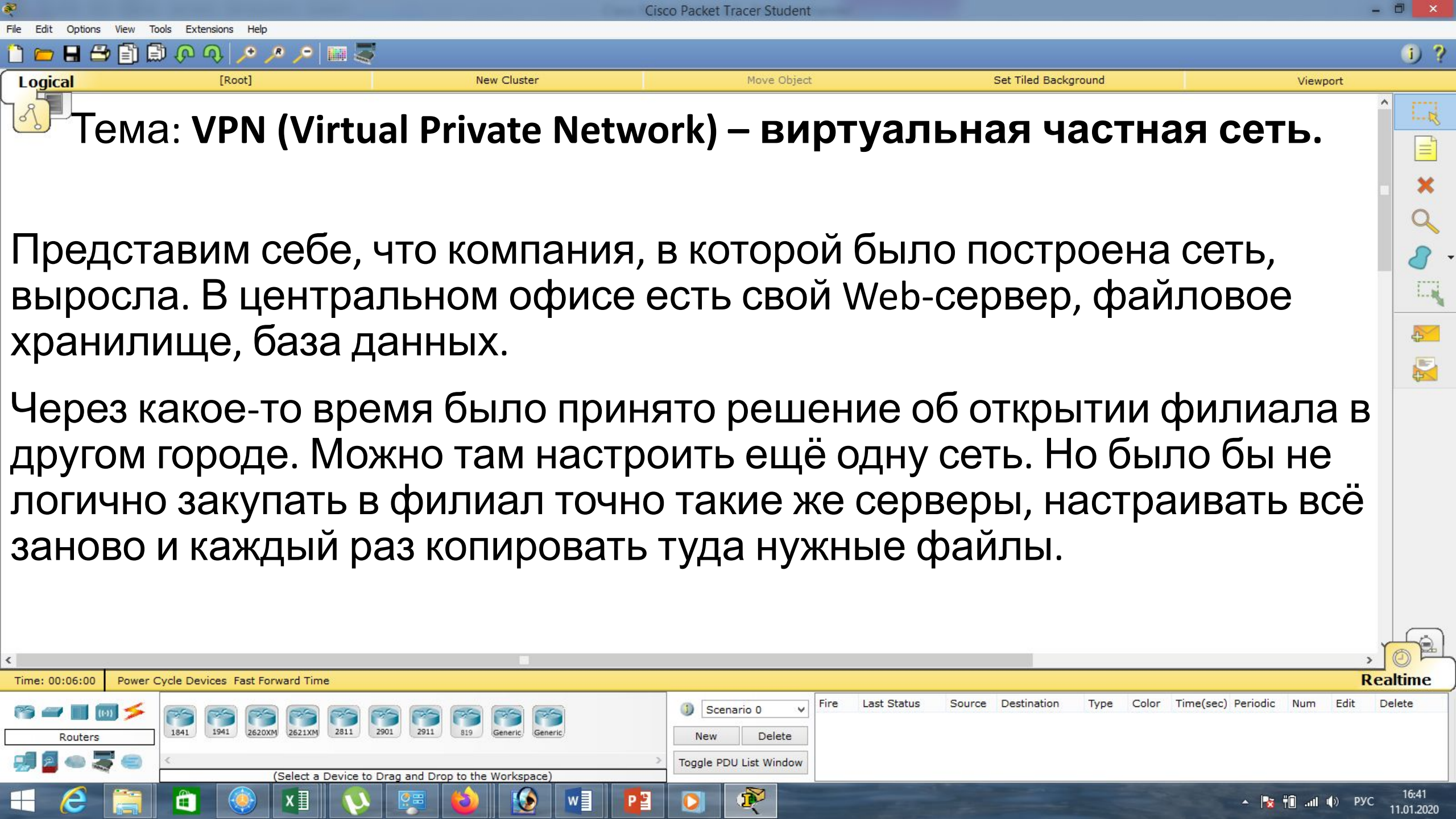


МДК.01.01
Организация, принципы
построения и функционирования
компьютерных сетей
3-курс

Практические занятия

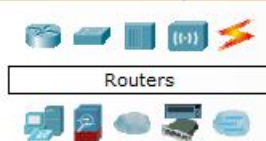
Занятие 16



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.



Routers



(Select a Device to Drag and Drop to the Workspace)

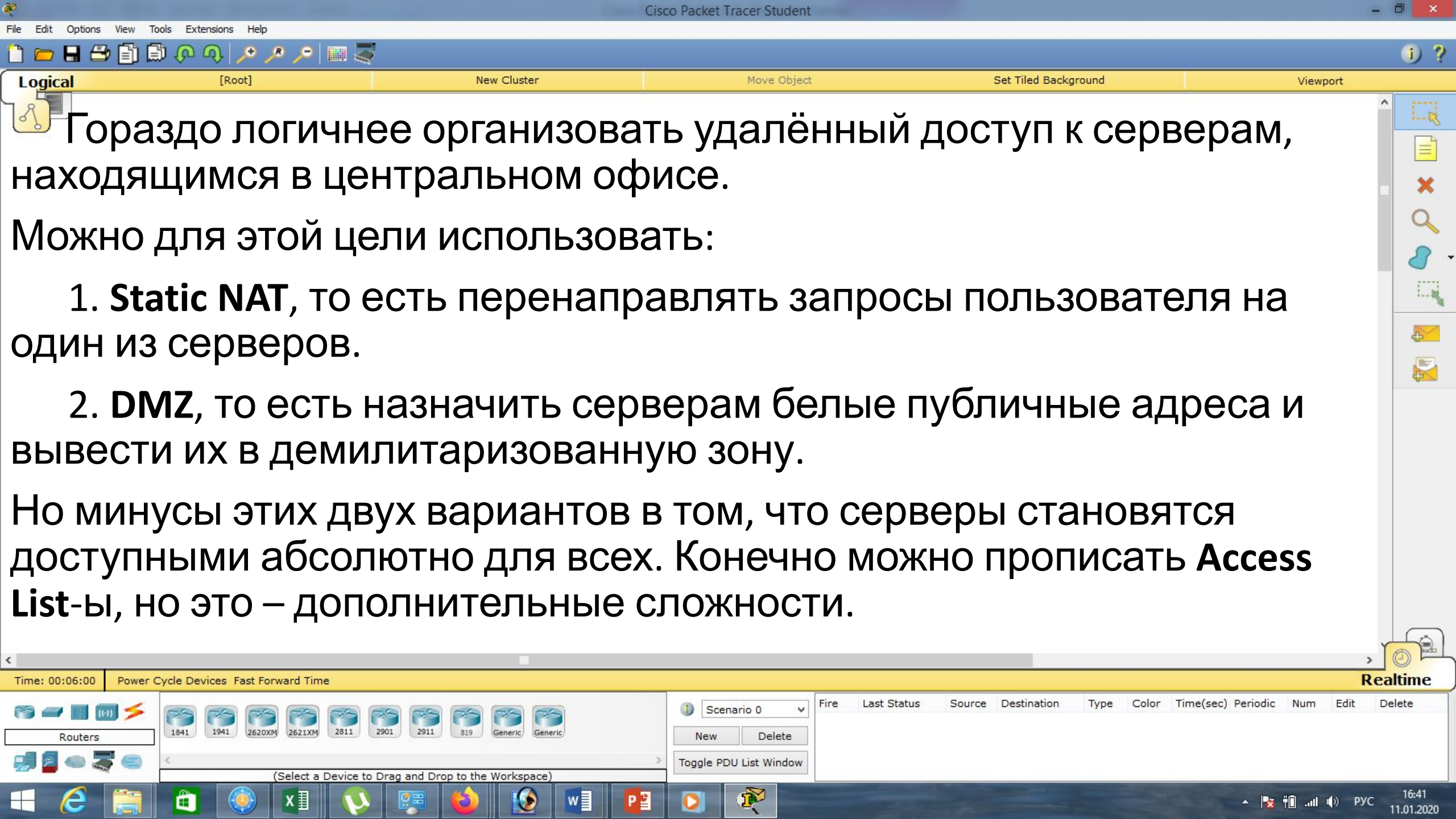
Scenario 0

New Delete

Toggle PDU List Window

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





Гораздо логичнее организовать удалённый доступ к серверам, находящимся в центральном офисе.

Можно для этой цели использовать:

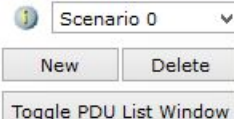
1. **Static NAT**, то есть перенаправлять запросы пользователя на один из серверов.

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.

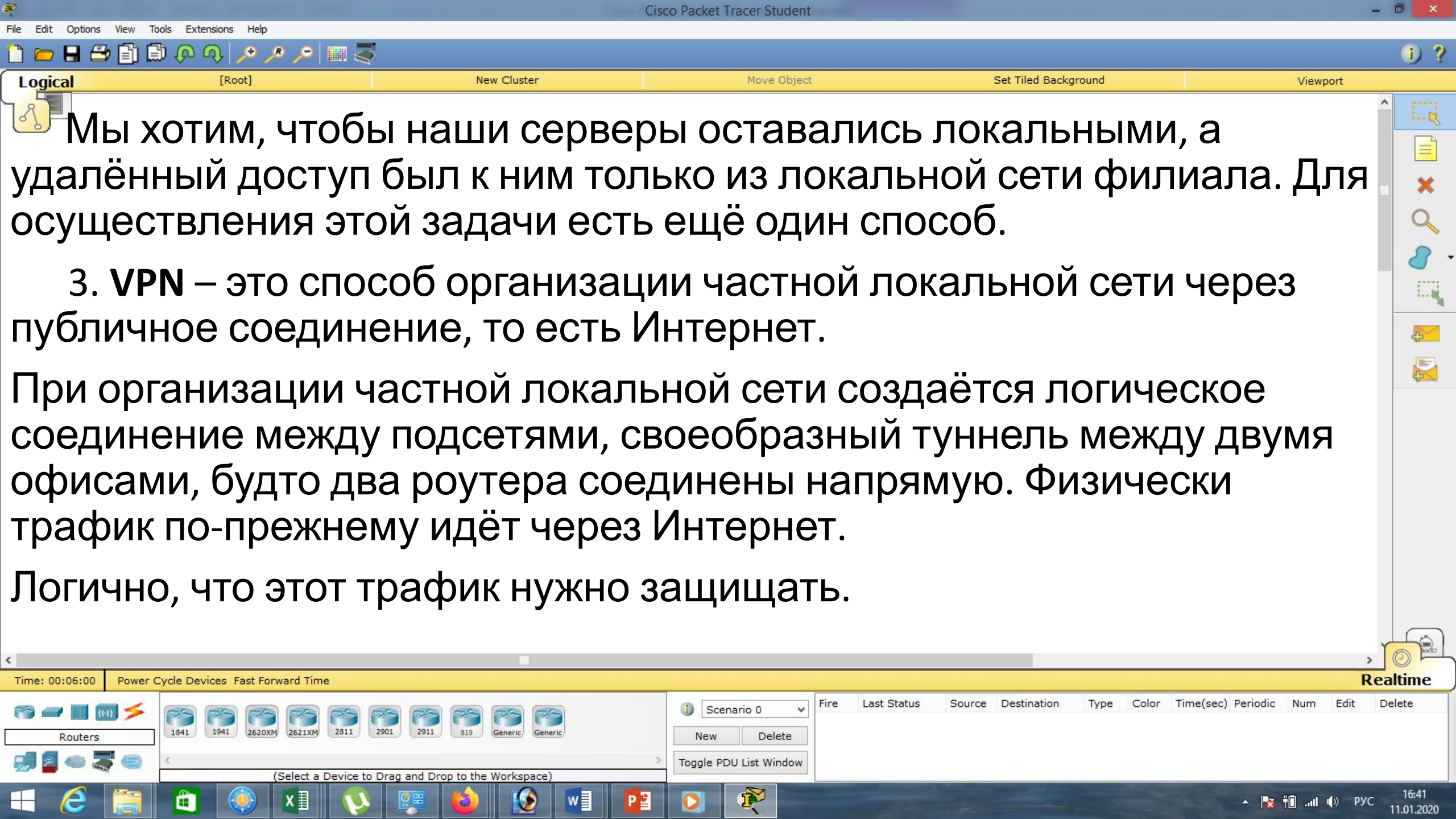


(Select a Device to Drag and Drop to the Workspace)



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





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.

FileEditOptionsViewToolsExtensionsHelp

Logical

[Root]

New Cluster

Move Object

Set Tiled Background

Viewport

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.

