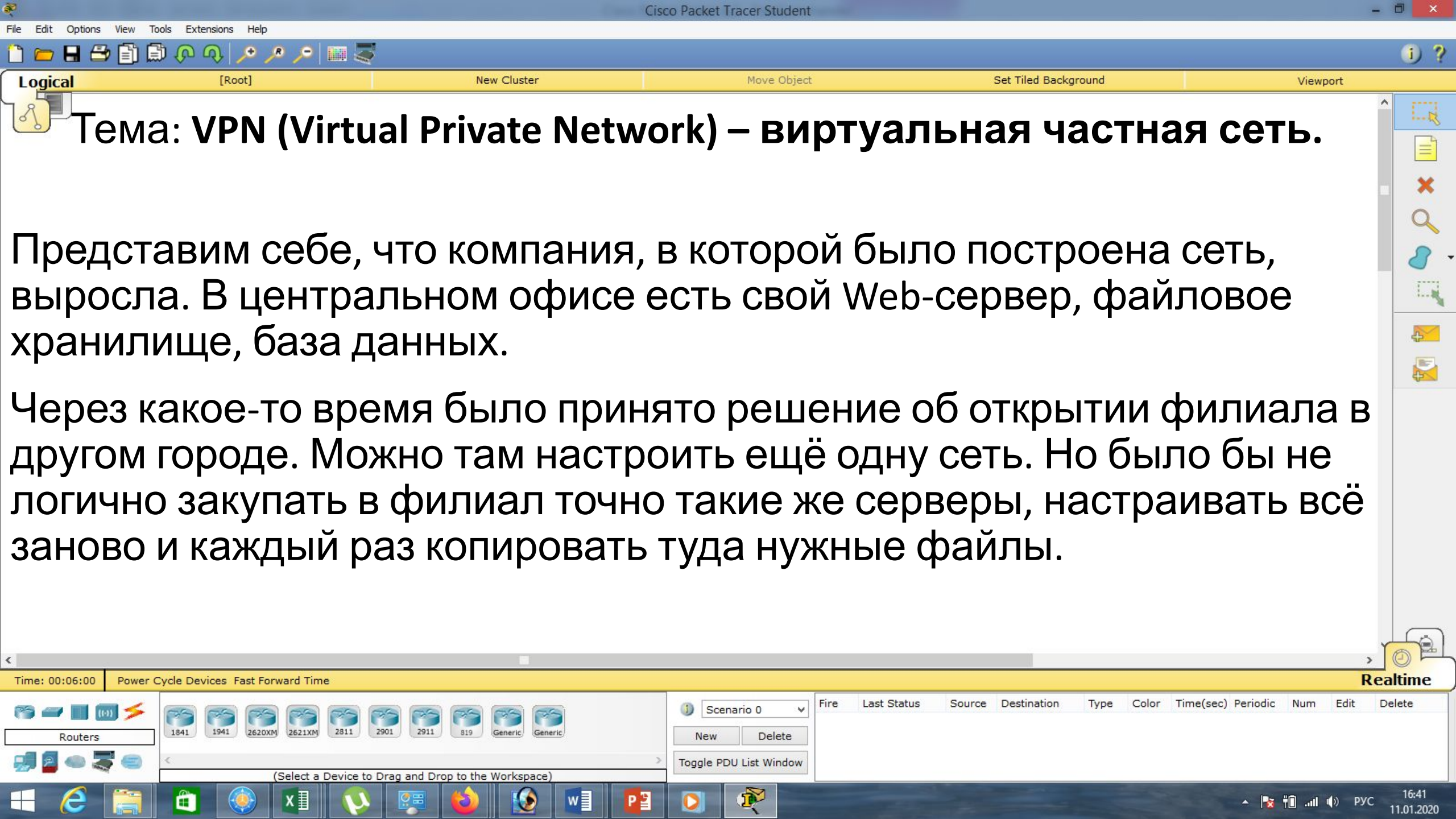
МДК.01.01

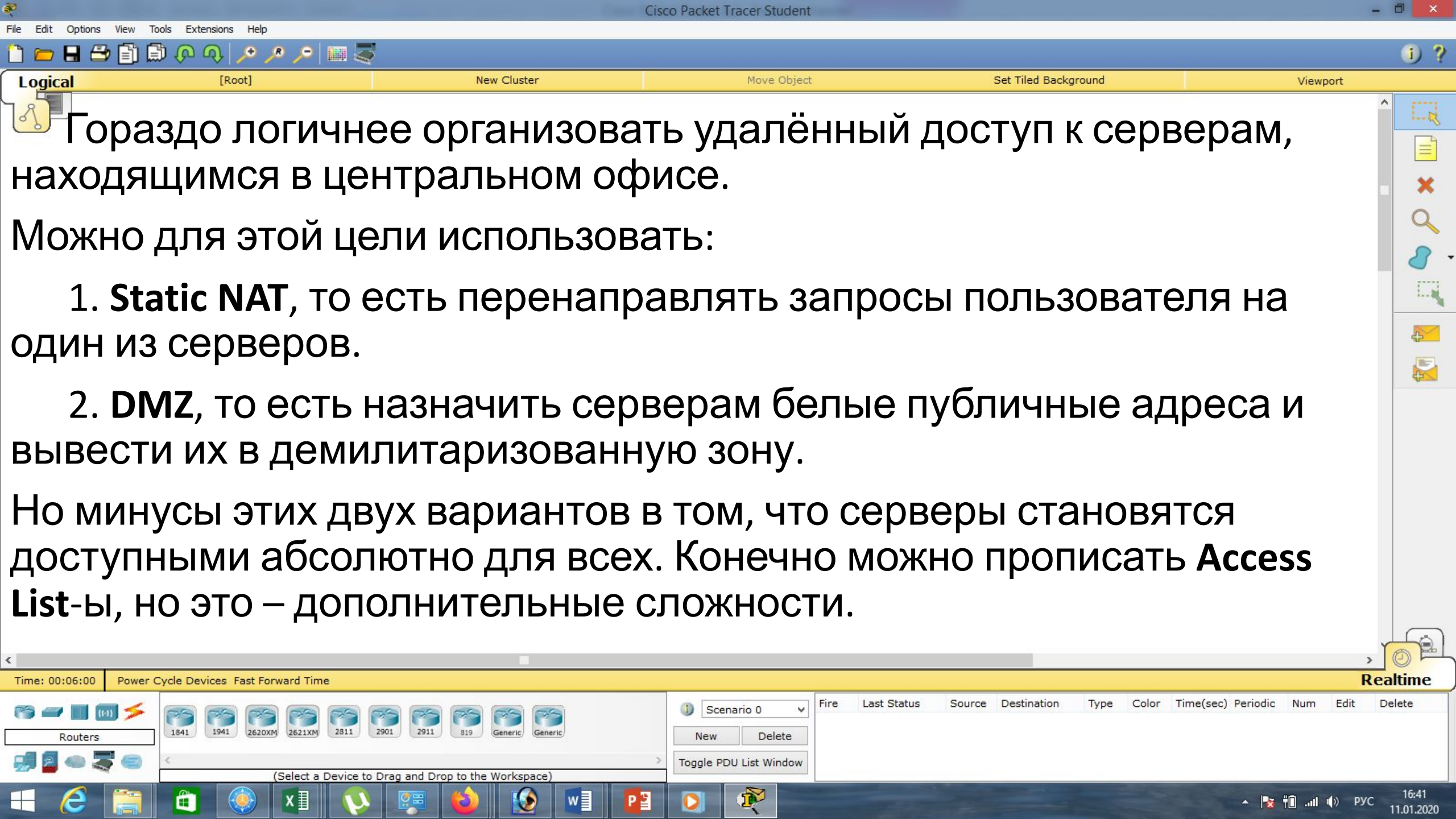
Организация, принципы построения и функционирования компьютерных сетей

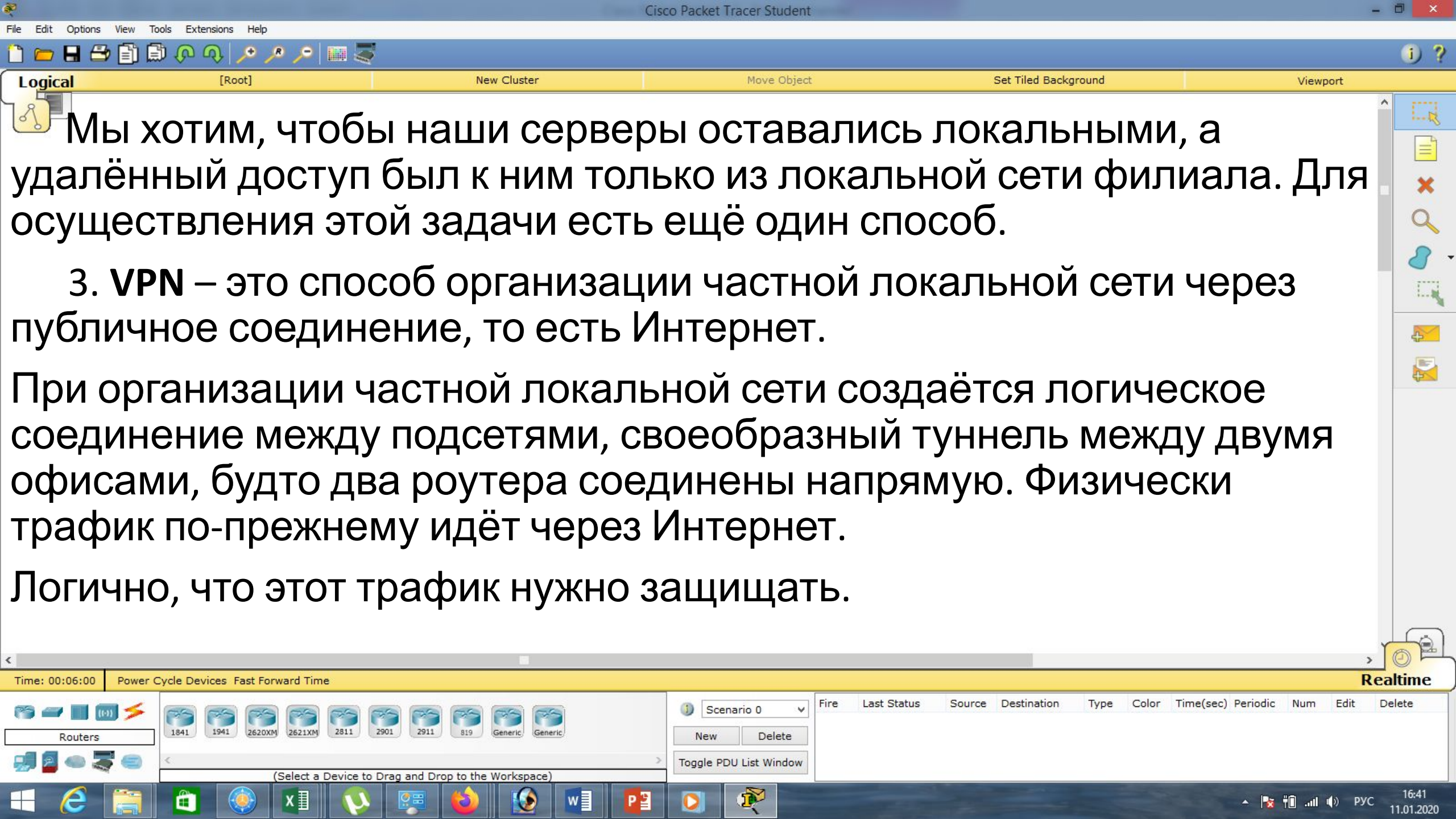
3-курс

Практические занятия

Занятие 16


Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
Тема: VPN (Virtual Private Network) – виртуальная частная сеть.
Представим себе, что компания, в которой было построена сеть, выросла. В центральном офисе есть свой Web-сервер, файловое хранилище, база данных.
Через какое-то время было принято решение об открытии филиала в другом городе. Можно там настроить ещё одну сеть. Но было бы не логично закупать в филиал точно такие же серверы, настраивать всё заново и каждый раз копировать туда нужные файлы.
Time: 00:06:00 Power Cycle Devices Fast Forward Time
Realtime
Routers
1841 1941 2620XM 2621XM 2811 2901 2911 819 Generic Generic
(Select a Device to Drag and Drop to the Workspace)
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
РУС 16:41 11.01.2020


Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
Гораздо логичнее организовать удалённый доступ к серверам, находящимся в центральном офисе.
Можно для этой цели использовать:
1. Static NAT, то есть перенаправлять запросы пользователя на один из серверов.
2. DMZ, то есть назначить серверам белые публичные адреса и вывести их в демилитаризованную зону.
Но минусы этих двух вариантов в том, что серверы становятся доступными абсолютно для всех. Конечно можно прописать Access List-ы, но это – дополнительные сложности.
Time: 00:06:00 Power Cycle Devices Fast Forward Time Realtime
Routers
1841 1941 2620XM 2621XM 2811 2901 2911 819 Generic Generic
(Select a Device to Drag and Drop to the Workspace)
Scenario 0 New Delete Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
РУС 16:41 11.01.2020


Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
Мы хотим, чтобы наши серверы оставались локальными, а удалённый доступ был к ним только из локальной сети филиала. Для осуществления этой задачи есть ещё один способ.
3. VPN – это способ организации частной локальной сети через публичное соединение, то есть Интернет.
При организации частной локальной сети создаётся логическое соединение между подсетями, своеобразный туннель между двумя офисами, будто два роутера соединены напрямую. Физически трафик по-прежнему идёт через Интернет.
Логично, что этот трафик нужно защищать.
Time: 00:06:00 Power Cycle Devices Fast Forward Time
Realtime
Routers
1841 1941 2620XM 2621XM 2811 2901 2911 819 Generic Generic
(Select a Device to Drag and Drop to the Workspace)
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
РУС 16:41 11.01.2020

Защита организуется с помощью различных протоколов. Самые распространённые из них – это:

- **IPsec Site-to-Site VPN** – объединение нескольких сетей;
- **IPsec Remout Access VPN** – подключение удаленного пользователя, например, руководителя организации из собственного дома.

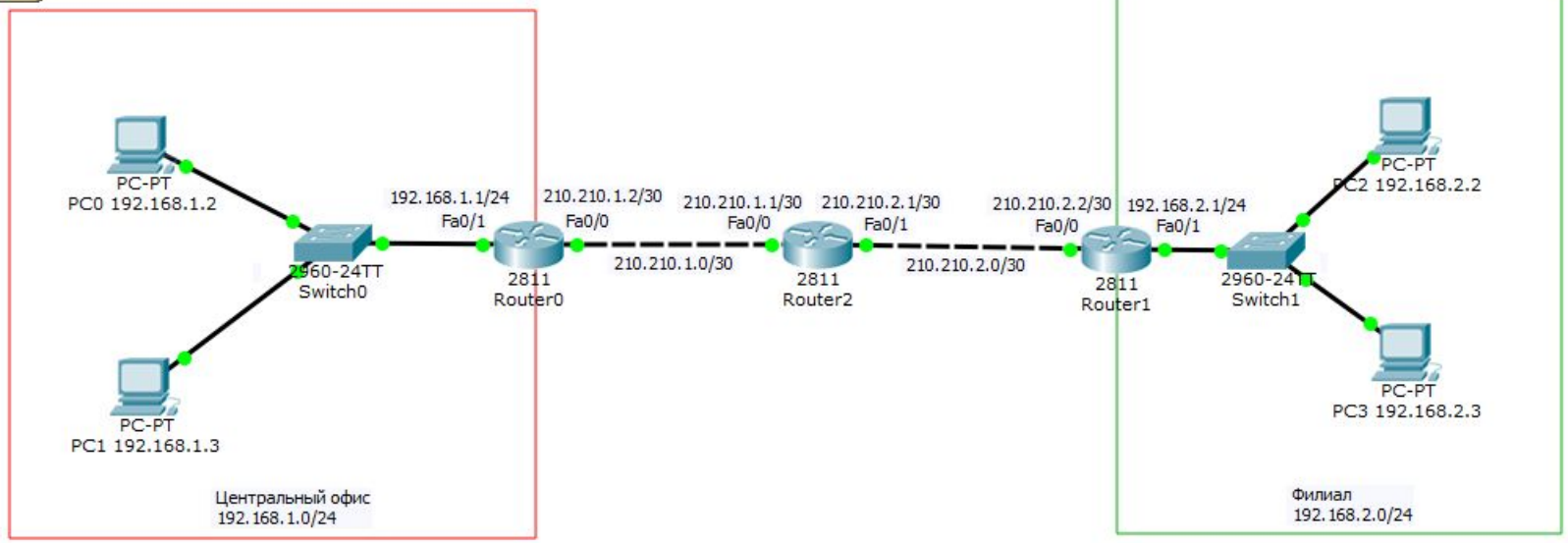
Построение **VPN**-соединения можно разбить на две фазы:

1. Две стороны договариваются о параметрах технологического соединения, если они идентифицирую друг друга, то возникает защищённый **SA** и **ISAKMP Tunnel**.
2. Поднимается **IPsec Tunnel**. После чего поднимается весь туннель.

Cisco Packet Tracer Student - D:\Андрей\Компьютерные сети\МДК.01.01 Организация, принципы построения и функционирования компьютерных сетей\Практические работы\Работа 30.pkt

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Tiled Background Viewport



Соберём схему, показанную на рисунке и наладим связь между Центральным офисом ***и*** Филиалом ***через*** VPN**.**

Time: 02:56:29 Power Cycle Devices Fast Forward Time Realtime

Routers

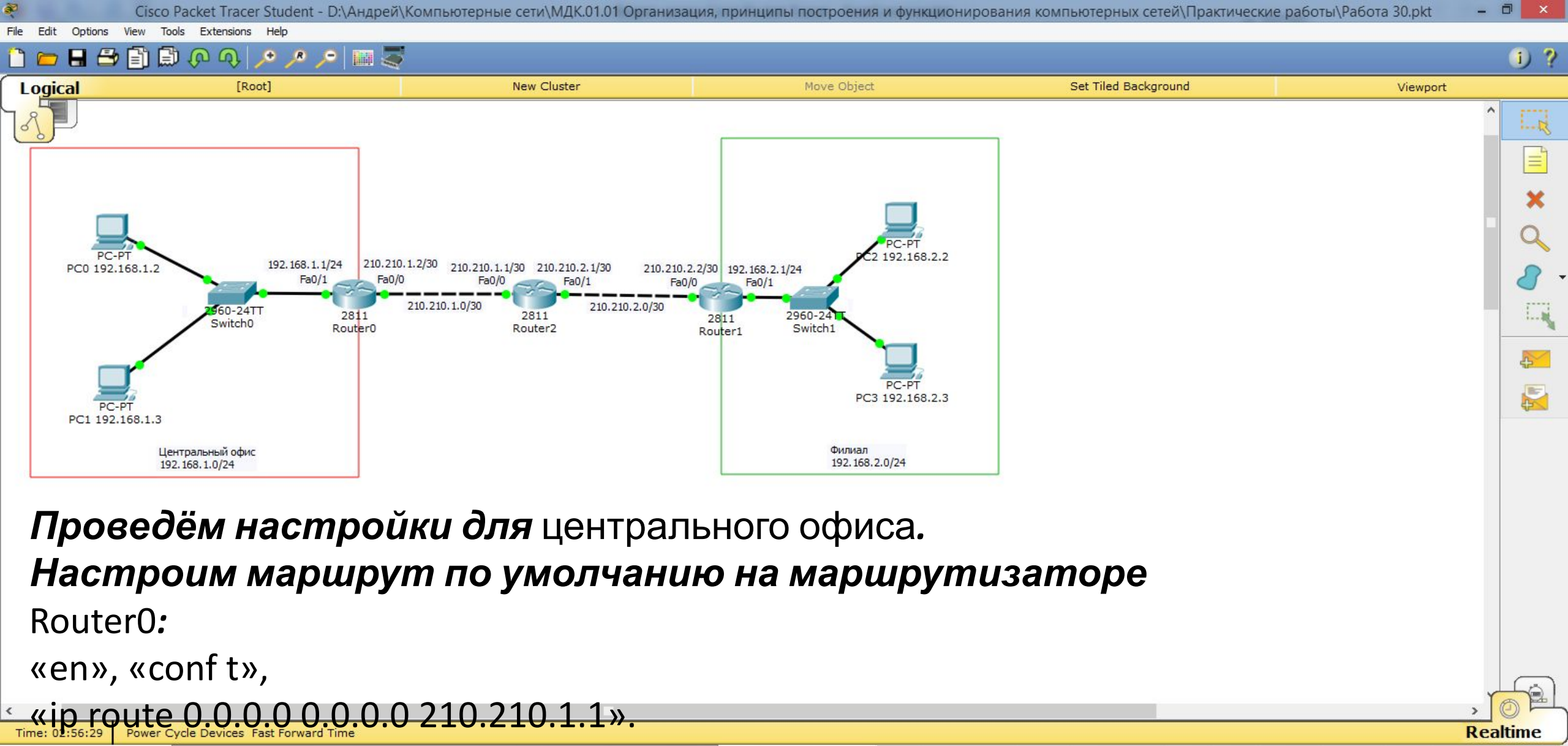
1841 1941 2620XM 2621XM 2811 2901 2911 819 Generic Generic

