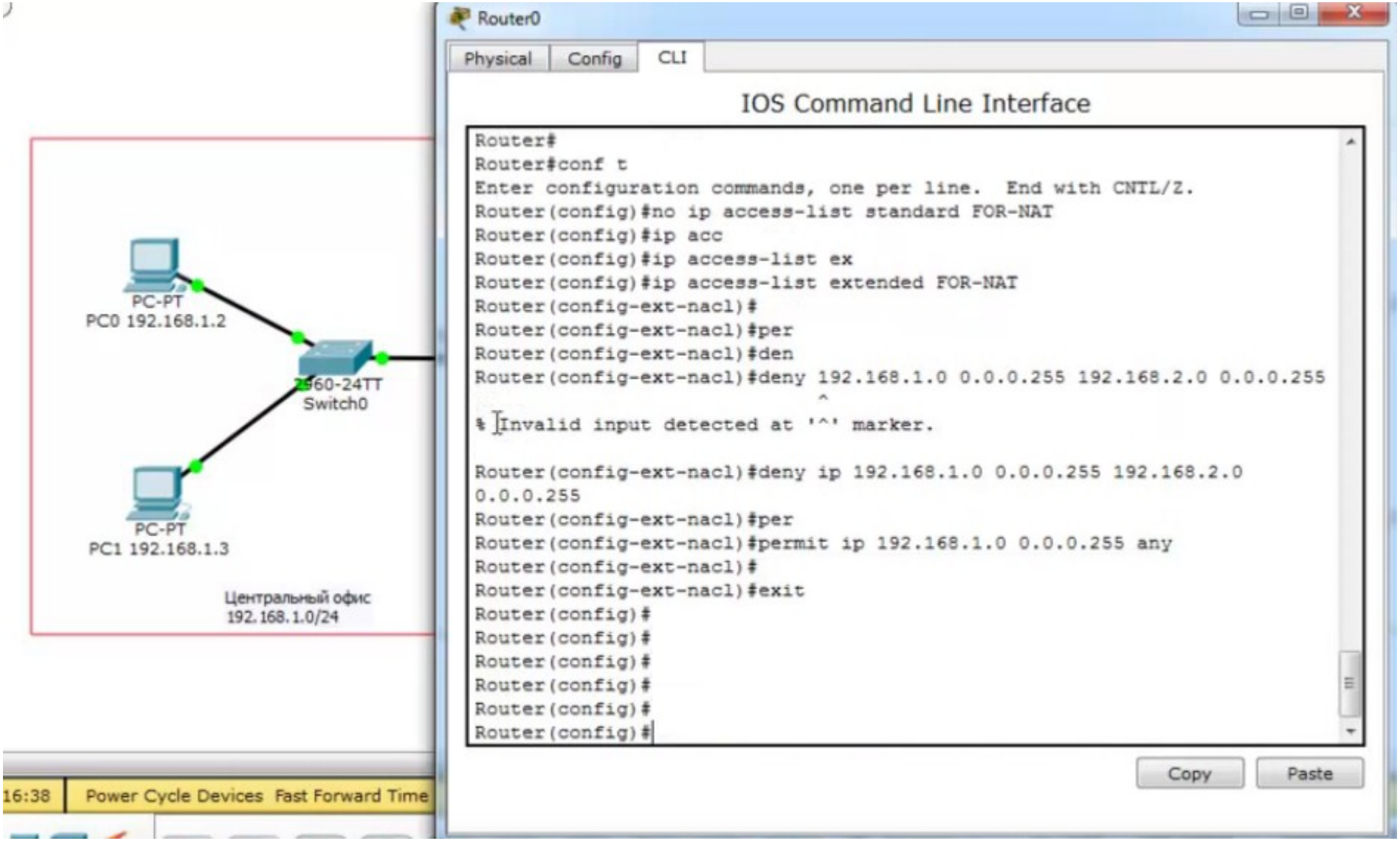
Смотрим настройки NAT на Router0. Траффик, который должен идти в VPN-канал, попадает под преобразования NAT. Посмотрим настройки access-list



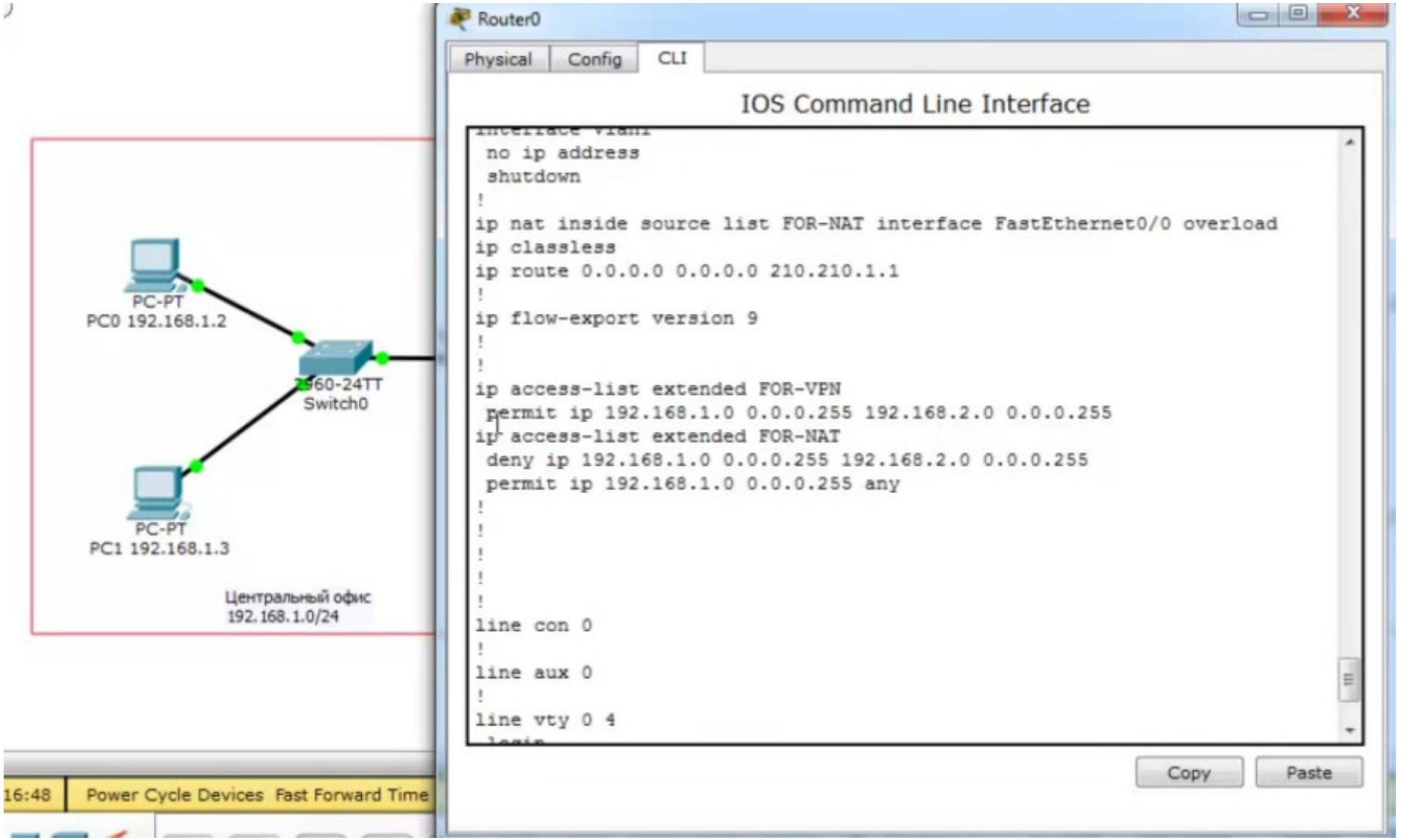
Под действие access-list попадает весь траффик 192.168.1.0, а это не совсем то, что нам нужно



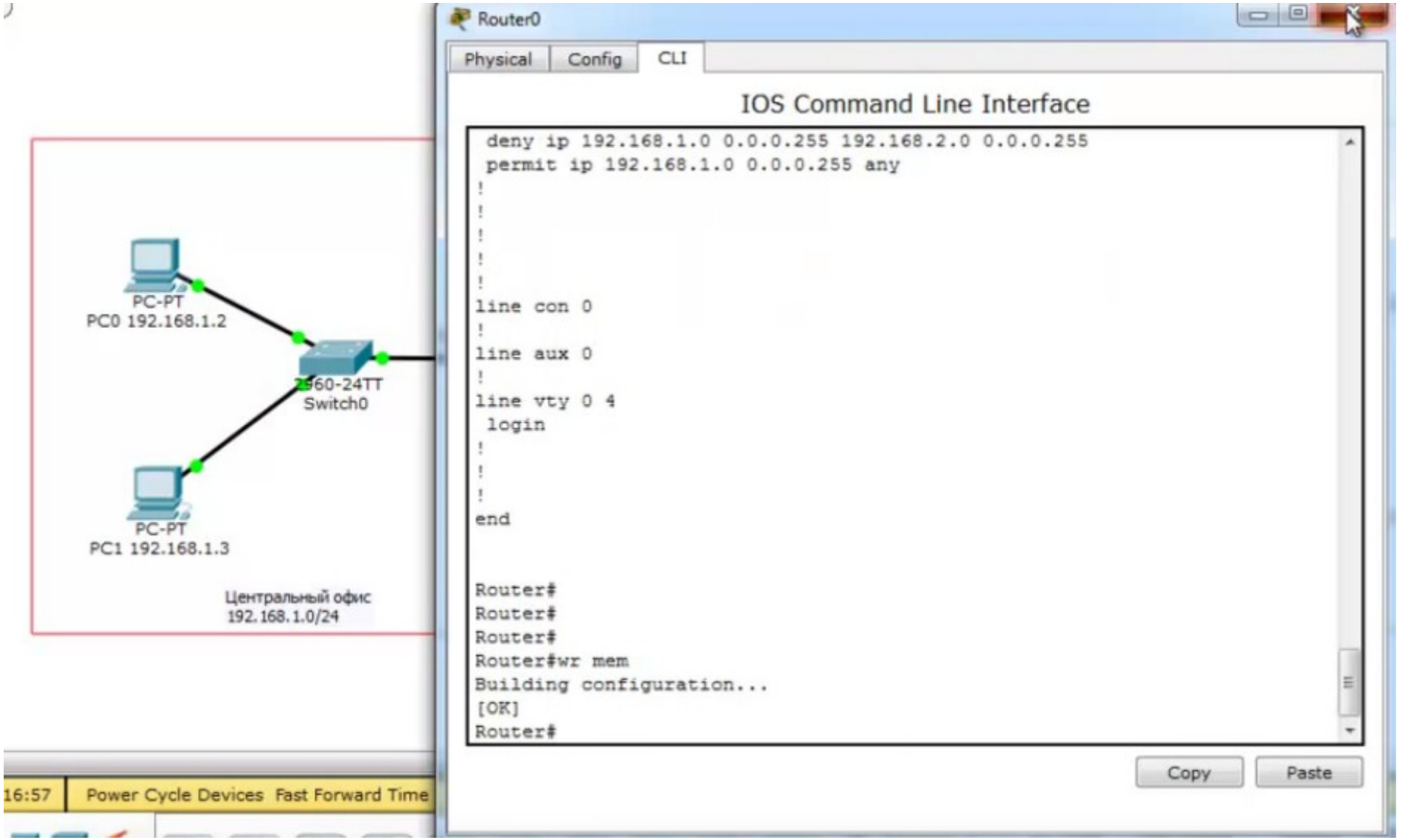
Удалим существующий access-list, добавим исправленный



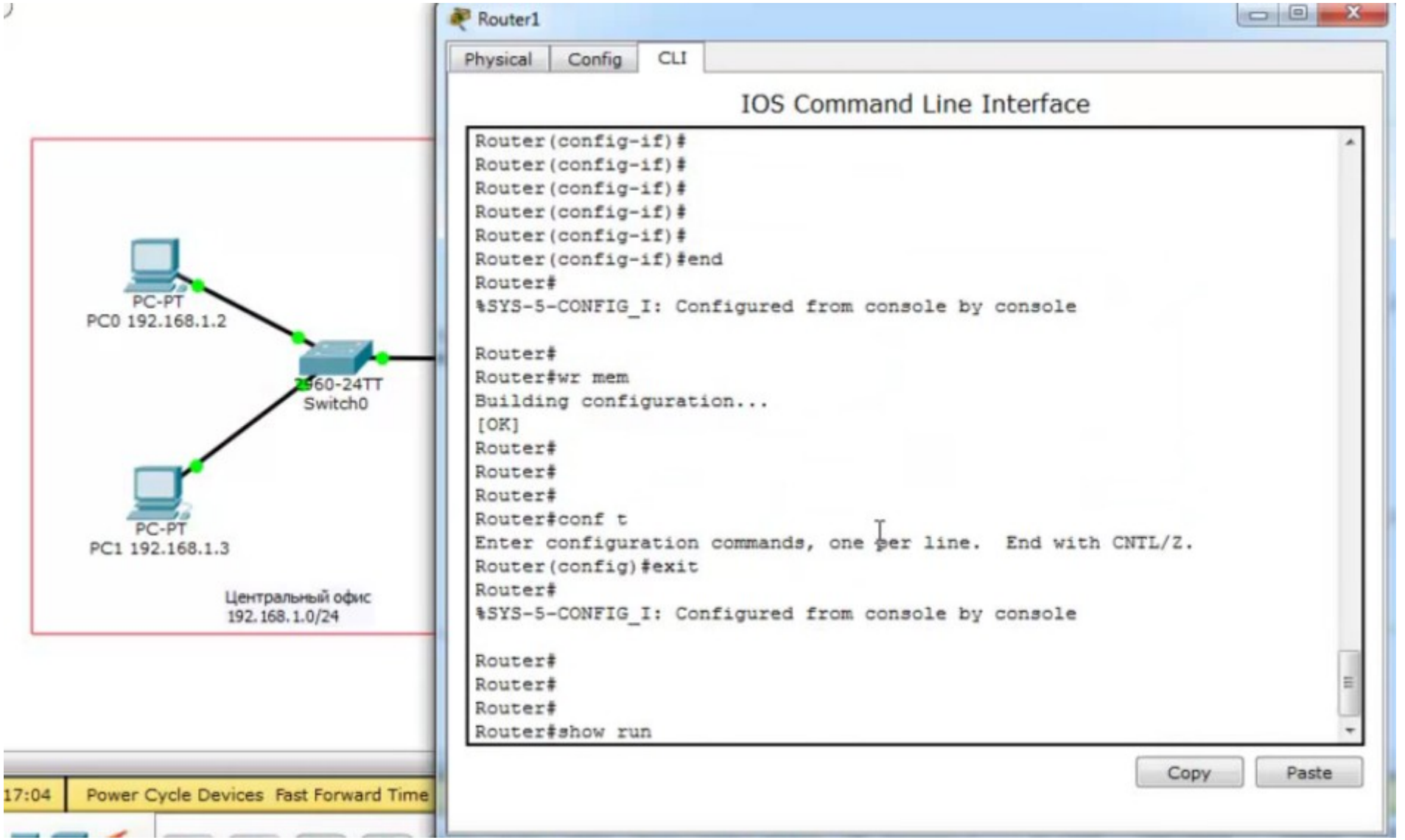
Проверим получившиеся настройки



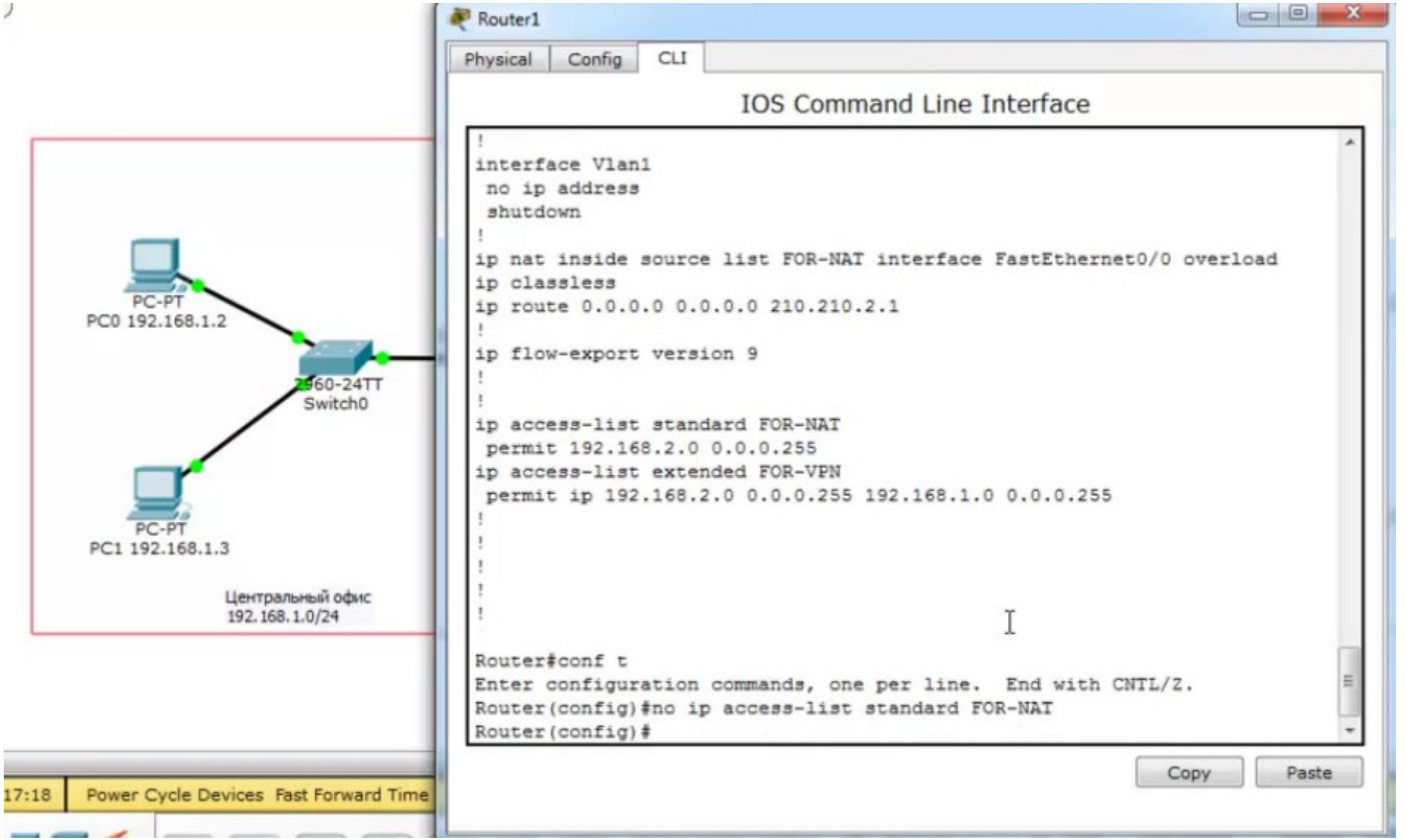
Сохраняем


PC-PT
PC0 192.168.1.2
2960-24TT
Switch0
PC-PT
PC1 192.168.1.3
Центральный офис
192.168.1.0/24
16:57
Power Cycle Devices
Fast Forward Time
Router0
Physical
Config
CLI
IOS Command Line Interface
deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 192.168.1.0 0.0.0.255 any
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
Router#
Router#
Router#
Router#wr mem
Building configuration...
[OK]
Router#
Copy
Paste

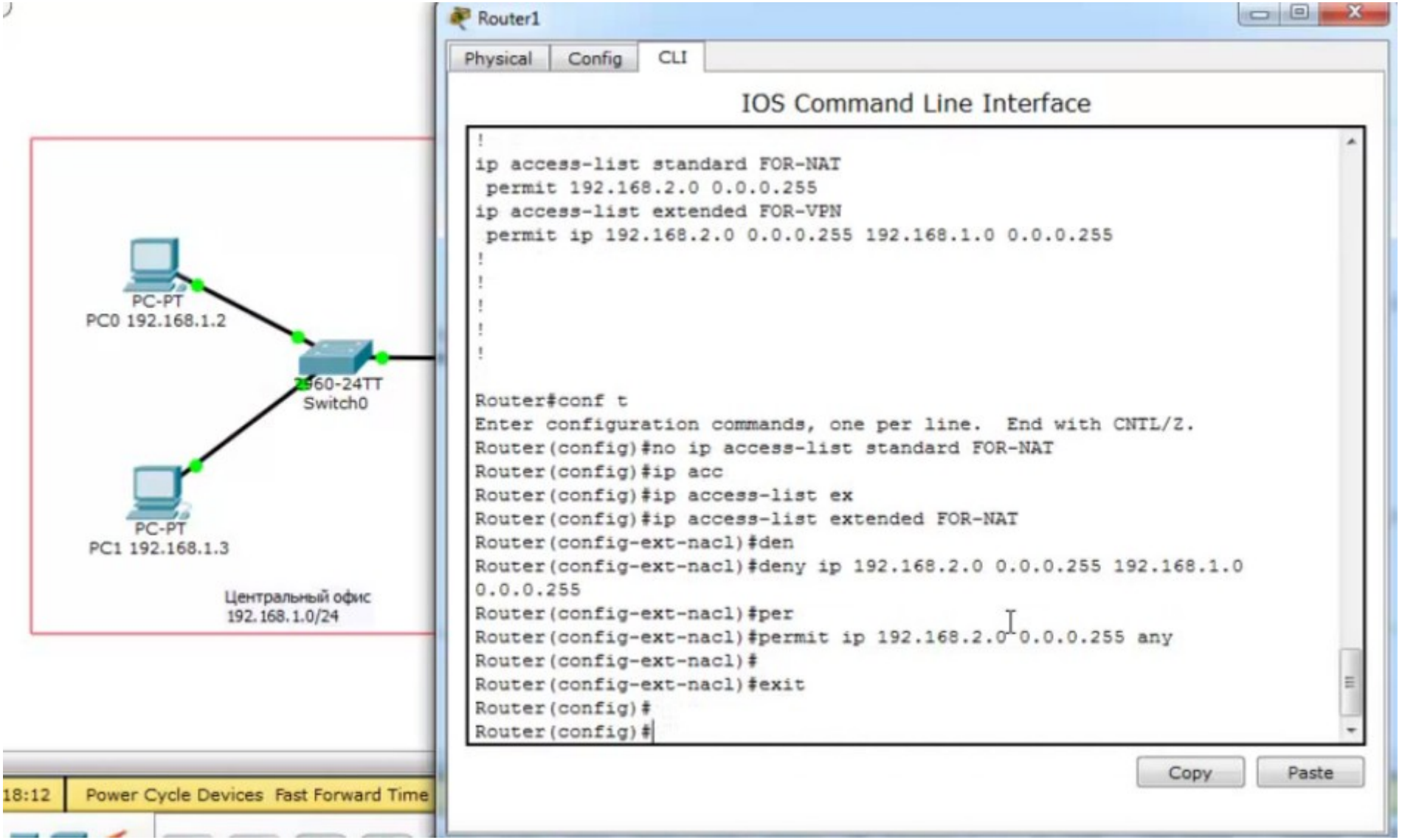
Зайдем на Router1 филиала, для выполнения тех же операций