Time: 00:06:00Power Cycle DevicesFast Forward Time

Routers

184119412620XM2621XM281129012911819GenericGeneric

(Select a Device to Drag and Drop to the Workspace)

Scenario 0

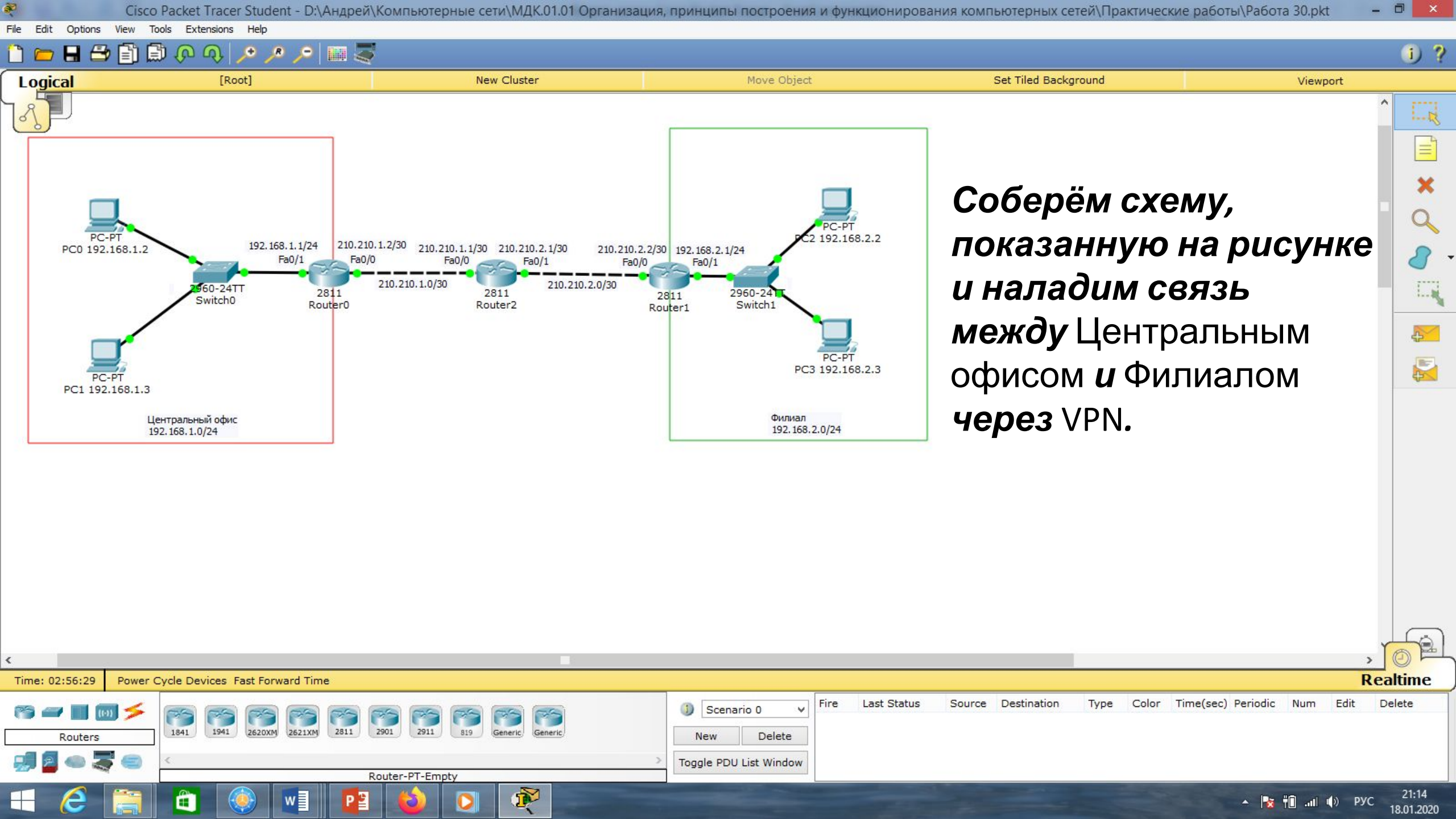
NewDelete

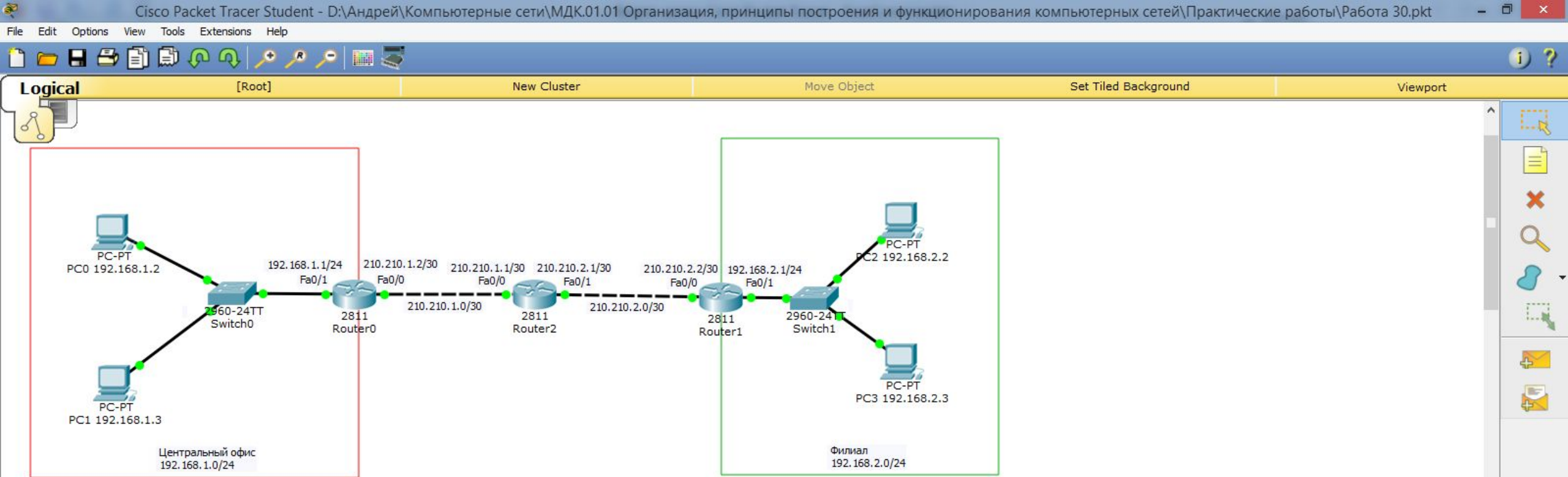
Toggle PDU List Window

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

WindowsTaskbar

16:4111.01.2020





**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».

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

Realtime

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

Router-PT-Empty

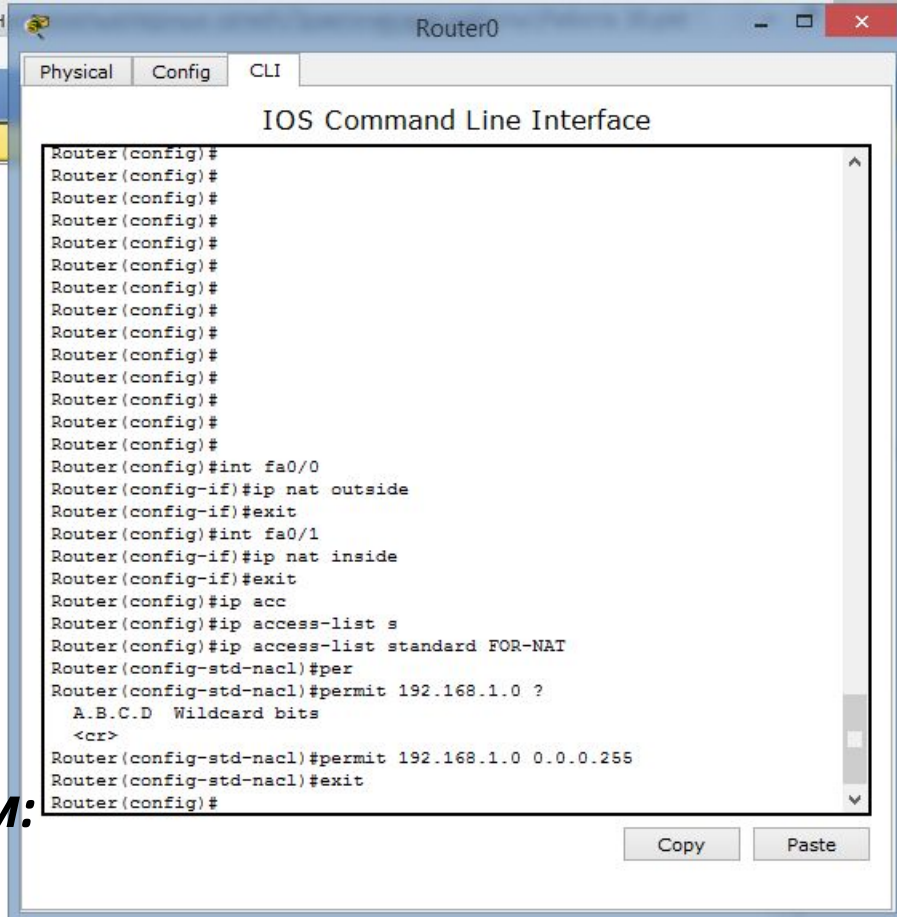
Scenario 0

New Delete

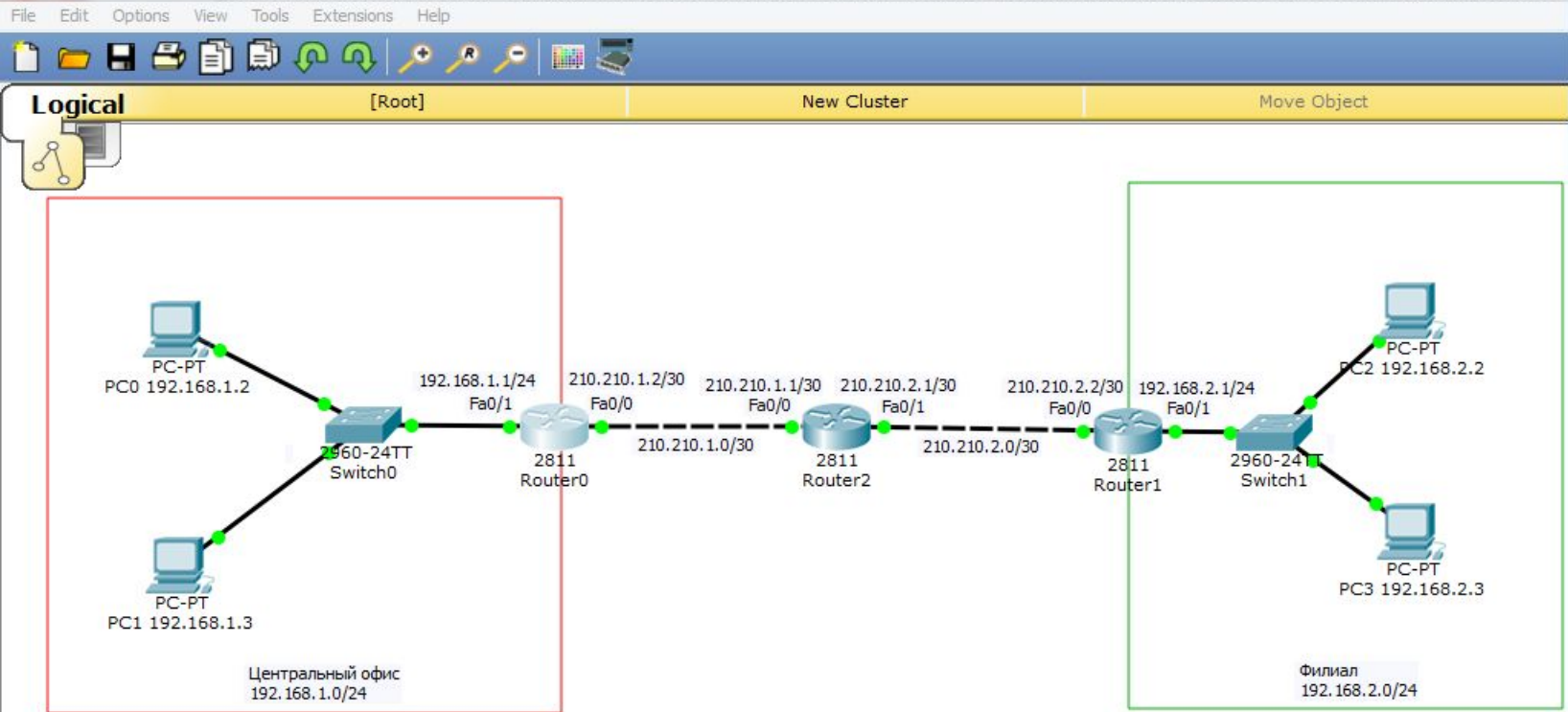
Toggle PDU List Window

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

Windows taskbar: 21:14 18.01.2020



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



Router0

Physical Config CLI

IOS Command Line Interface

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip nat ins
Router(config)#ip nat inside sor
Router(config)#ip nat inside sou
Router(config)#ip nat inside source list FOR-NAT int
Router(config)#ip nat inside source list FOR-NAT interface fa0/0 ov
Router(config)#ip nat inside source list FOR-NAT interface fa0/0 overload
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