Router-PT-Empty

Scenario 0 New Delete Toggle PDU List Window

Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete

РУС 21:14 18.01.2020



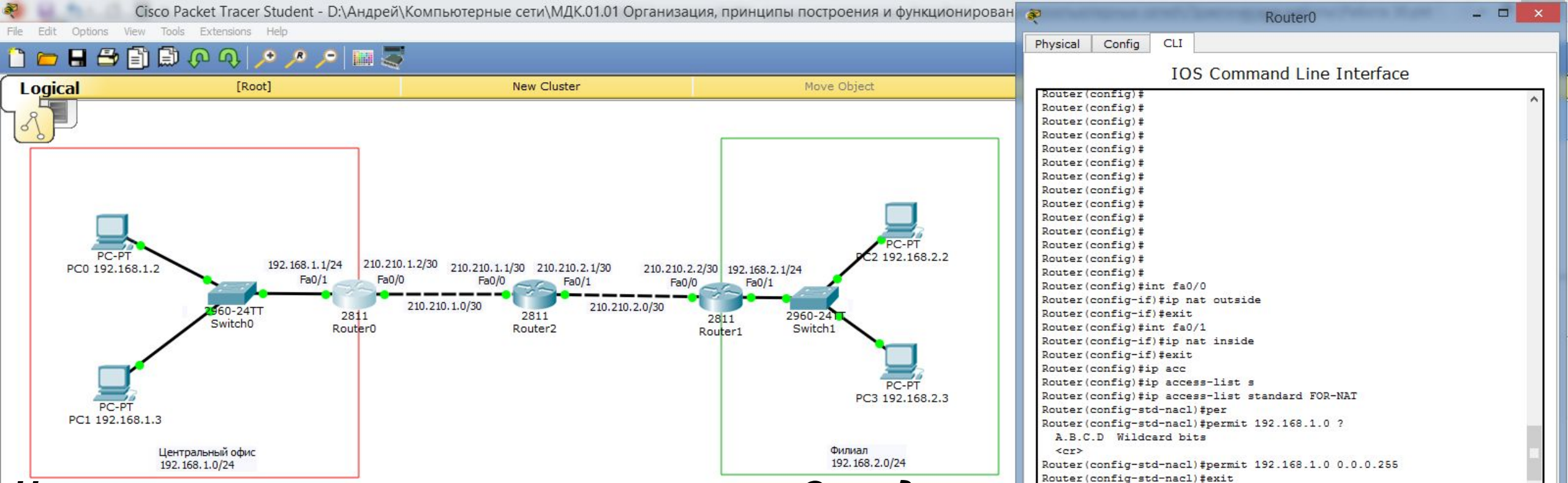
Проведём настройки для центрального офиса***.***

Настроим маршрут по умолчанию на маршрутизаторе

Router0***:***

«en», «conf t»,

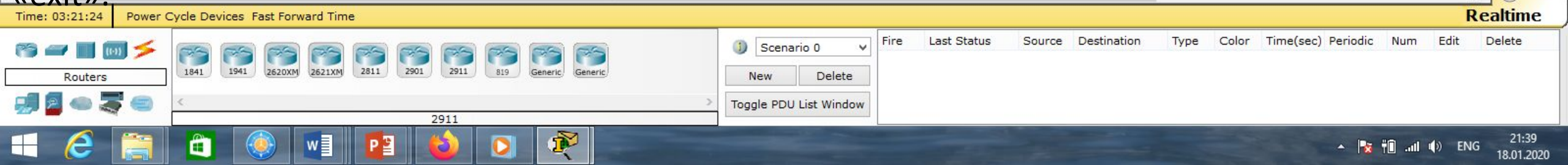
«ip route 0.0.0.0 0.0.0.0 210.210.1.1».

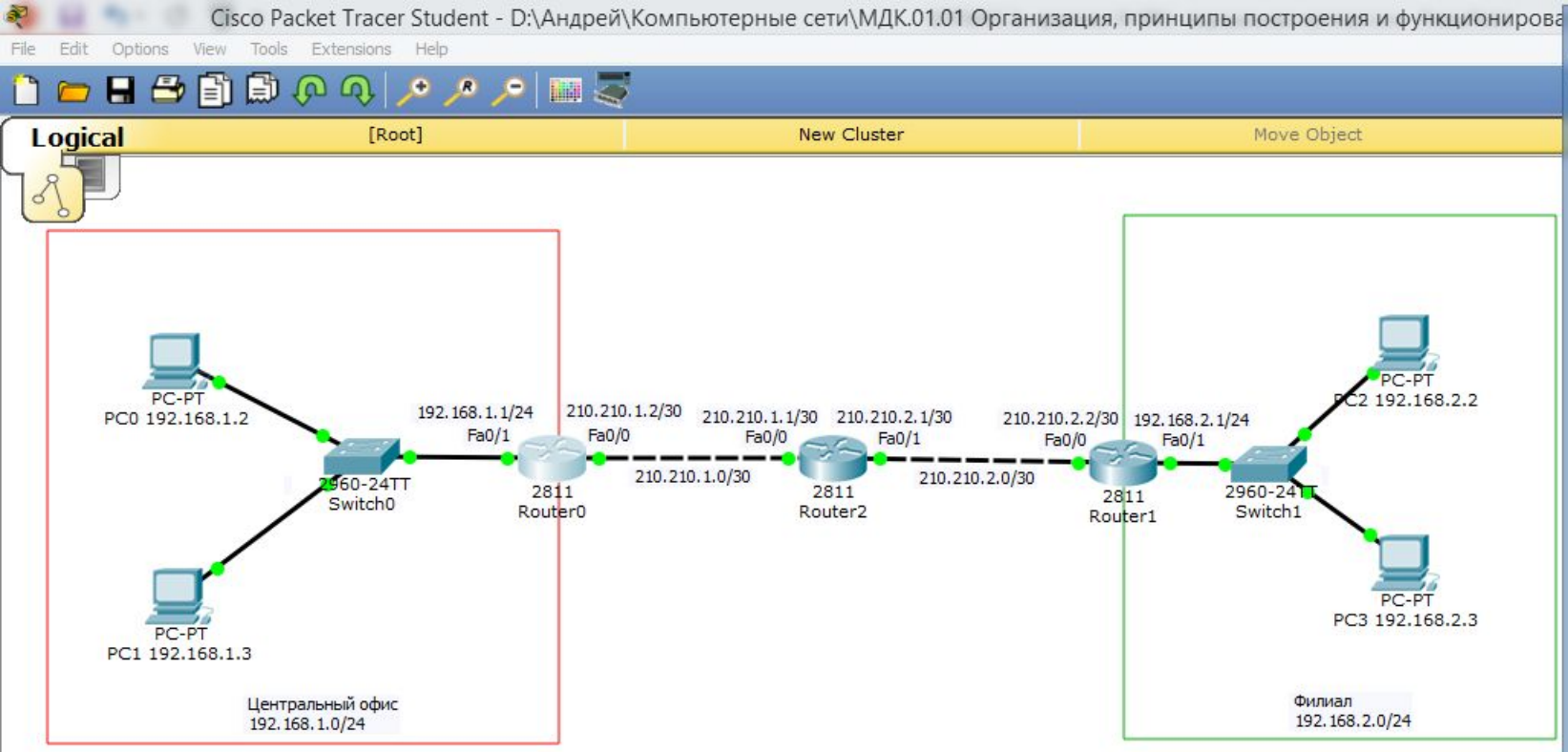


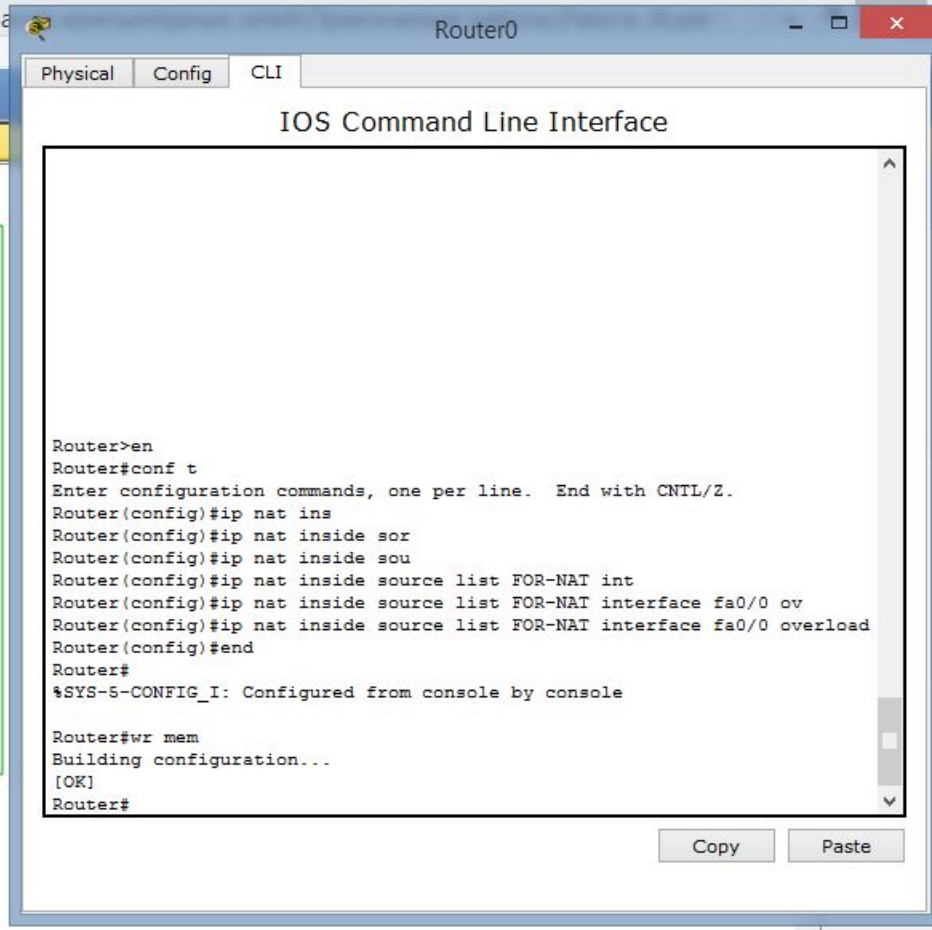
Настроим NAT ***на маршрутизаторе*** Router0***. Определяем:*** ***внешний интерфейс:*** «int fa0/0», «ip nat outside», «exit» ***и внутренний интерфейс:*** «int fa0/1», «ip nat inside», «exit».

Создаём Access List ***с именем*** FOR-NAT***:*** «ip access-list standard FOR-NAT».

Указываем разрешающий трафик для нашей сети: «permit 192.168.1.0 0.0.0.255», «exit».





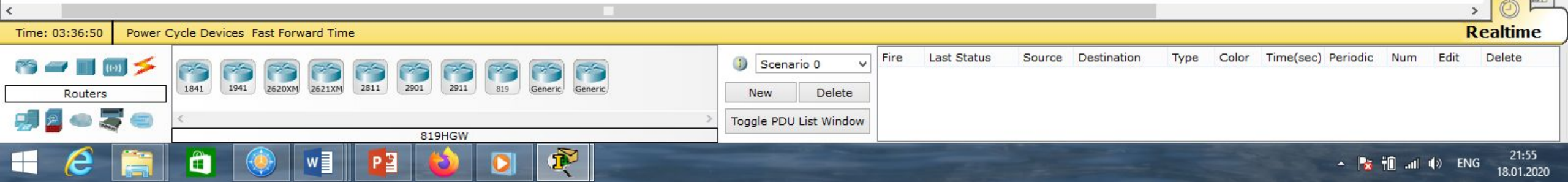


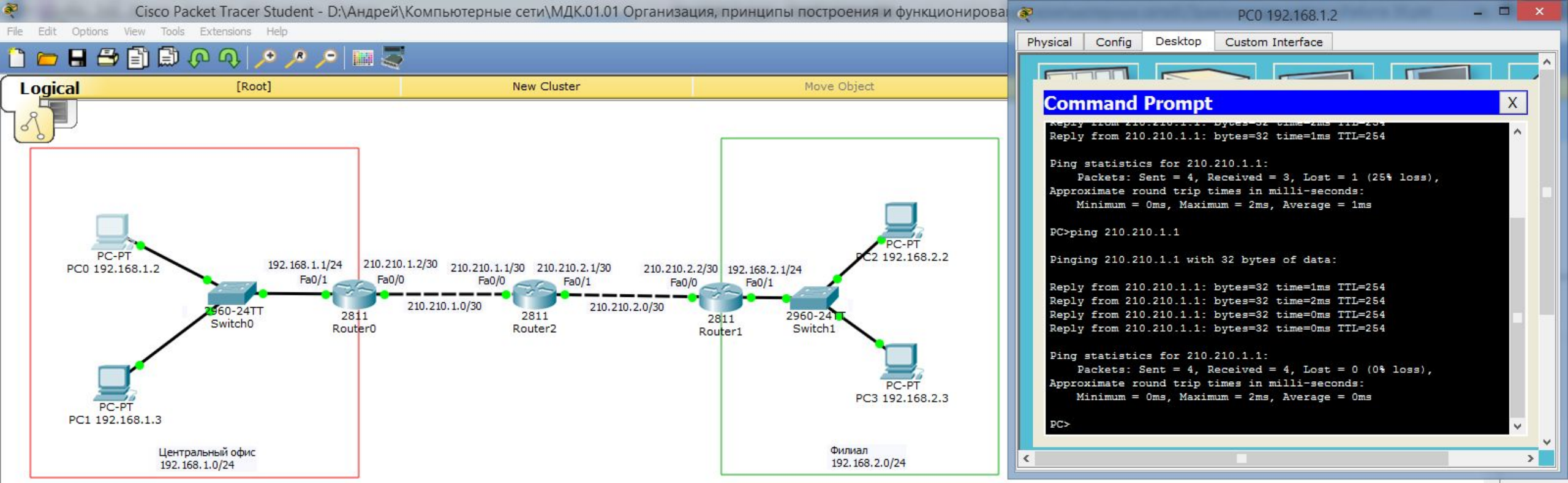
Завершающая длинная команда:

«ip nat inside source list FOR-NAT interface fa0/0 overload»,

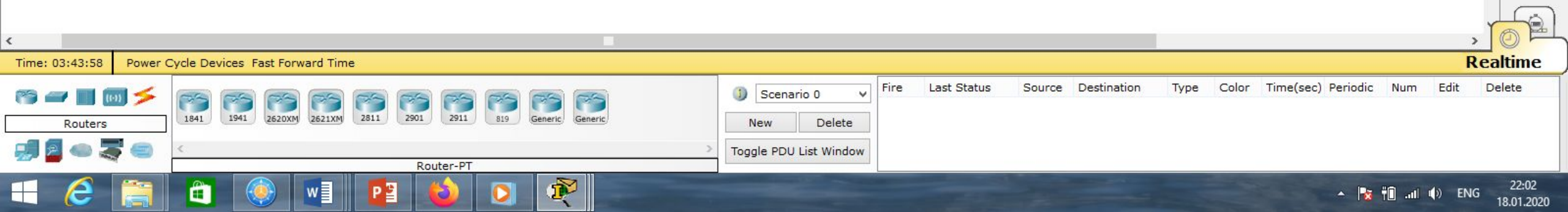
«end»,

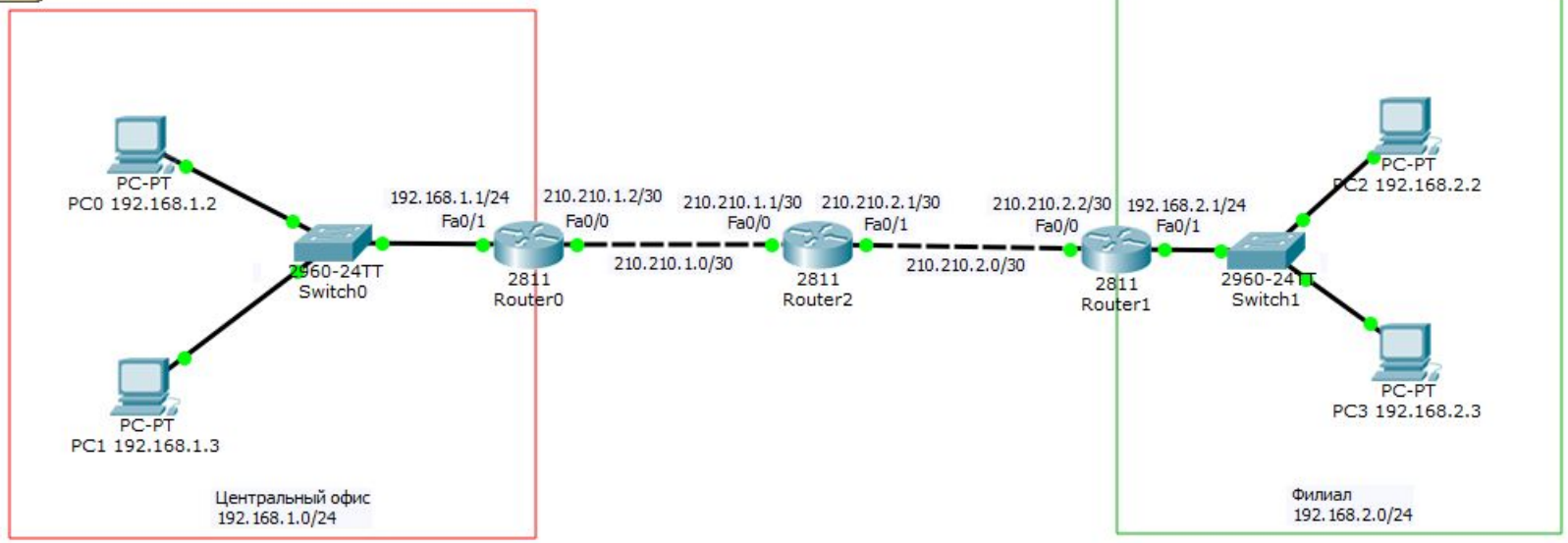
«wr mem».





Проверим связь компьютера с маршрутизатором провайдера Router2***:***
«ping 210.210.1.1».
Связь есть!!!





Повторим эти же настройки для филиала***.***

Настроим маршрут по умолчанию на маршрутизаторе

Router1***:***

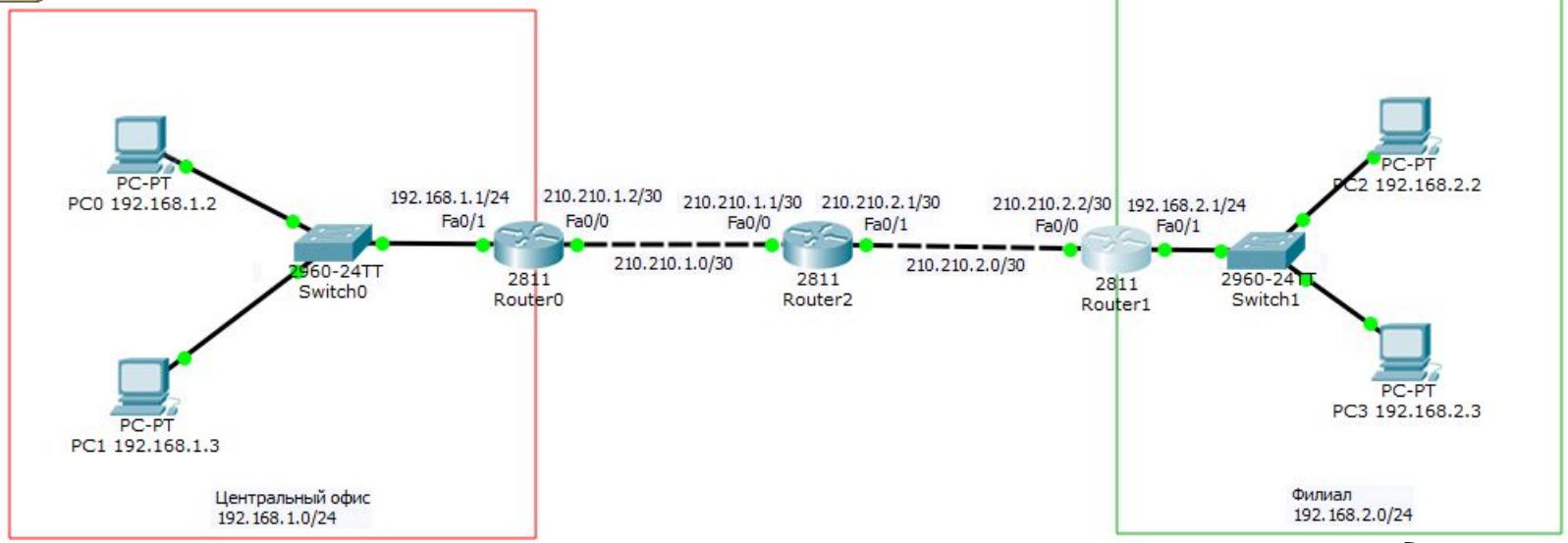
«en», «conf t»,

«ip route 0.0.0.0 0.0.0.0 210.210.2.1».