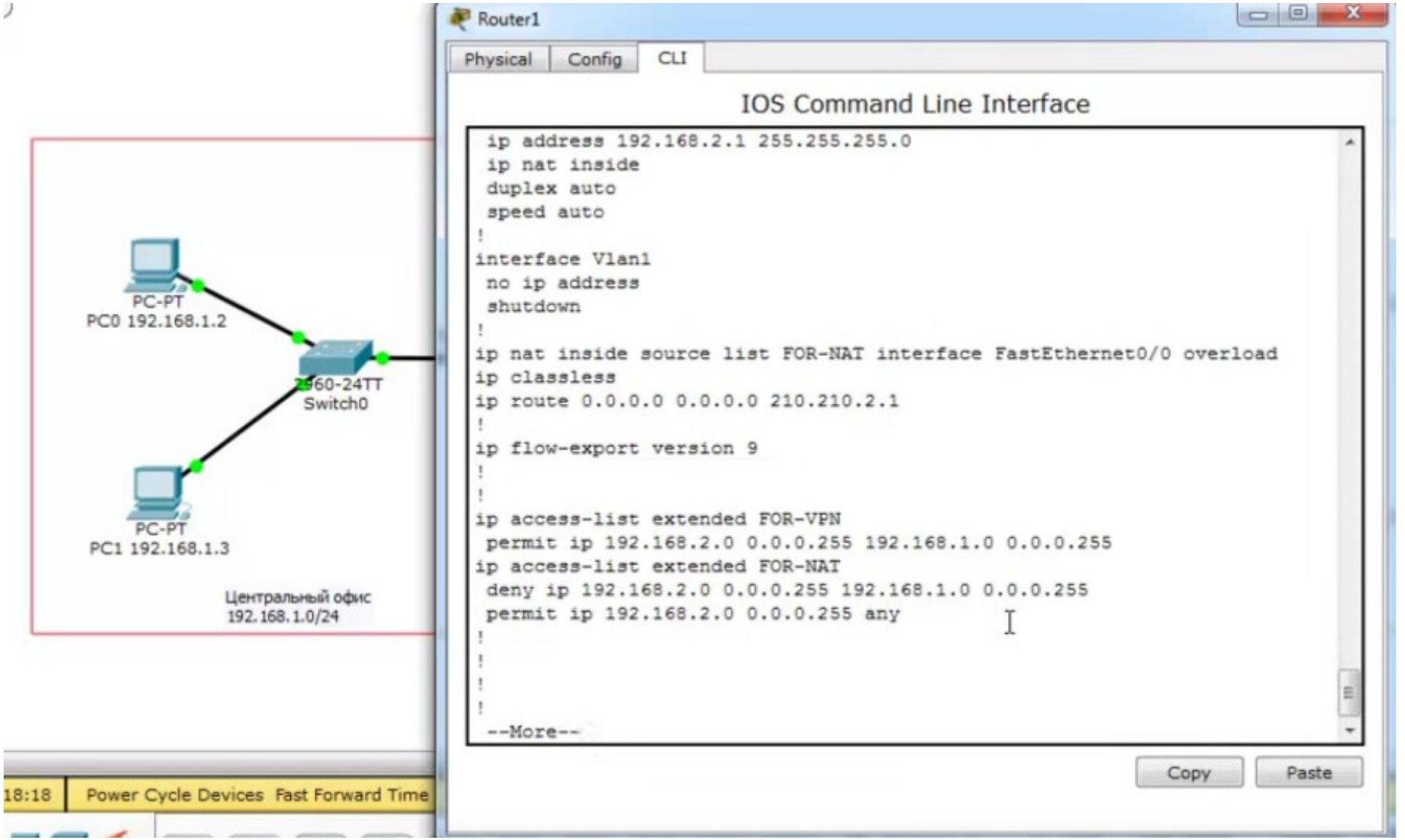
Удалим существующий access list



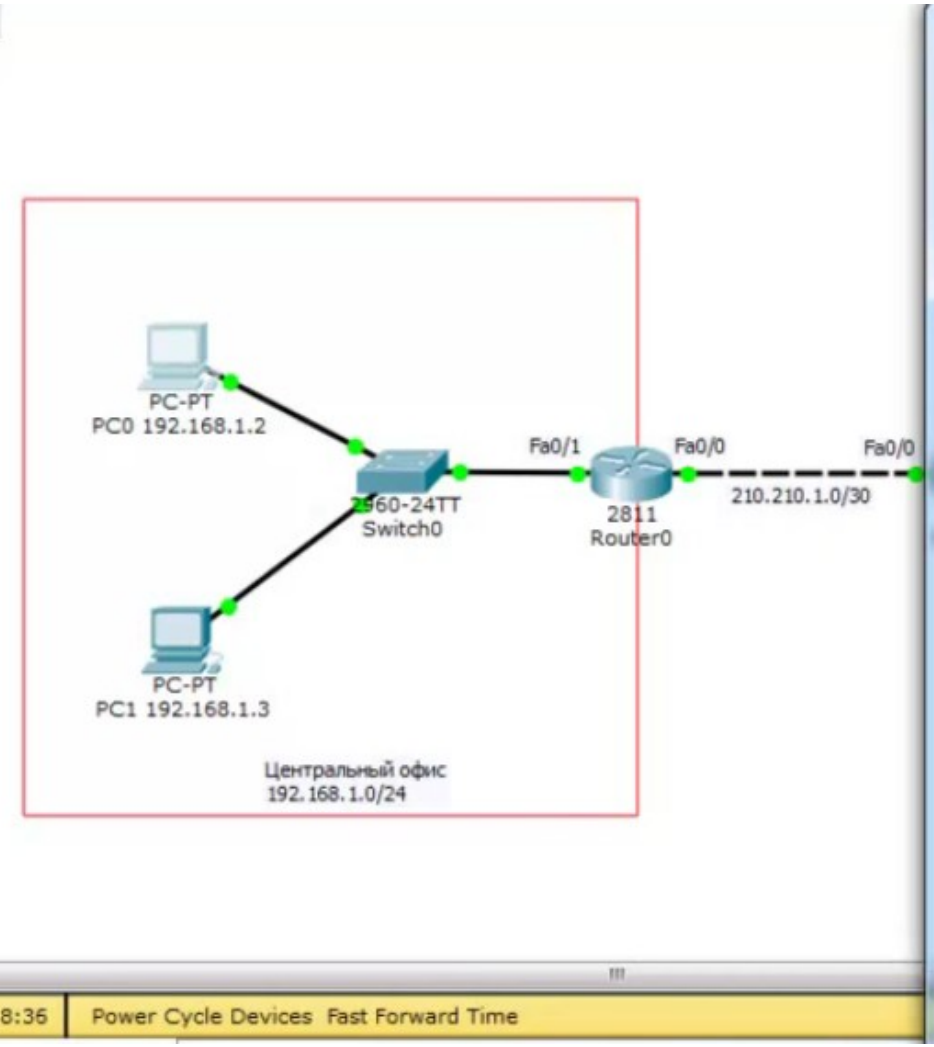
и создадим расширенный

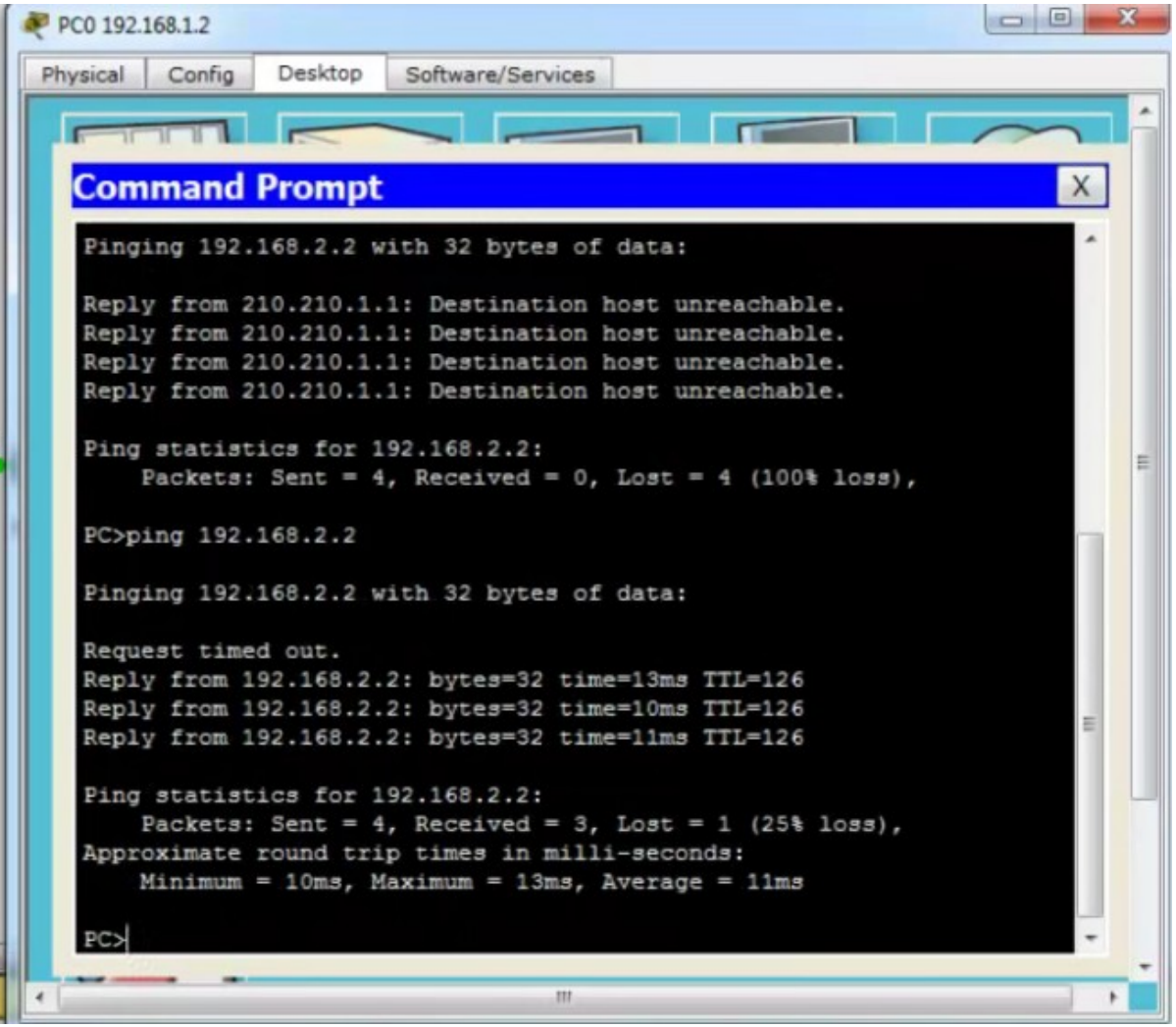


Проверим получившиеся настройки

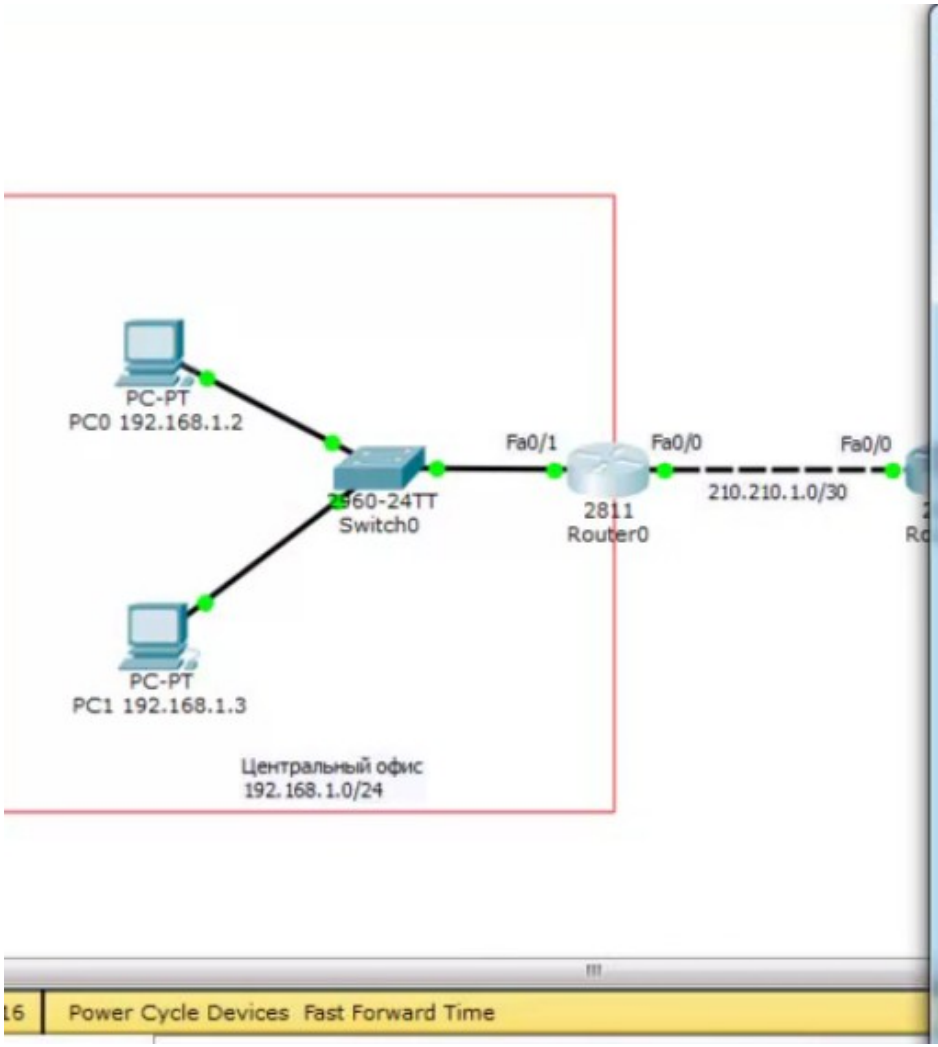


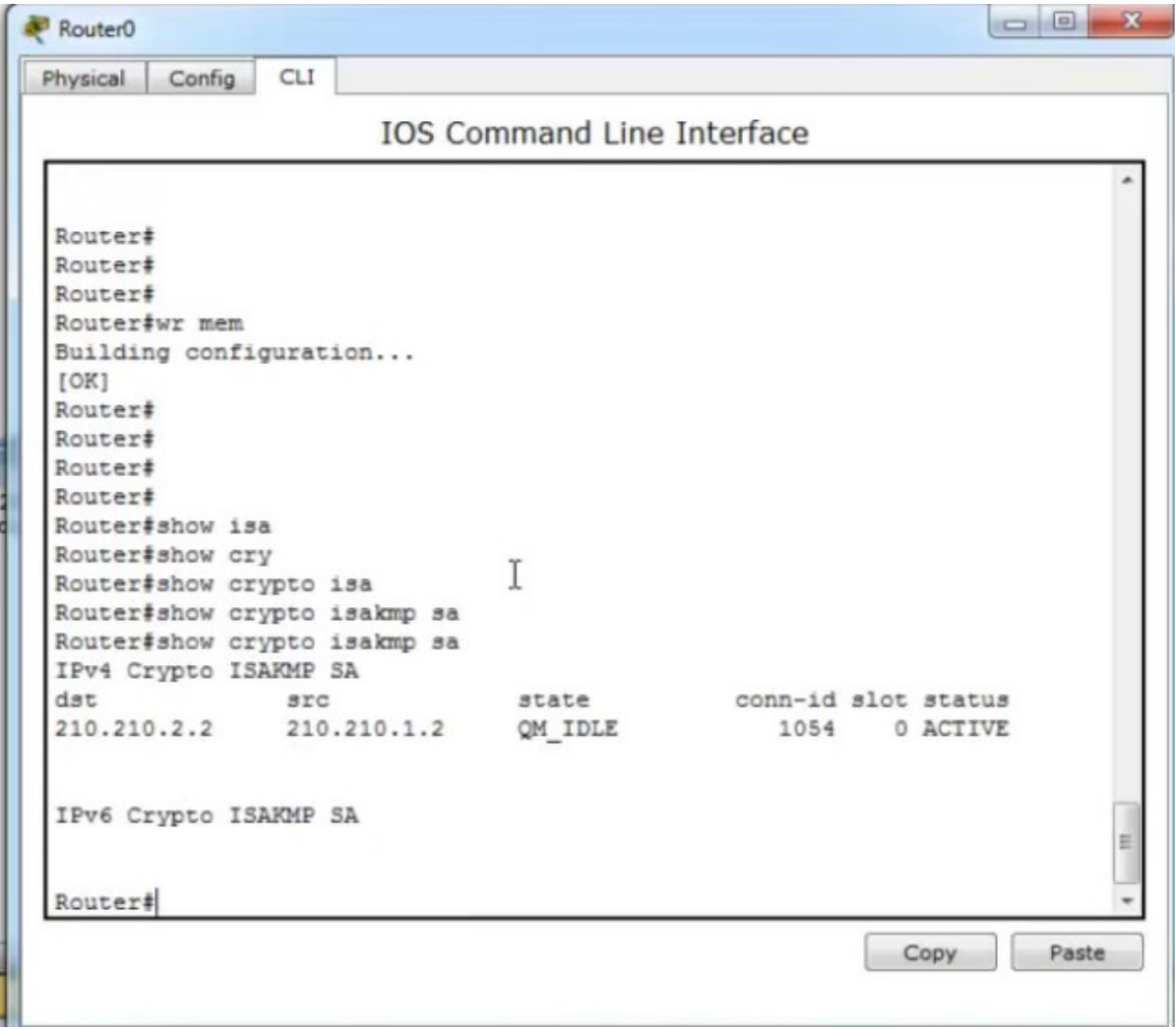
Проверим ping с PC0 на PC2 - идет



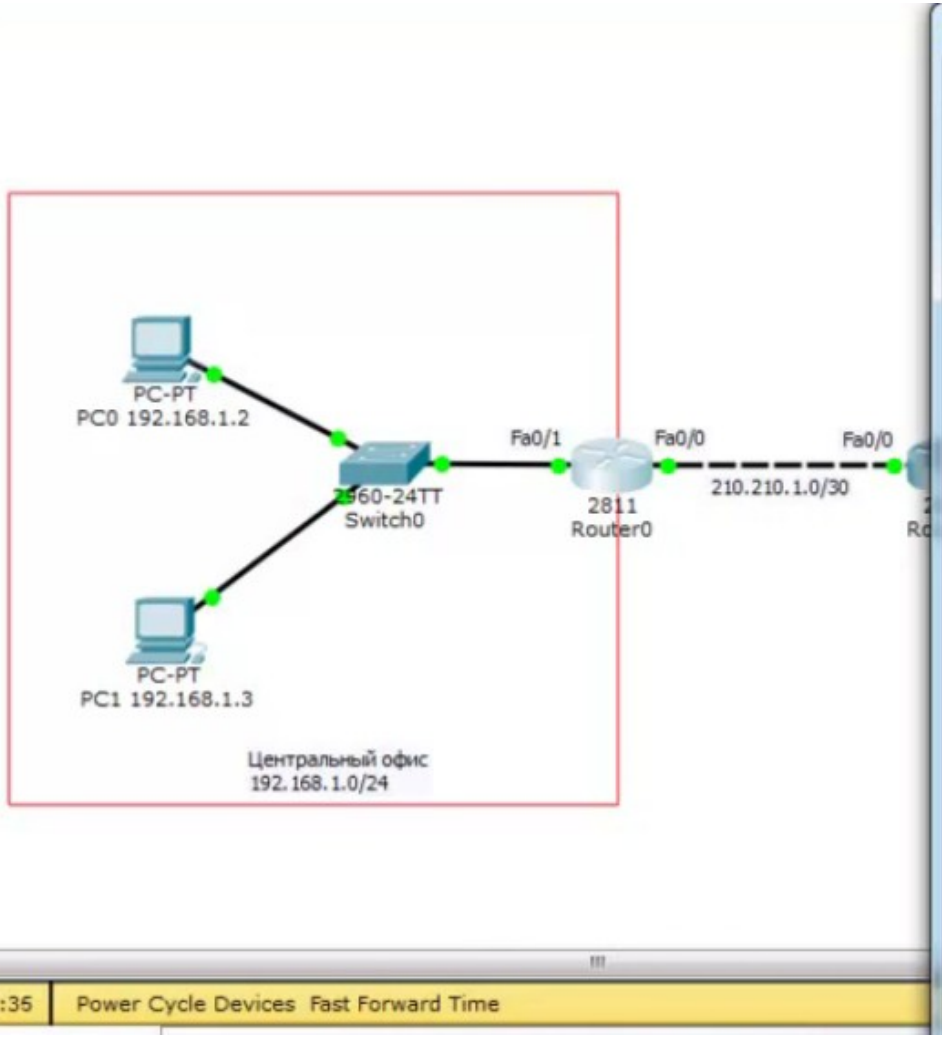


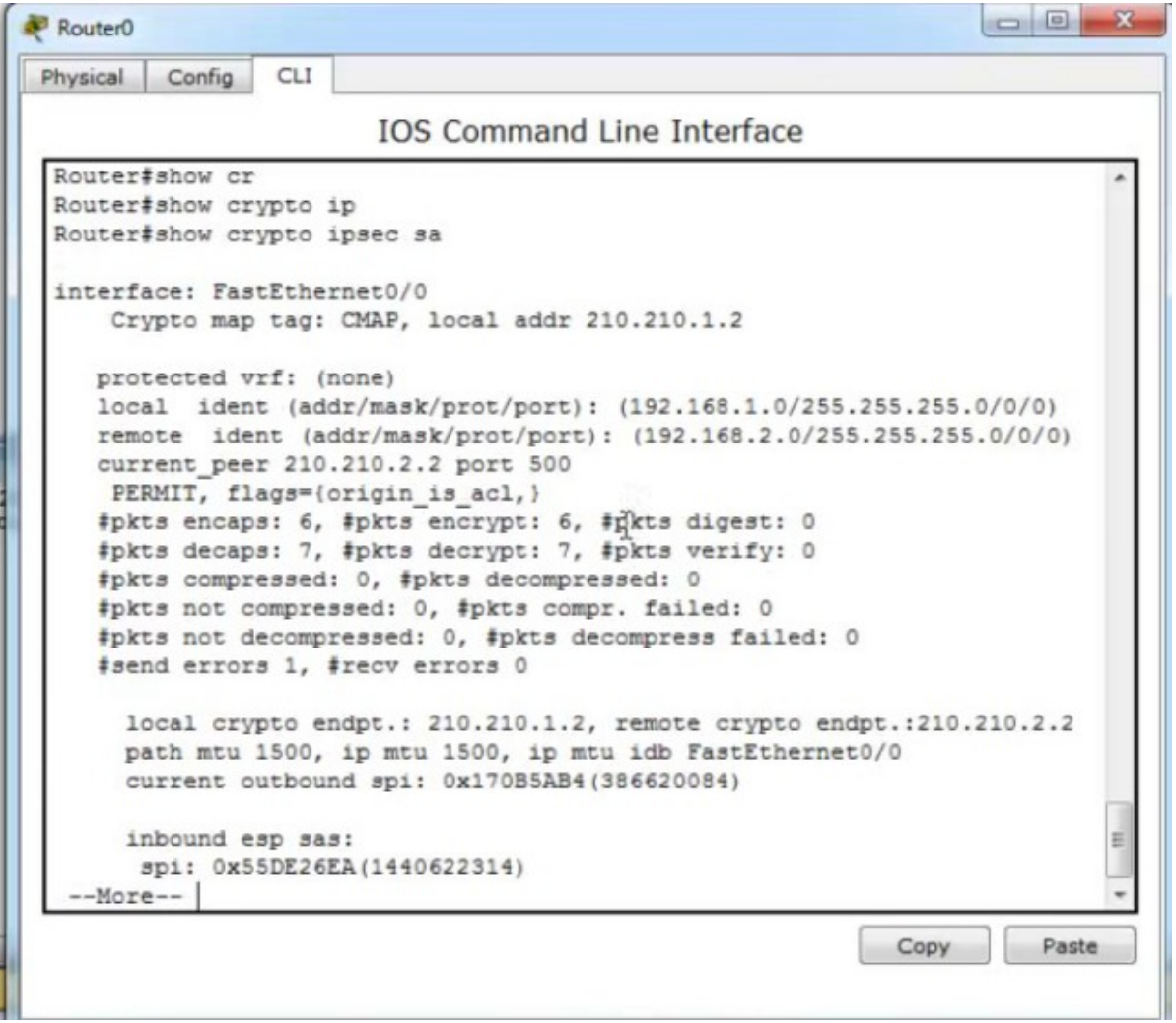
Проверим на роутере наличие «технологического» VPN тоннеля





и наличие ipsec VPN тоннеля