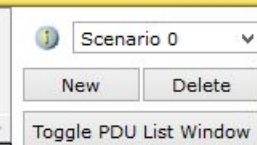
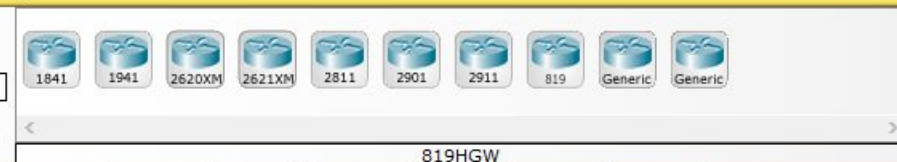
Router#wr mem
Building configuration...
[OK]
Router#
```

Copy Paste

Завершающая длинная команда:

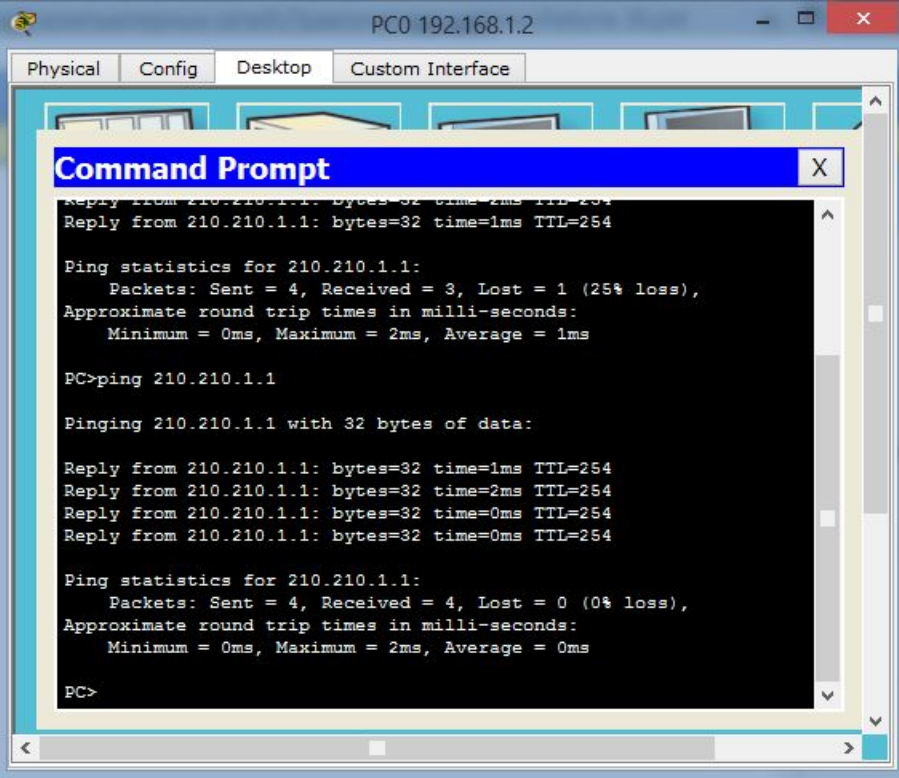
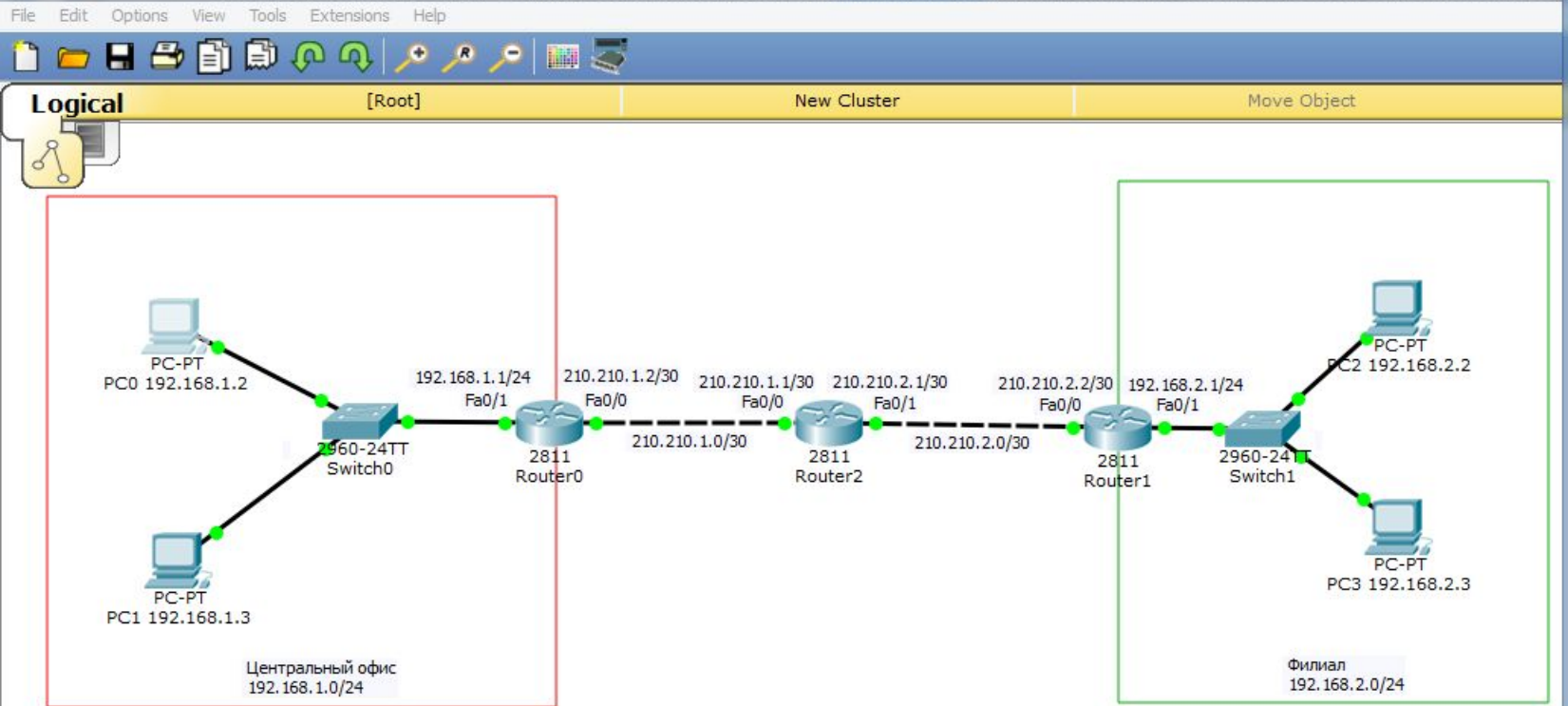
«ip nat inside source list FOR-NAT interface fa0/0 overload»,
«end»,
«wr mem».

Time: 03:36:50 Power Cycle Devices Fast Forward Time

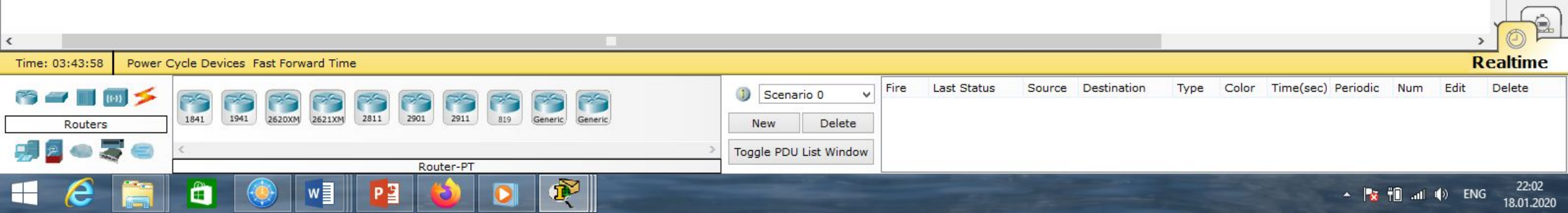


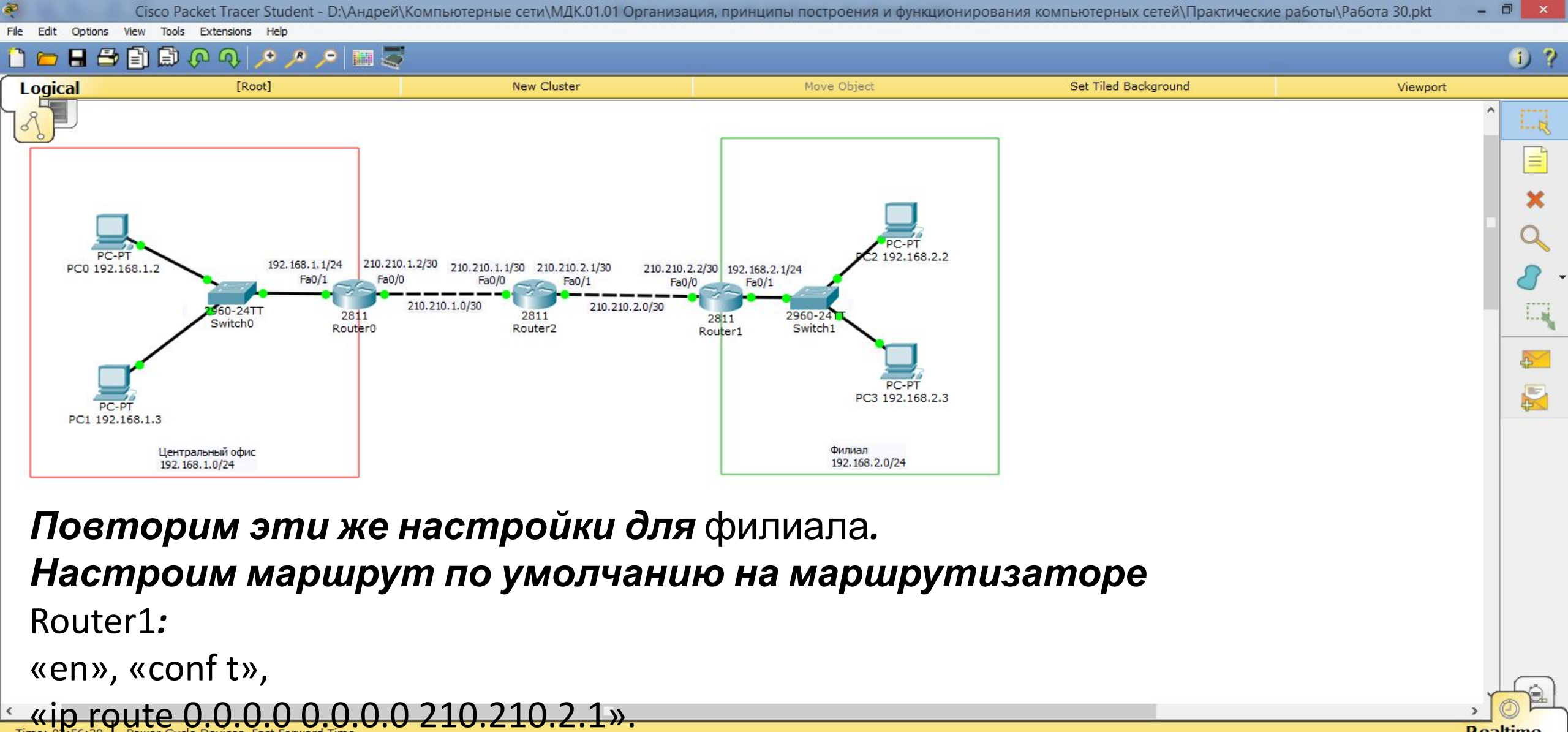
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete





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».



Logical

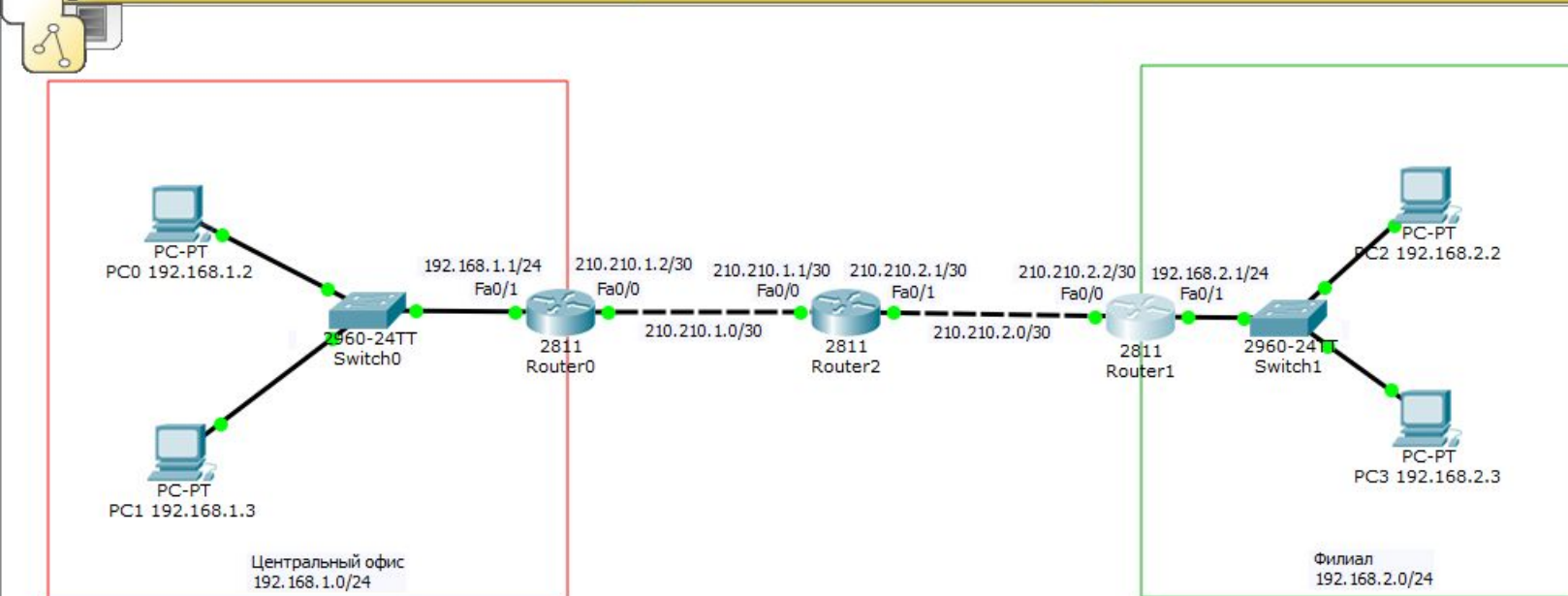
[Root]

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



819HGW

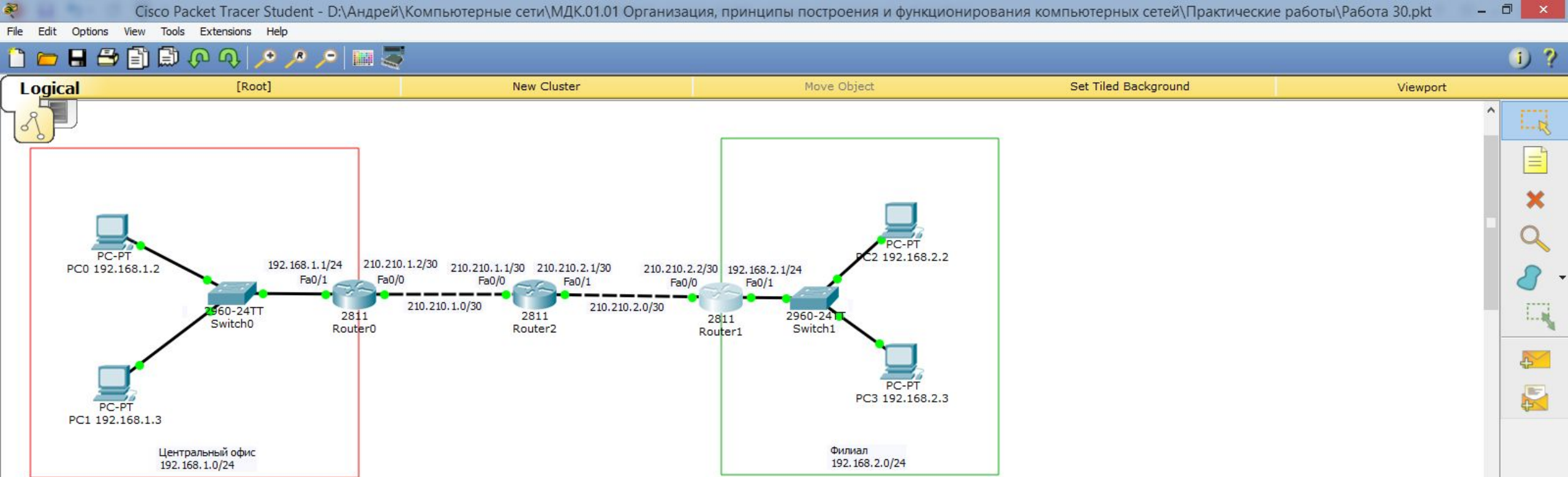
Scenario 0

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





Завершающая длинная команда:

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

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

Realtime

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
Delete Scenario and All PDUs (Ctrl+Shift+D)										

Scenario 0

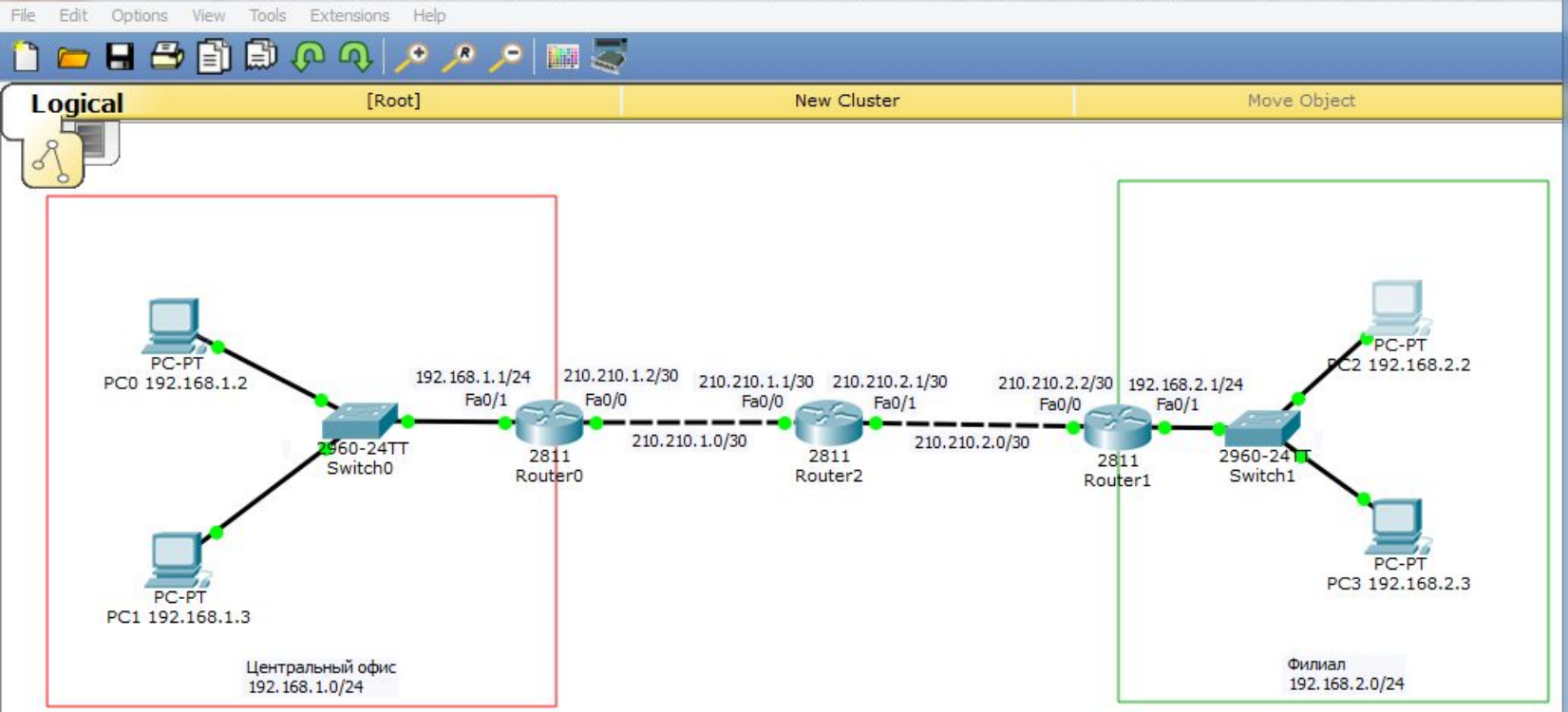
New Delete

Toggle PDU L

819HGW