Cisco Packet Tracer Student - D:\Андрей\Компьютерные сети\МДК.01.01 Организация, принципы построения и функционирования компьютерных сетей\Практические работы\Работа 30.pkt

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Tiled Background Viewport



Настроим NAT ***на маршрутизаторе*** Router1***. Определяем:***
внешний интерфейс: «int fa0/0», «ip nat outside», «exit» ***и***
внутренний интерфейс: «int fa0/1», «ip nat inside», «exit».
Создаём Access List ***с именем*** FOR-NAT***:*** «ip access-list standard FOR-NAT».
Указываем разрешающий трафик для нашей сети: «permit 192.168.2.0 0.0.0.255», «exit».

Time: 03:55:05 Power Cycle Devices Fast Forward Time Realtime

Routers

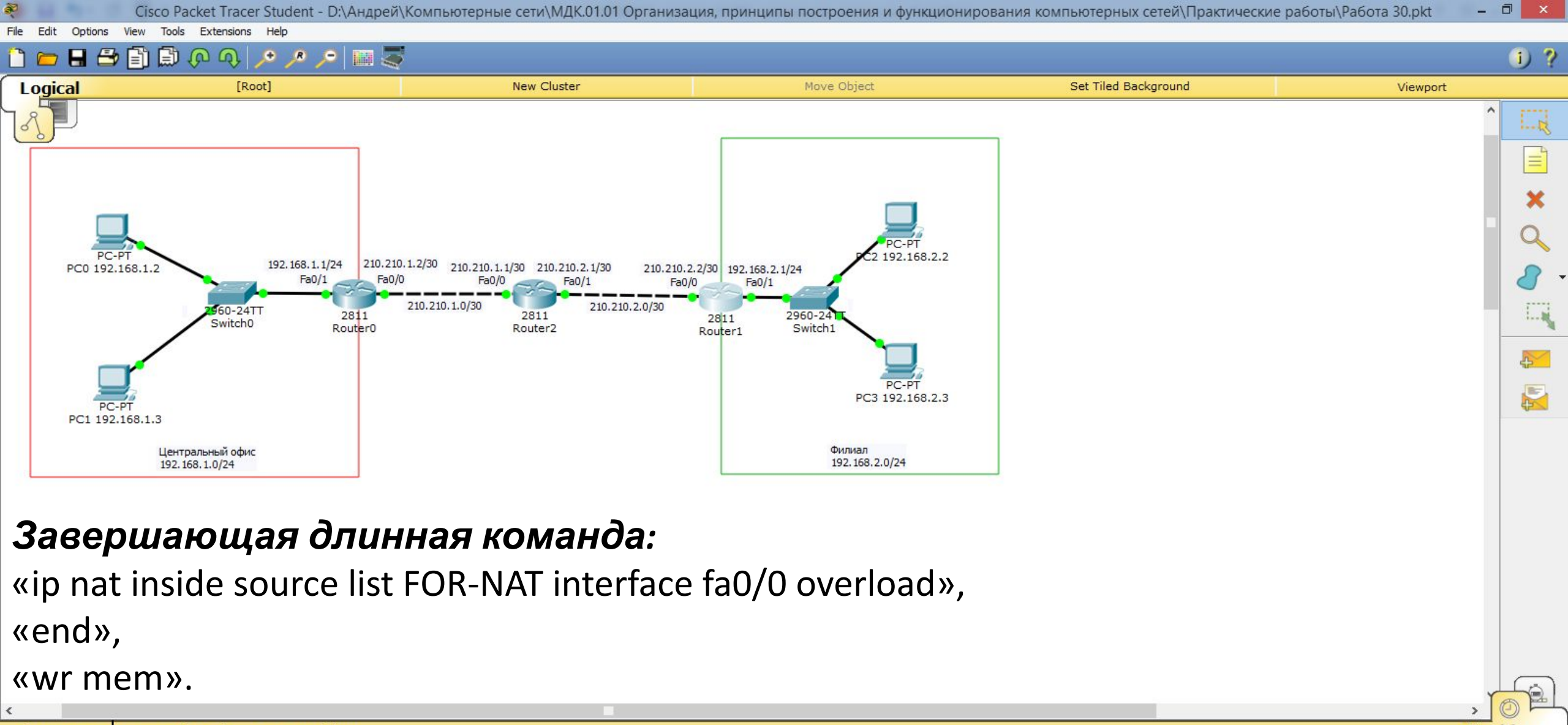
1841 1941 2620XM 2621XM 2811 2901 2911 819 Generic Generic

819HGW

Scenario 0 New Delete Toggle PDU L Delete Scenario and All PDUs (Ctrl+Shift+D)

Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete

РУС 22:13 18.01.2020

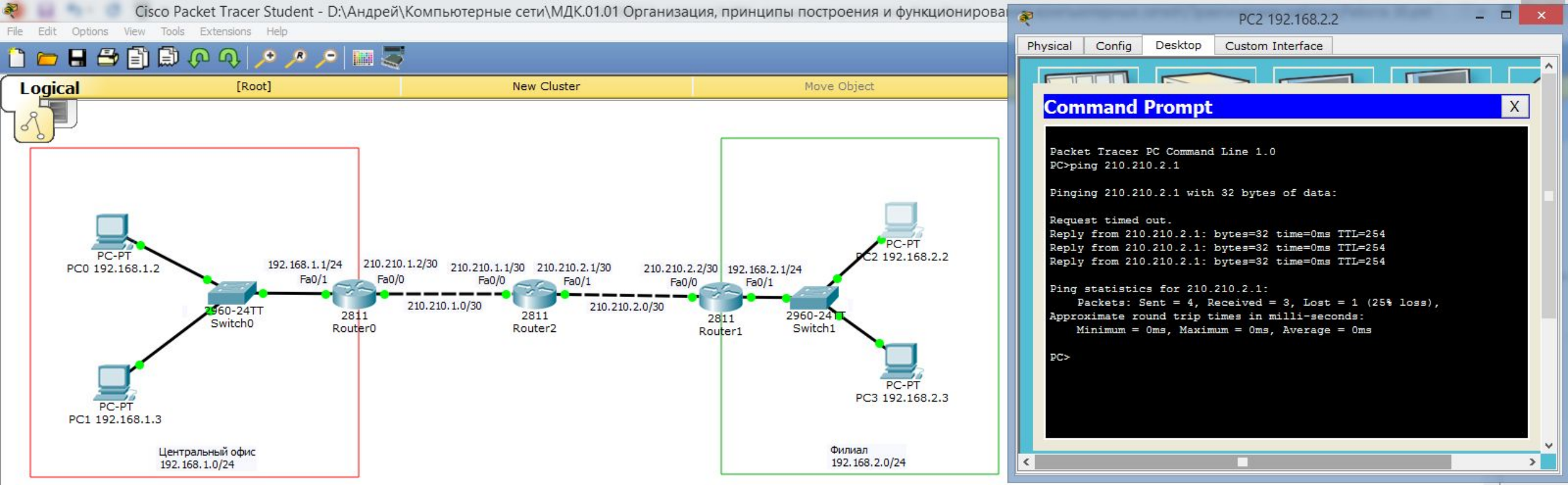


Завершающая длинная команда:

«ip nat inside source list FOR-NAT interface fa0/0 overload»,

«end»,

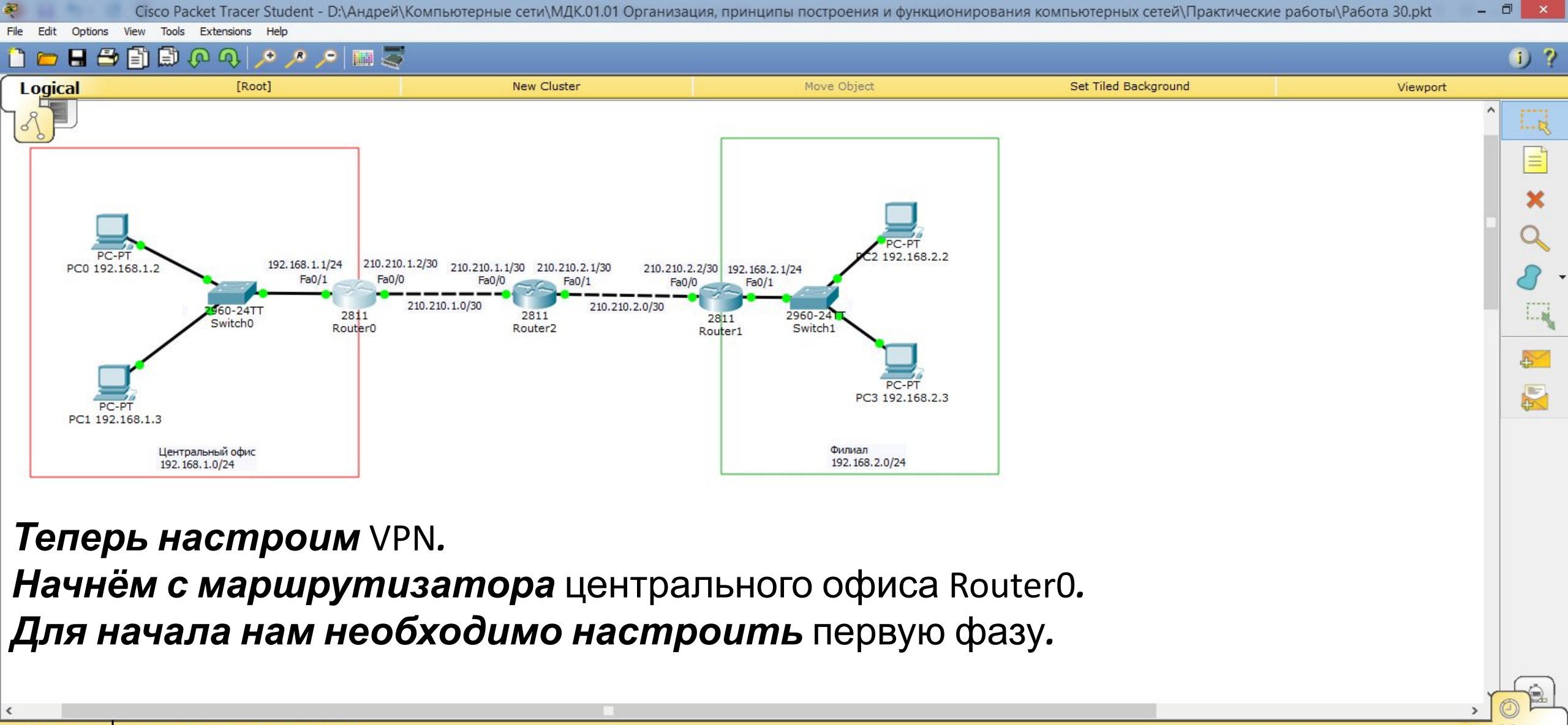
«wr mem».



Проверим связь компьютера с маршрутизатором провайдера Router2***:***

«ping 210.210.2.1».

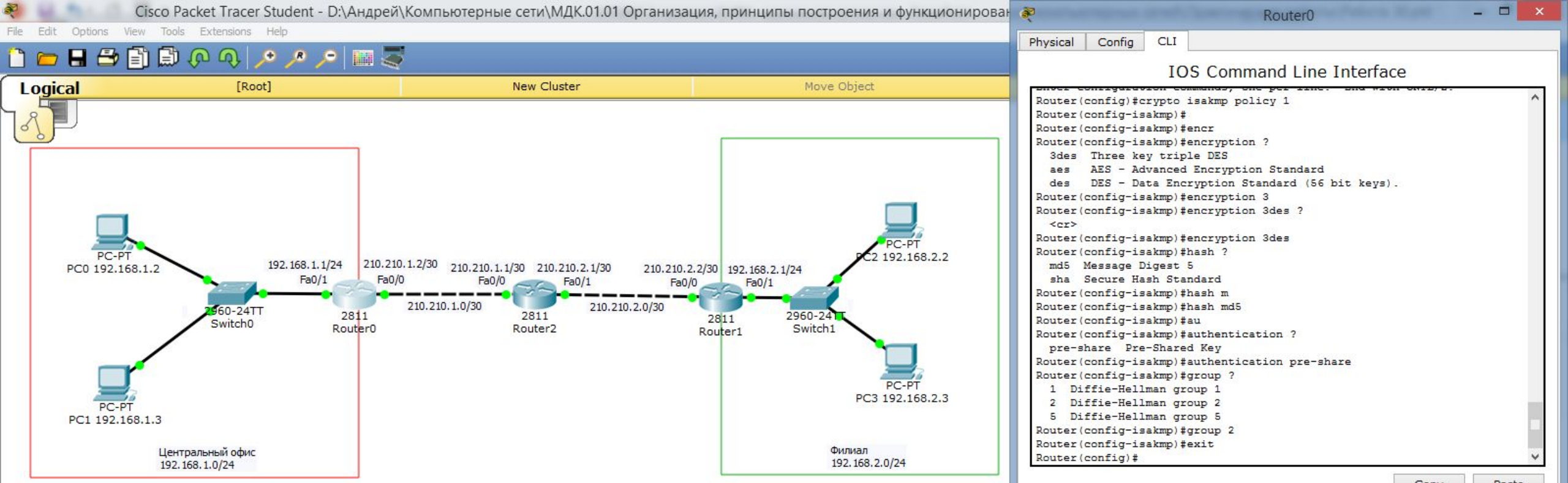
Связь есть!!!



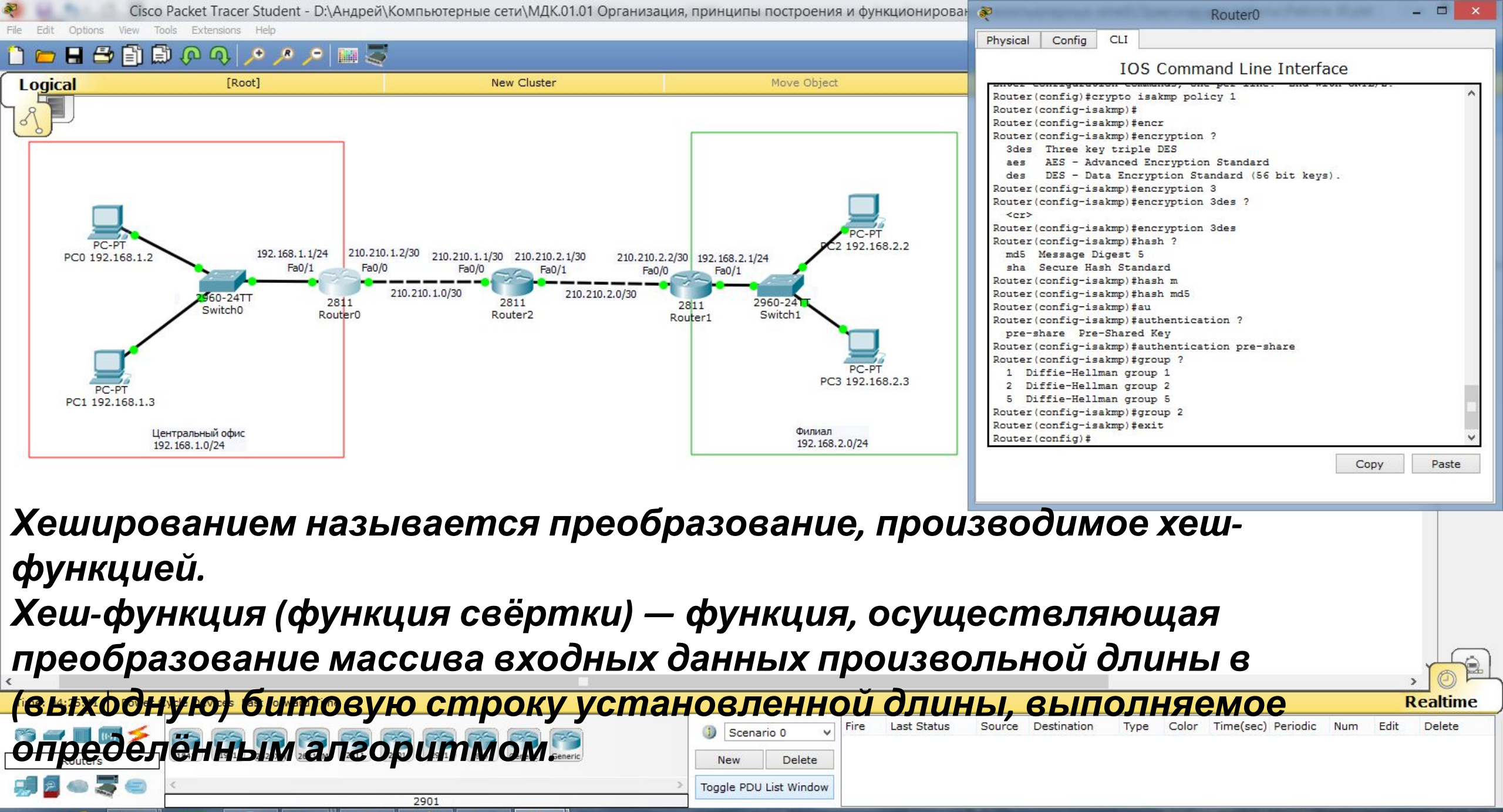
Теперь настроим VPN***.***

Начнём с маршрутизатора центрального офиса Router0***.***

Для начала нам необходимо настроить первую фазу***.***

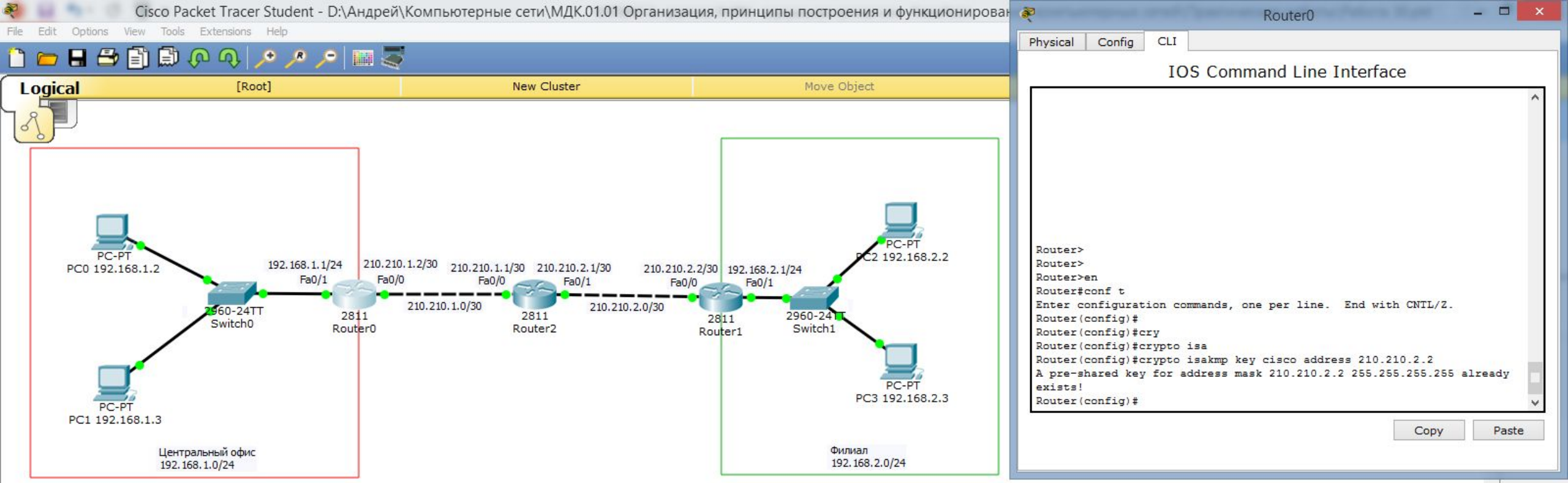


Для этого создаётся политика***:*** «conf t», «crypto isakmp policy 1» ***где мы указываем алгоритм шифрования*** 3des ***(это параметры для построения мини туннеля*** ISAKMP-туннеля***, через который будут передаваться параметры основного*** Ipsec-туннеля***):*** «encryption 3des», ***алгоритм хеширования*** md5***:*** «hash md5», ***тип аутентификации*** Pre-Shared Key***:*** «authentication pre-share» ***и алгоритм Диффи — Хеллмана:*** «group 2», «exit».