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 fairewall и более старой технологией CBAC (Context Based Access Control)

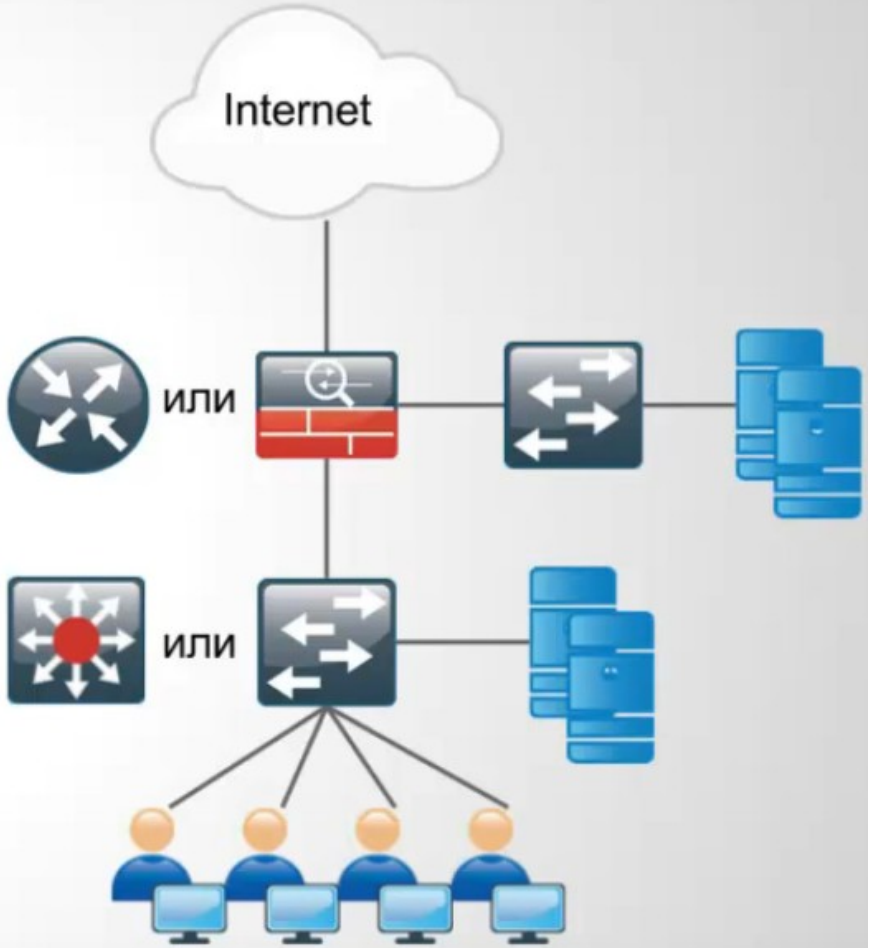
Как правило выделяют минимум три зоны:

1. Внешний сегмент (outside)
2. DMZ сегмент (DMZ)
3. Внутренний сегмент (inside)

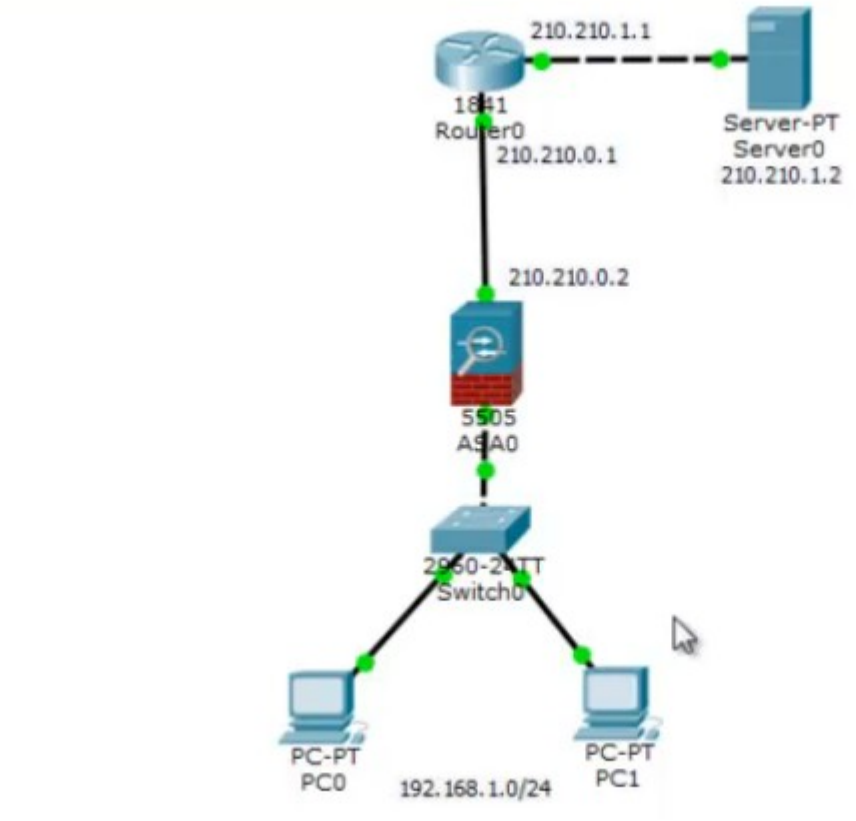
И три основные политики взаимодействия зон:

1. inside -> outside
2. inside -> DMZ
3. outside -> DMZ

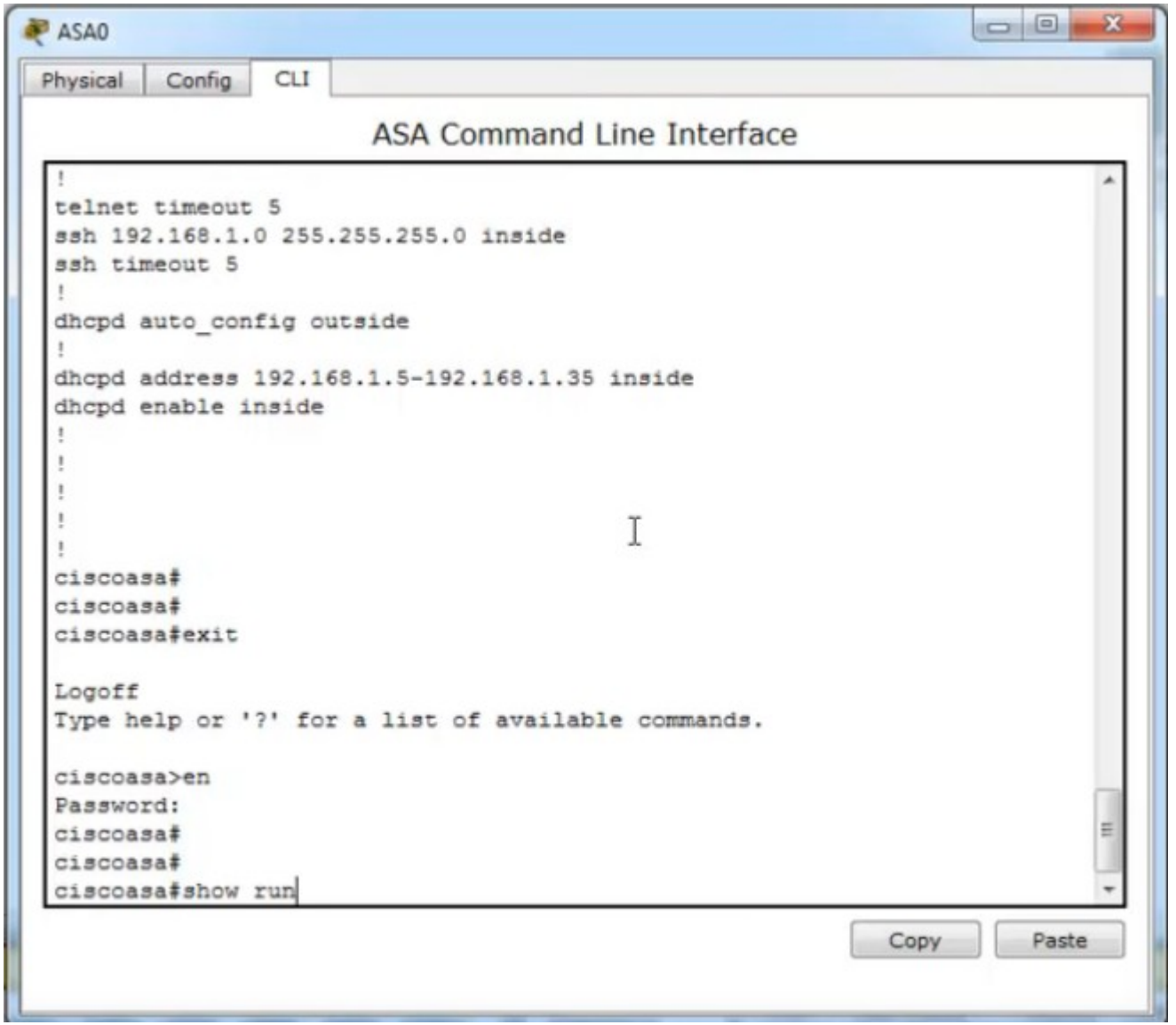
Более подробно о приведенных технологиях можно почитать здесь, здесь, здесь и здесь