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

Windows taskbar: 22:13 18.01.2020



PC2 192.168.2.2

Physical Config Desktop Custom Interface

Command Prompt

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

Pinging 210.210.2.1 with 32 bytes of data:

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

Ping statistics for 210.210.2.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```

Проверим связь компьютера с маршрутизатором провайдера Router2:
«ping 210.210.2.1».
Связь есть!!!

Time: 03:57:47 Power Cycle Devices Fast Forward Time

Scenario 0

New Delete

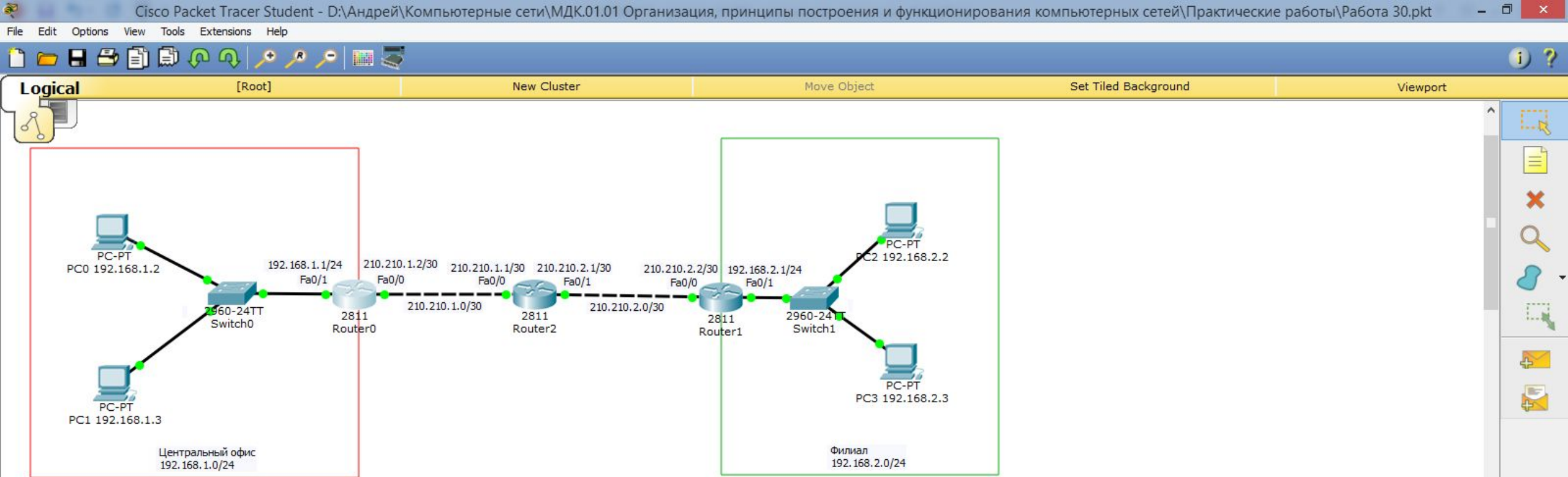
Toggle PDU List Window

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

819HWG

Realtime

22:16 18.01.2020



Теперь настроим VPN.
Начнём с маршрутизатора центрального офиса Router0.
Для начала нам необходимо настроить первую фазу.

Time: 04:26:45 Power Cycle Devices Fast Forward Time

Realtime

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

Scenario 0

New Delete

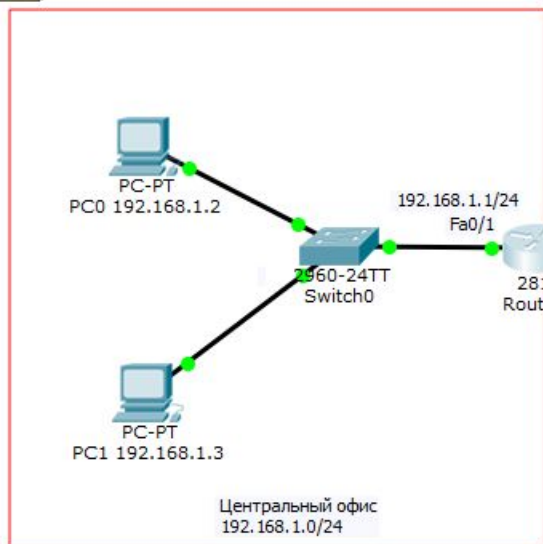
Toggle PDU List Window

819HGW

Windows taskbar: 22:45 18.01.2020



Logical [Root] New Cluster Move Object



Router0

Physical Config CLI

IOS Command Line Interface