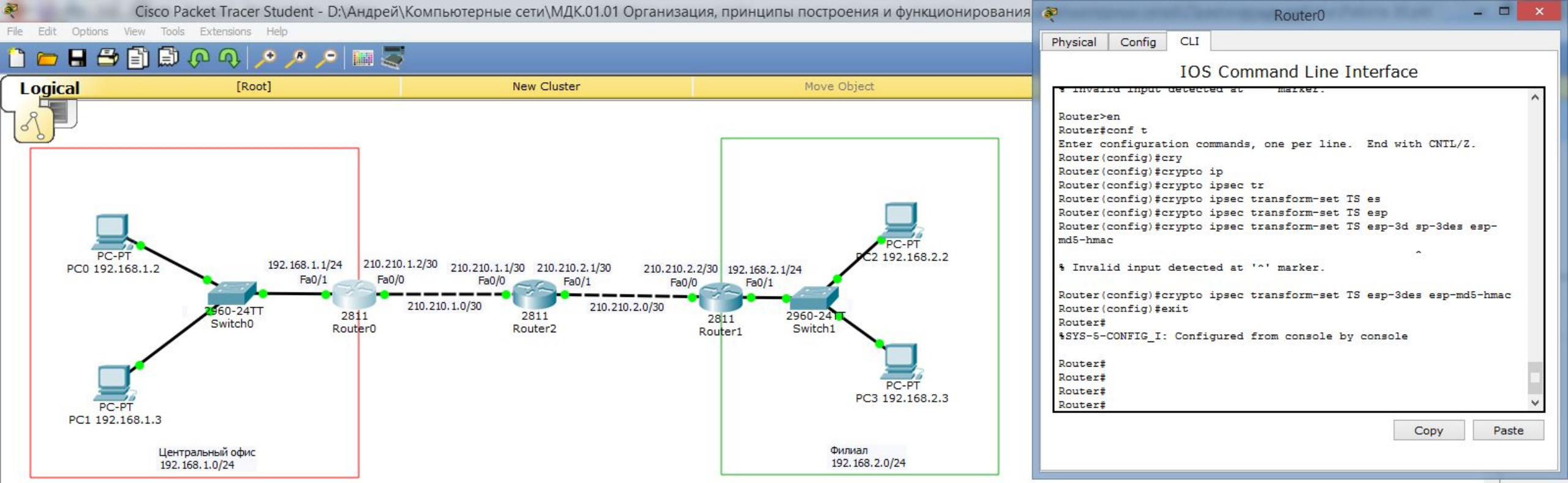


Хешированием называется преобразование, производимое хеш-функцией.

Хеш-функция (функция свёртки) — функция, осуществляющая преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом.



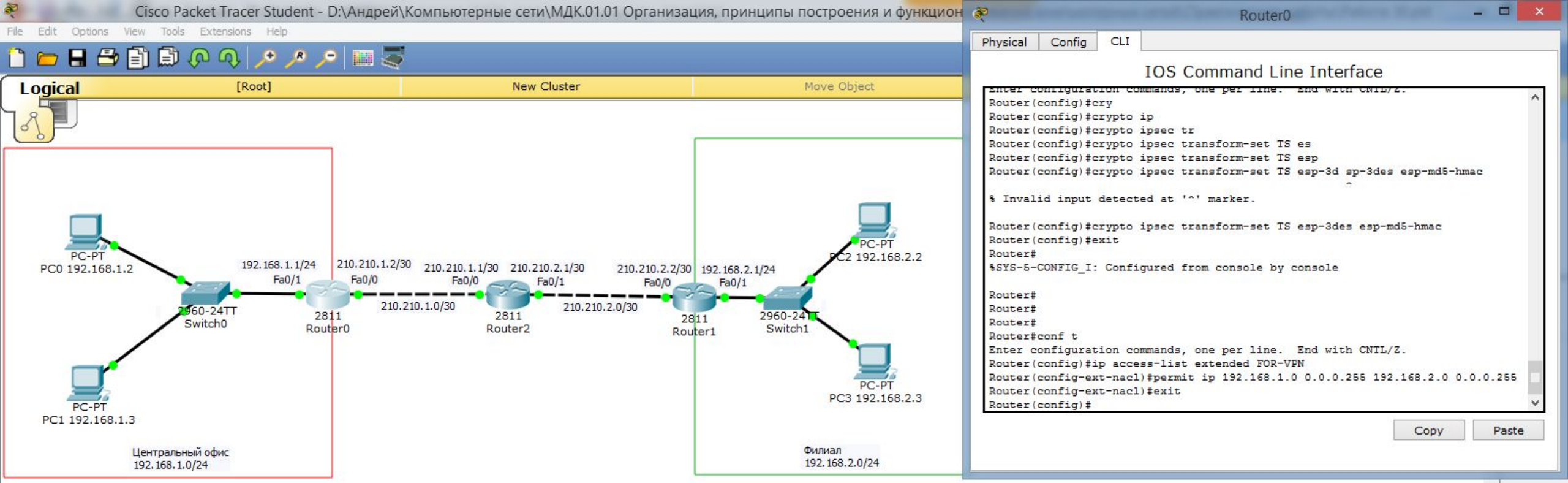
Настроим ключ аутентификации и адреса пира***, то есть внешнего*** ip-адреса ***маршрутизатора*** Router1***, с которым будем строить*** VPN***:*** «crypto isakmp key cisco address 210.210.2.2». ***Мы настроили параметры, необходимые для первой фазы. Переходим ко второй фазе.***



Указываем параметры для построения ipsec-***туннеля с именем*** TS***, далее указываем алгоритм шифрования и хэширования:***

«crypto ipsec transform-set TS esp-3des esp-md5-hmac»,

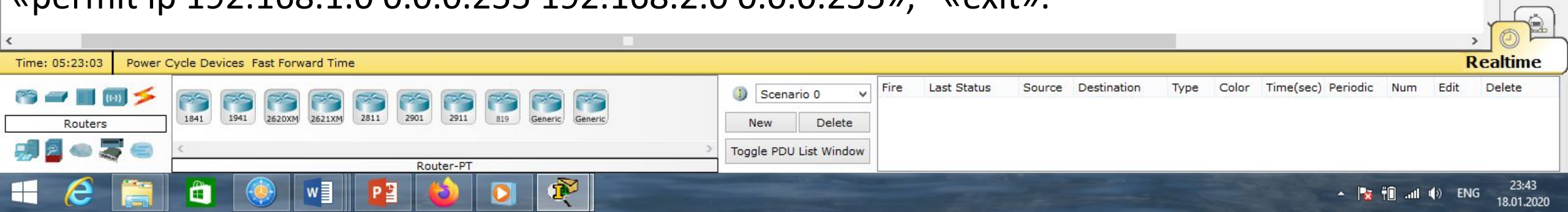
«exit».

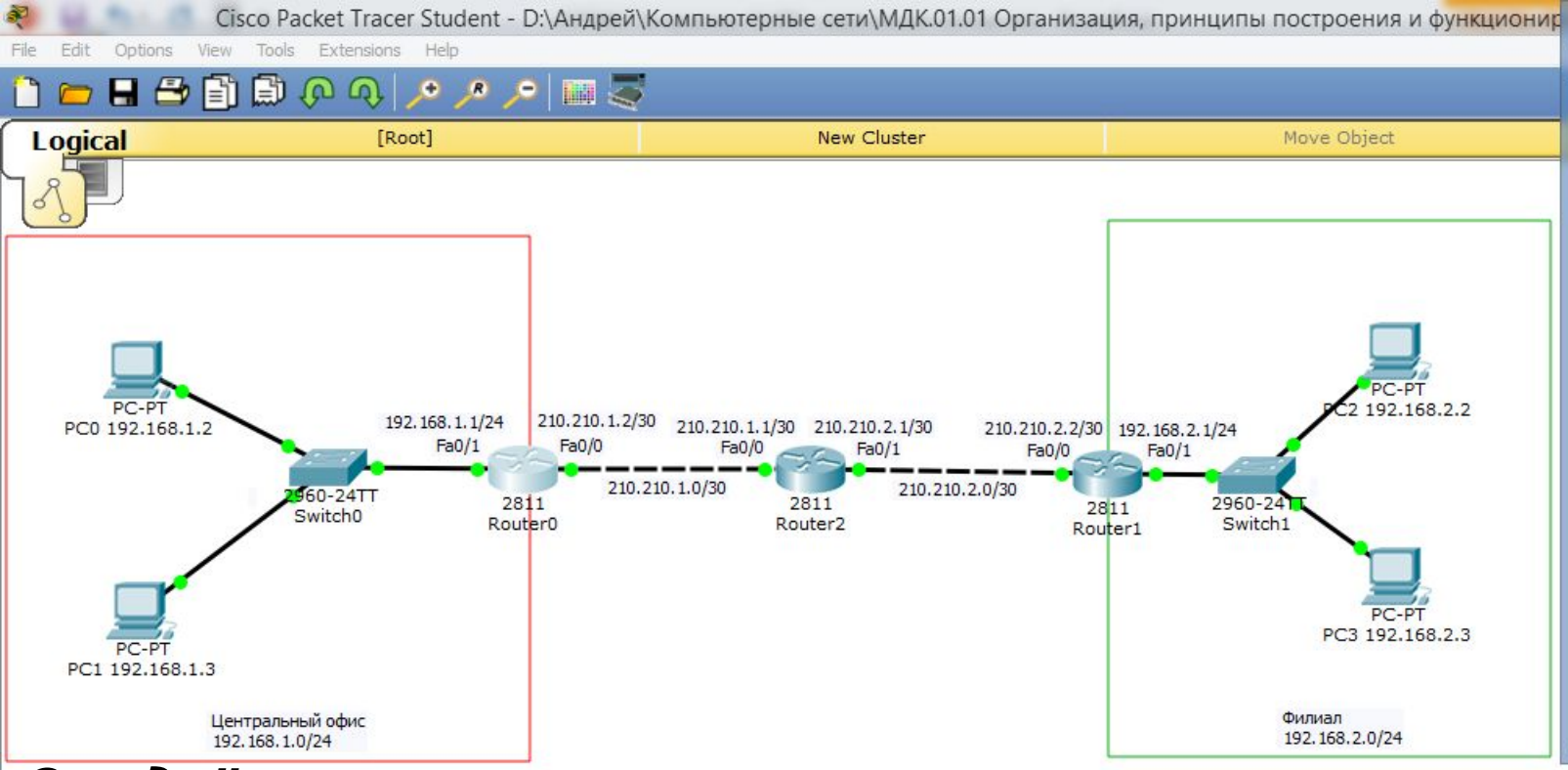


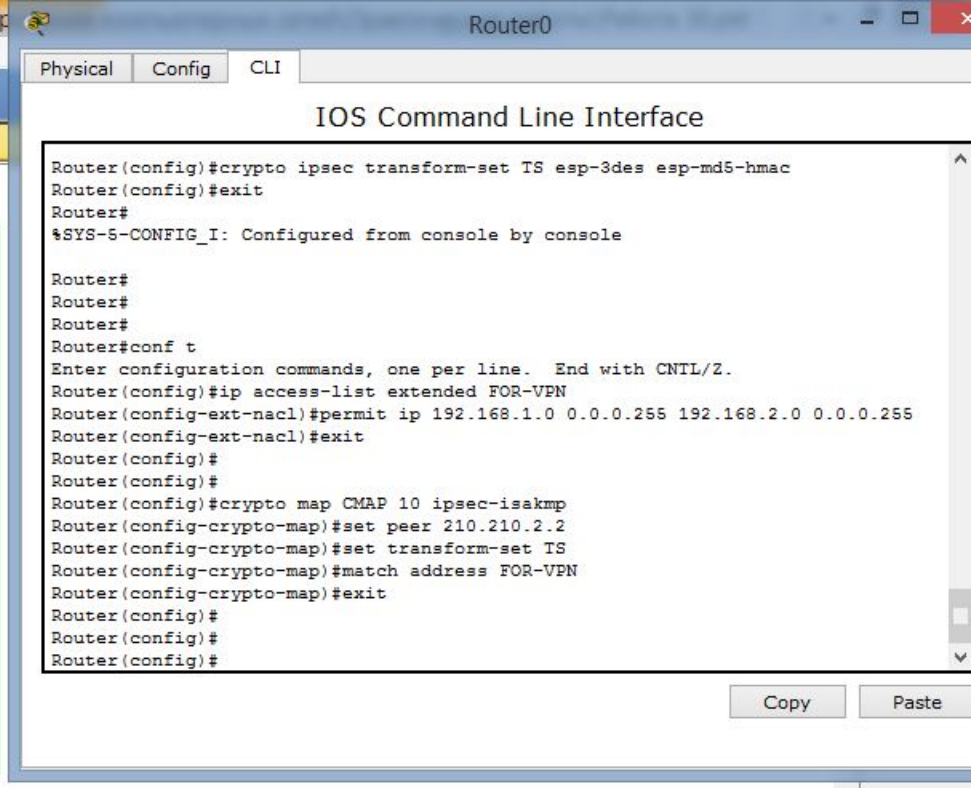
Далее мы должны создать Access List ***с именем*** FOR-VPN***, то есть определить, какой трафик мы будем направлять в*** VPN ***-туннель:***

«conf t», «ip access-list extended FOR-VPN»,

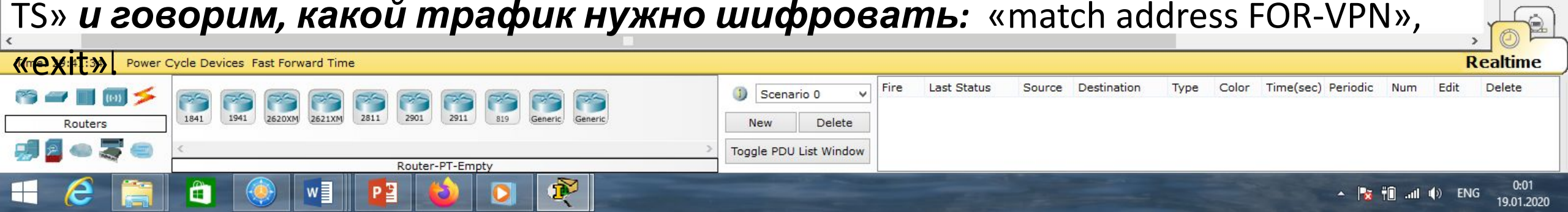
«permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255», «exit».

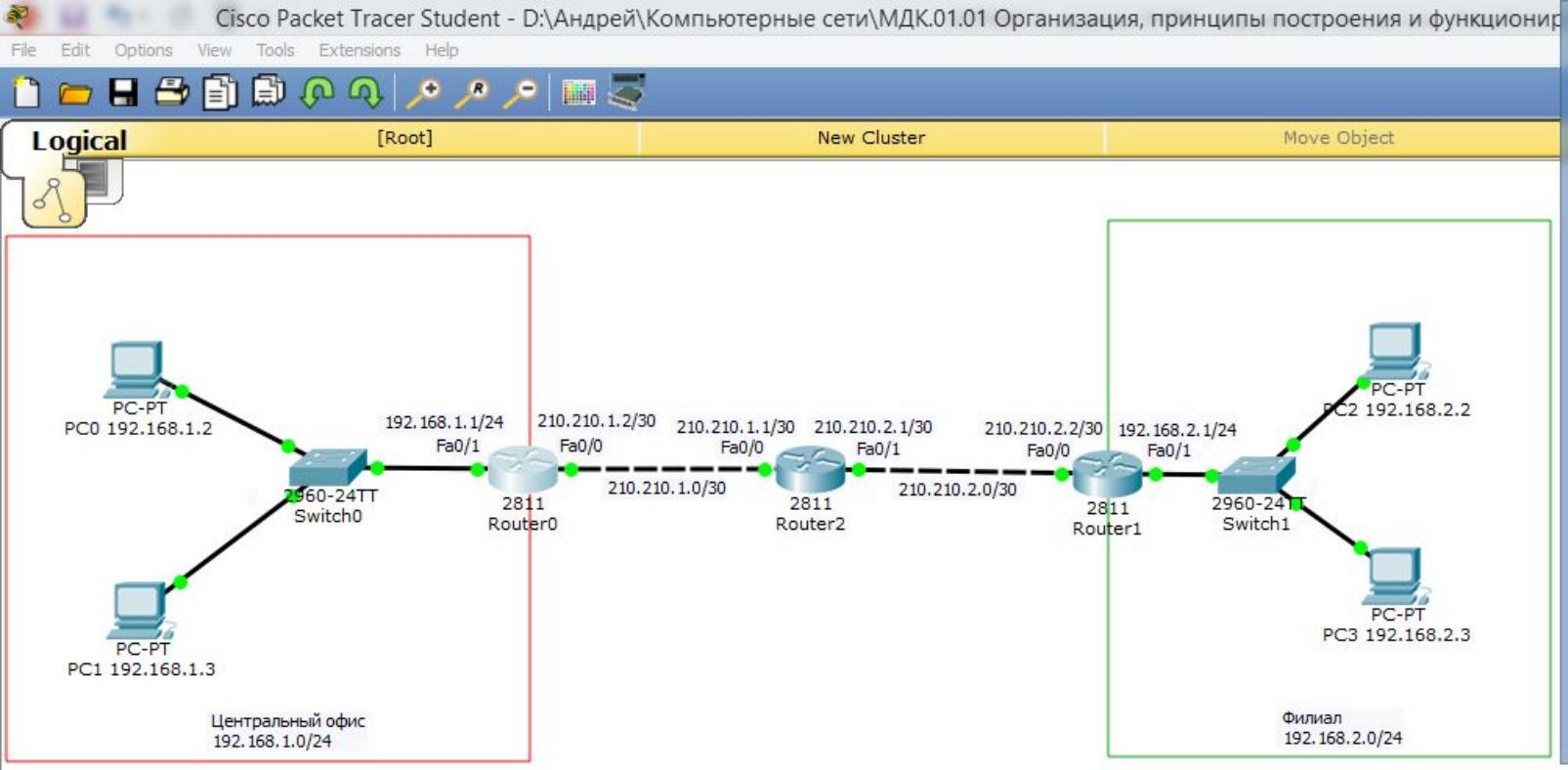


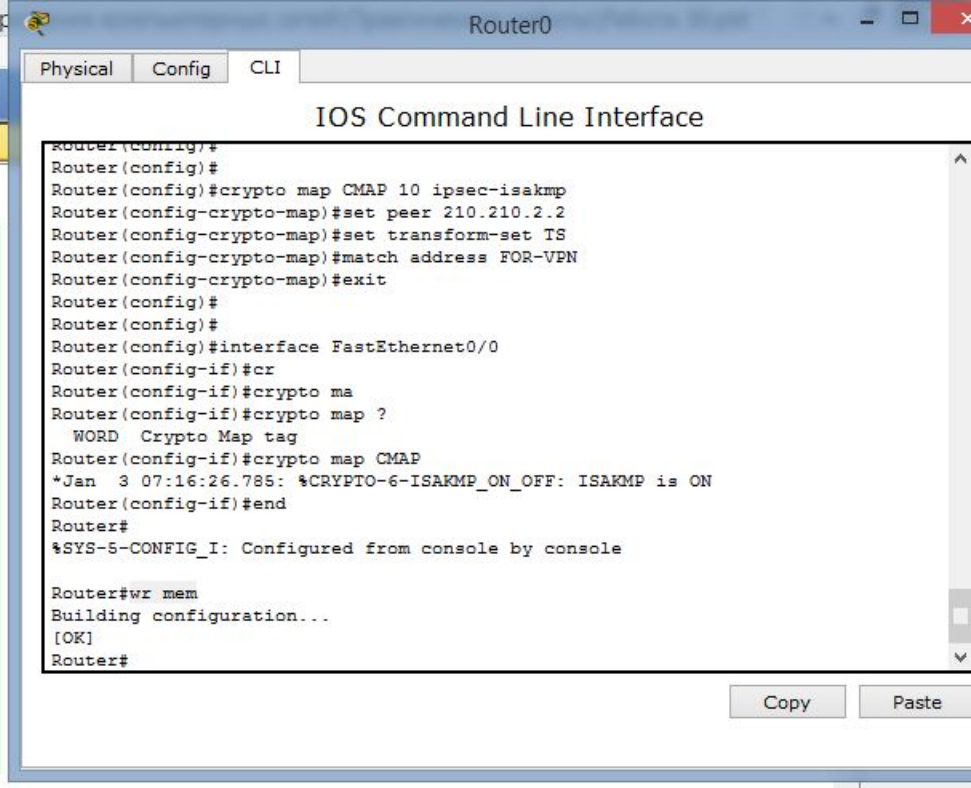




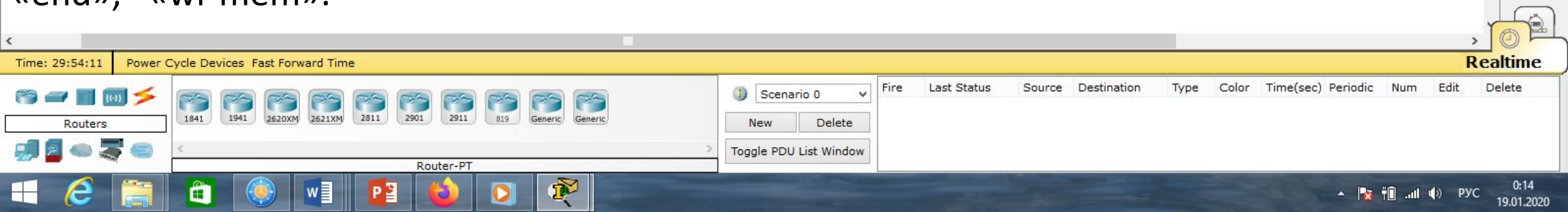
Создаём крипто-карту***:***
«crypto map CMAP 10 ipsec-isakmp»,
указываем пир, то есть внешний ip-адрес ***маршрутизатора*** Router1***:***
«set peer 210.210.2.2***», указываем параметры*** ipsec -туннеля: «set transform-set TS» ***и говорим, какой трафик нужно шифровать:*** «match address FOR-VPN», «exit».