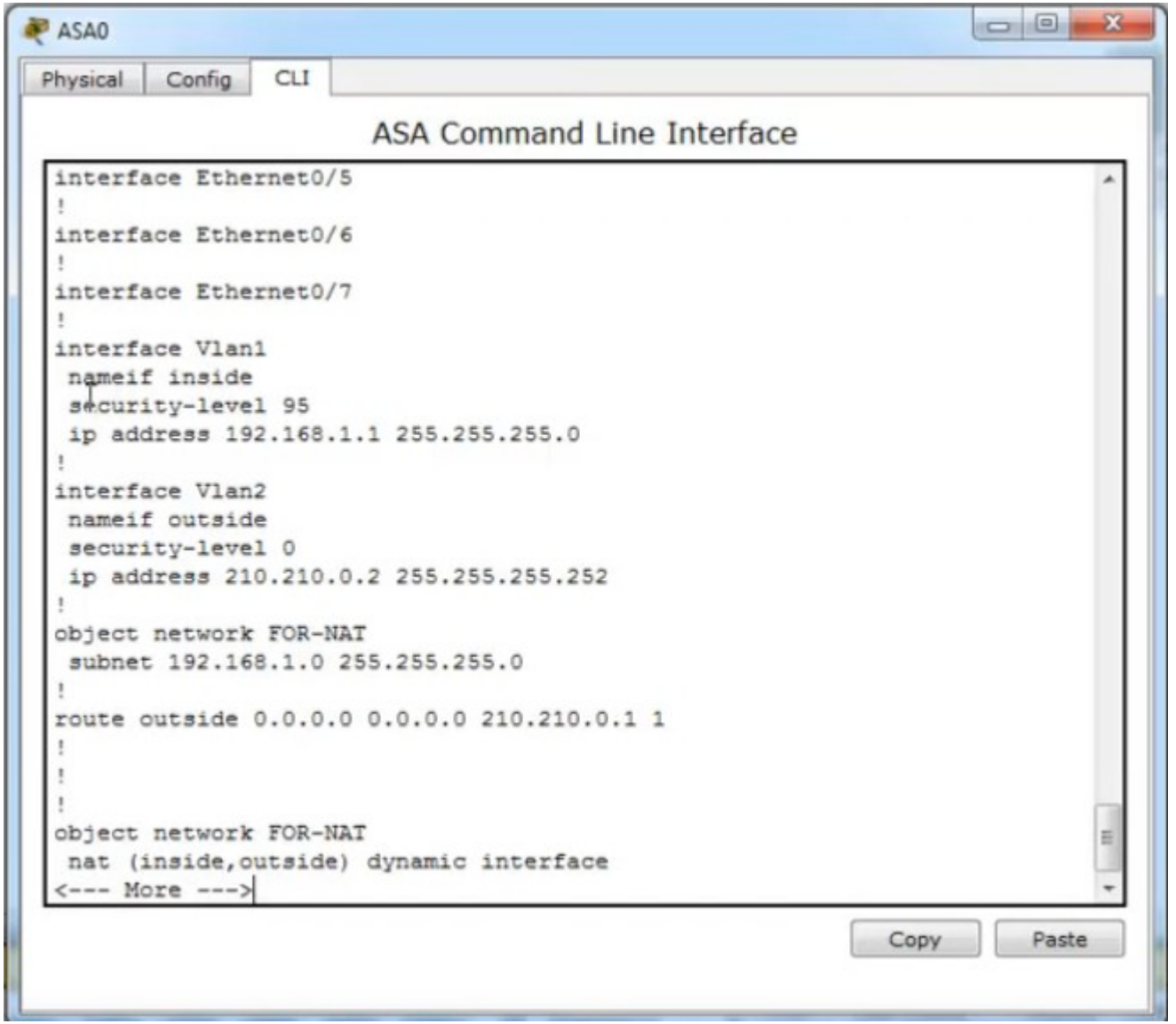
Изначально используется схема Cisco ASA



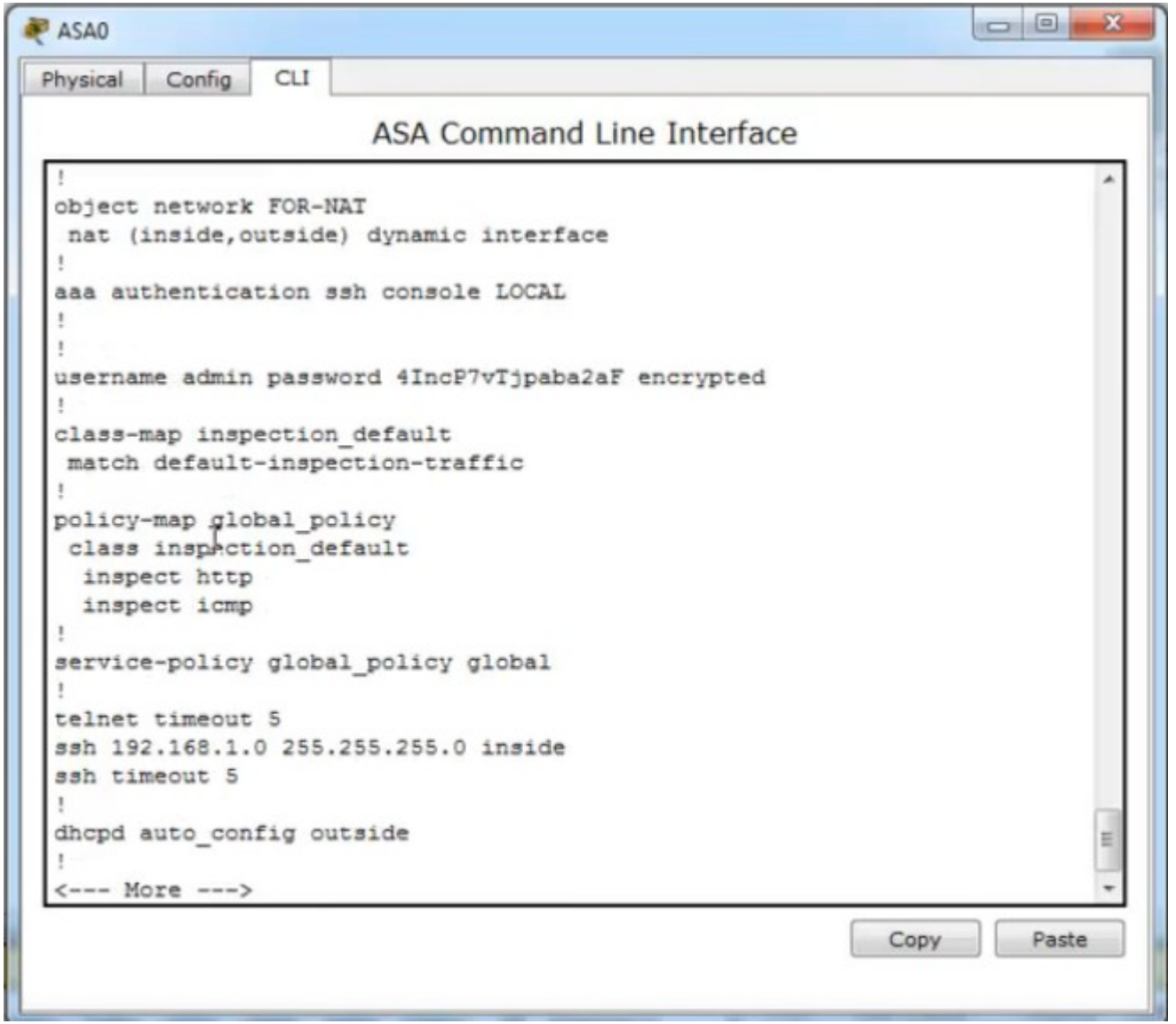
На asa0 настроен пароль cisco



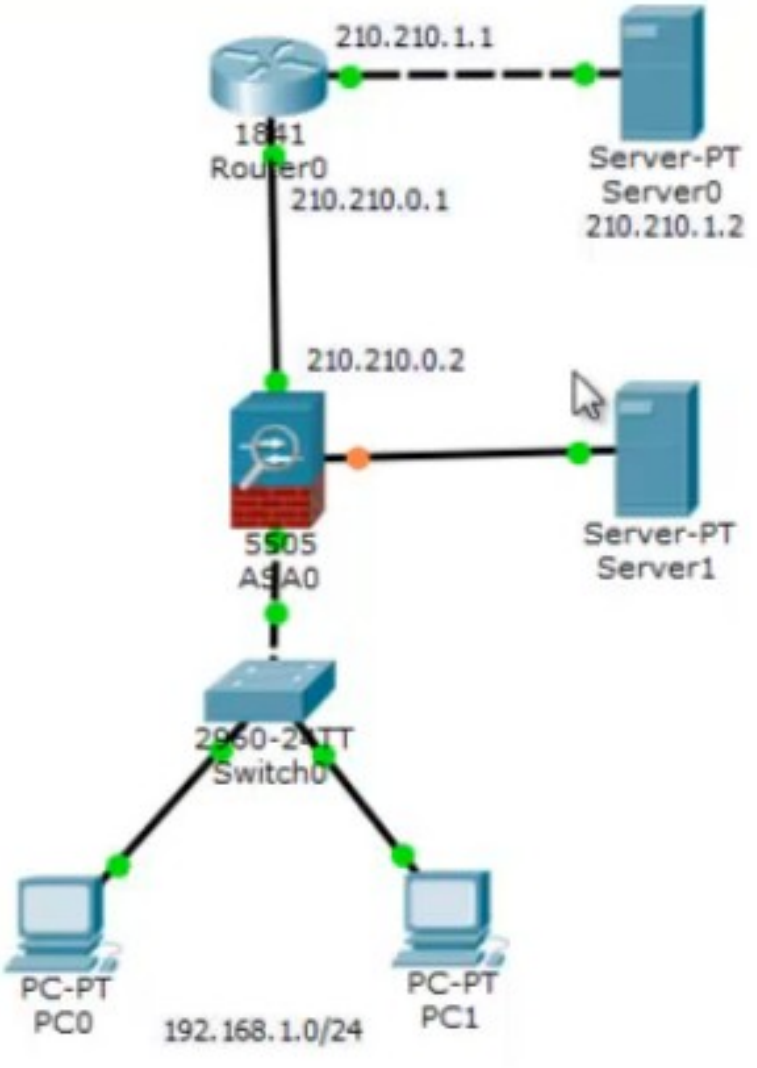
На asa0 настроен NAT



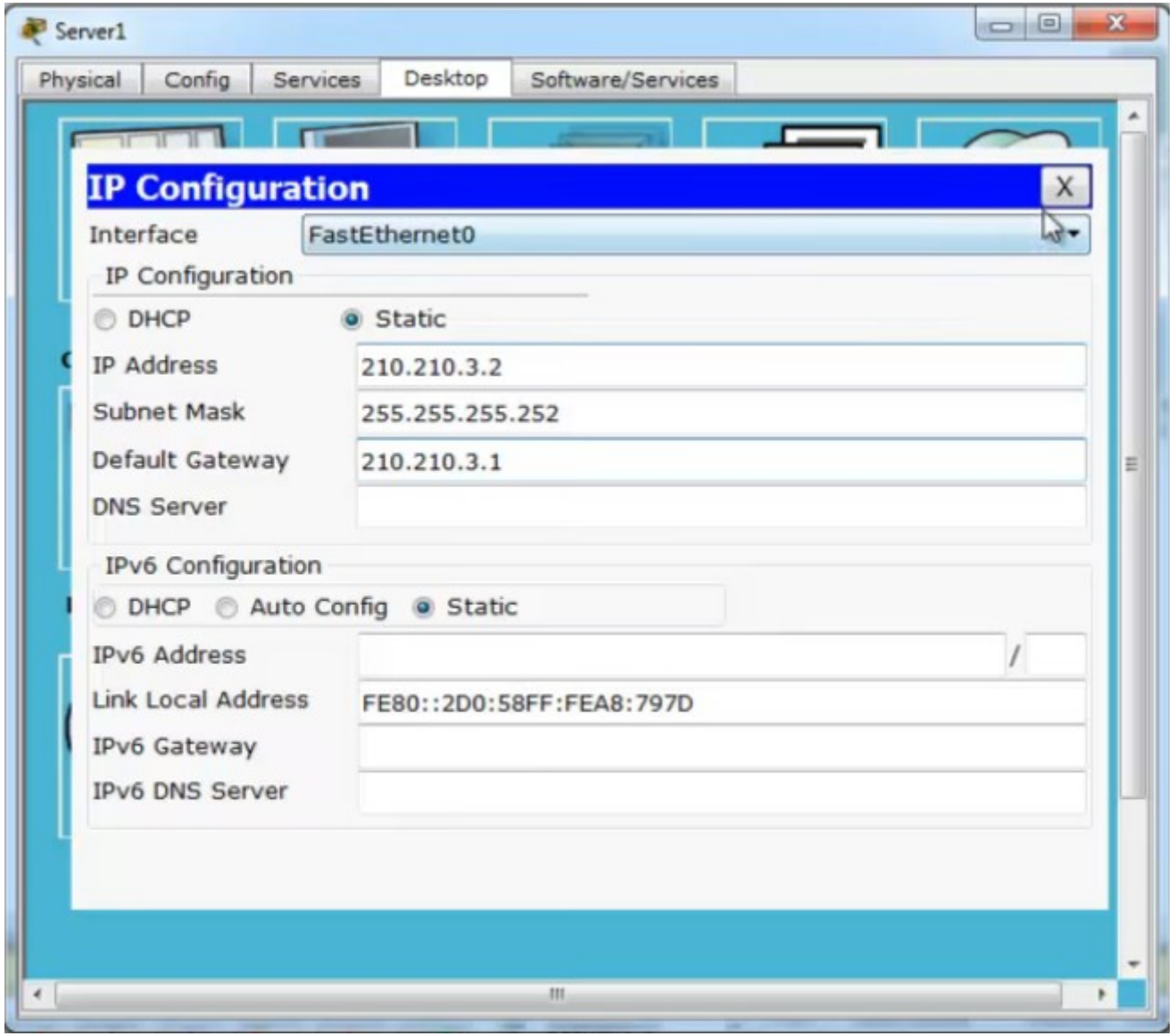
На asa0 настроено инспектирование траффика



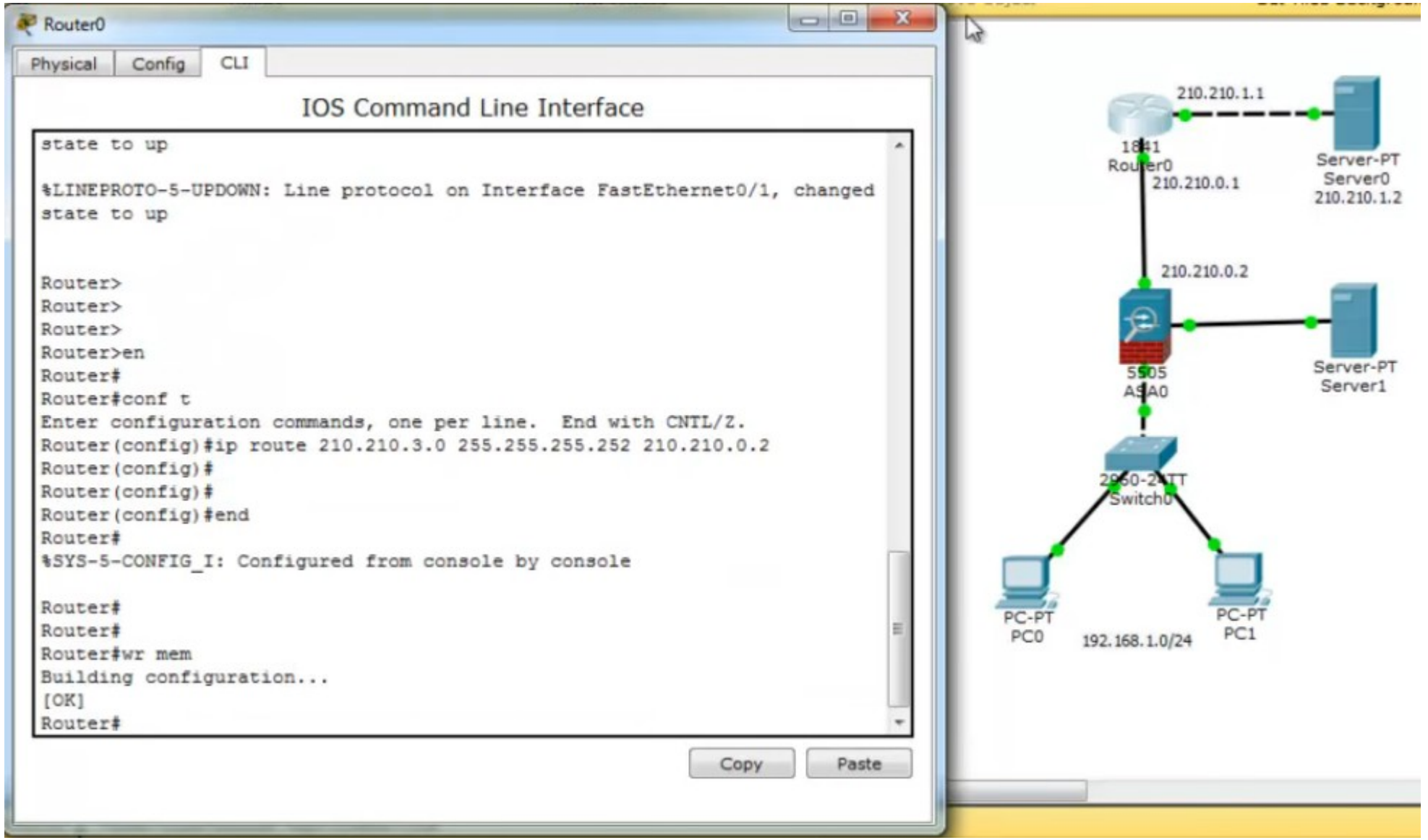
Добавим Server1, который мы будем выделять в DMZ



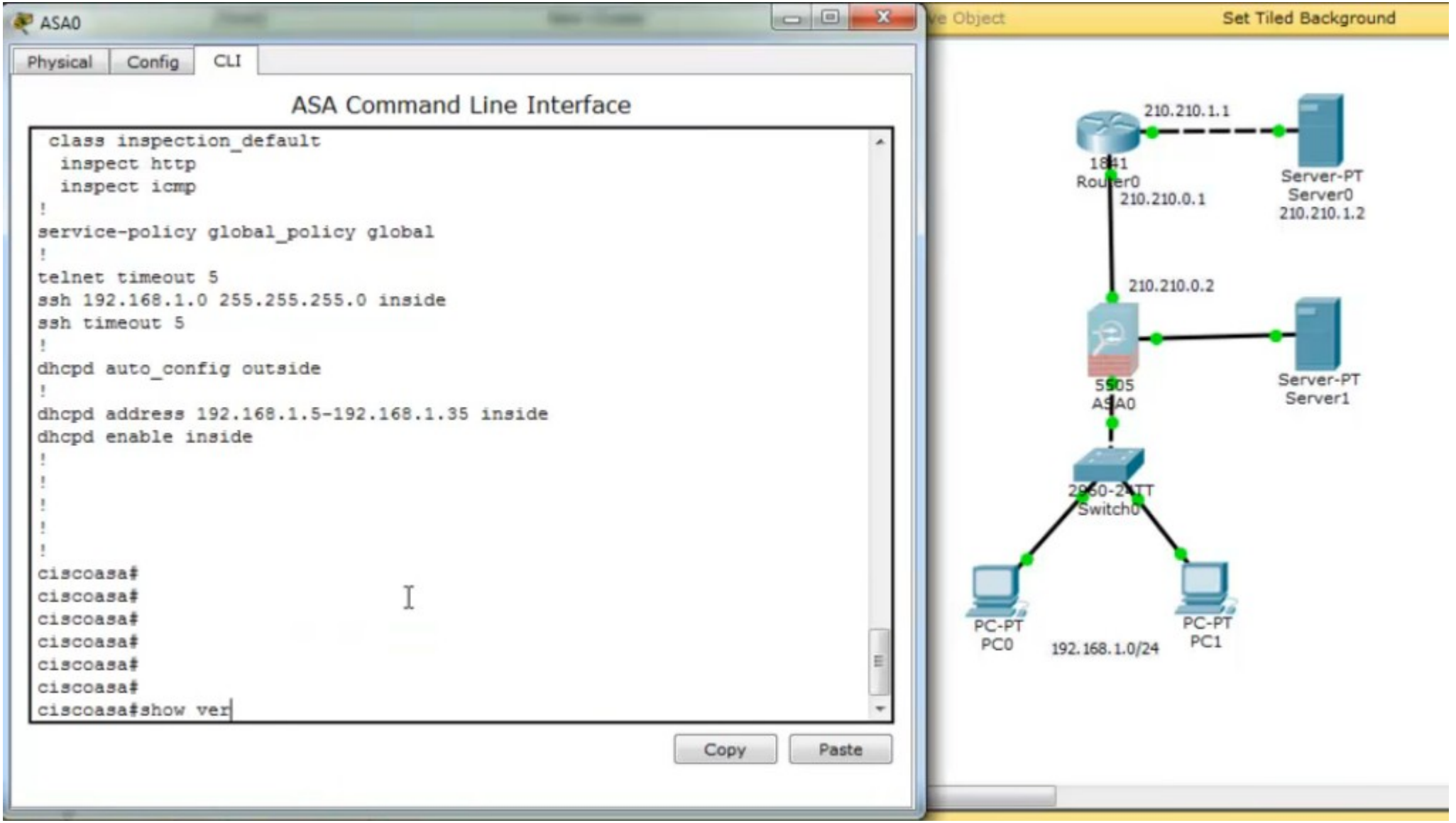
Зададим серверу Server1 статический ip адрес