```

Router(config)#crypto isakmp policy 1
Router(config-isakmp)#
Router(config-isakmp)#encr
Router(config-isakmp)#encryption ?
  3des  Three key triple DES
  aes   AES - Advanced Encryption Standard
  des   DES - Data Encryption Standard (56 bit keys).
Router(config-isakmp)#encryption 3
Router(config-isakmp)#encryption 3des ?
<cr>
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash ?
  md5  Message Digest 5
  sha  Secure Hash Standard
Router(config-isakmp)#hash m
Router(config-isakmp)#hash md5
Router(config-isakmp)#au
Router(config-isakmp)#authentication ?
  pre-share  Pre-Shared Key
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group ?
  1  Diffie-Hellman group 1
  2  Diffie-Hellman group 2
  5  Diffie-Hellman group 5
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#
  
```

Copy Paste

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».

Time: 04:25:41 Power Cycle Devices Fast Forward Time

Routers

Scenario 0

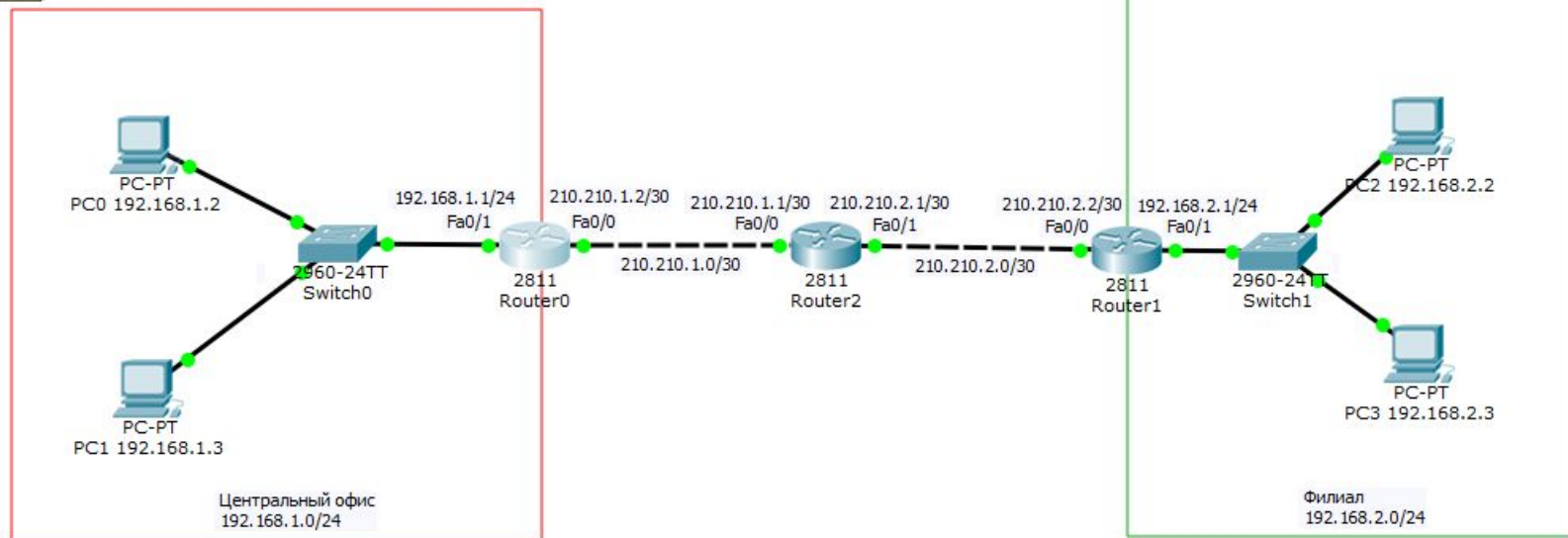
New Delete

Toggle PDU List Window

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



Logical [Root] New Cluster Move Object



Router0

Physical Config CLI

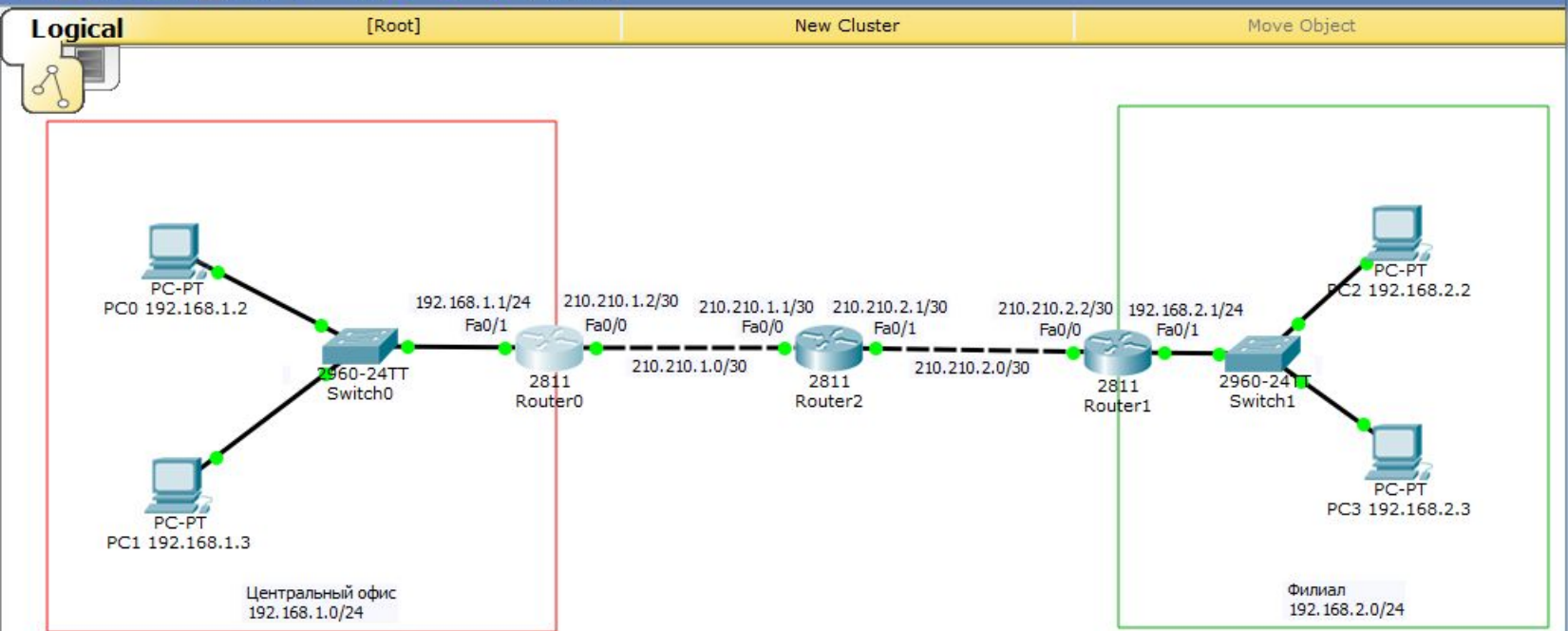
IOS Command Line Interface

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#
Router(config-isakmp)#encr
Router(config-isakmp)#encryption ?
  3des  Three key triple DES
  aes   AES - Advanced Encryption Standard
  des   DES - Data Encryption Standard (56 bit keys).
Router(config-isakmp)#encryption 3
Router(config-isakmp)#encryption 3des ?
<cr>
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash ?
  md5  Message Digest 5
  sha  Secure Hash Standard
Router(config-isakmp)#hash m
Router(config-isakmp)#hash md5
Router(config-isakmp)#au
Router(config-isakmp)#authentication ?
  pre-share  Pre-Shared Key
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group ?
  1  Diffie-Hellman group 1
  2  Diffie-Hellman group 2
  5  Diffie-Hellman group 5
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#
```

Copy Paste

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.





Router0

Physical Config CLI

IOS Command Line Interface

```
Router>
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#cry
Router(config)#crypto isa
Router(config)#crypto isakmp key cisco address 210.210.2.2
A pre-shared key for address mask 210.210.2.2 255.255.255.255 already exists!
Router(config)#
```

Copy Paste

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.

Time: 04:45:25 Power Cycle Devices Fast Forward Time Realtime

Scenario 0

New Delete

Toggle PDU List Window

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

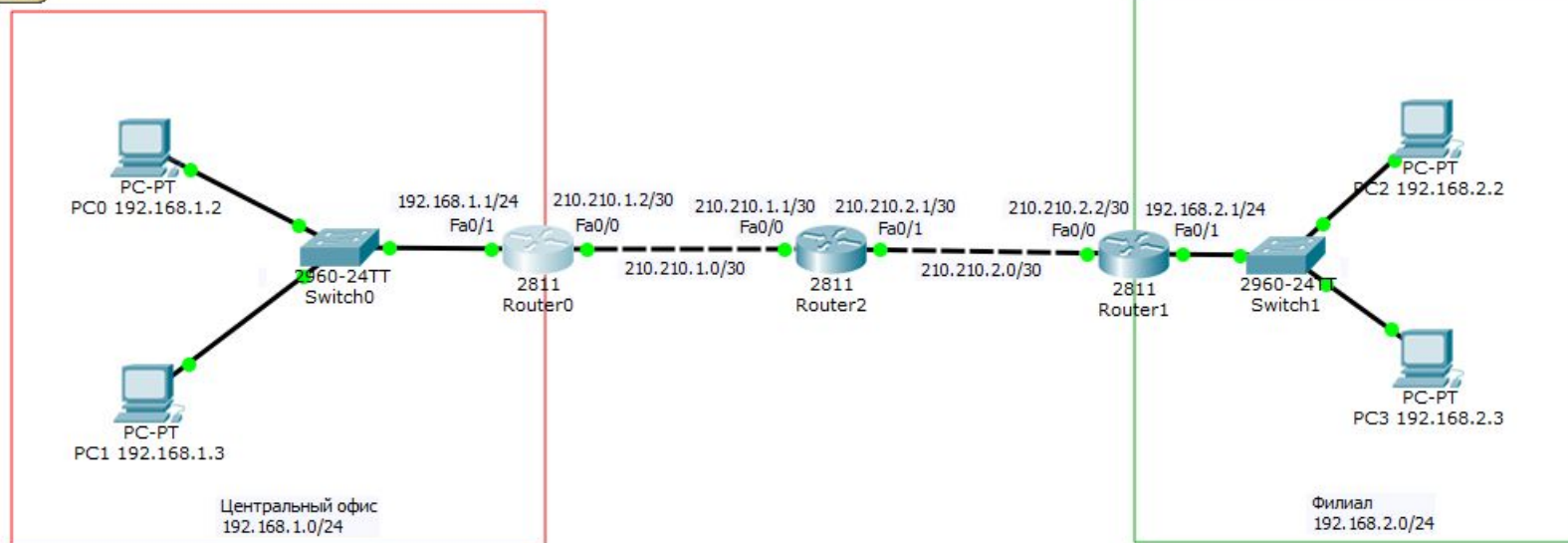
819HGW

Windows taskbar icons: Internet Explorer, File Explorer, Microsoft Store, Clock, Word, PowerPoint, Firefox, VLC, and a folder icon.

System tray: ENG, 23:04, 18.01.2020



Logical [Root] New Cluster Move Object



Router0

Physical Config CLI

IOS Command Line Interface

```

Router>en
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 es
Router(config)#crypto ipsec transform-set TS esp
Router(config)#crypto ipsec transform-set TS esp-3des esp-
md5-hmac

% Invalid input detected at '^' marker.

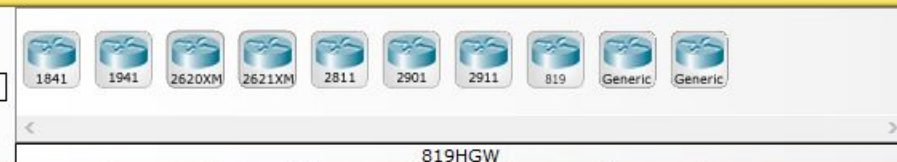
Router(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#
Router#
Router#
  
```

Copy Paste

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».

Time: 05:10:06 Power Cycle Devices Fast Forward Time



Scenario 0

New Delete

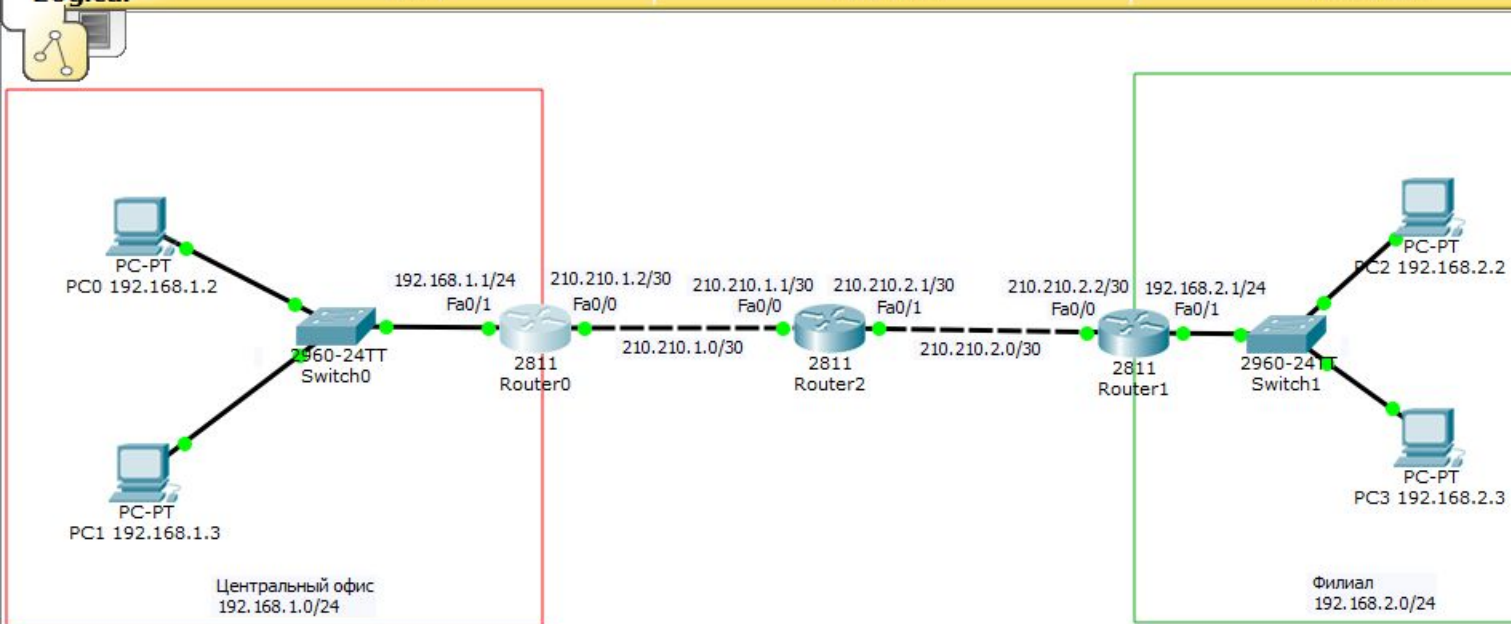
Toggle PDU List Window

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





Logical [Root] New Cluster Move Object



Router0

Physical Config CLI

IOS Command Line Interface

```
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 es
Router(config)#crypto ipsec transform-set TS esp
Router(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
Router(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
Router(config)#exit
Router#
% Invalid input detected at '^' marker.

Router(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
Router(config)#exit
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list extended FOR-VPN
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)#exit
Router(config)#
```

Copy Paste

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».

Time: 05:23:03 Power Cycle Devices Fast Forward Time

Realtime

Scenario 0

New Delete

Toggle PDU List Window

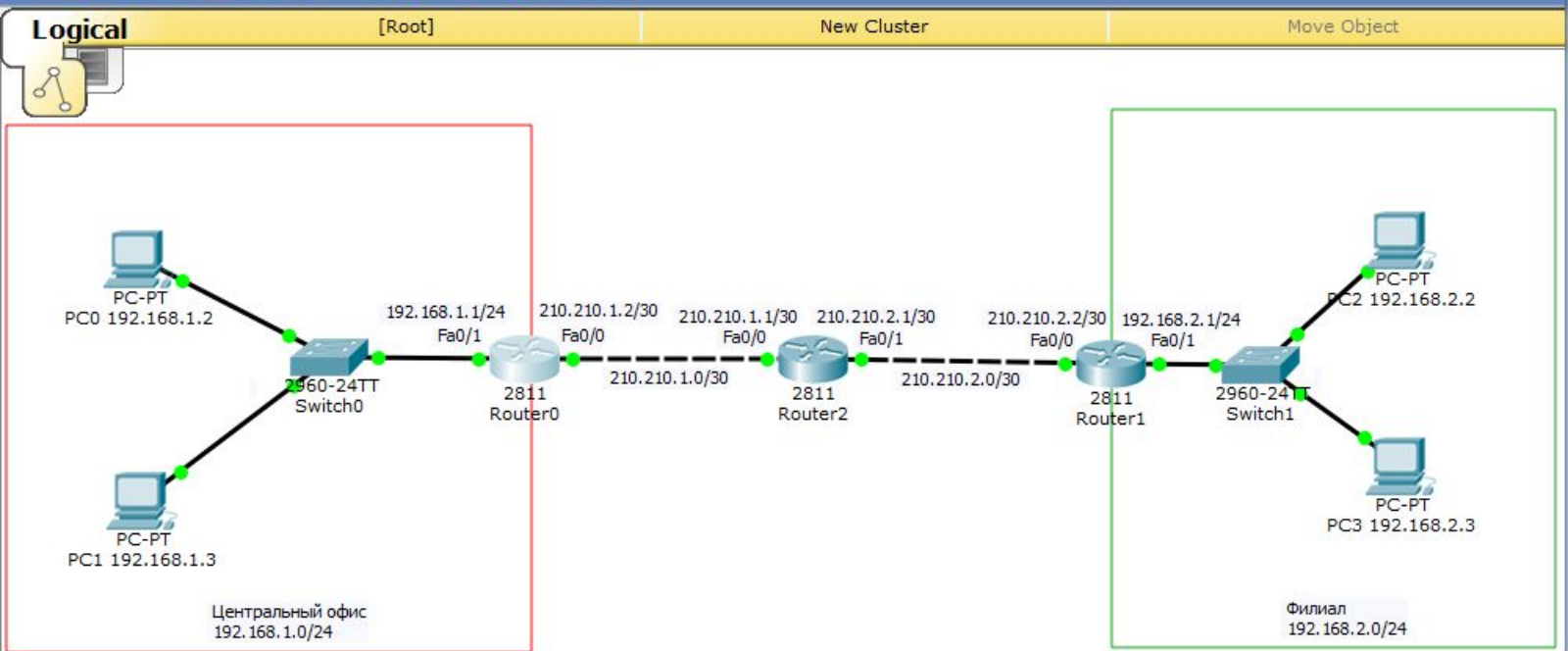
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Router-PT

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

Windows taskbar icons: Internet Explorer, File Explorer, Microsoft Store, Clock, Word, PowerPoint, Firefox, VLC, and a folder icon.