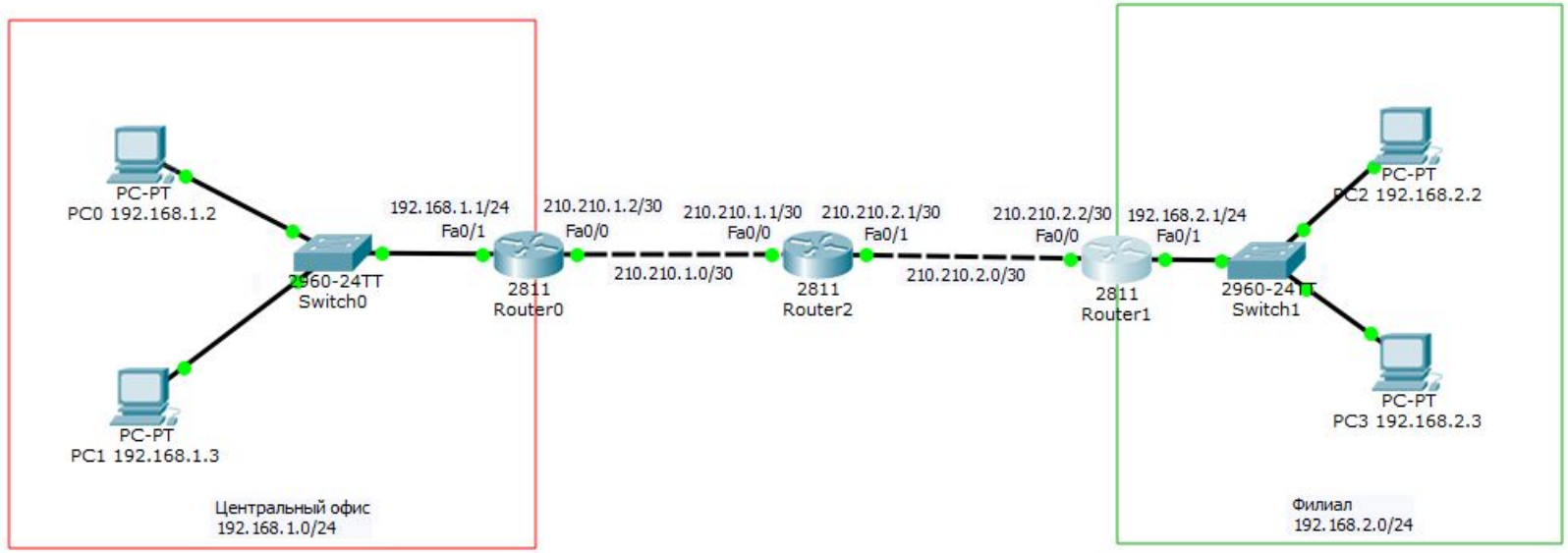
Привяжем эту крипто-карту ***к внешнему интерфейсу:***
«interface FastEthernet0/0»,
командой: «crypto map CMAP»,
«end», «wr mem».



Cisco Packet Tracer Student - D:\Андрей\Компьютерные сети\МДК.01.01 Организация, принципы построения и функционирования компьютерных сетей\Практические работы\Работа 30.pkt

File Edit Options View Tools Extensions Help

Logical | [Root] | New Cluster | Move Object | Set Tiled Background | Viewport



Проделаем тоже самое для маршрутизатора Router1***.***
У него будут отличаться только некоторые параметры.

Time: 29:56:33 | Power Cycle Devices | Fast Forward Time | Realtime

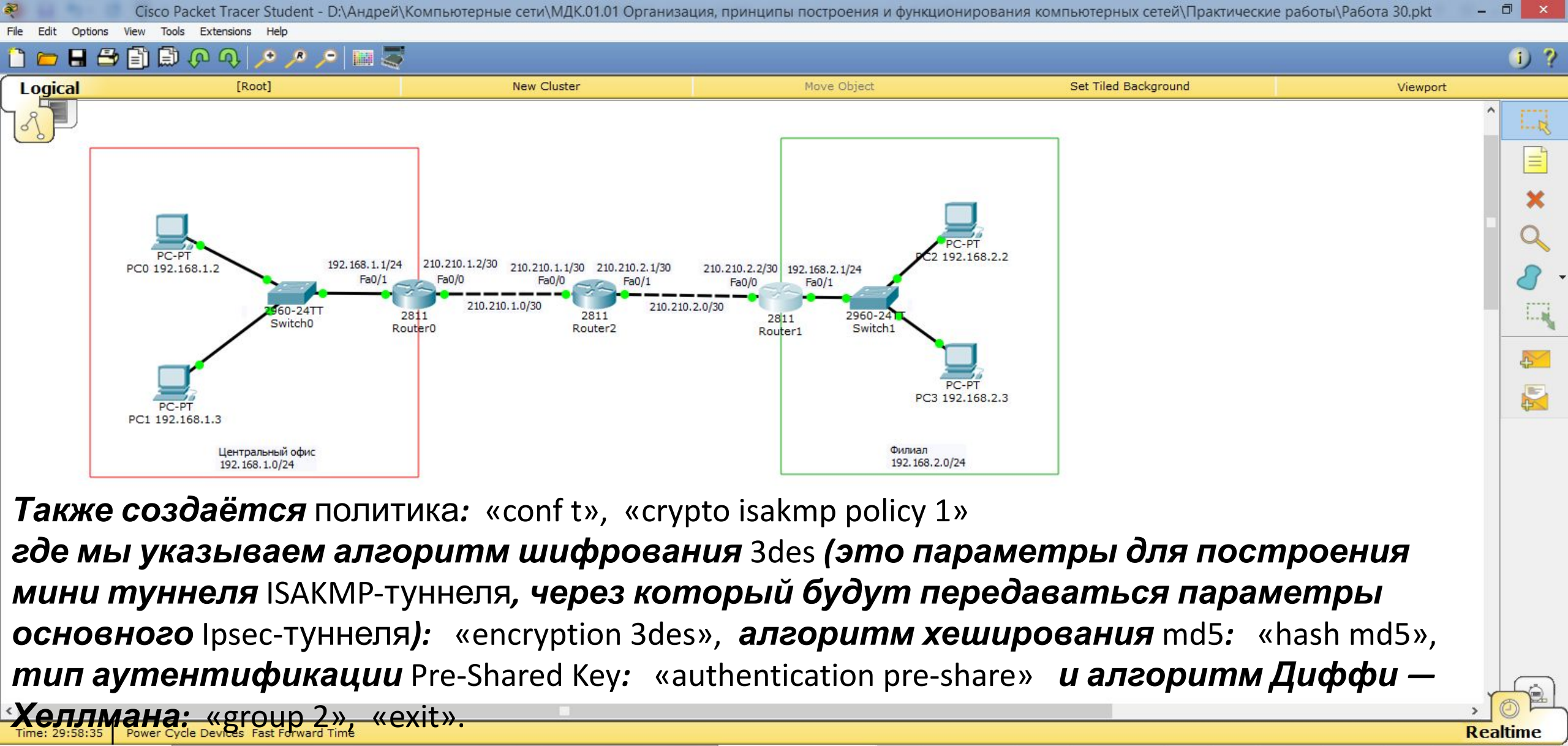
Routers | 1841 | 1941 | 2620XM | 2621XM | 2811 | 2901 | 2911 | 819 | Generic | Generic

819HGW

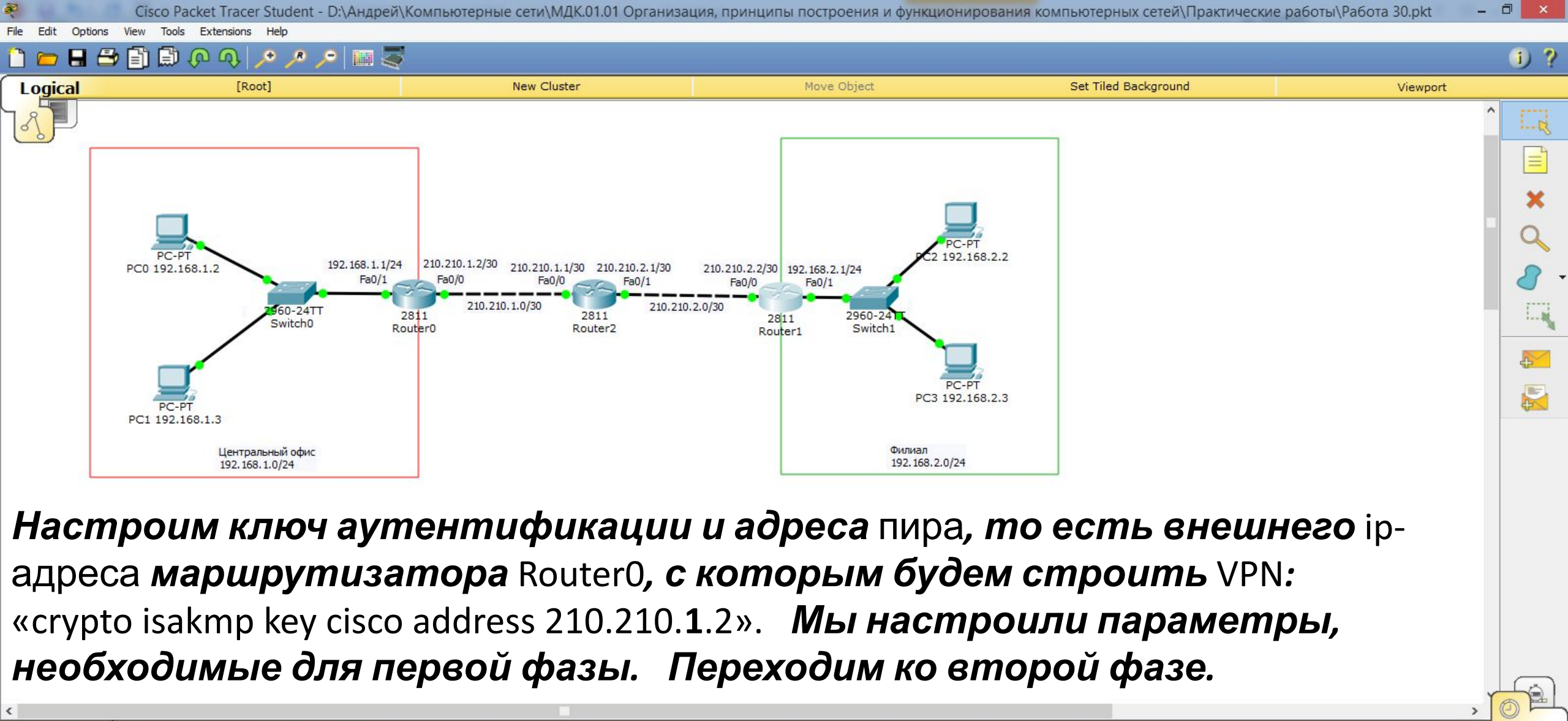
Scenario 0 | New | Delete | Toggle PDU List Window

Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Delete

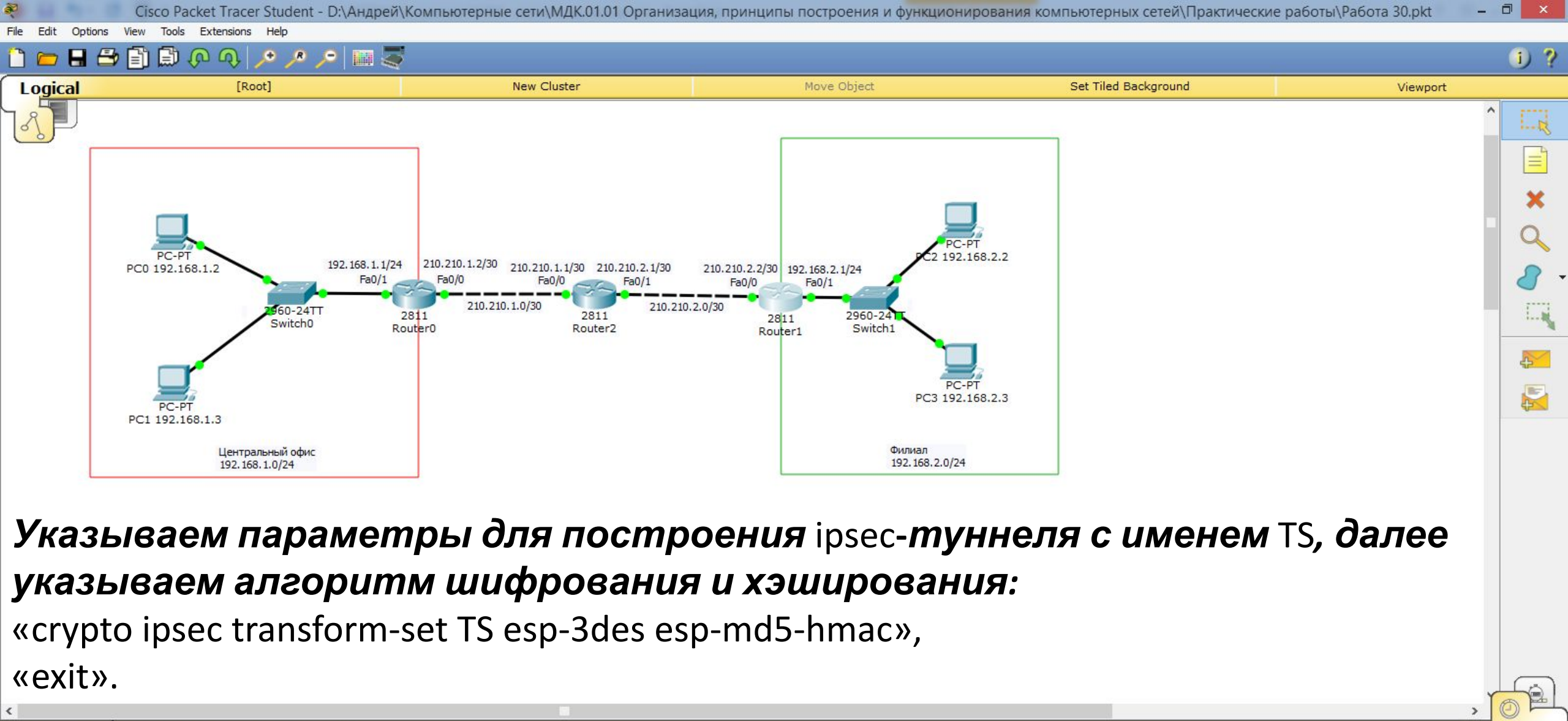
РУС 0:16 19.01.2020



Также создаётся политика***:*** «conf t», «crypto isakmp policy 1»
где мы указываем алгоритм шифрования 3des ***(это параметры для построения мини туннеля*** ISAKMP-туннеля***, через который будут передаваться параметры основного*** Ipsec-туннеля***):*** «encryption 3des», ***алгоритм хеширования*** md5***:*** «hash md5», ***тип аутентификации*** Pre-Shared Key***:*** «authentication pre-share» ***и алгоритм Диффи — Хеллмана:*** «group 2», «exit».



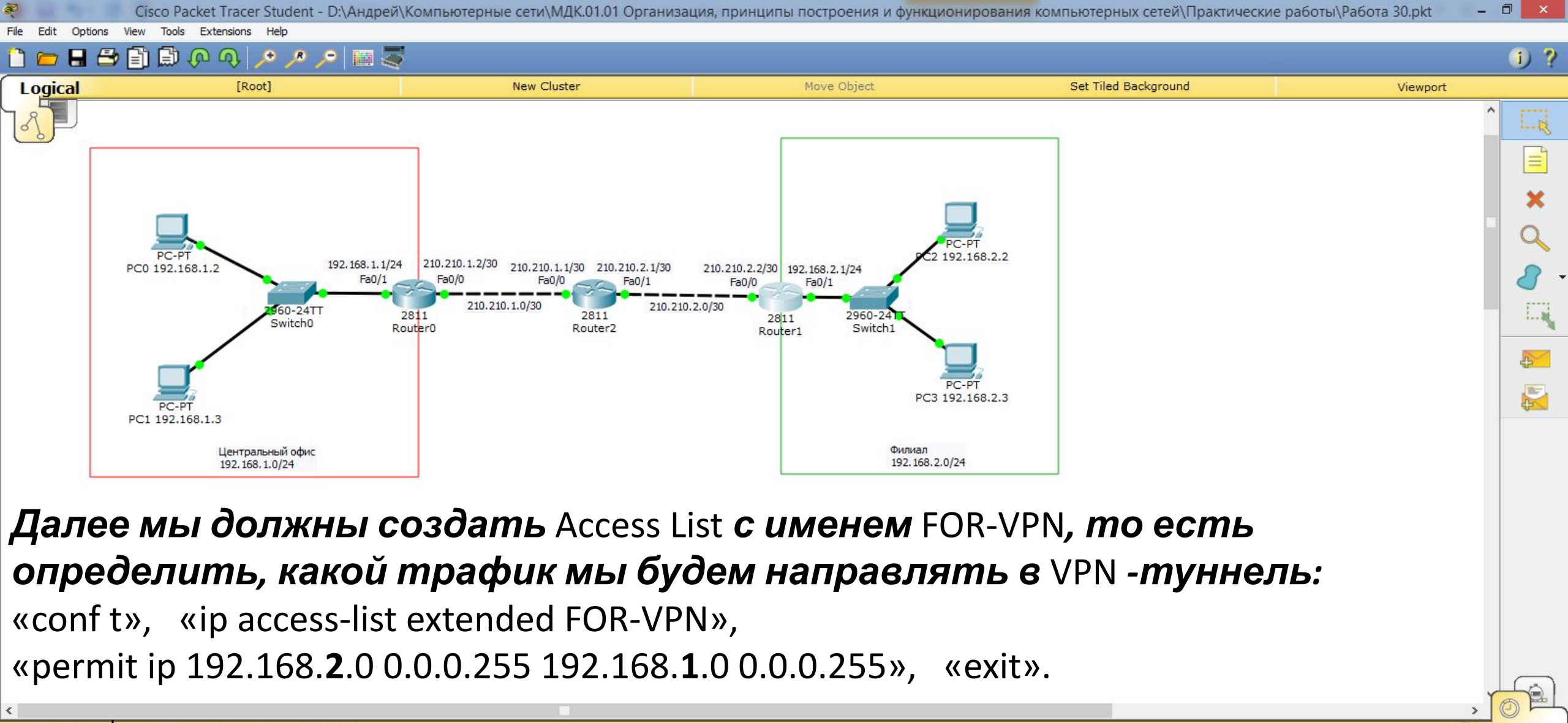
Настроим ключ аутентификации и адреса пира***, то есть внешнего*** ip-адреса ***маршрутизатора*** Router0***, с которым будем строить*** VPN***:*** «crypto isakmp key cisco address 210.210.**1**.2». ***Мы настроили параметры, необходимые для первой фазы. Переходим ко второй фазе.***