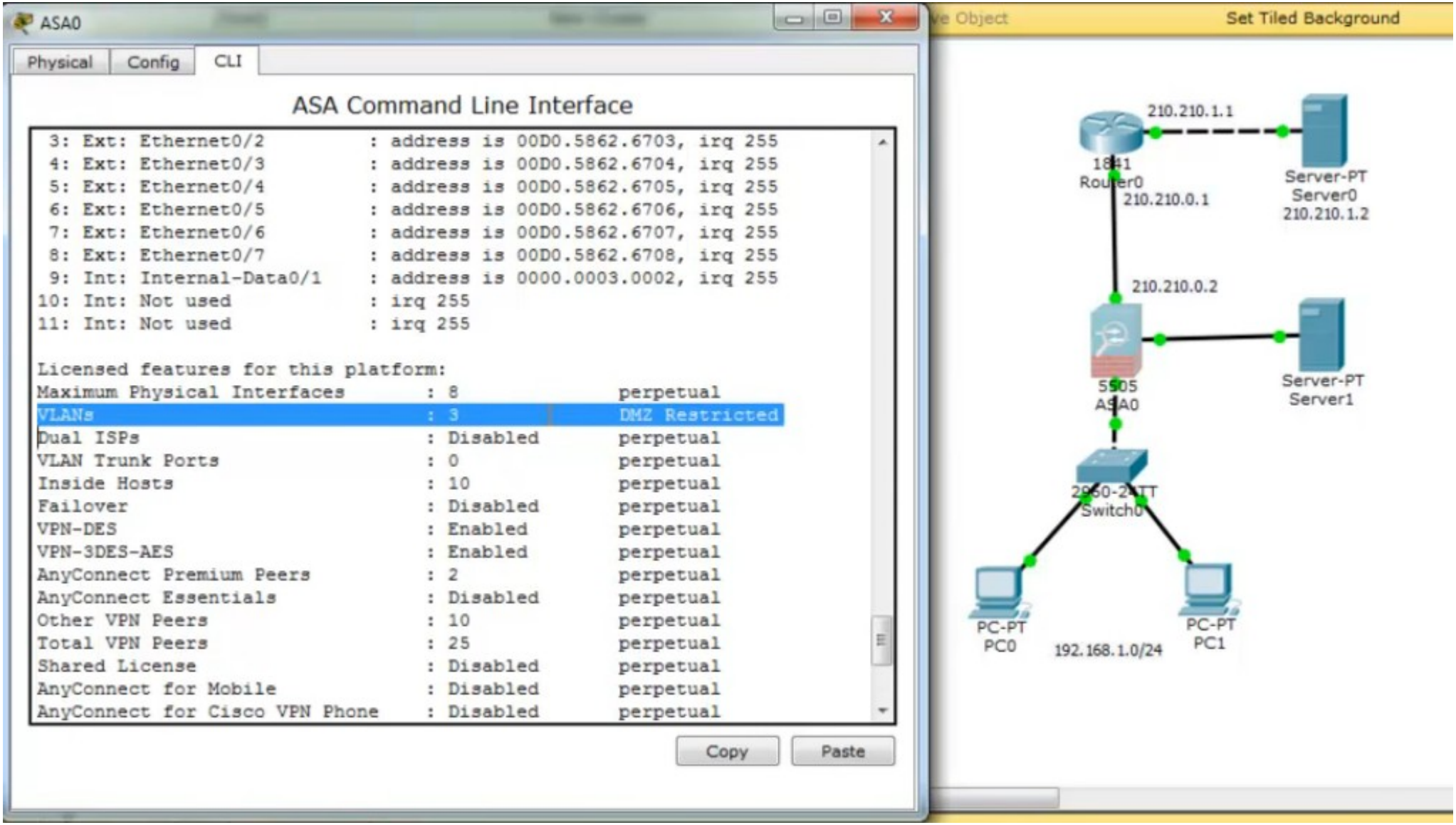
Добавим маршрут к Server1 на Router0



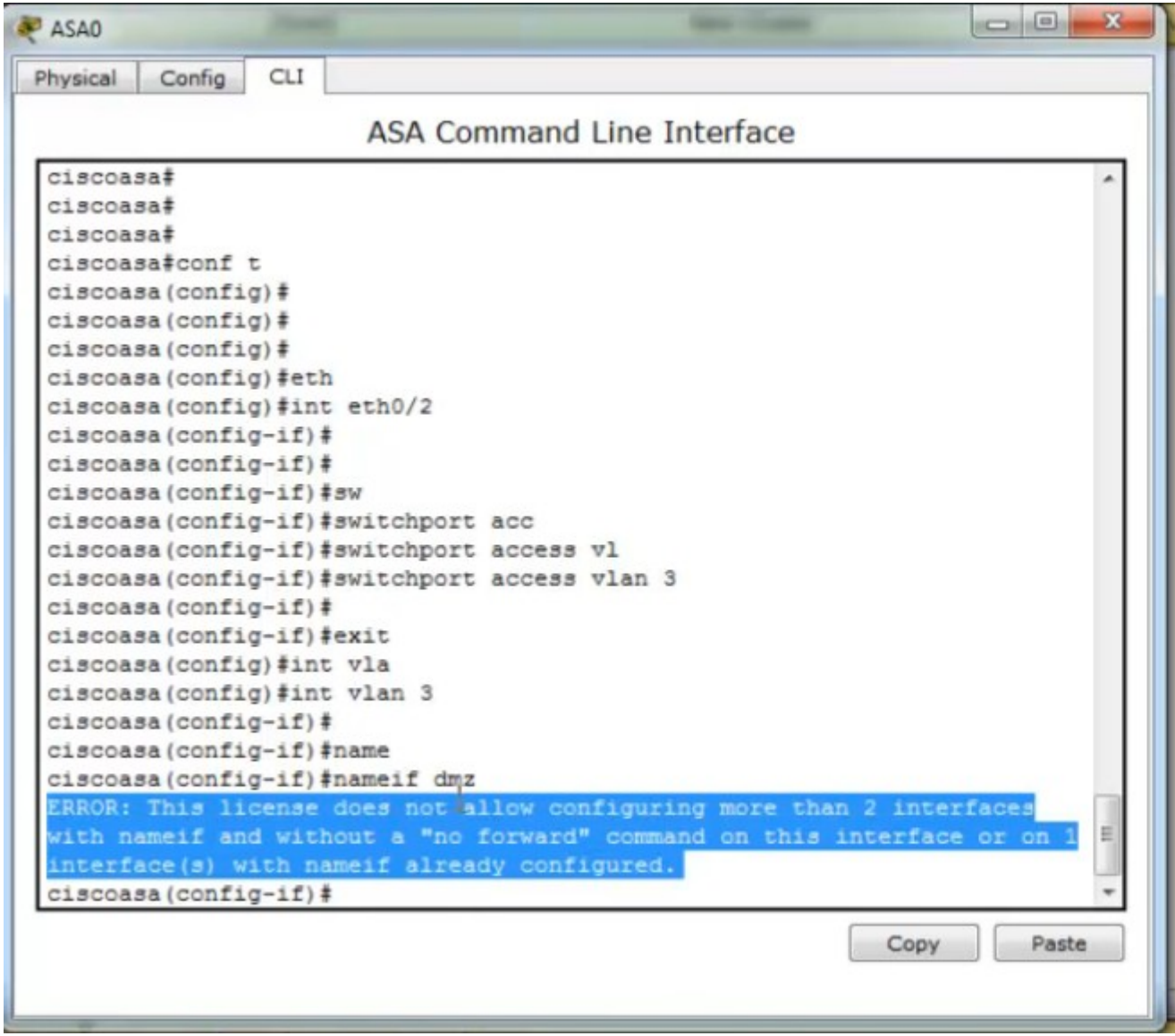
Посмотрим конфигурацию ASA

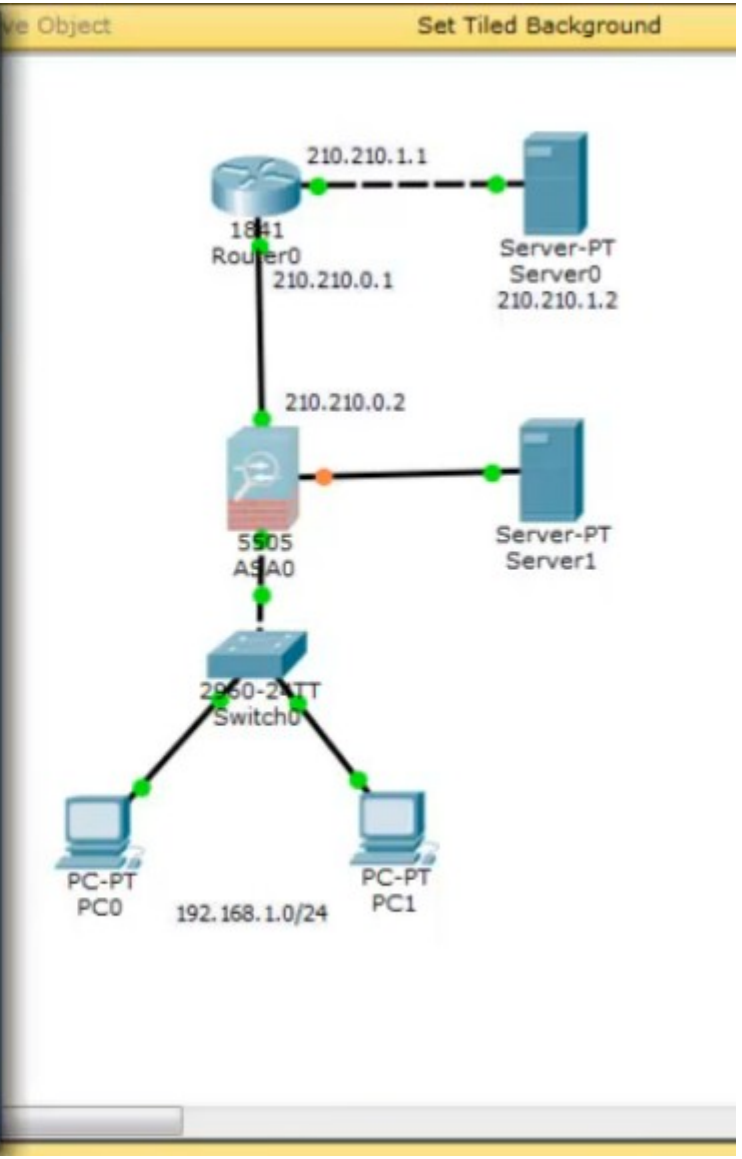


У нас доступно только 3 VLAN и ограниченный DMZ

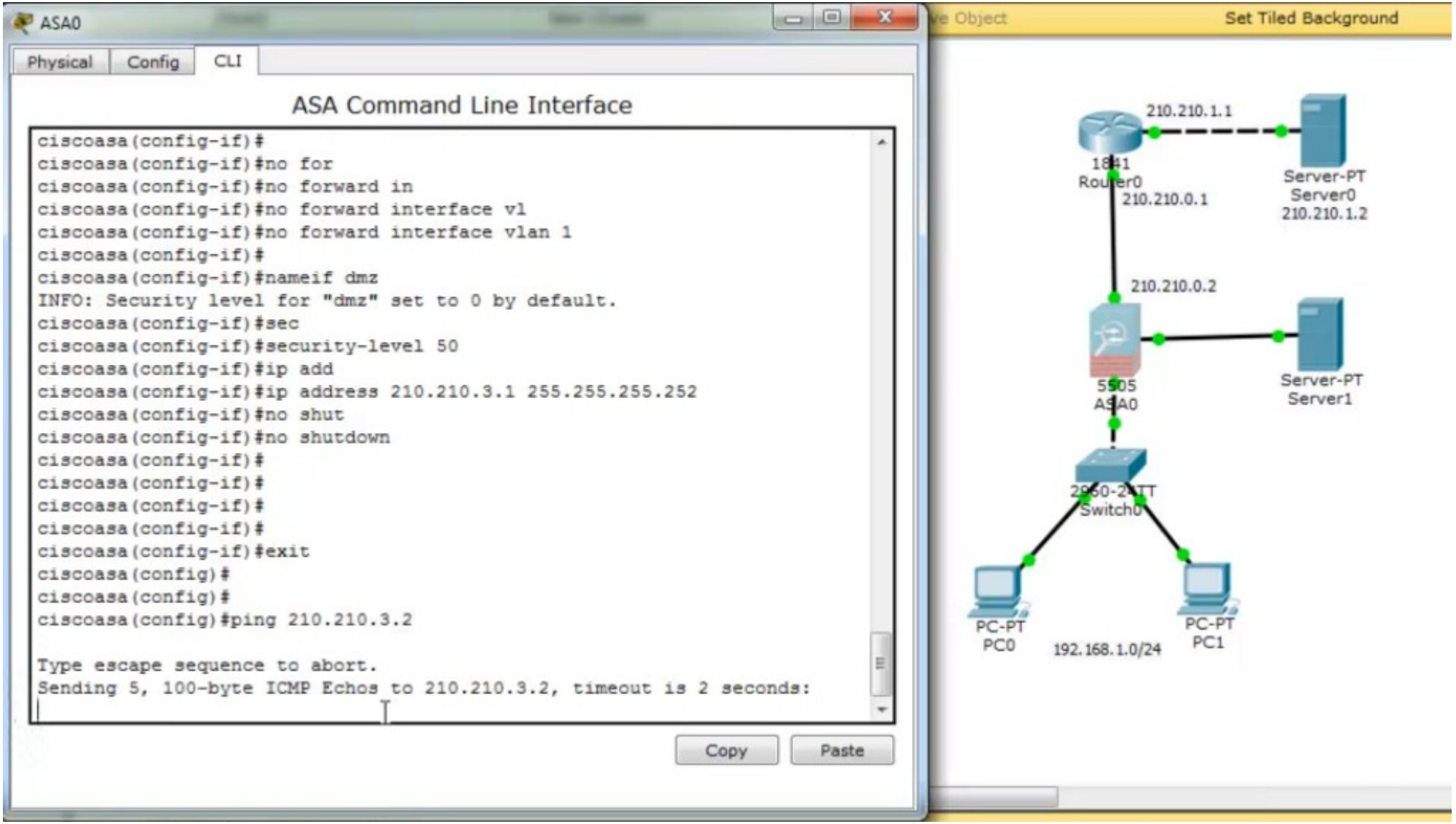


Определим новый VLAN3, и получаем ошибку, что на ASA нельзя использовать больше 2 интерфейсов без no forward из-за ограничений лицензии оборудования

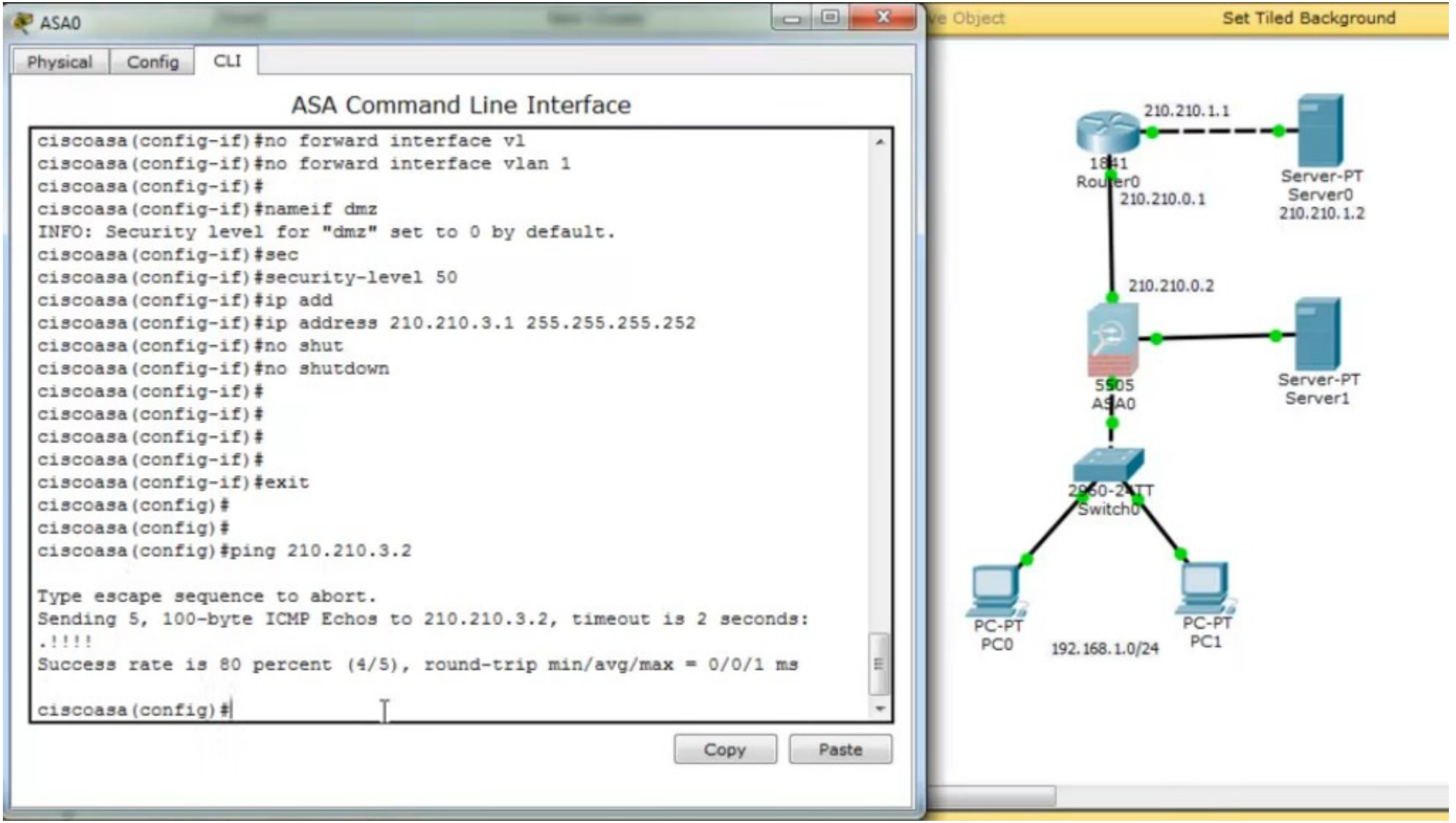




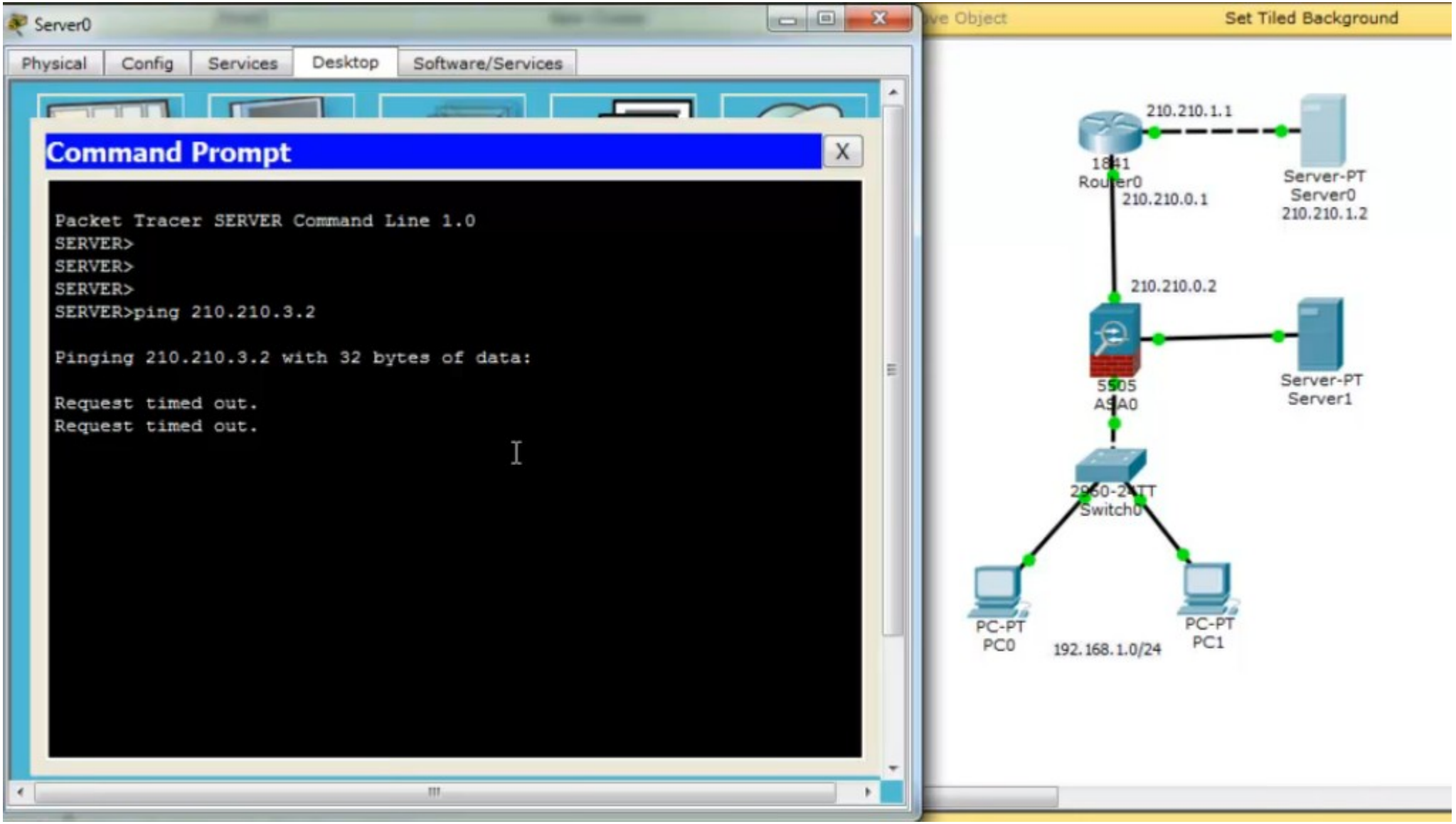
Назначим VLAN1 с указанием «no forward», т. е. с VLAN3 на VLAN1 передача траффика будет невозможна из-за ограничений лицензии



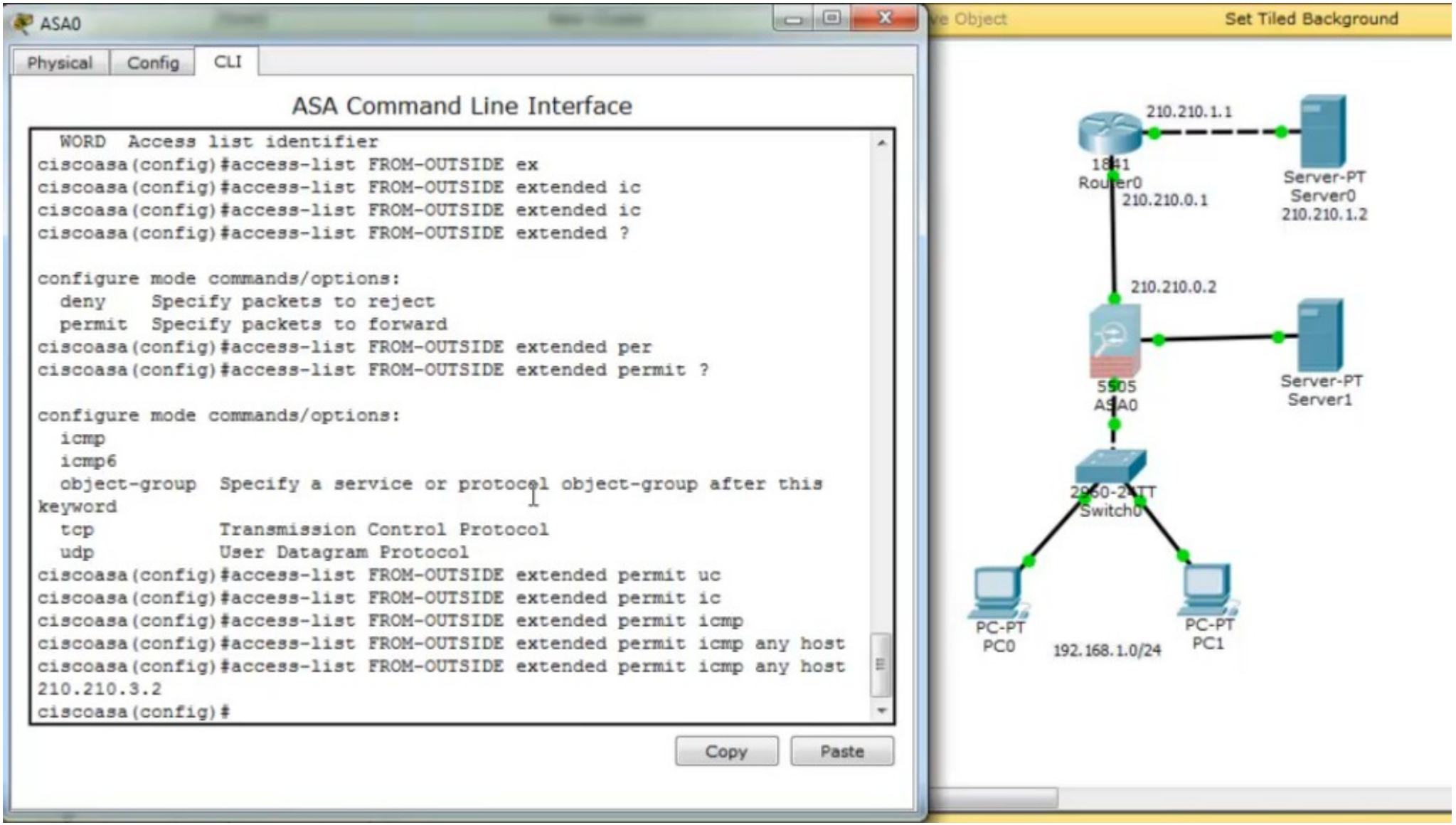
Проверяем доступен ли Server1 с ASA0 - доступен



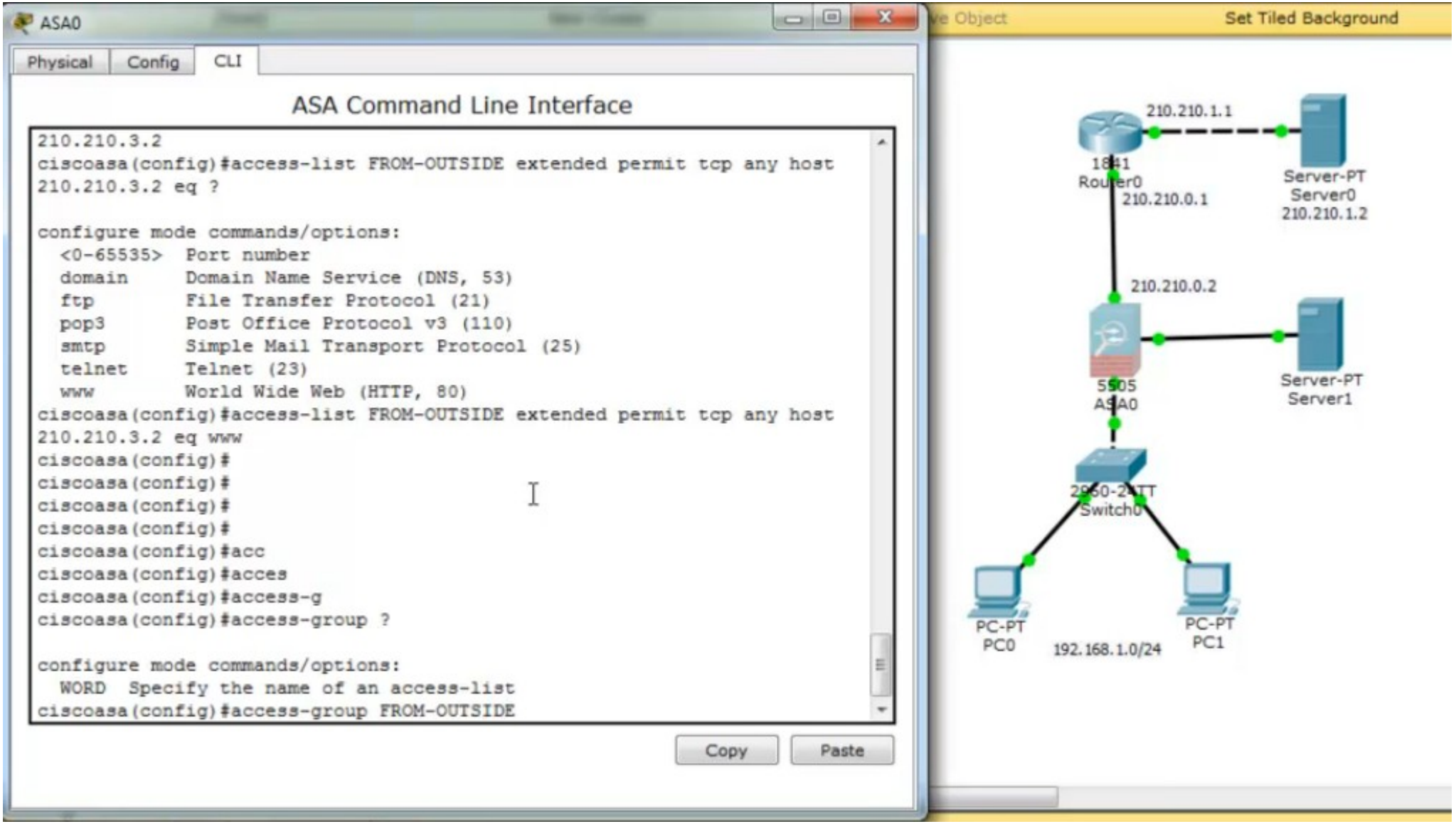
Пробуем пинговать Server1 с Server0 — не проходит



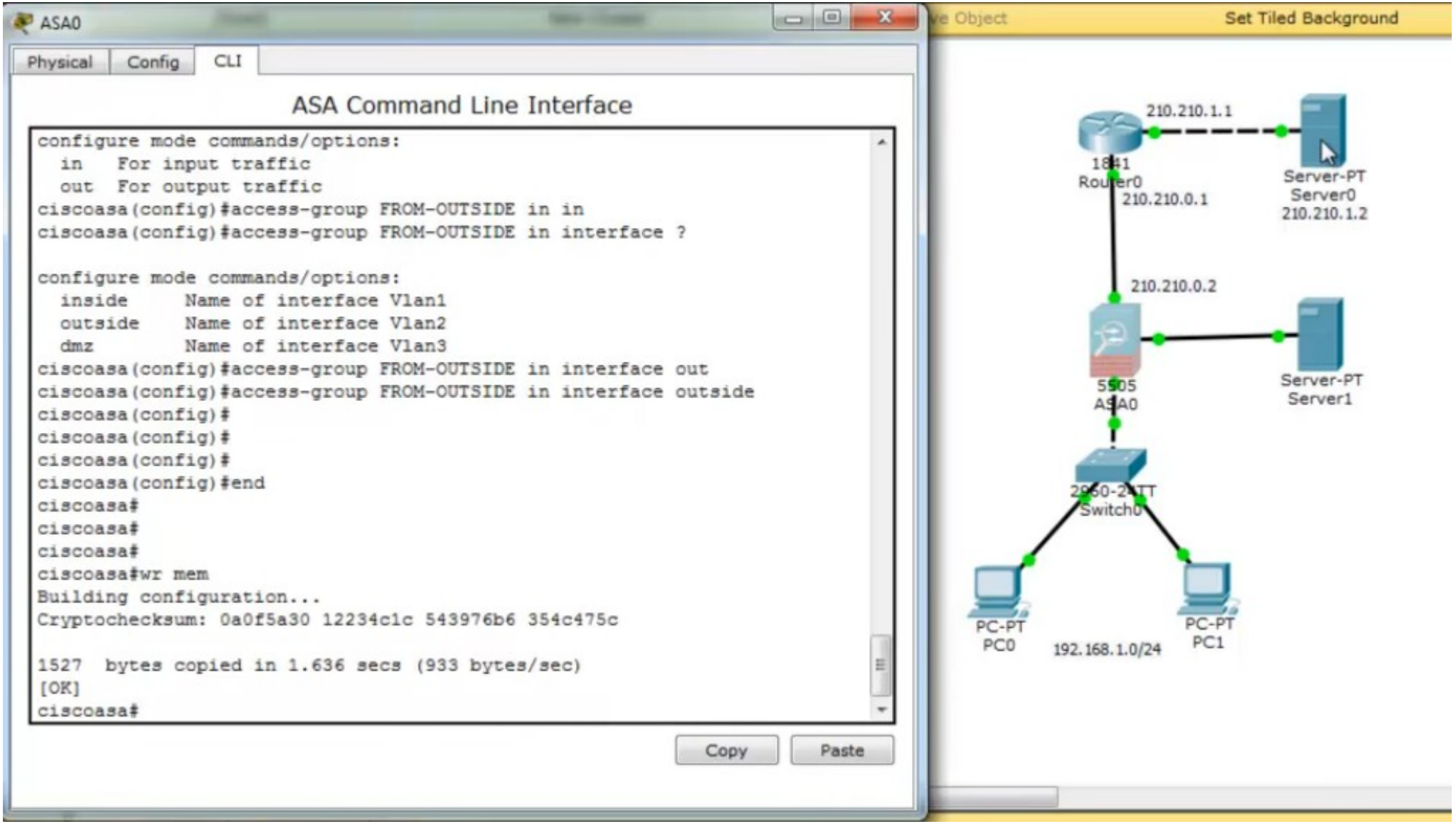
Чтобы устранить проблему — добавим access list на ASA0