System tray: ENG, 23:43, 18.01.2020



Router0

Physical Config CLI

IOS Command Line Interface

```
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#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list extended FOR-VPN
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)#exit
Router(config)#
Router(config)#
Router(config)#crypto map CMAP 10 ipsec-isakmp
Router(config-crypto-map)#set peer 210.210.2.2
Router(config-crypto-map)#set transform-set TS
Router(config-crypto-map)#match address FOR-VPN
Router(config-crypto-map)#exit
Router(config)#
Router(config)#
Router(config)#
```

Copy Paste

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»

Power Cycle Devices Fast Forward Time

Scenario 0

New Delete

Toggle PDU List Window

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

Router-PT-Empty

Realtime

0:01 19.01.2020

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

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object

Центральный офис
192.168.1.0/24

Филиал
192.168.2.0/24

Router0

Physical Config CLI

IOS Command Line Interface

```
Router>configure
Router(config)#
Router(config)#crypto map CMAP 10 ipsec-isakmp
Router(config-crypto-map)#set peer 210.210.2.2
Router(config-crypto-map)#set transform-set TS
Router(config-crypto-map)#match address FOR-VPN
Router(config-crypto-map)#exit
Router(config)#
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#cr
Router(config-if)#crypto ma
Router(config-if)#crypto map ?
WORD Crypto Map tag
Router(config-if)#crypto map CMAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#end
Router#
$SYS-5-CONFIG_I: Configured from console by console

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

Copy Paste

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

Time: 29:54:11 Power Cycle Devices Fast Forward Time

Realtime

Scenario 0

New Delete

Toggle PDU List Window

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

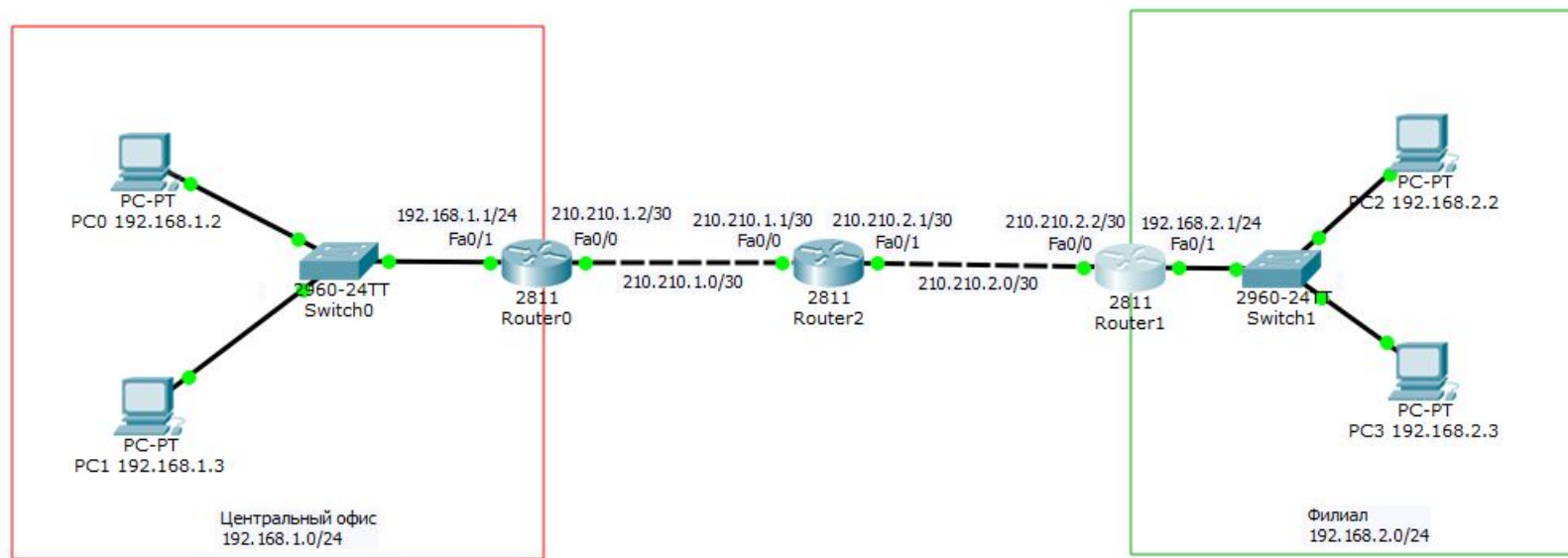
Routers

Router-PT

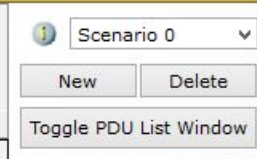
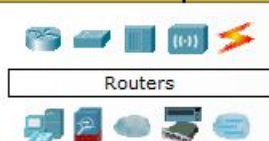
1841 1941 2620XM 2621XM 2811 2901 2911 819 Generic Generic

Windows Taskbar: File Explorer, Word, PowerPoint, Firefox, VLC, etc.

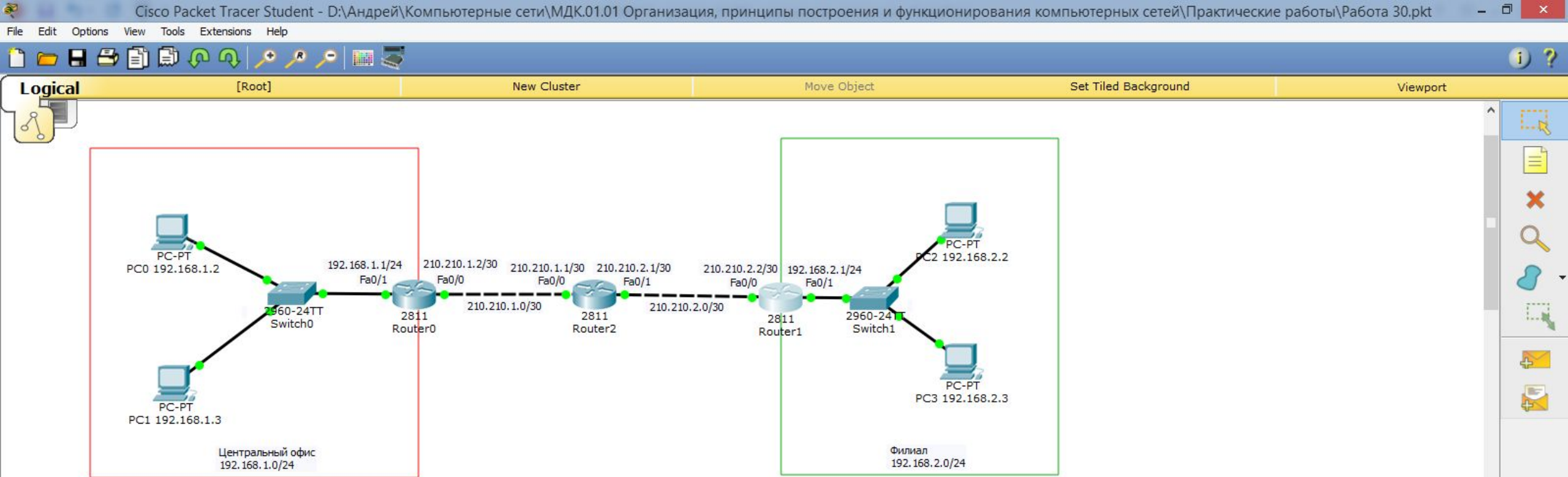
System Tray: 0:14 19.01.2020



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



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



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».

Time: 29:58:35 Power Cycle Devices Fast Forward Time

Realtime

Scenario 0

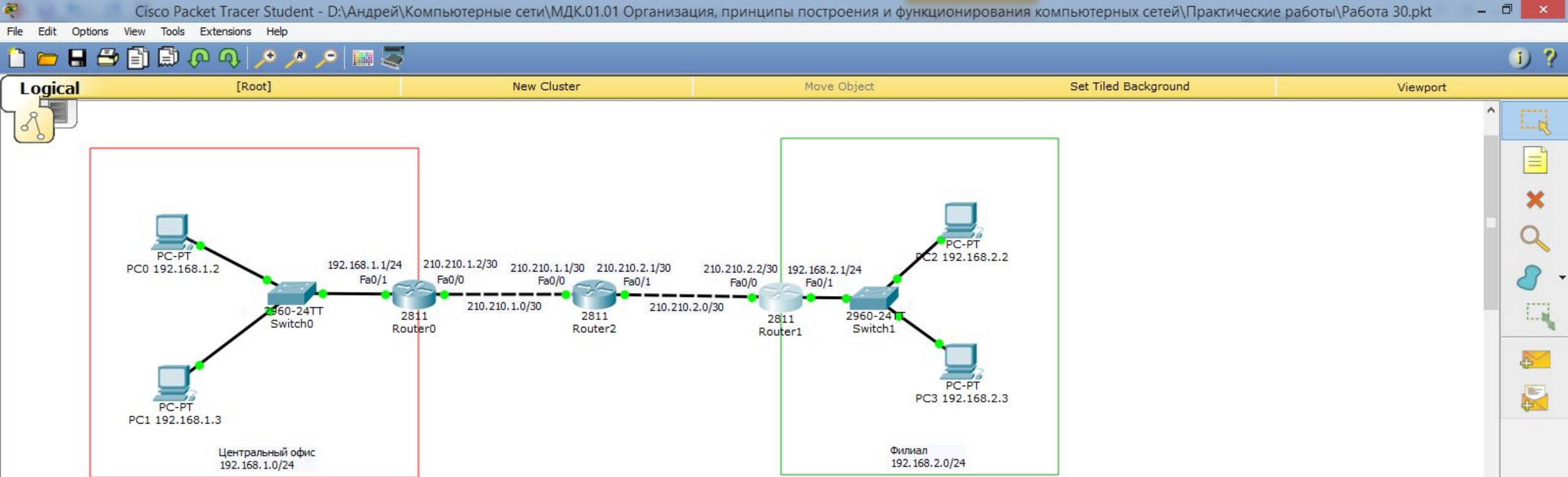
New Delete

Toggle PDU List Window

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

2811

0:19 19.01.2020



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.

Time: 30:02:30 Power Cycle Devices Fast Forward Time

Realtime

Scenario 0

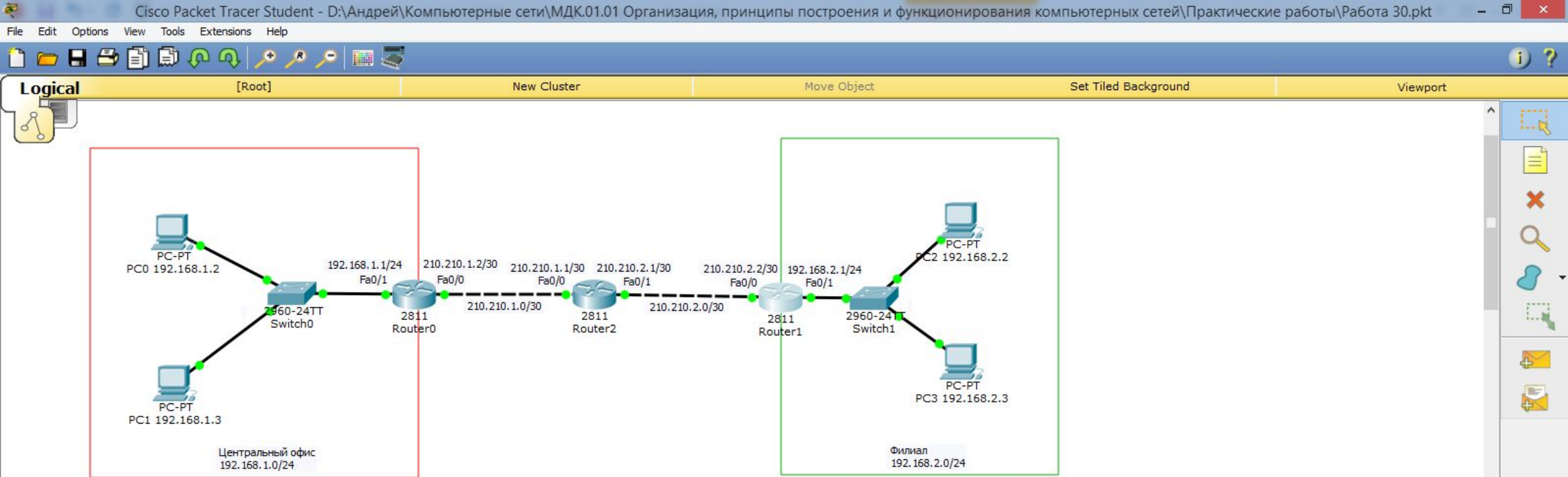
New Delete

Toggle PDU List Window

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

819HGW

Windows Taskbar: 0:22 19.01.2020



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».

Time: 30:04:22 Power Cycle Devices Fast Forward Time Realtime

Scenario 0

New Delete

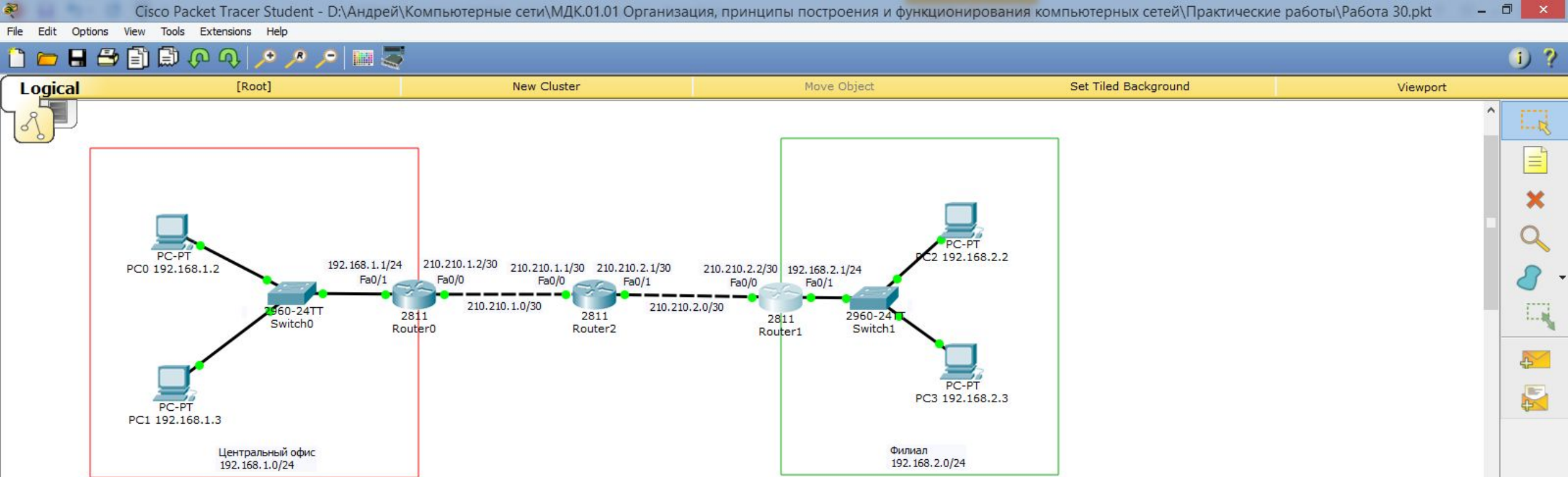
Toggle PDU List Window

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

Router-PT

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

Windows taskbar: 0:24 19.01.2020



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».

Time: 30:04:22 Power Cycle Devices Fast Forward Time

Realtime

Scenario 0

New Delete

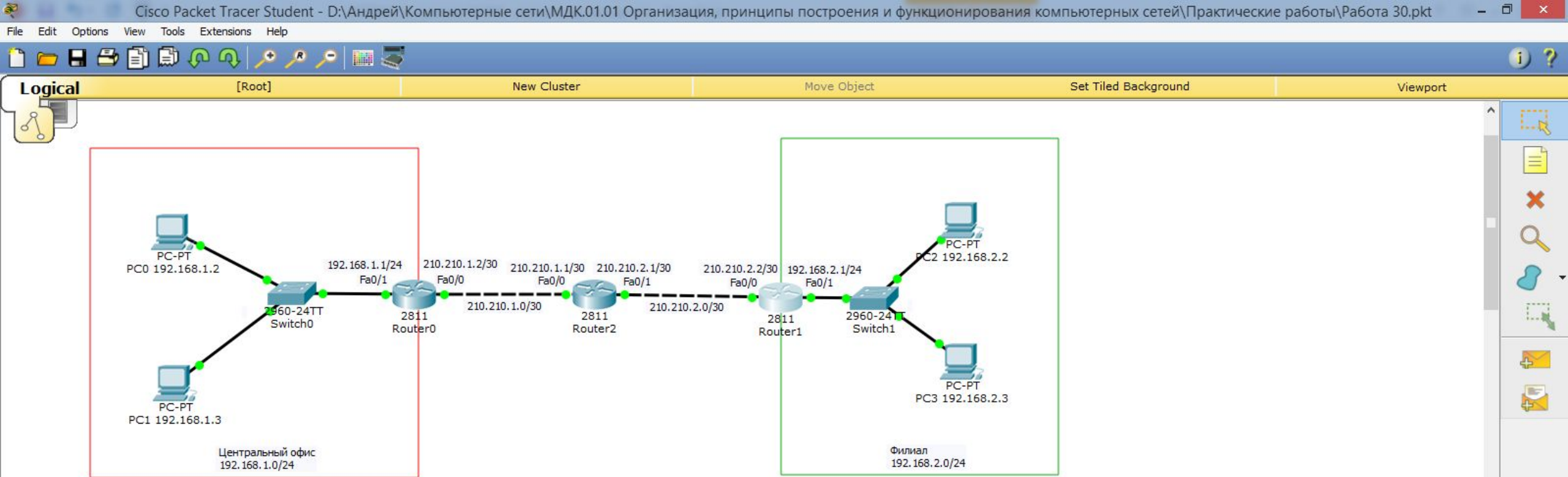
Toggle PDU List Window

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

Router-PT

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

Windows Taskbar: 0:24 19.01.2020



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»

Power Cycle Devices Fast Forward Time

Realtime

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

Scenario 0

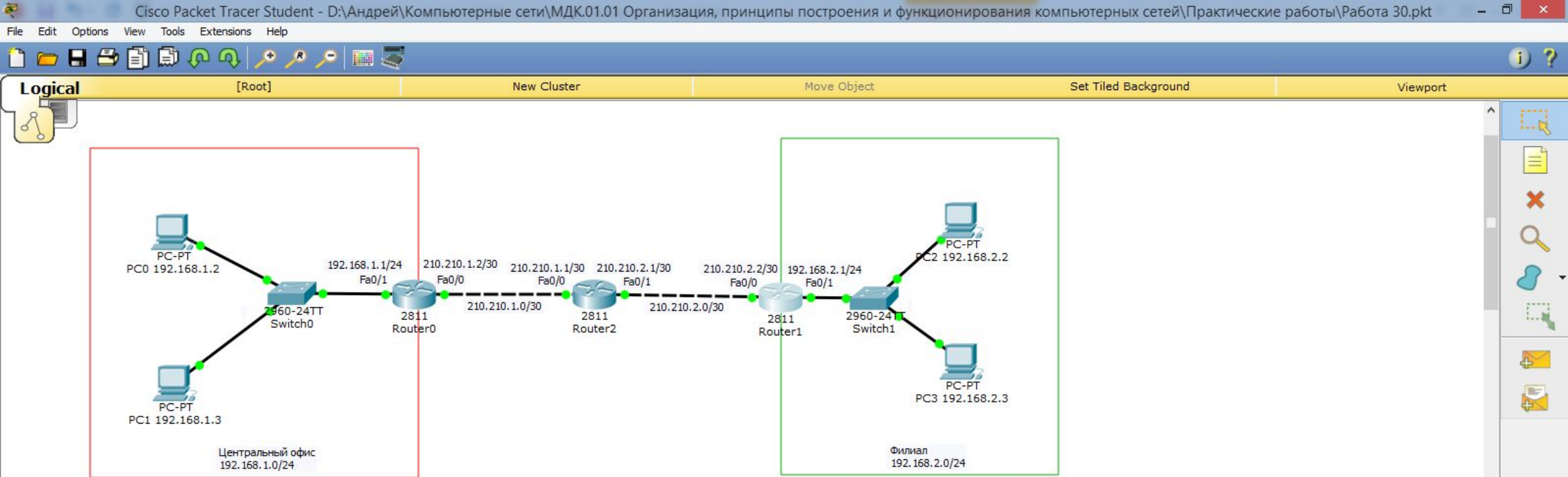
New Delete

Toggle PDU List Window

Router-PT

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

Windows Taskbar: 0:24 19.01.2020



Привяжем эту крипто-карту **к внешнему интерфейсу:**

«interface FastEthernet0/0»,

командой: «crypto map CMAP»,

«end», «wr mem».

Time: 30:04:22 Power Cycle Devices Fast Forward Time

Realtime

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

Scenario 0

New Delete

Toggle PDU List Window

Routers

Router-PT

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

Windows taskbar: 0:24 19.01.2020

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

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object

PC-PT PC0 192.168.1.2
PC-PT PC1 192.168.1.3
2960-24TT Switch0
2811 Router0
210.210.1.2/30 Fa0/0
210.210.1.1/30 Fa0/0
210.210.2.1/30 Fa0/1
210.210.2.2/30 Fa0/0
192.168.1.1/24 Fa0/1
2811 Router1
2960-24 Switch1
PC-PT PC2 192.168.2.2
PC-PT PC3 192.168.2.3
Центральный офис 192.168.1.0/24
Филиал 192.168.2.0/24

Physical Config Desktop Custom Interface

Command Prompt