Указываем параметры для построения ipsec***-туннеля с именем*** TS***, далее указываем алгоритм шифрования и хэширования:***

«crypto ipsec transform-set TS esp-3des esp-md5-hmac»,

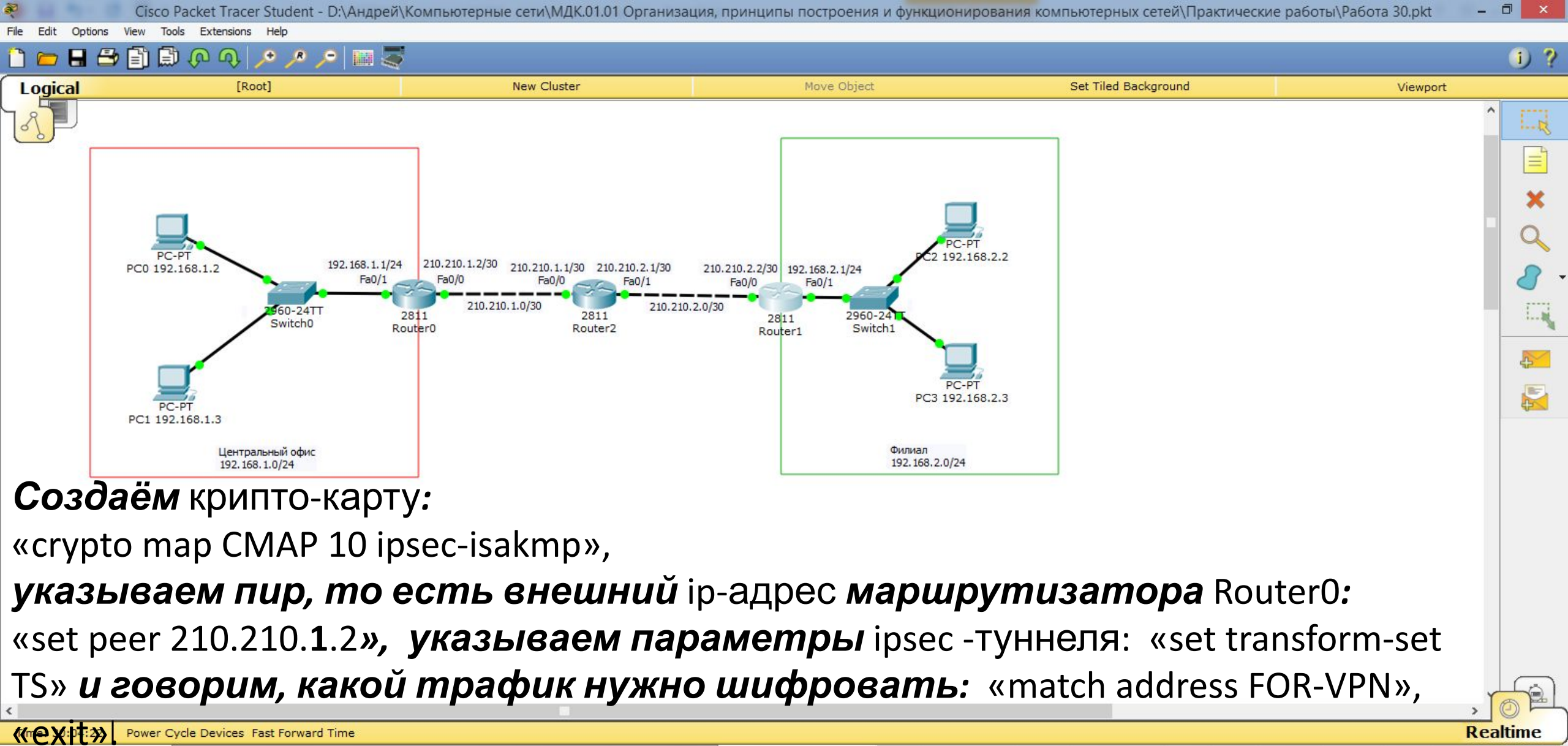
«exit».



Далее мы должны создать Access List ***с именем*** FOR-VPN***, то есть определить, какой трафик мы будем направлять в*** VPN ***-туннель:***

«conf t», «ip access-list extended FOR-VPN»,

«permit ip 192.168.**2**.0 0.0.0.255 192.168.**1**.0 0.0.0.255», «exit».

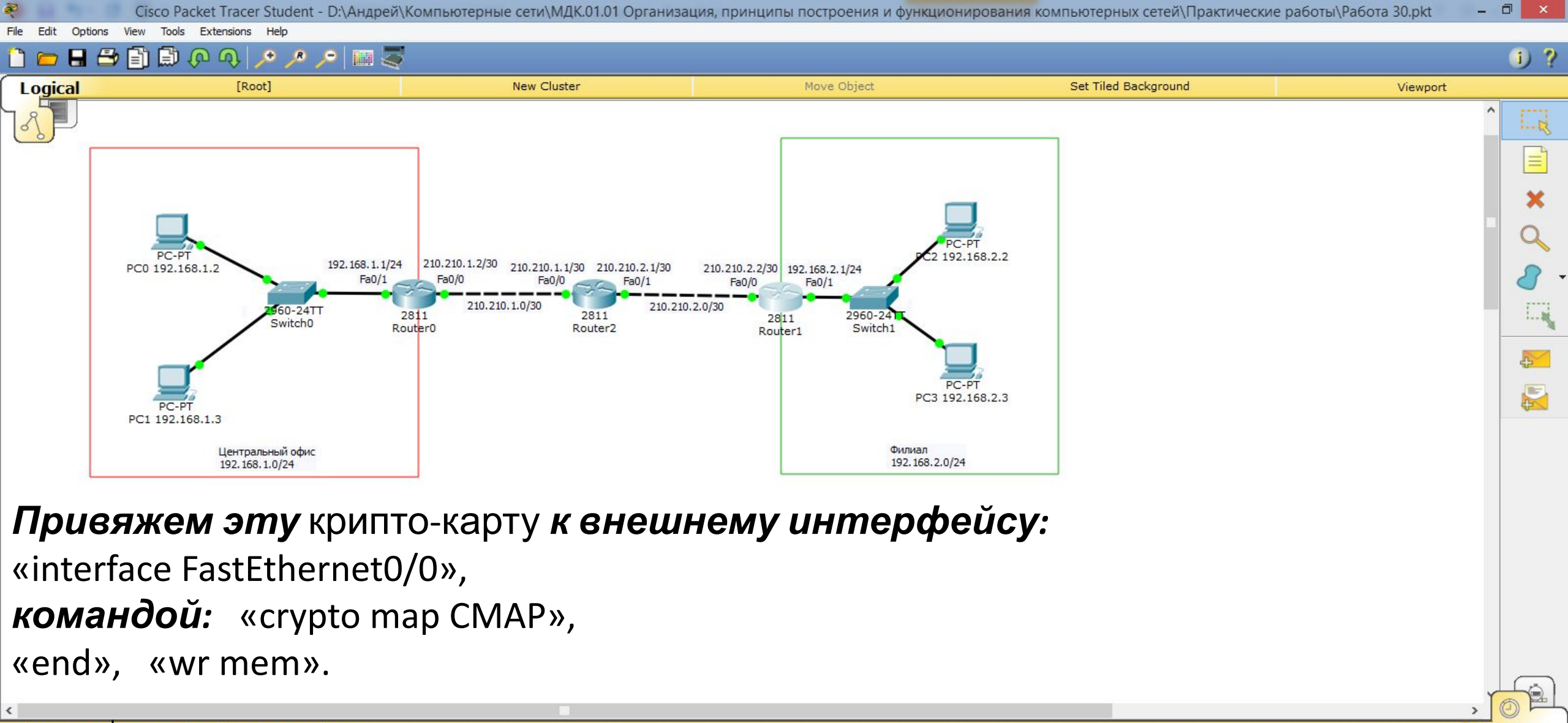


Создаём крипто-карту***:***

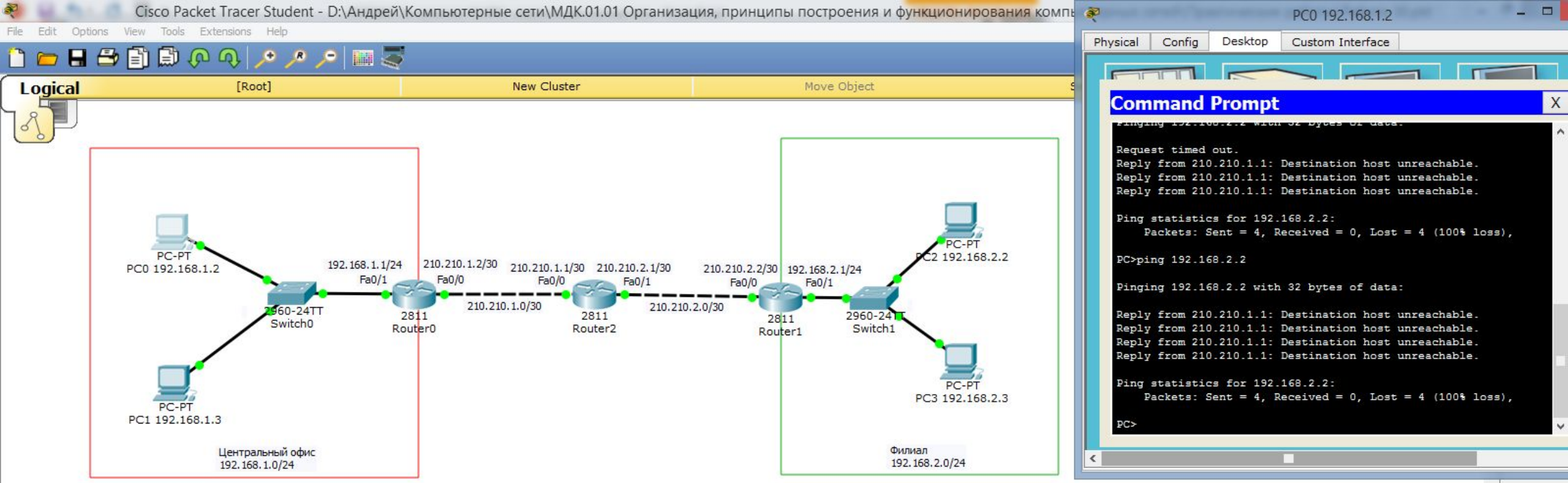
«crypto map CMAP 10 ipsec-isakmp»,

указываем пир, то есть внешний ip-адрес ***маршрутизатора*** Router0***:***

«set peer 210.210.**1**.2***»,*** ***указываем параметры*** ipsec -туннеля: «set transform-set TS» ***и говорим, какой трафик нужно шифровать:*** «match address FOR-VPN», «exit».



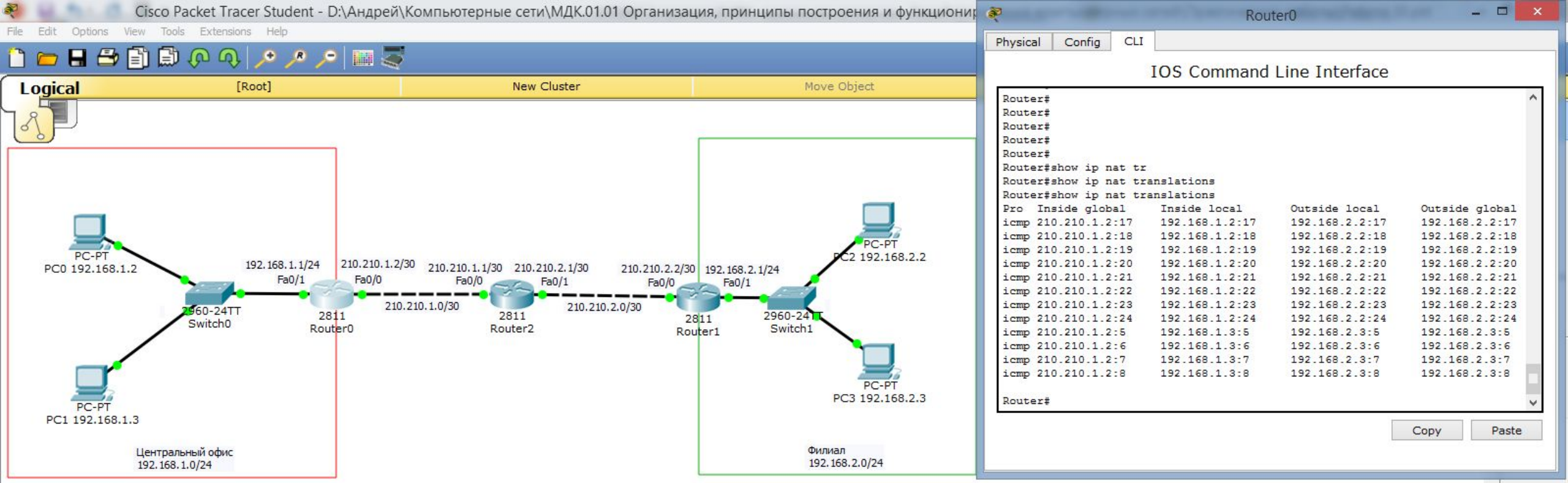
Привяжем эту крипто-карту ***к внешнему интерфейсу:***
«interface FastEthernet0/0»,
командой: «crypto map CMAP»,
«end», «wr mem».



Пробуем наш VPN***. Проверим связь одного из компьютеров*** Центрального офиса ***с компьютером*** филиала***:*** «ping 192.168.2.2».

Связи нет.

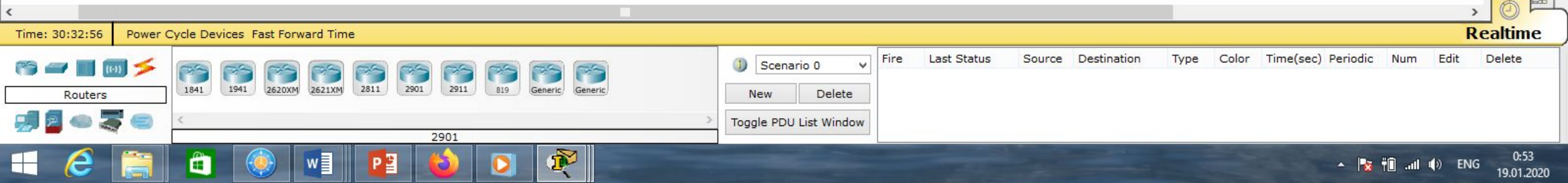
Всё дело в настройках NAT***.***

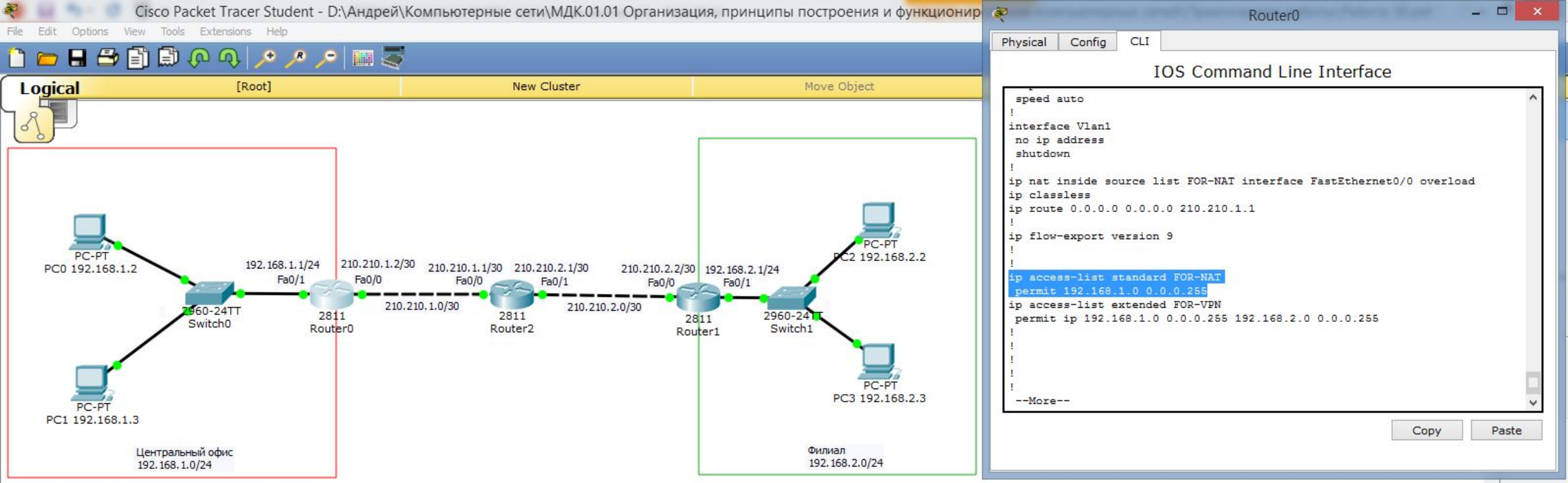


Наберём команду:

«show ip nat translations».

Наши попытки связи не попадают в VPN-тоннель***. Виной тому настройка*** NAT***. Чтобы исправить ситуацию, нужно изменить*** Access List ***для*** NAT***.***

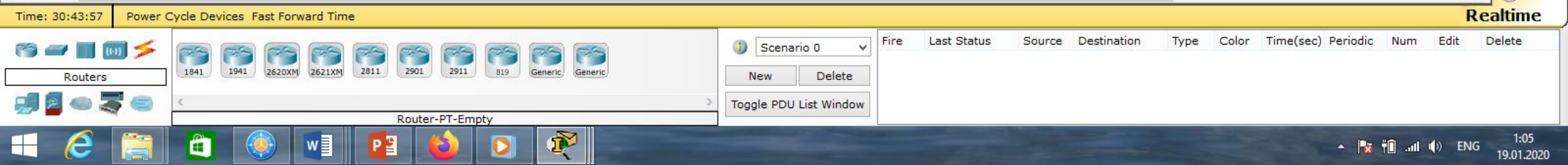


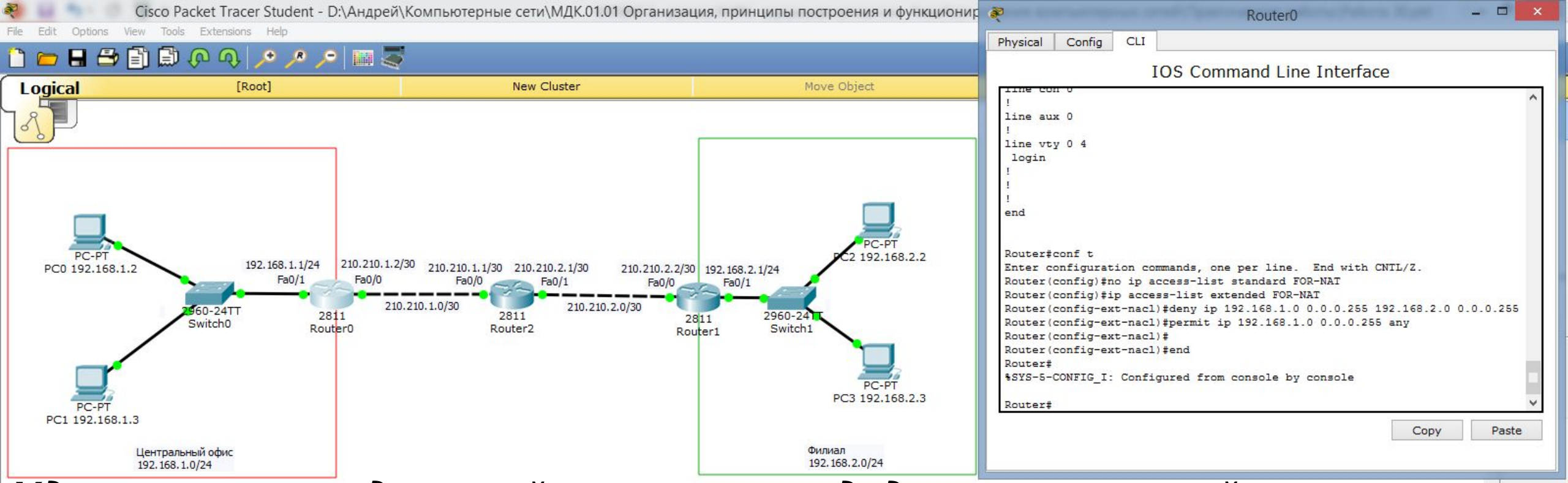


Посмотрим настройки , для этого наберём команду:

«show run».