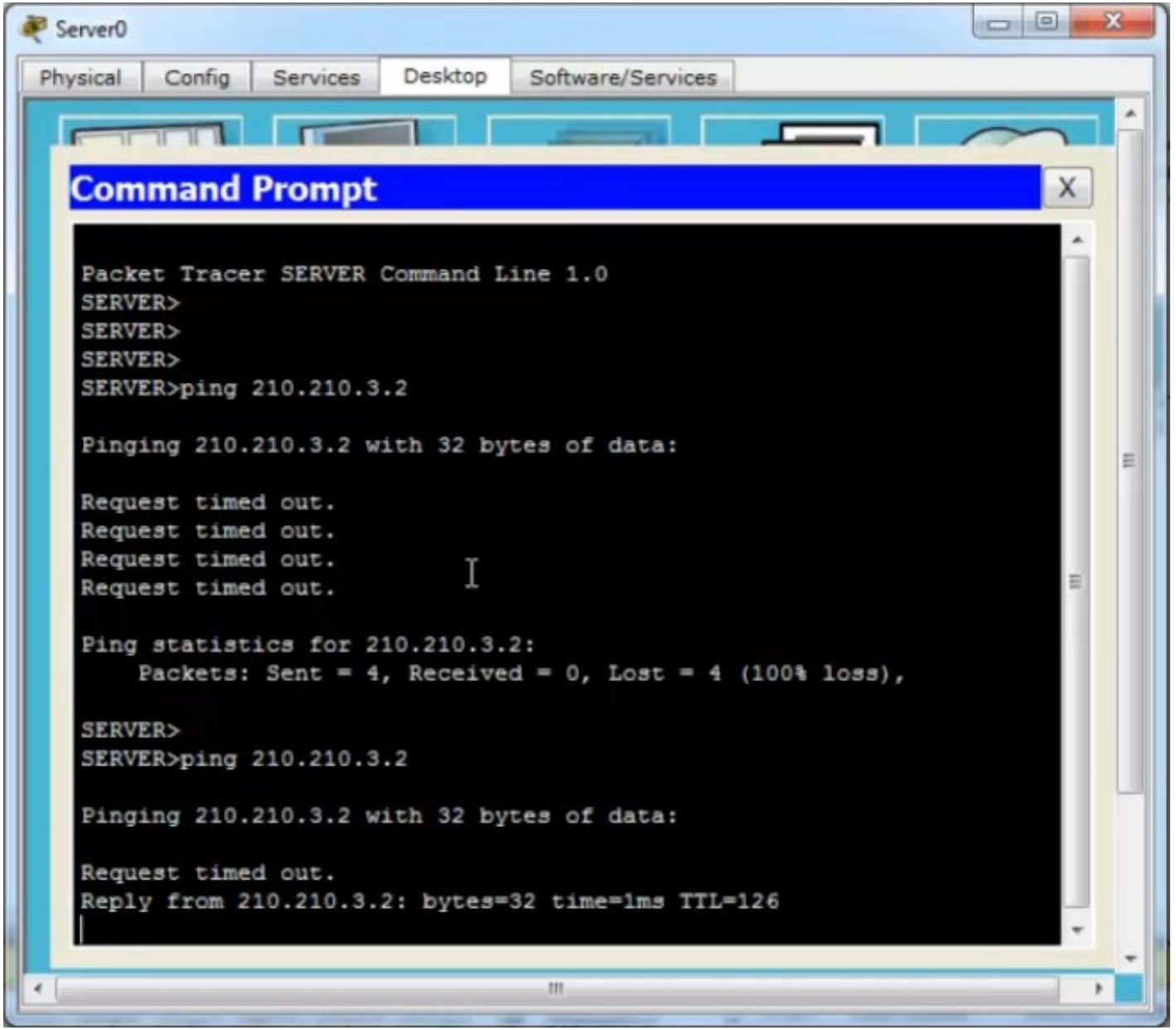
Добавим правило для www траффика



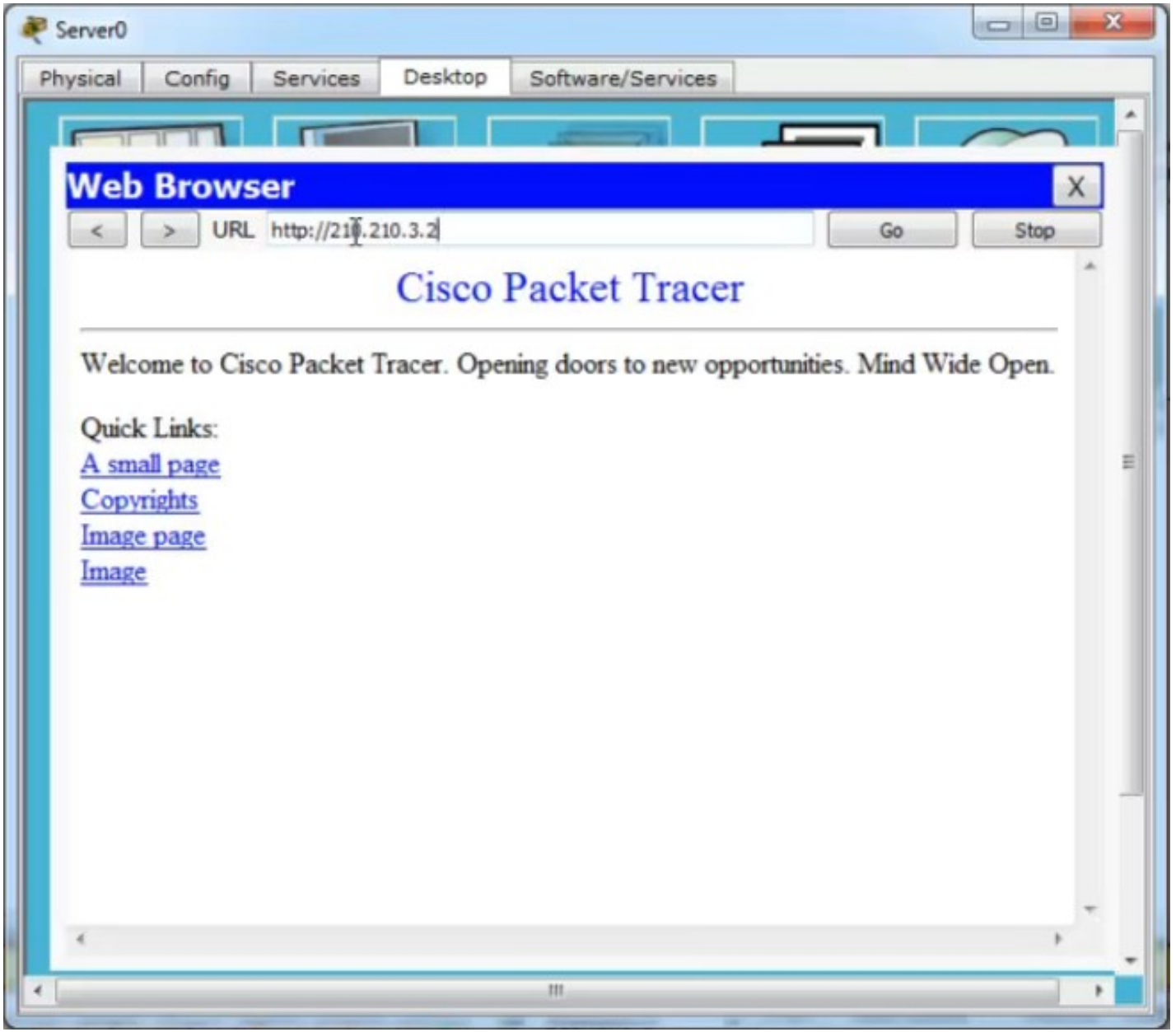
Добавим access group



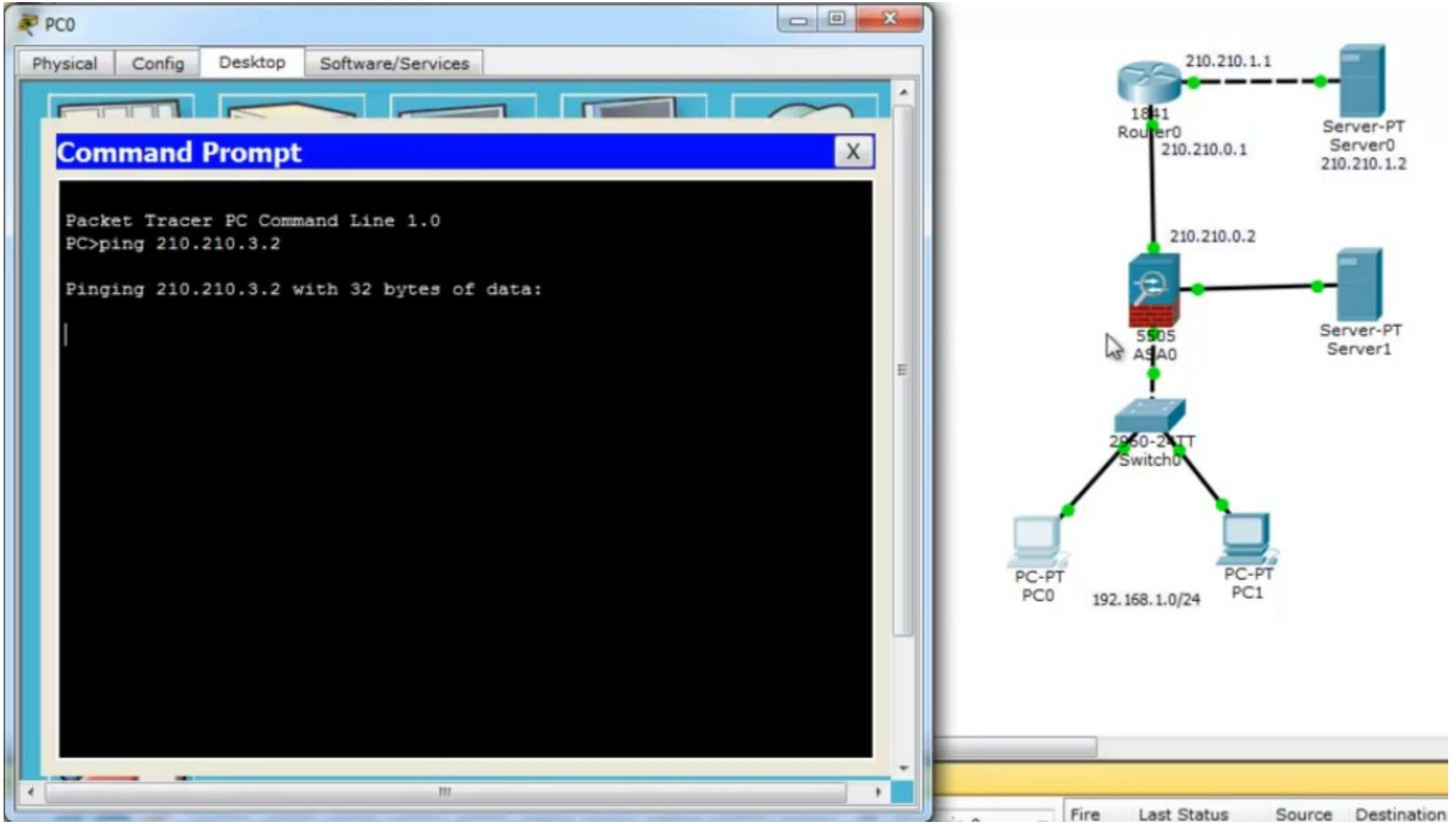
Снова проверим доступ с Server0 на Server1 — работает



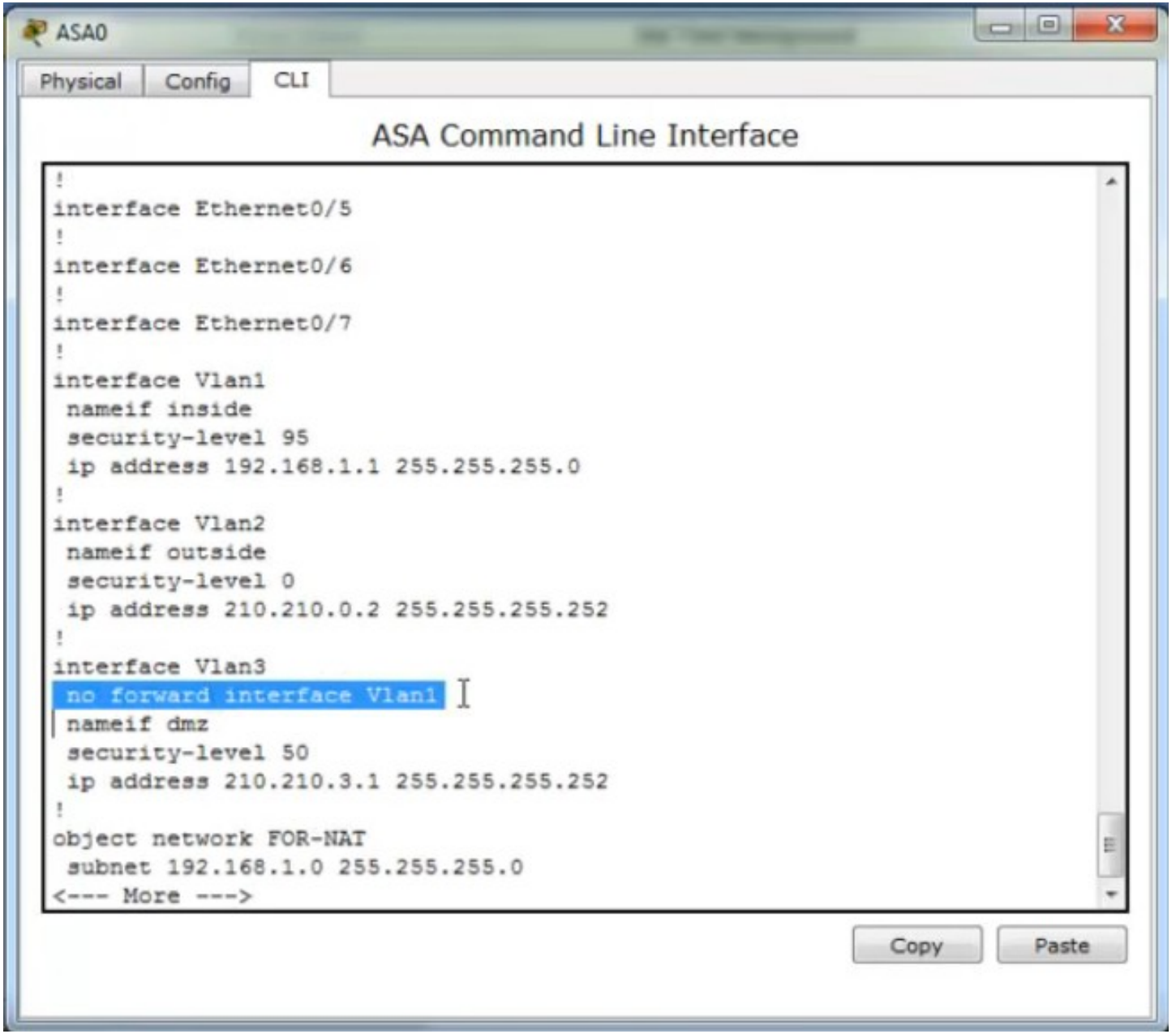
Снова проверим доступность веб-сервера на Server1 — работает



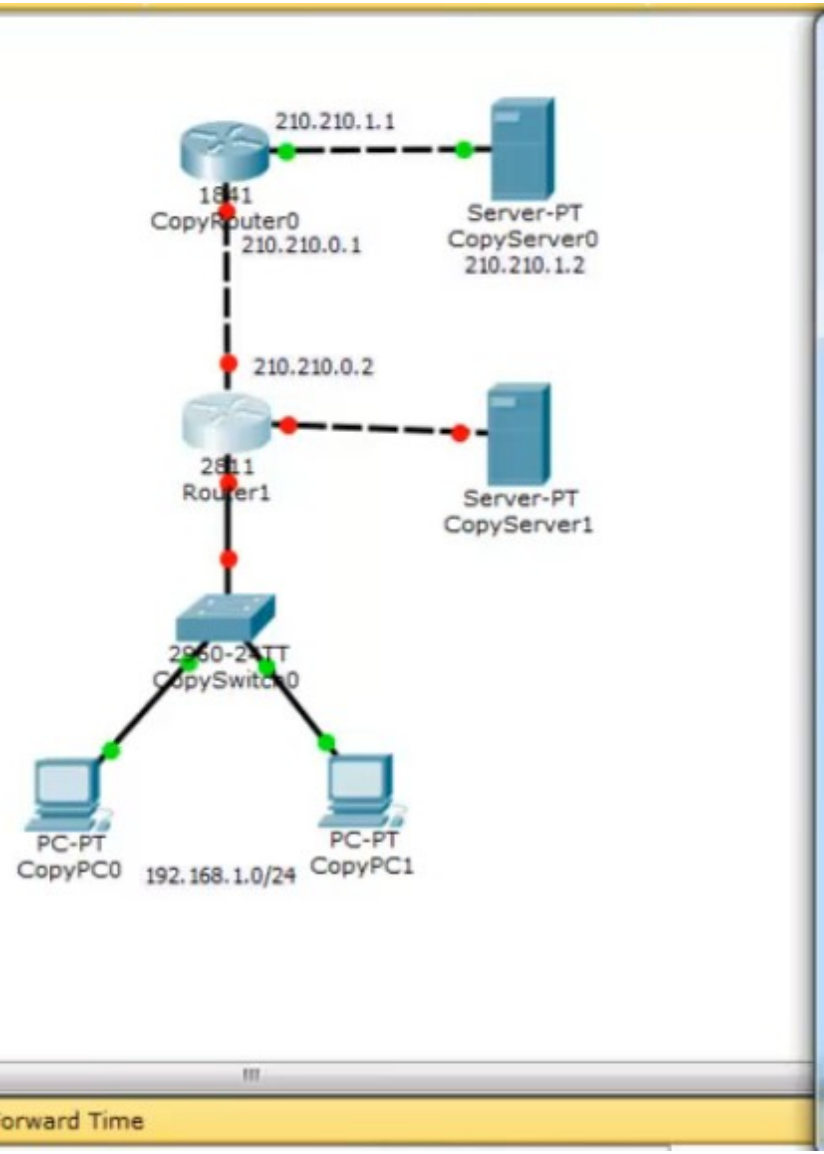
При этом доступ на Server1 с PC0 — не работает