```
Pinging 192.168.2.2 with 32 bytes of data:  
  
Request timed out.  
Reply from 210.210.1.1: Destination host unreachable.  
Reply from 210.210.1.1: Destination host unreachable.  
Reply from 210.210.1.1: Destination host unreachable.  
  
Ping statistics for 192.168.2.2:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
PC>ping 192.168.2.2  
  
Pinging 192.168.2.2 with 32 bytes of data:  
  
Reply from 210.210.1.1: Destination host unreachable.  
Reply from 210.210.1.1: Destination host unreachable.  
Reply from 210.210.1.1: Destination host unreachable.  
Reply from 210.210.1.1: Destination host unreachable.  
  
Ping statistics for 192.168.2.2:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
PC>
```

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.

Time: 30:21:53 Power Cycle Devices Fast Forward Time Realtime

Routers

Scenario 0

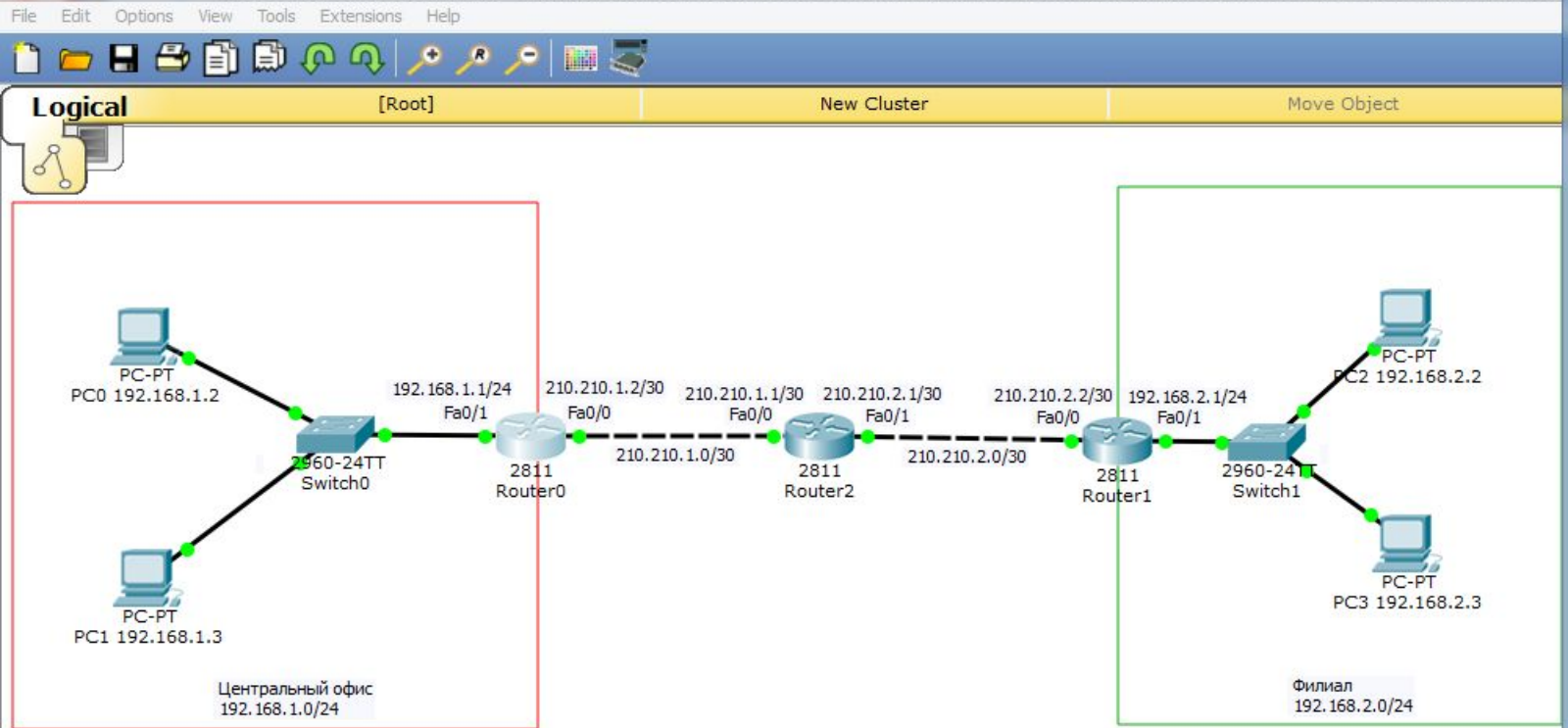
New Delete

Toggle PDU List Window

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

819HGW

Windows taskbar: 0:42 19.01.2020



Router0

Physical Config CLI

IOS Command Line Interface

```
Router#
Router#
Router#
Router#
Router#
Router#show ip nat tr
Router#show ip nat translations
Router#show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
icmp	210.210.1.2:17	192.168.1.2:17	192.168.2.2:17	192.168.2.2:17
icmp	210.210.1.2:18	192.168.1.2:18	192.168.2.2:18	192.168.2.2:18
icmp	210.210.1.2:19	192.168.1.2:19	192.168.2.2:19	192.168.2.2:19
icmp	210.210.1.2:20	192.168.1.2:20	192.168.2.2:20	192.168.2.2:20
icmp	210.210.1.2:21	192.168.1.2:21	192.168.2.2:21	192.168.2.2:21
icmp	210.210.1.2:22	192.168.1.2:22	192.168.2.2:22	192.168.2.2:22
icmp	210.210.1.2:23	192.168.1.2:23	192.168.2.2:23	192.168.2.2:23
icmp	210.210.1.2:24	192.168.1.2:24	192.168.2.2:24	192.168.2.2:24
icmp	210.210.1.2:5	192.168.1.3:5	192.168.2.3:5	192.168.2.3:5
icmp	210.210.1.2:6	192.168.1.3:6	192.168.2.3:6	192.168.2.3:6
icmp	210.210.1.2:7	192.168.1.3:7	192.168.2.3:7	192.168.2.3:7
icmp	210.210.1.2:8	192.168.1.3:8	192.168.2.3:8	192.168.2.3:8

Router#

Copy Paste

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.