Видим, что технология используется для всего трафика, поэтому он не попадает в VPN-тоннель***. Нужно это исправить.***





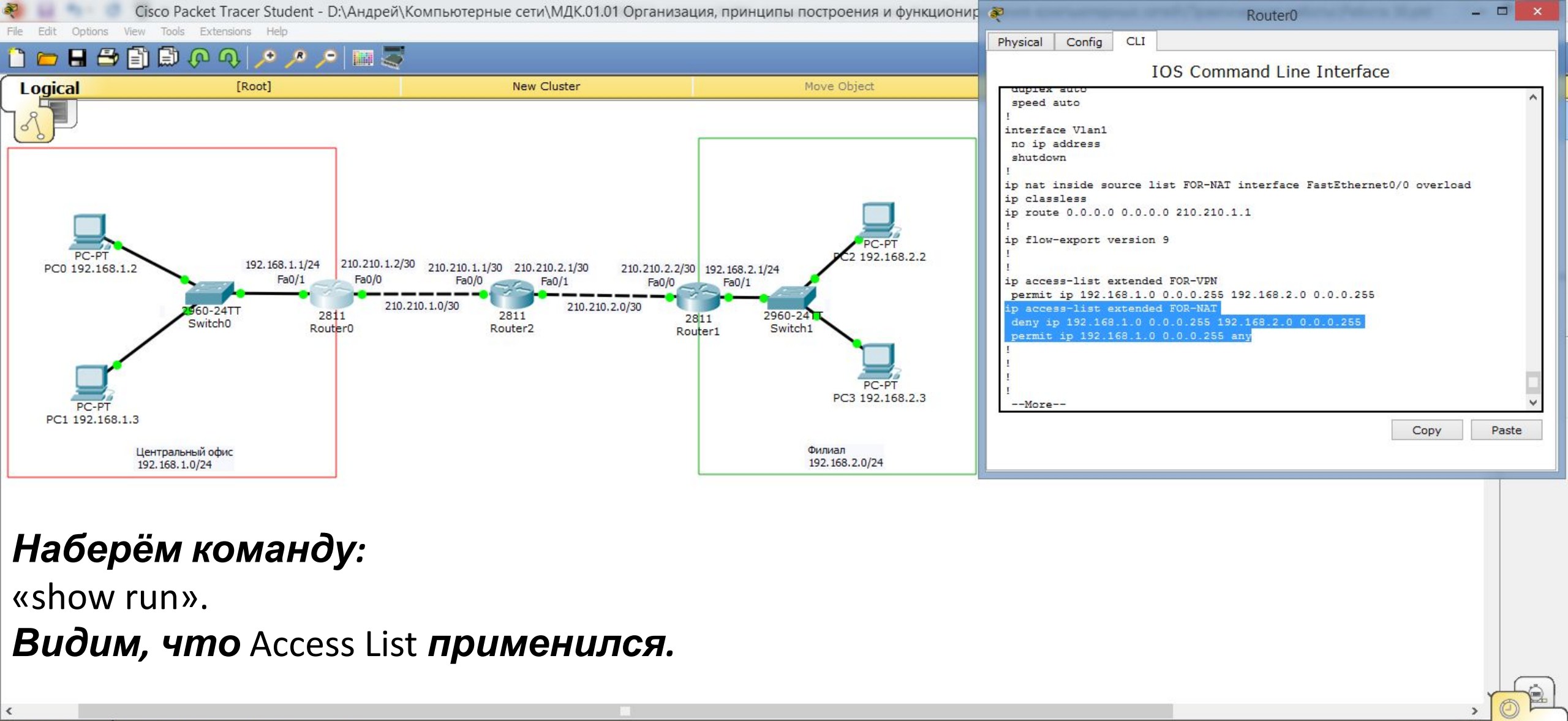
Удалим наш стандартный Access List ***и создадим расширенный*** Access List***:***

«conf t», «no ip access-list standard FOR-NAT», «ip access-list **extended** FOR-NAT».

Сначала укажем запрещённый трафик, а потом разрешённый:

«deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255»,

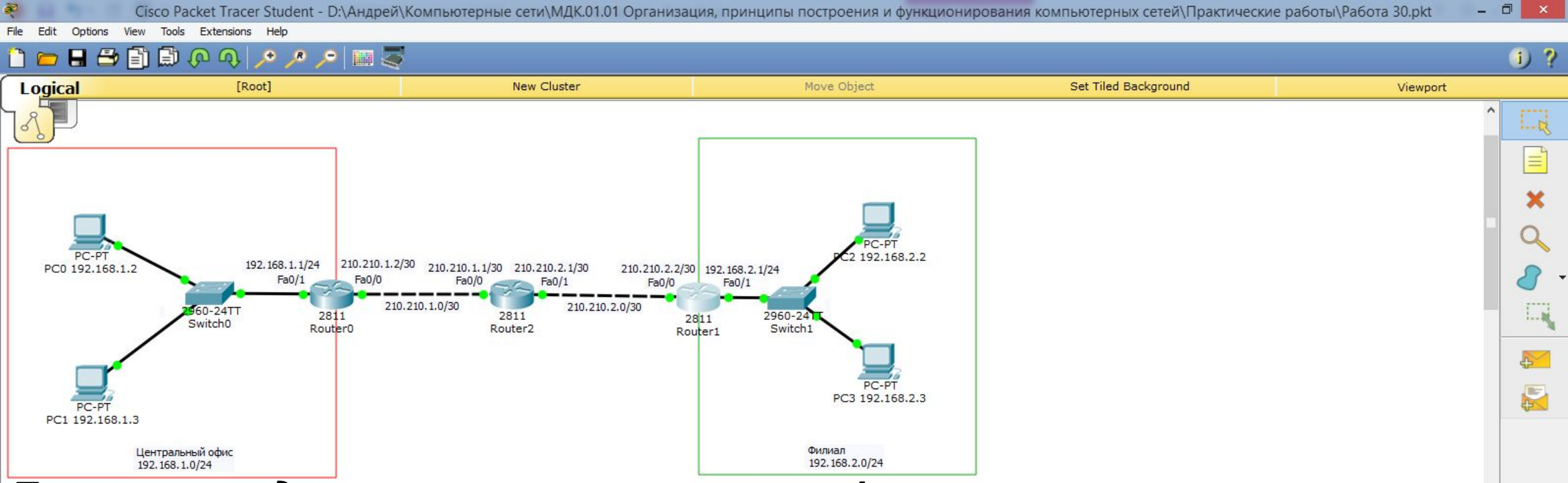
«permit ip 192.168.1.0 0.0.0.255 any», «end», «wr mem».



Наберём команду:

«show run».

Видим, что Access List ***применился.***



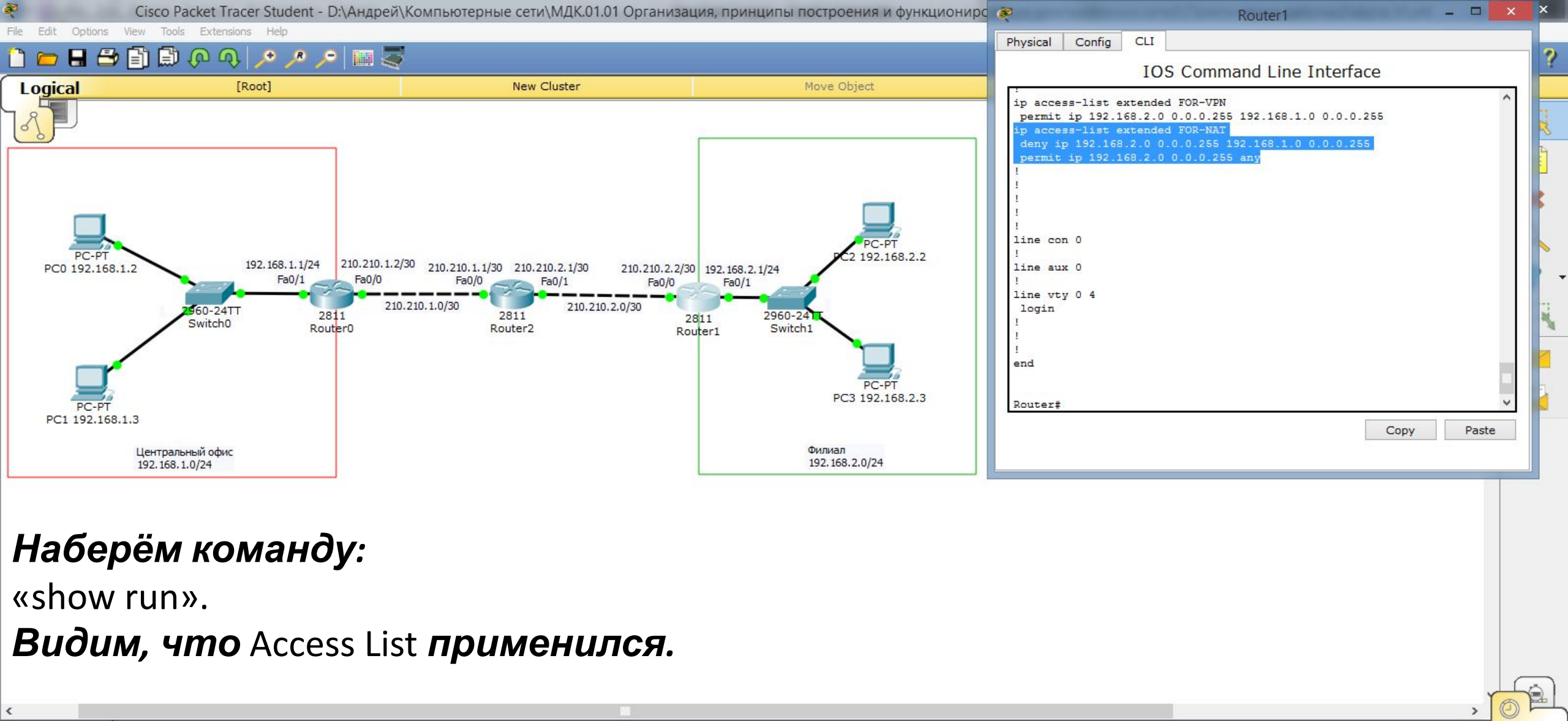
Тоже самое сделаем на маршрутизаторе филиала:

«conf t», «no ip access-list standard FOR-NAT», «ip access-list **extended** FOR-NAT».

Сначала укажем запрещённый трафик, а потом разрешённый:

«deny ip 192.168.**2**.0 0.0.0.255 192.168.**1**.0 0.0.0.255»,

«permit ip 192.168.**2**.0 0.0.0.255 any», «end», «wr mem».



Наберём команду:

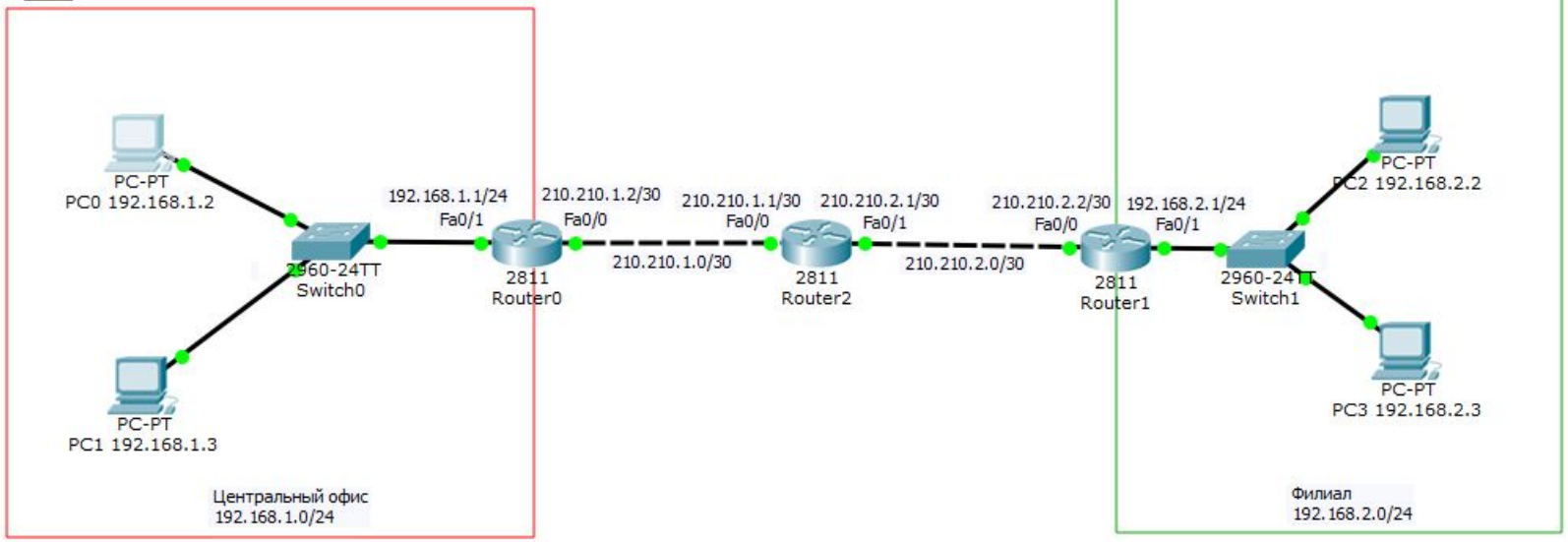
«show run».

Видим, что Access List ***применился.***

Cisco Packet Tracer Student - D:\Андрей\Компьютерные сети\МДК.01.01 Организация, принципы построения и функционирования компь

File Edit Options View Tools Extensions Help

Logical | [Root] | New Cluster | Move Object



PC0 192.168.1.2

Physical | Config | Desktop | Custom Interface

Command Prompt

```
Reply from 192.168.2.2: bytes=32 time=12ms TTL=126
Reply from 192.168.2.2: bytes=32 time=12ms 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 = 12ms, Maximum = 12ms, Average = 12ms

PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=13ms TTL=126
Reply from 192.168.2.2: bytes=32 time=13ms TTL=126
Reply from 192.168.2.2: bytes=32 time=14ms TTL=126
Reply from 192.168.2.2: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 14ms, Average = 13ms

PC>
```

Ещё раз проверим связь одного из компьютеров Центрального офиса ***с компьютером*** филиала***:*** «ping 192.168.2.2».

Связь есть!!!

Мы только что построили VPN-соединение ***между двумя подсетями.***

Time: 31:11:38 | Power Cycle Devices | Fast Forward Time | Realtime

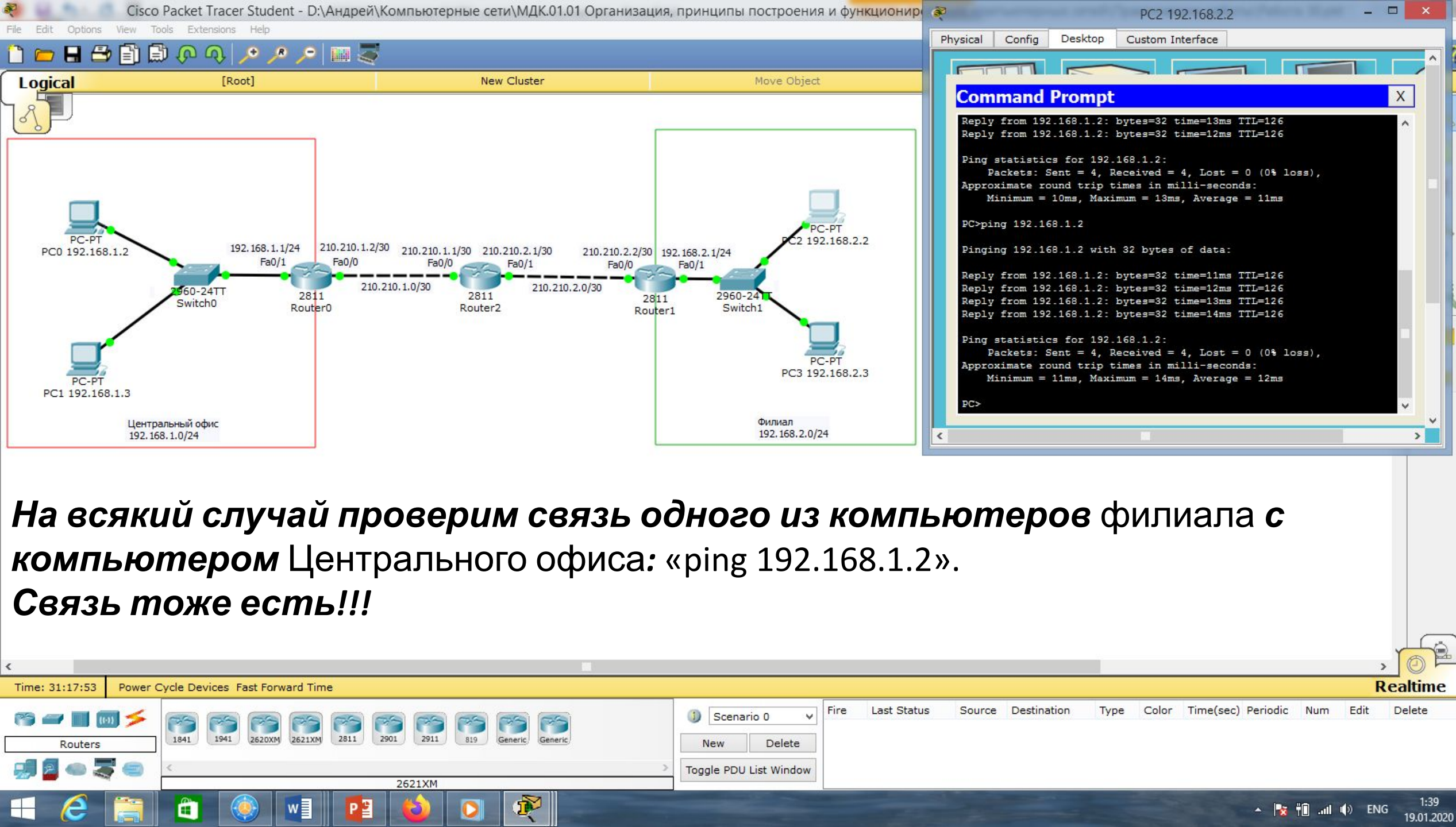
Routers | 1841 | 1941 | 2620XM | 2621XM | 2811 | 2901 | 2911 | 819 | Generic | Generic

2911

Scenario 0 | New | Delete | Toggle PDU List Window

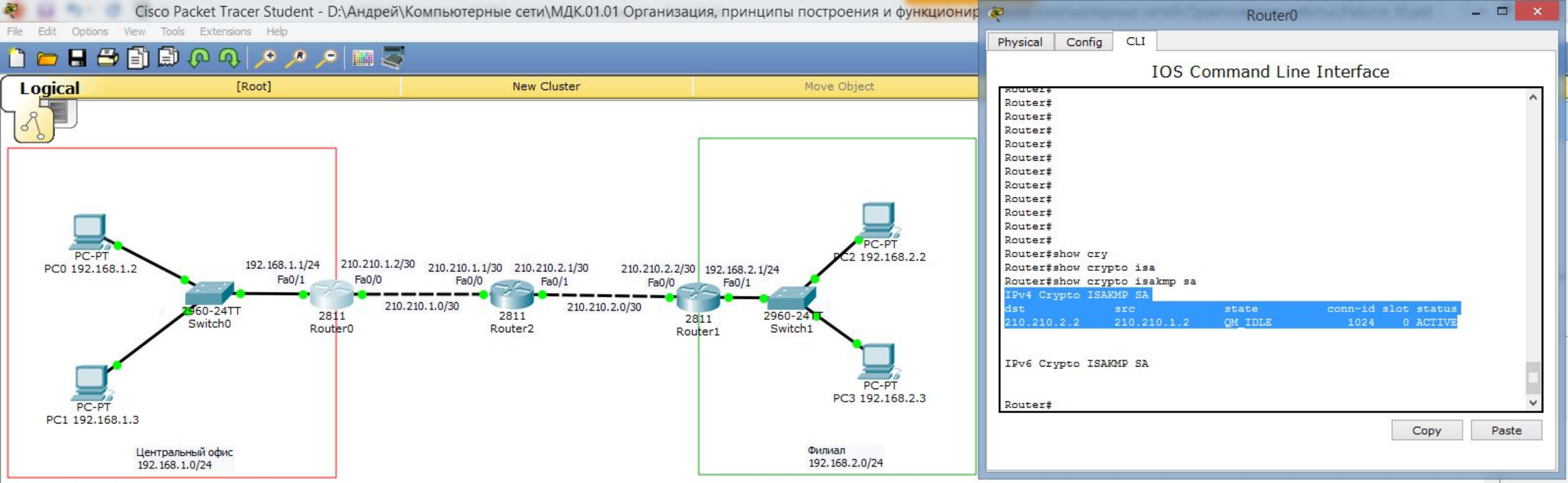
Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Delete

РУС 1:33 19.01.2020



На всякий случай проверим связь одного из компьютеров филиала ***с компьютером*** Центрального офиса***:*** «ping 192.168.1.2».