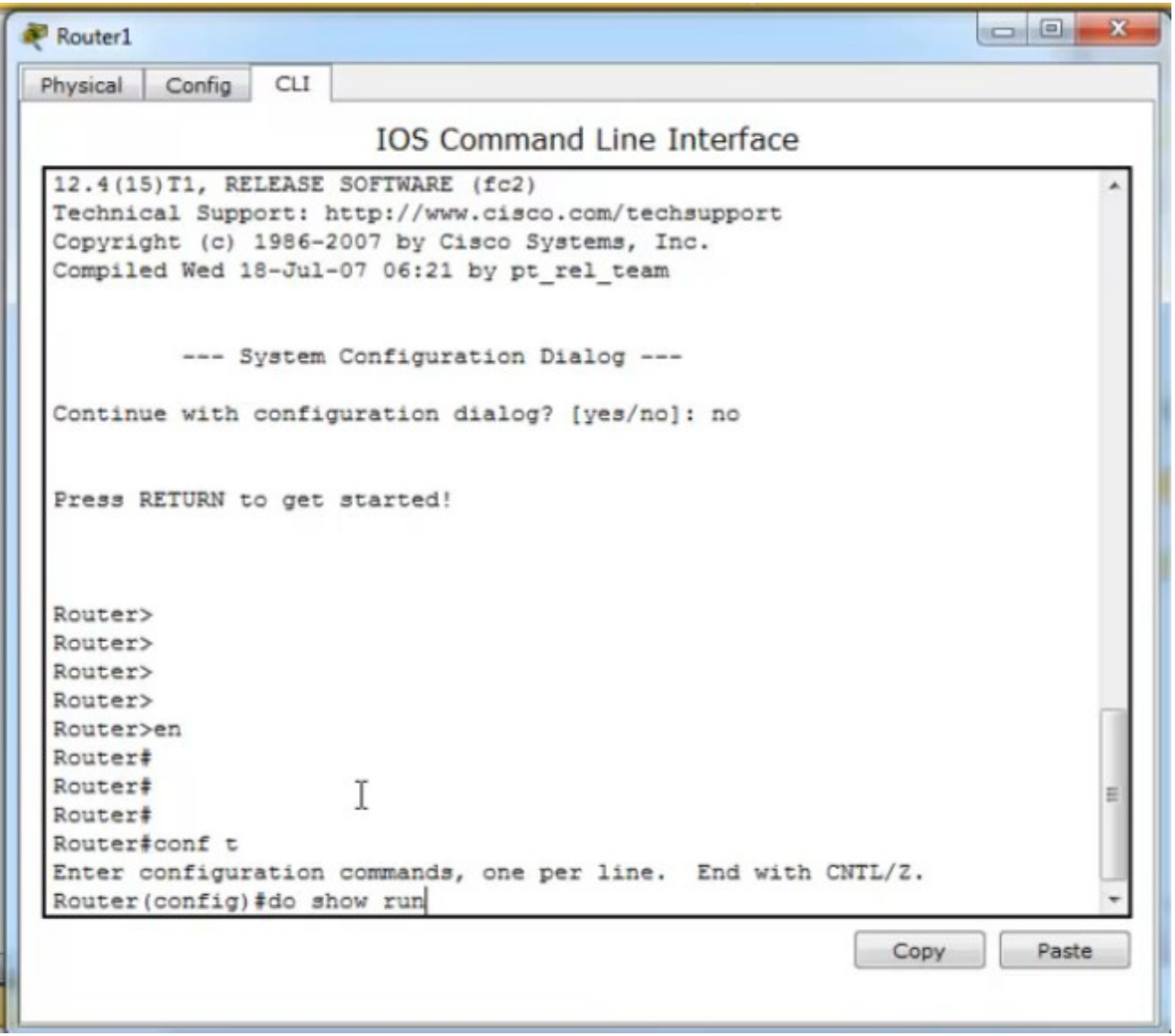


не работает из-за no forward между VLAN3 и VLAN1

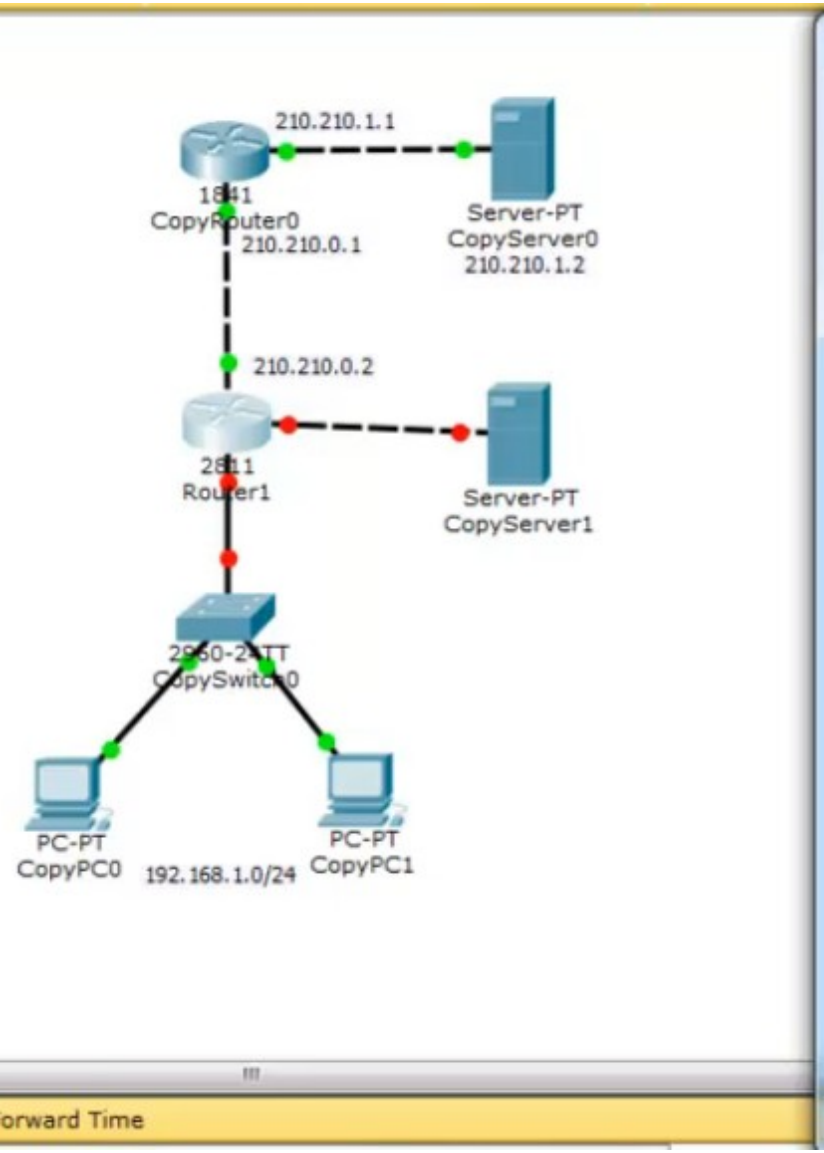


Скопируем сеть зажав Ctrl и заменим ASA на Router 2811





На новом Router1 запустим интерфейсы и настроим NAT



Router1

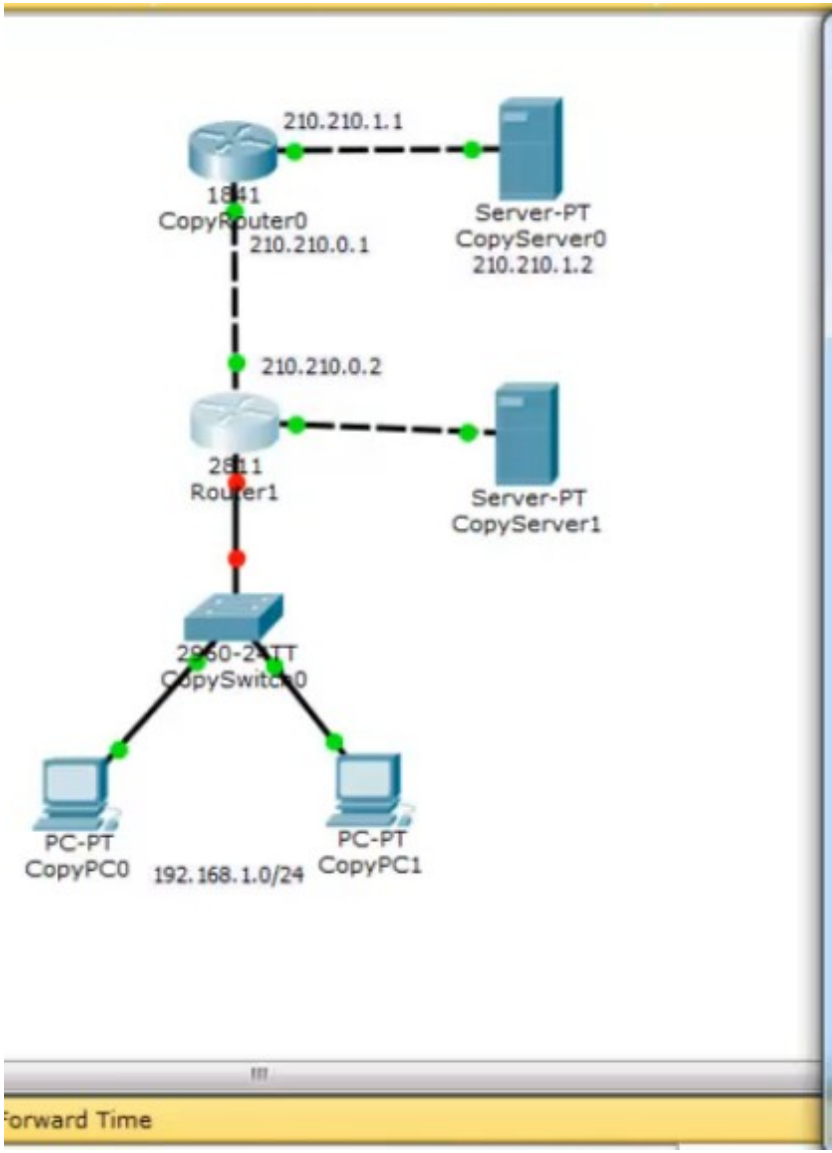
Physical | Config | CLI

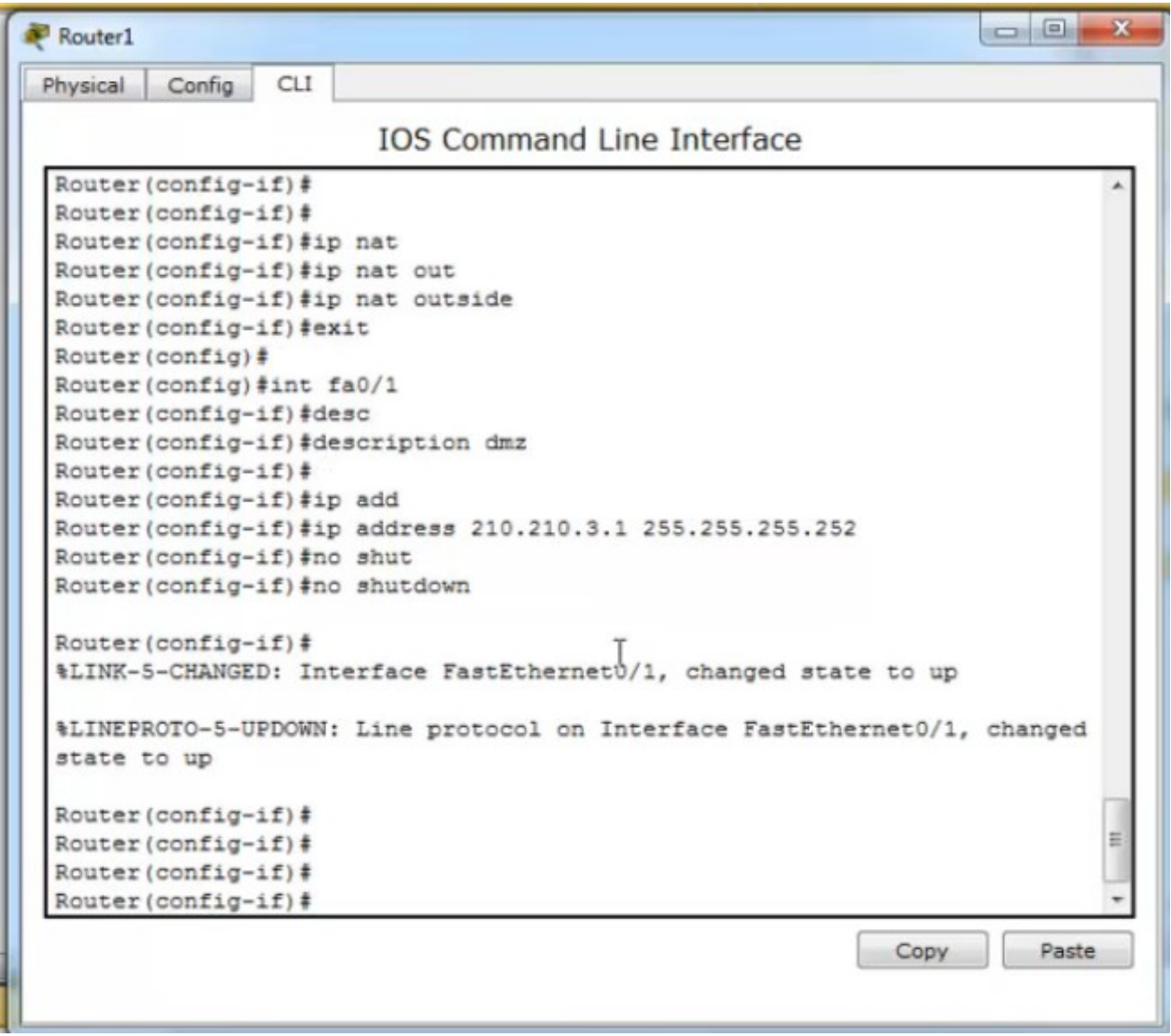
IOS Command Line Interface

```
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)#
```

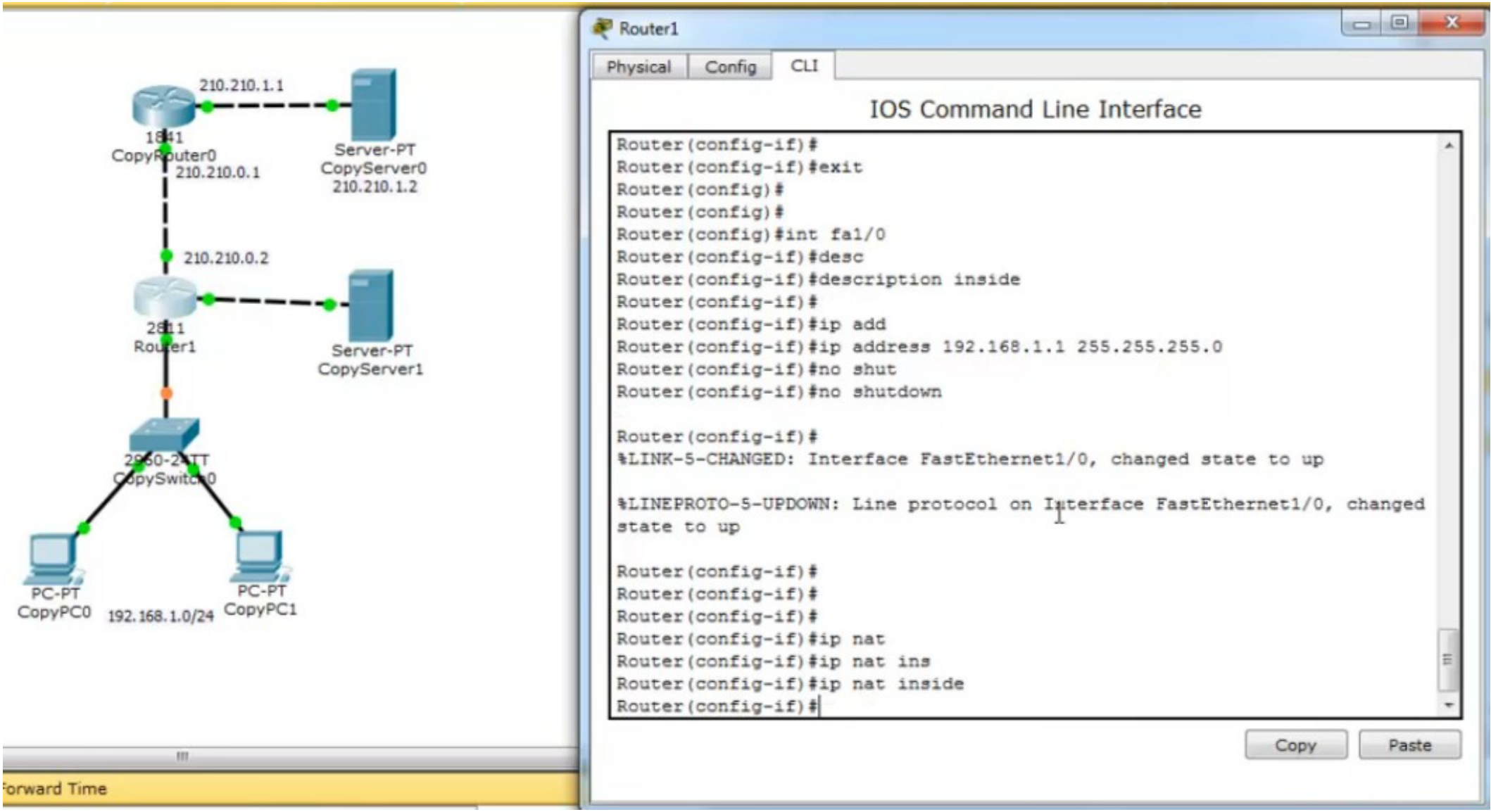
Copy | Paste

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

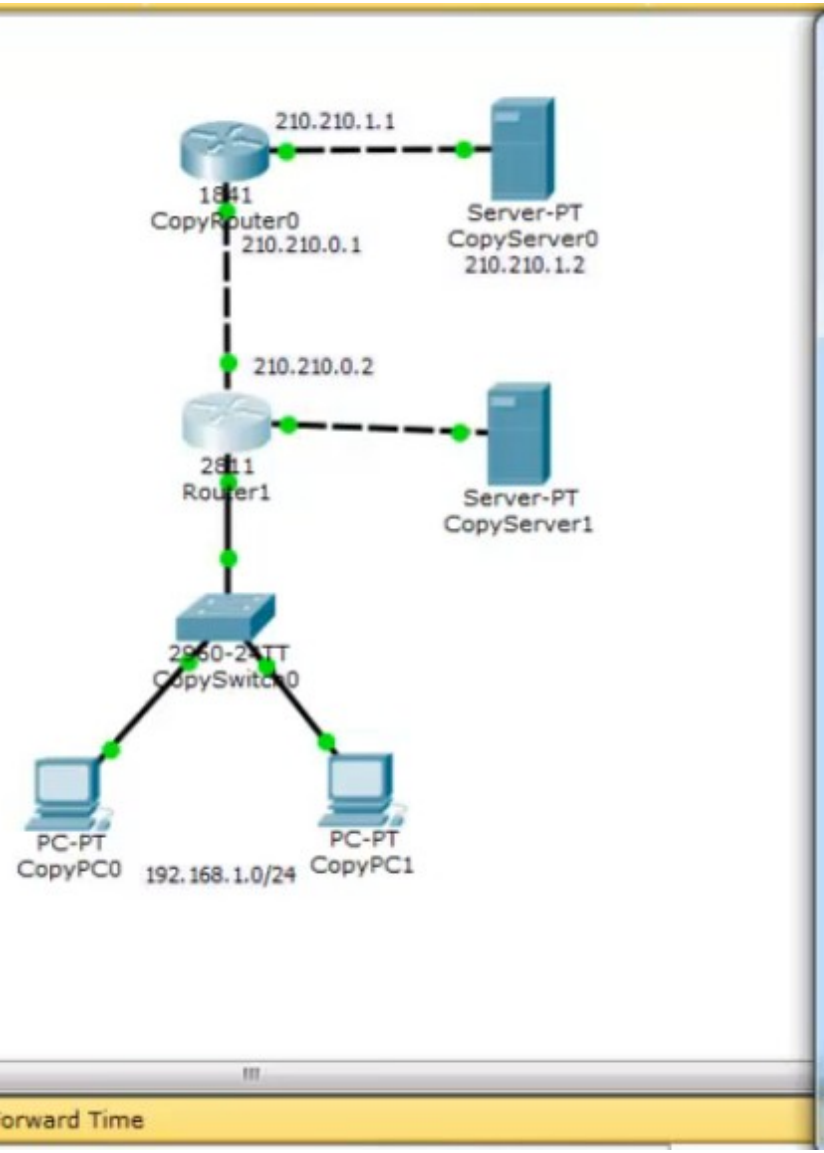


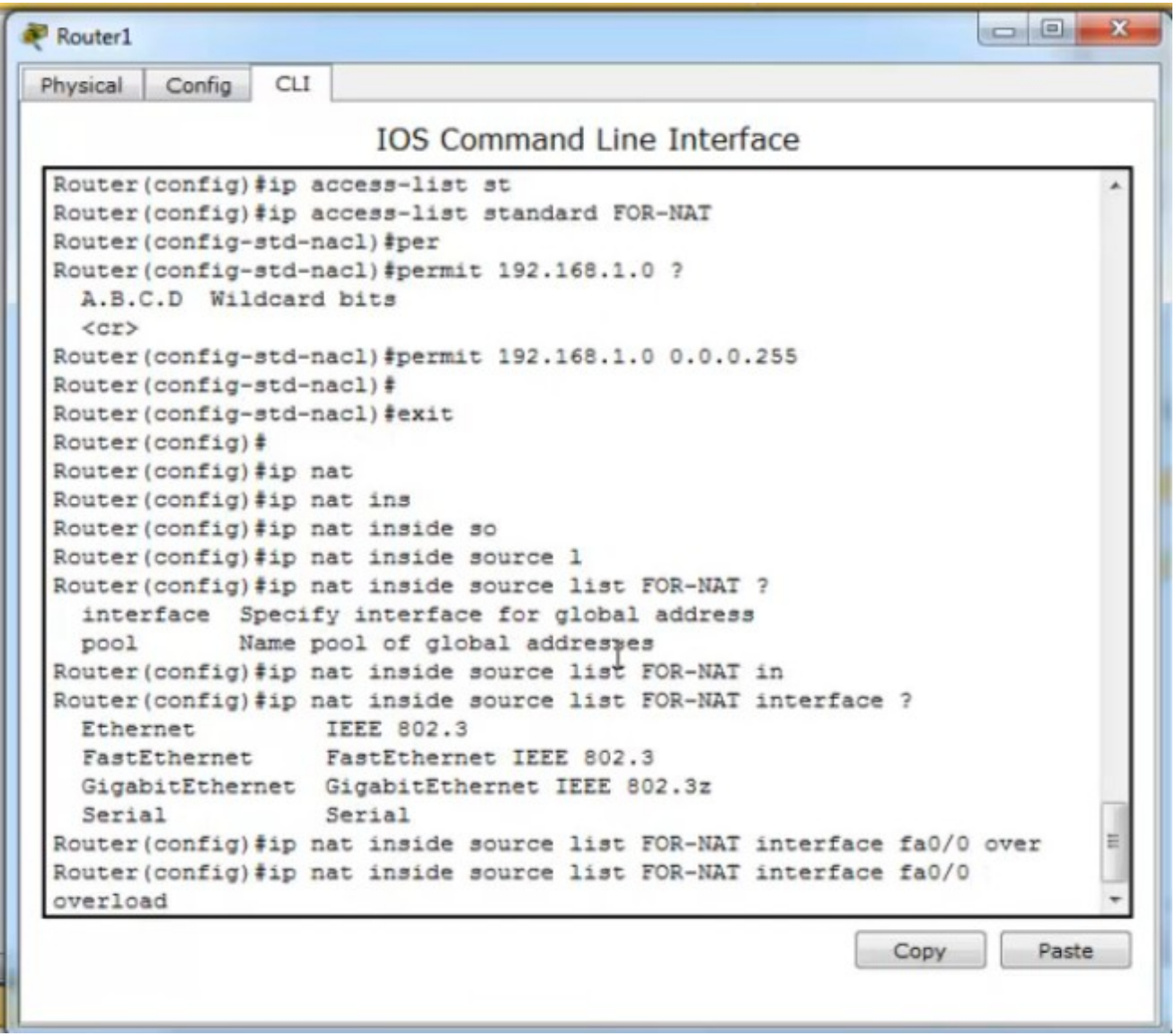


Зададим ip адрес на fa1/0, внутреннем

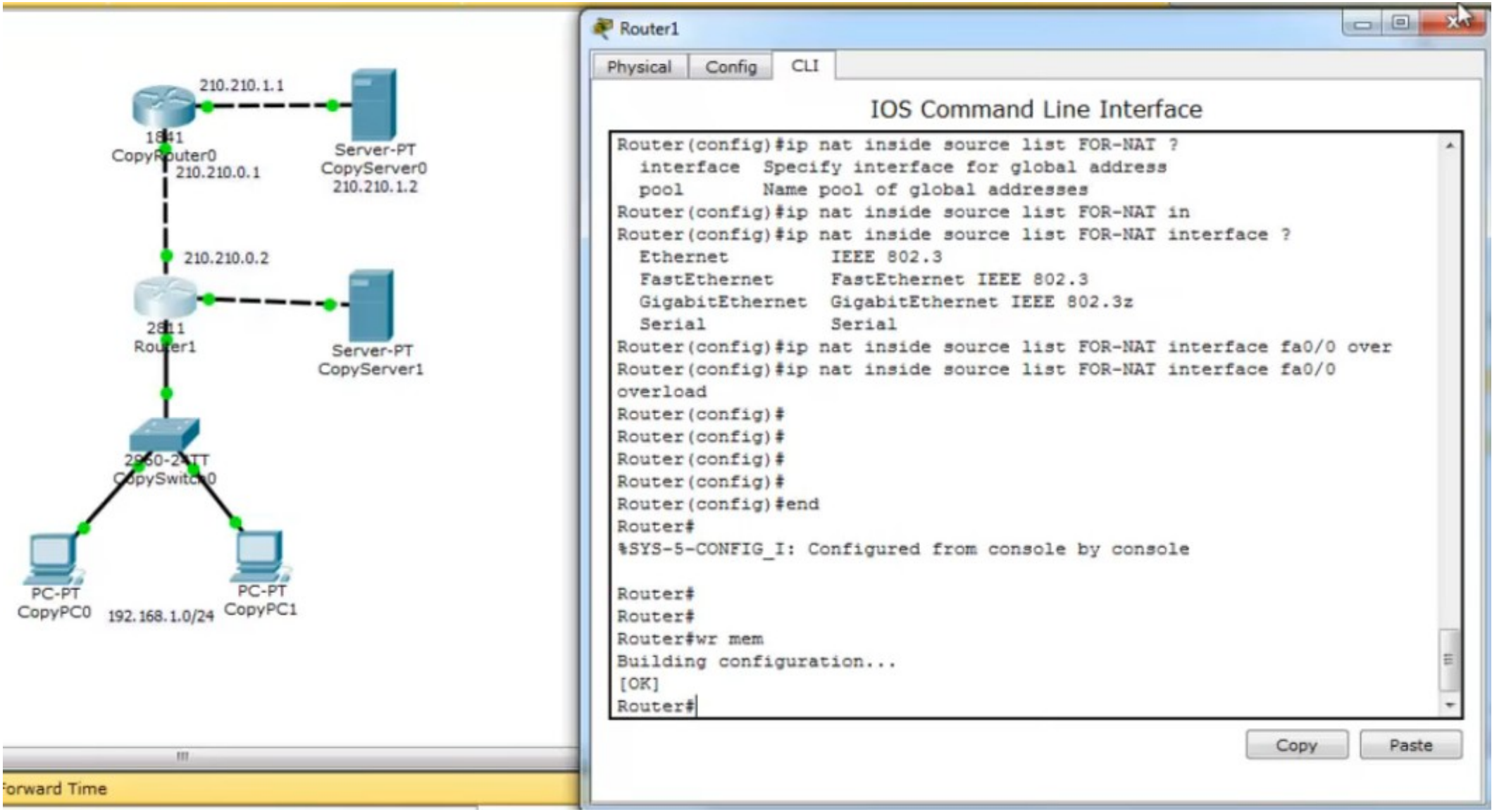


Создадим access-list

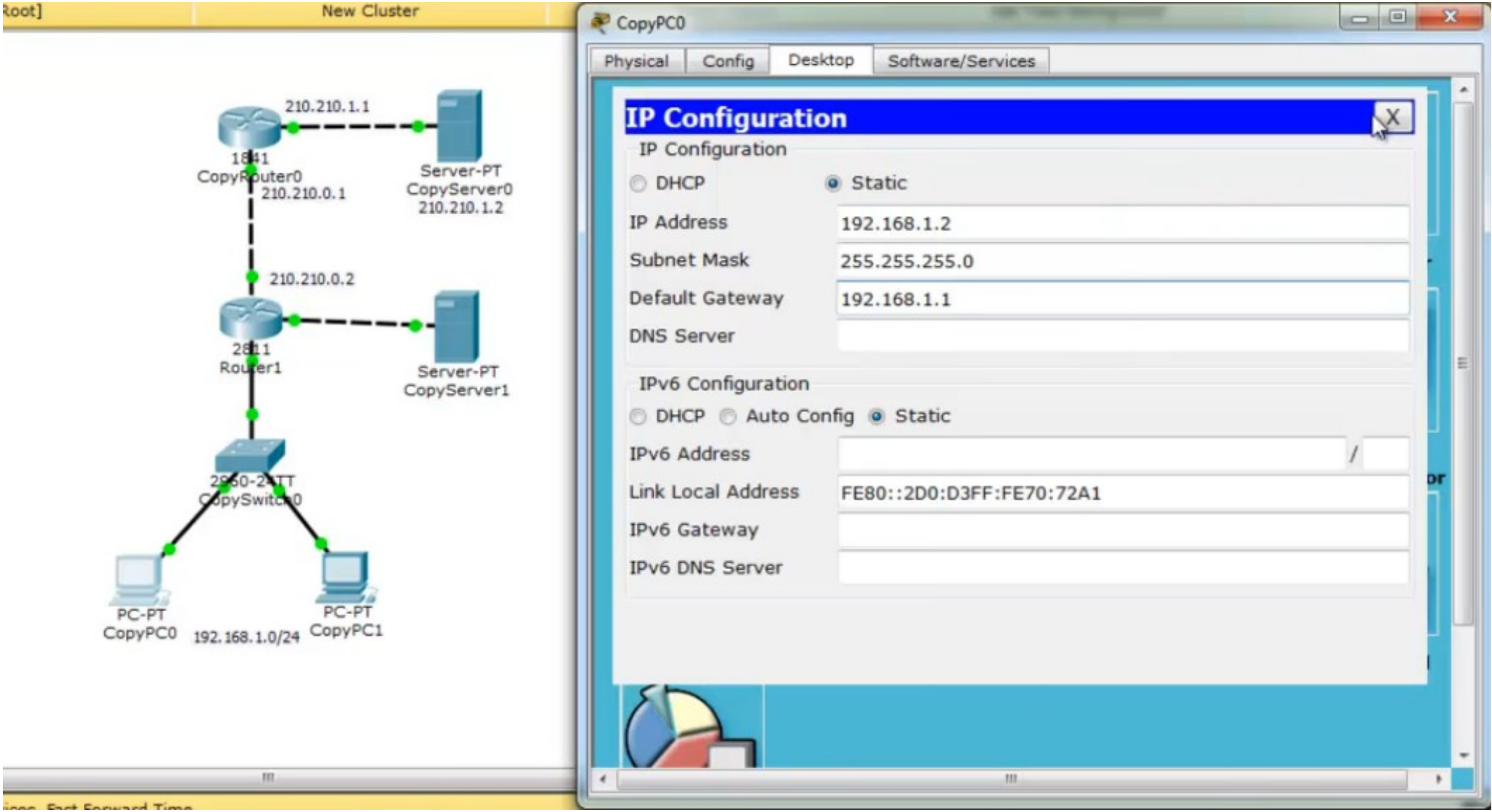




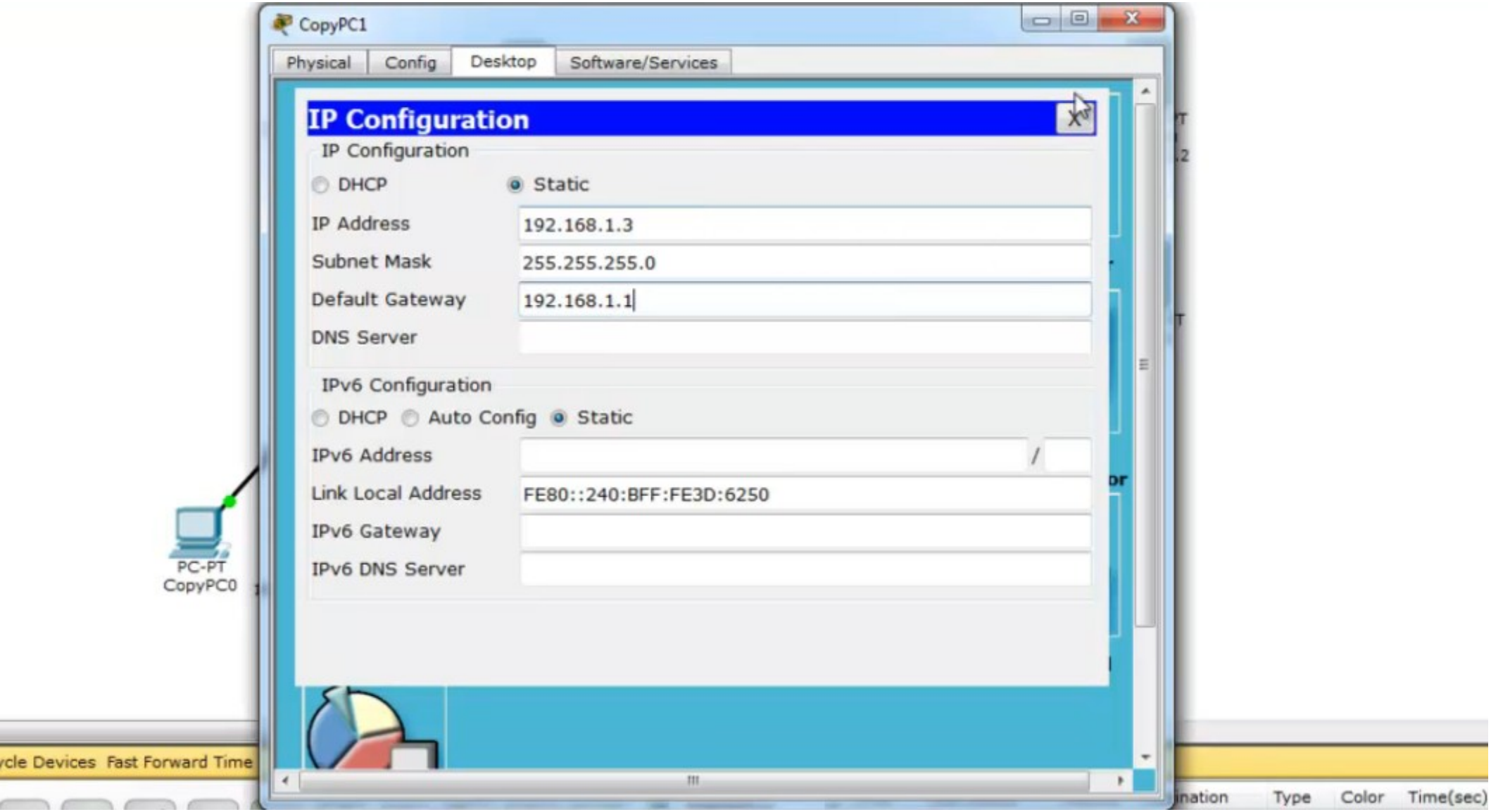
Сохраняем настройки



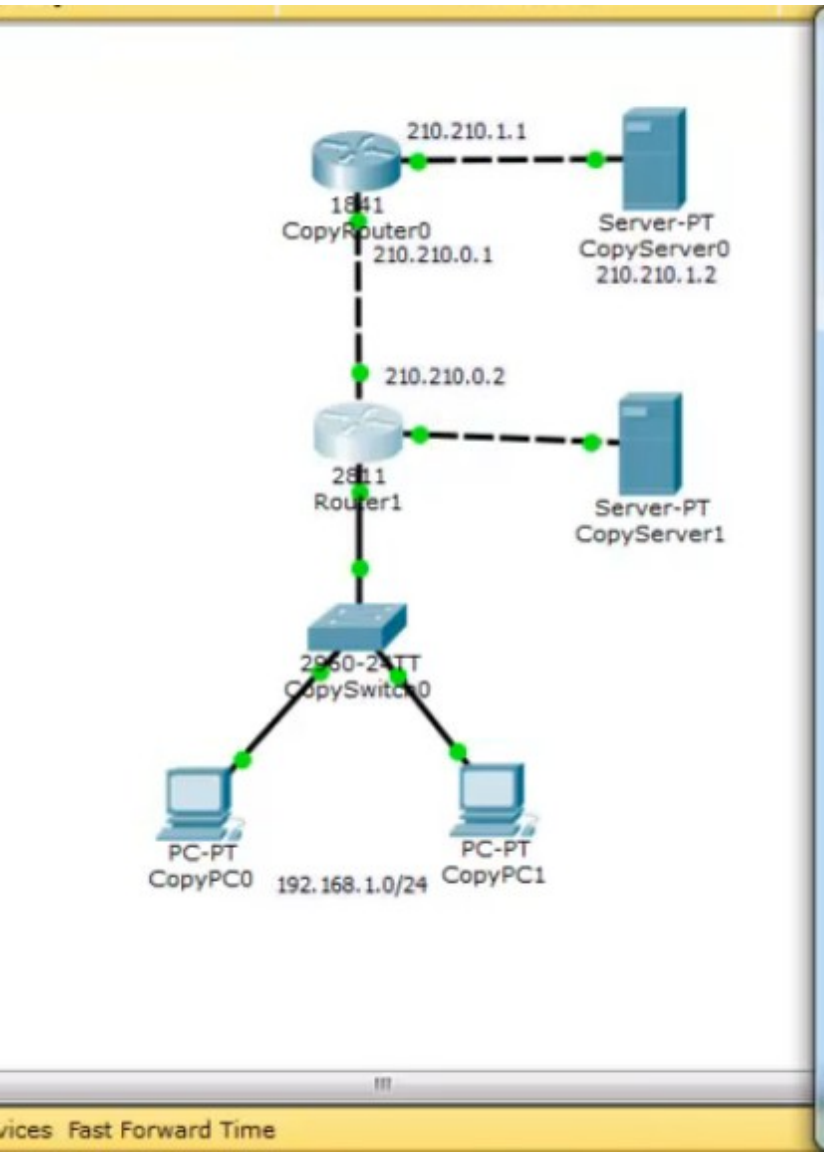
Зададим ip на PC0, т. к. DHCP сервера у нас нет



Зададим ip на PC1



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



Router1

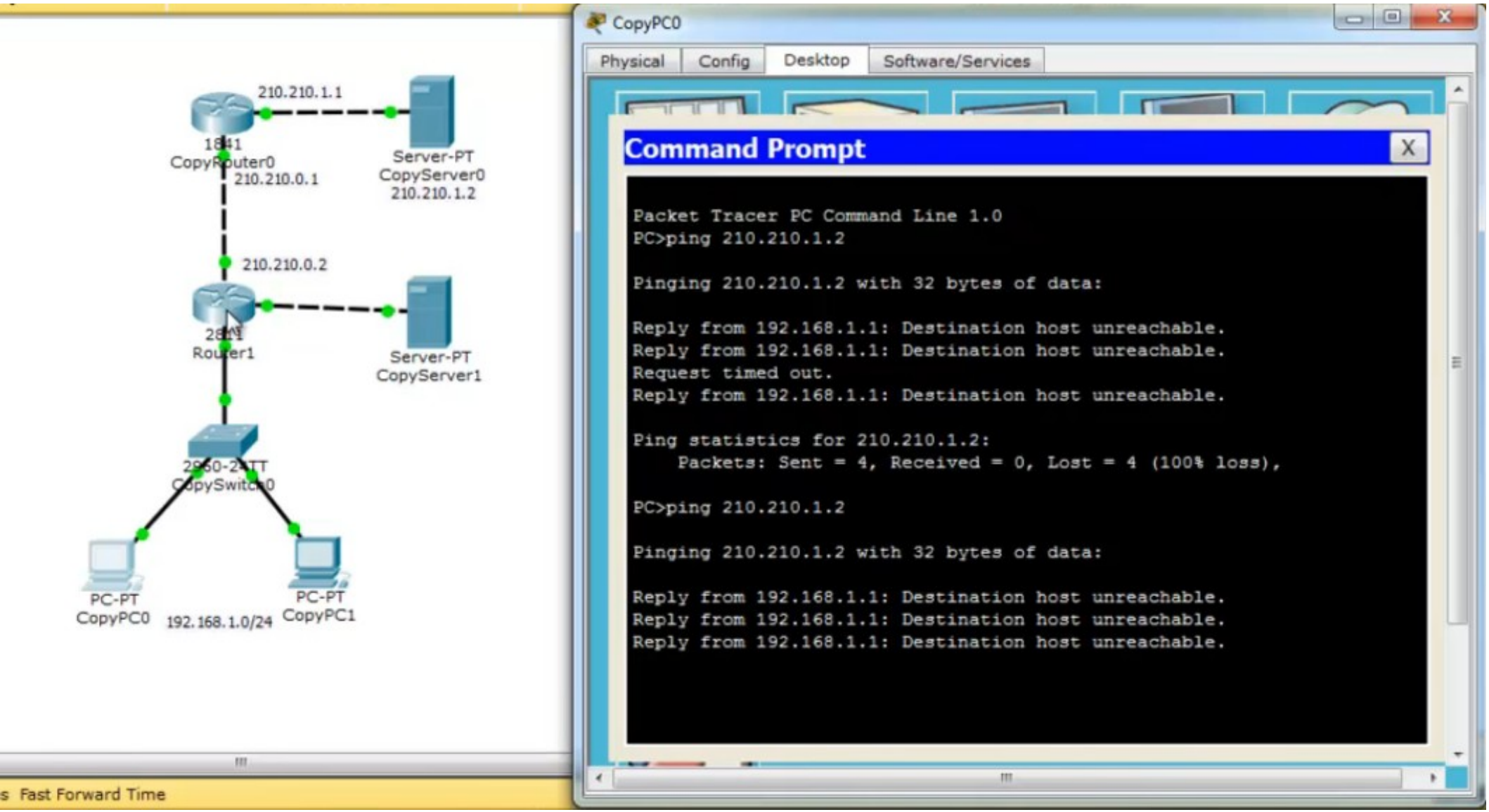
Physical | Config | CLI

IOS Command Line Interface

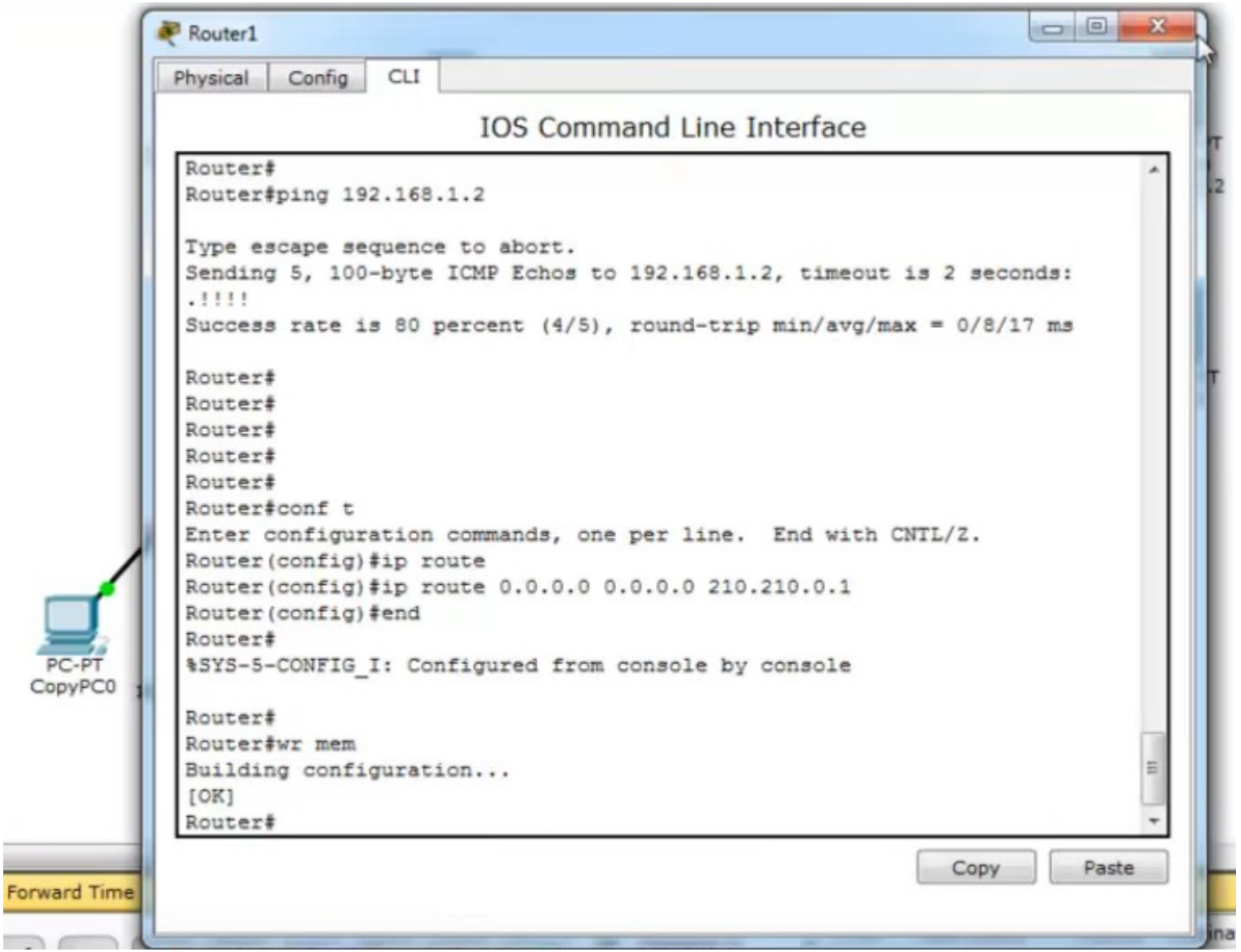
```
Router#
Router#
Router#ping 210.210.0.1

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#
```

Copy | Paste

Проверяем доступ с PC0 к Server1 — не проходит



Чтобы исправить добавляем маршрут на Router1



Теперь с PC0 доступны Server0, Server1