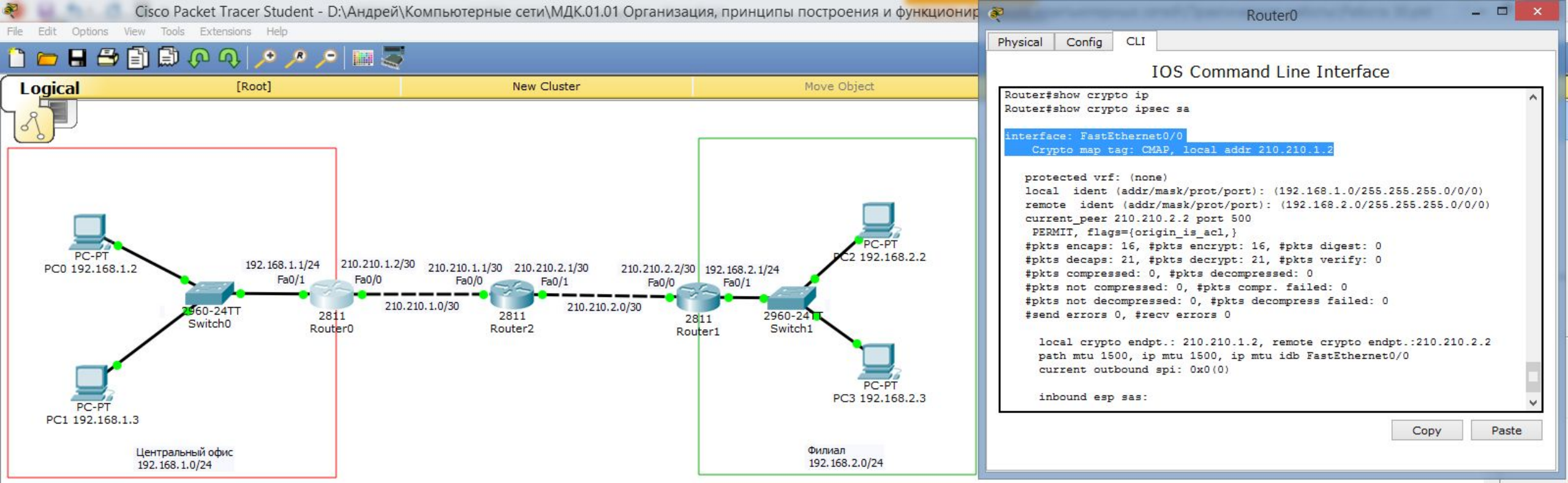
Связь тоже есть!!!



На маршрутизаторе Центрального офиса ***посмотрим, построился ли тот самый технологический туннель:***

«show crypto isakmp sa».

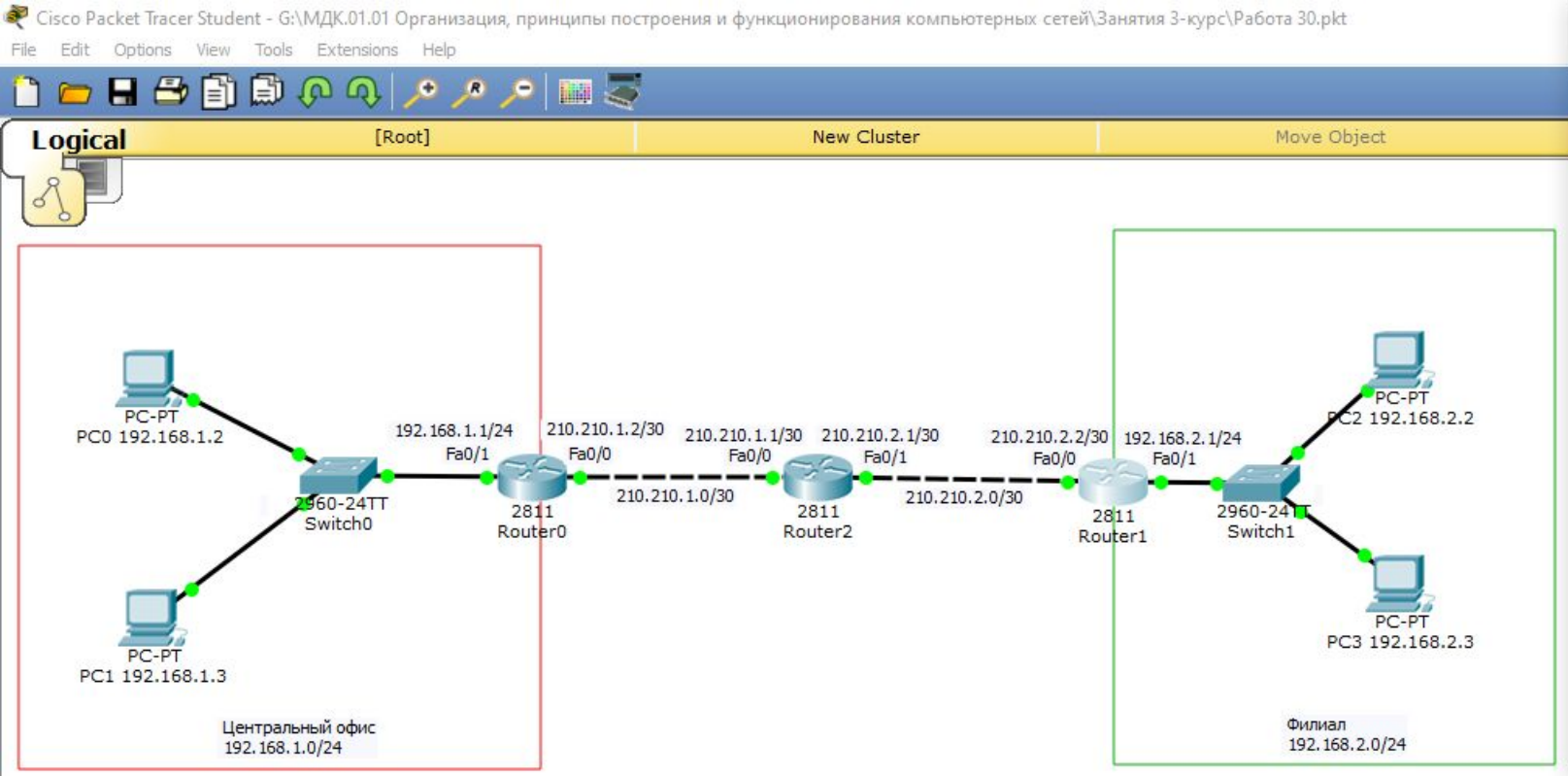
Видим, что туннель есть.

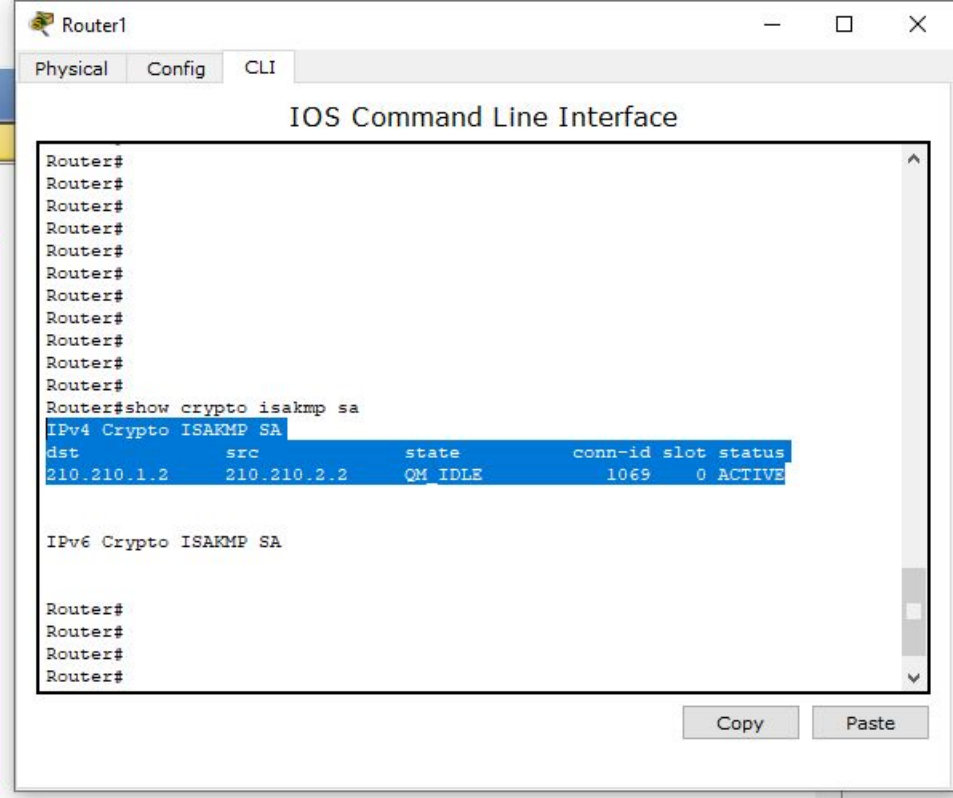


Посмотрим, построился ли ipsec-туннель***: на маршрутизаторе*** Центрального офиса***:***

«show crypto ipsec sa».

Видим, что туннель есть. Здесь мы можем найти все необходимые данные, например, сколько пакетов зашифровалось и расшифровалось.

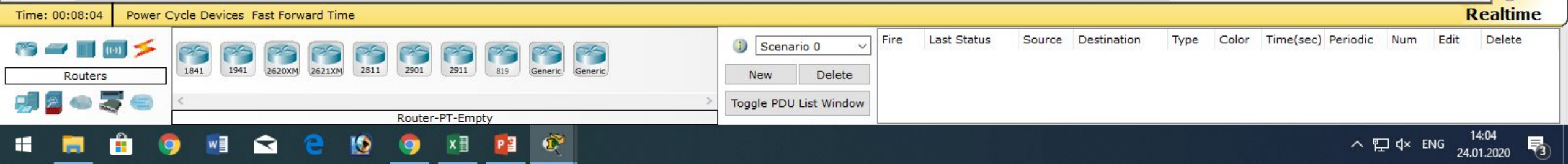


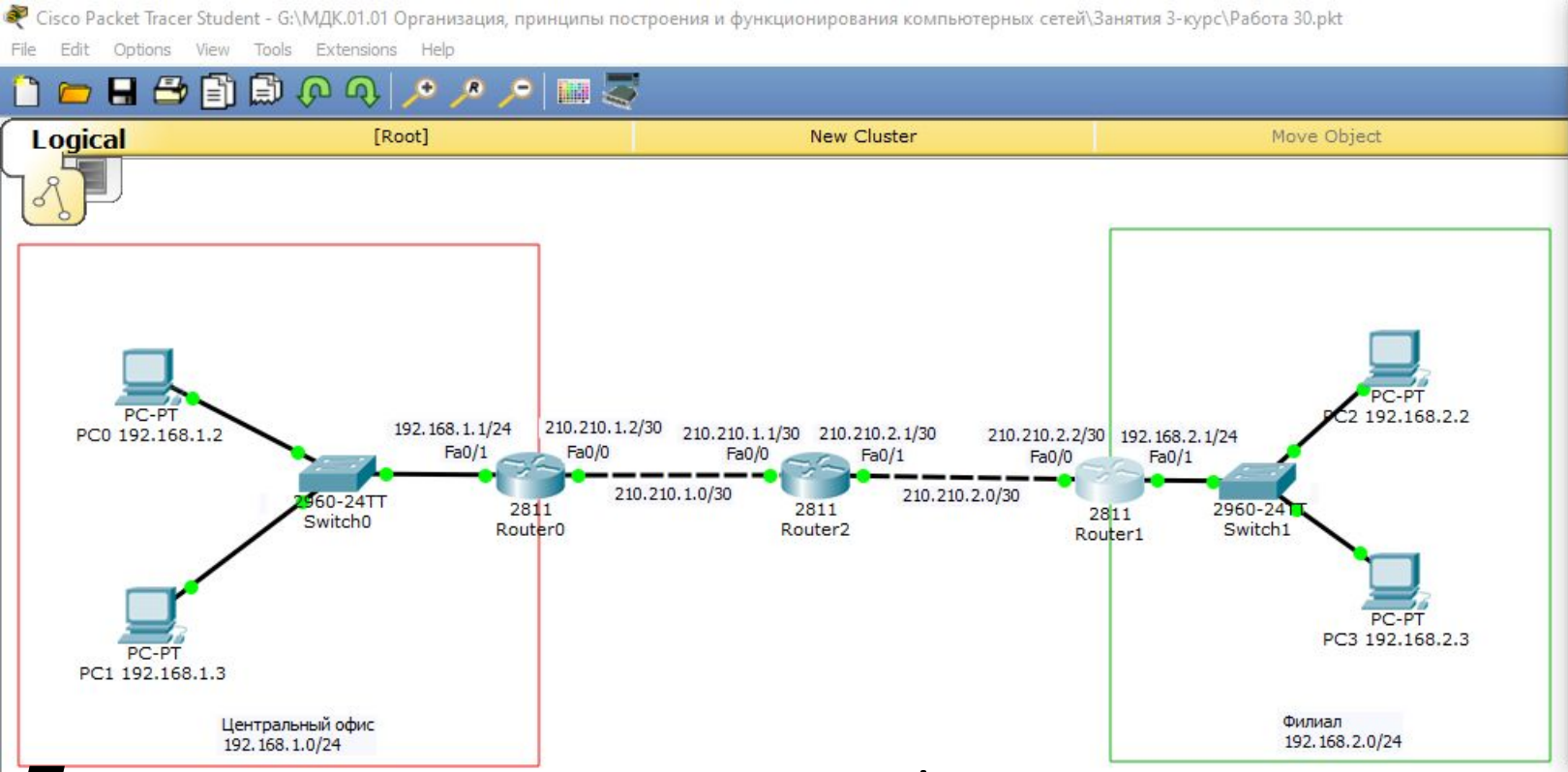


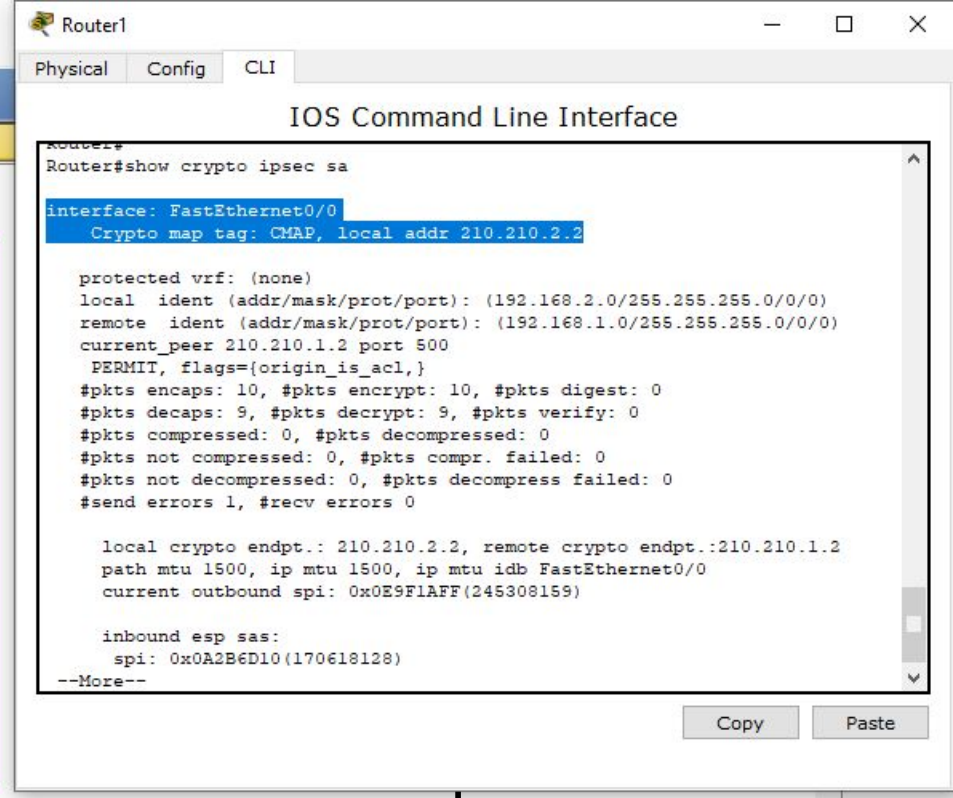
На маршрутизаторе филиала ***посмотрим, построился ли тот самый технологический туннель:***

«show crypto isakmp sa».

Видим, что туннель есть.

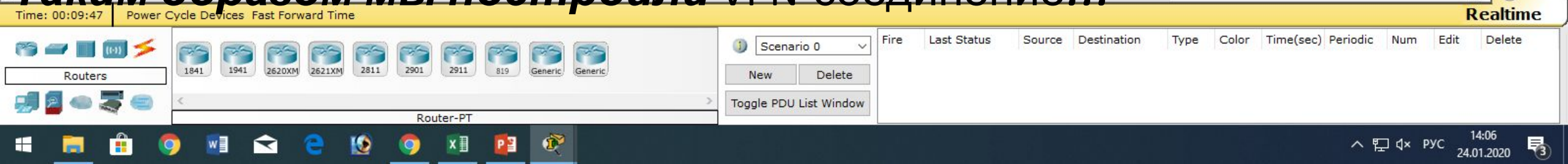






Посмотрим, построился ли ipsec-туннель ***на маршрутизаторе*** филиала***:*** «show crypto ipsec sa». ***Видим, что туннель есть. Здесь мы тоже можем найти все необходимые данные, например, сколько пакетов зашифровалось и расшифровалось***.

Таким образом мы построили VPN-соединение***!!!***



Маска подсети	Маска в двоичной системе	Префикс	Количество адресов	Обратная маска
255.255.255.255	11111111.11111111.11111111.11111111	/32	1	0.0.0.0
255.255.255.254	11111111.11111111.11111111.11111110	/31	2	0.0.0.1
255.255.255.252	11111111.11111111.11111111.11111100	/30	4	0.0.0.3
255.255.255.248	11111111.11111111.11111111.11111000	/29	8	0.0.0.7
255.255.255.240	11111111.11111111.11111111.11110000	/28	16	0.0.0.15
255.255.255.224	11111111.11111111.11111111.11100000	/27	32	0.0.0.31
255.255.255.192	11111111.11111111.11111111.11000000	/26	64	0.0.0.63
255.255.255.128	11111111.11111111.11111111.10000000	/25	128	0.0.0.127
255.255.255.0	11111111.11111111.11111111.00000000	/24	256	0.0.0.255
255.255.254.0	11111111.11111111.11111110.00000000	/23	512	0.0.1.255
255.255.252.0	11111111.11111111.11111100.00000000	/22	1024	0.0.3.255
255.255.248.0	11111111.11111111.11111000.00000000	/21	2048	0.0.7.255
255.255.240.0	11111111.11111111.11110000.00000000	/20	4096	0.0.15.255
255.255.224.0	11111111.11111111.11100000.00000000	/19	8192	0.0.31.255
255.255.192.0	11111111.11111111.11000000.00000000	/18	16384	0.0.63.255
255.255.128.0	11111111.11111111.10000000.00000000	/17	32768	0.0.127.255
255.255.0.0	11111111.11111111.00000000.00000000	/16	65536	0.0.255.255
255.254.0.0	11111111.11111110.00000000.00000000	/15	131072	0.1.255.255
255.252.0.0	11111111.11111100.00000000.00000000	/14	262144	0.3.255.255
255.248.0.0	11111111.11111000.00000000.00000000	/13	524288	0.7.255.255
255.240.0.0	11111111.11110000.00000000.00000000	/12	1048576	0.15.255.255

Список литературы:

1. Компьютерные сети. Н.В. Максимов, И.И. Попов, 4-е издание, переработанное и дополненное, «Форум», Москва, 2010.
2. Компьютерные сети. Принципы, технологии, протоколы, В. Олифер, Н. Олифер (5-е издание), «Питер», Москва, Санк-Петербург, 2016.
3. Компьютерные сети. Э. Таненбаум, 4-е издание, «Питер», Москва, Санк-Петербург, 2003.

Список ссылок:

http://blog.netskills.ru/2014/03/firewall-vs-router.html

https://drive.google.com/file/d/0B-5kZl7ixcSKS0ZlUHZ5WnhWeVk/view

Спасибо за внимание!

Преподаватель: Солодухин Андрей Геннадьевич

Электронная почта: asoloduhin@kait20.ru