Time: 30:32:56 Power Cycle Devices Fast Forward Time

Realtime

Scenario 0

New Delete

Toggle PDU List Window

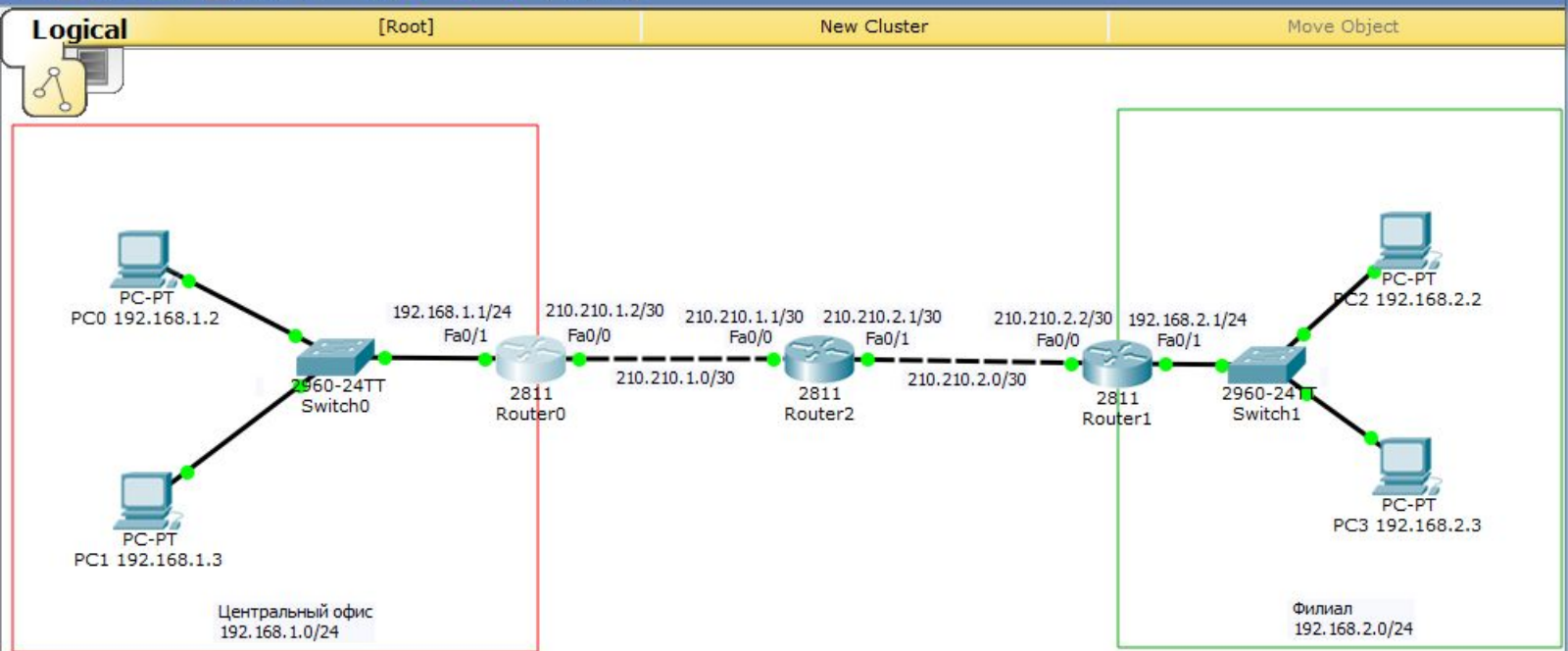
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

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

2901

Windows Taskbar: File Explorer, Word, PowerPoint, Firefox, VLC, etc.

System Tray: ENG, 0:53, 19.01.2020



Router0

Physical Config CLI

IOS Command Line Interface

```
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip access-list standard FOR-NAT
Router(config)#ip access-list extended FOR-NAT
Router(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 any
Router(config-ext-nacl)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Copy Paste

Удалим наш стандартный Access List и создадим расширенный Access List:

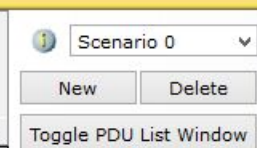
«conf t», «no ip access-list standard FOR-NAT», «ip access-list extended FOR-NAT».

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»,

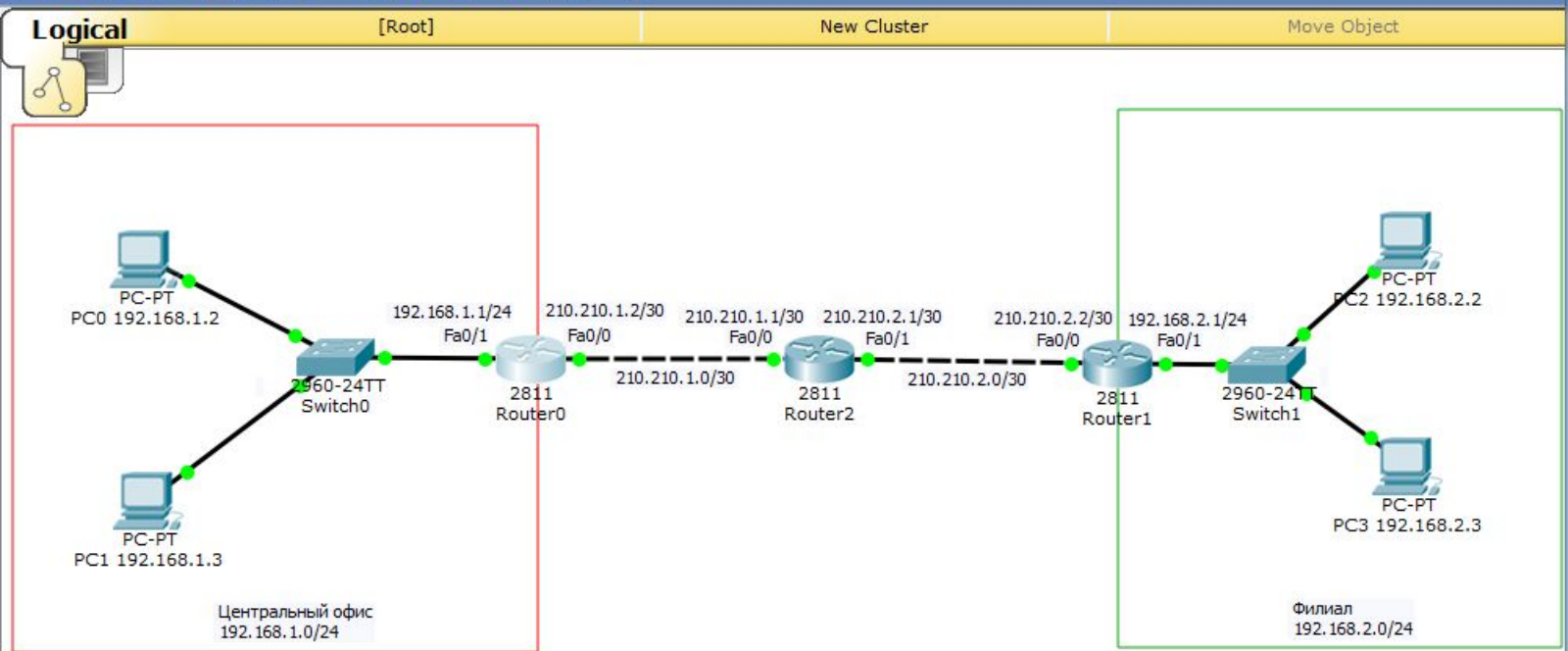
«permit ip 192.168.1.0 0.0.0.255 any», «end», «wr mem».

Time: 30:59:42 Power Cycle Devices Fast Forward Time



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





Router0

Physical Config CLI

IOS Command Line Interface

```
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip nat inside source list FOR-NAT interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 210.210.1.1
!
ip flow-export version 9
!
!
ip access-list extended FOR-VPN
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
ip access-list extended FOR-NAT
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
!
!
!
--More--
```

Copy Paste

Наберём команду:

«show run».

Видим, что Access List применился.

Routers

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

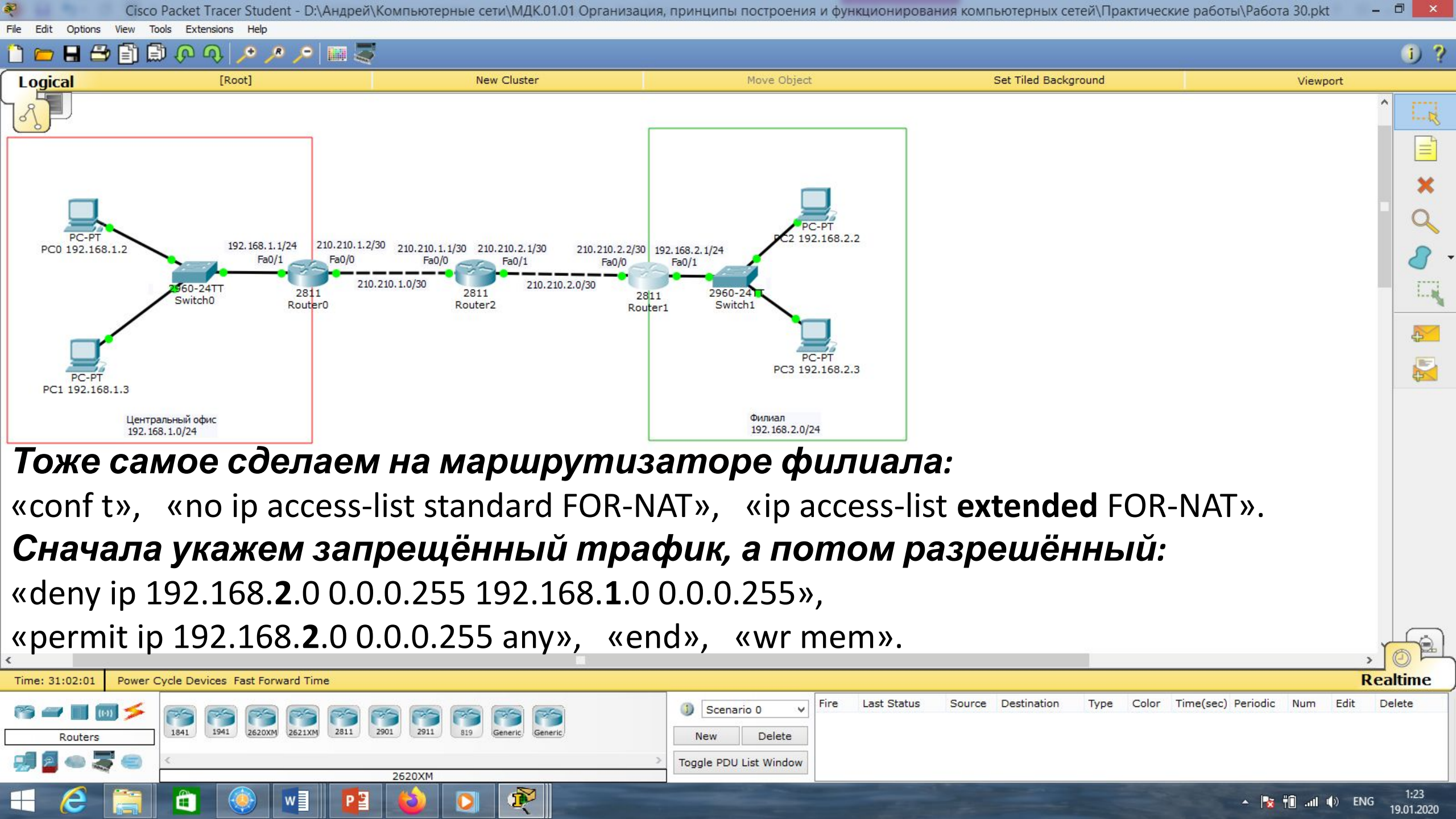
2901

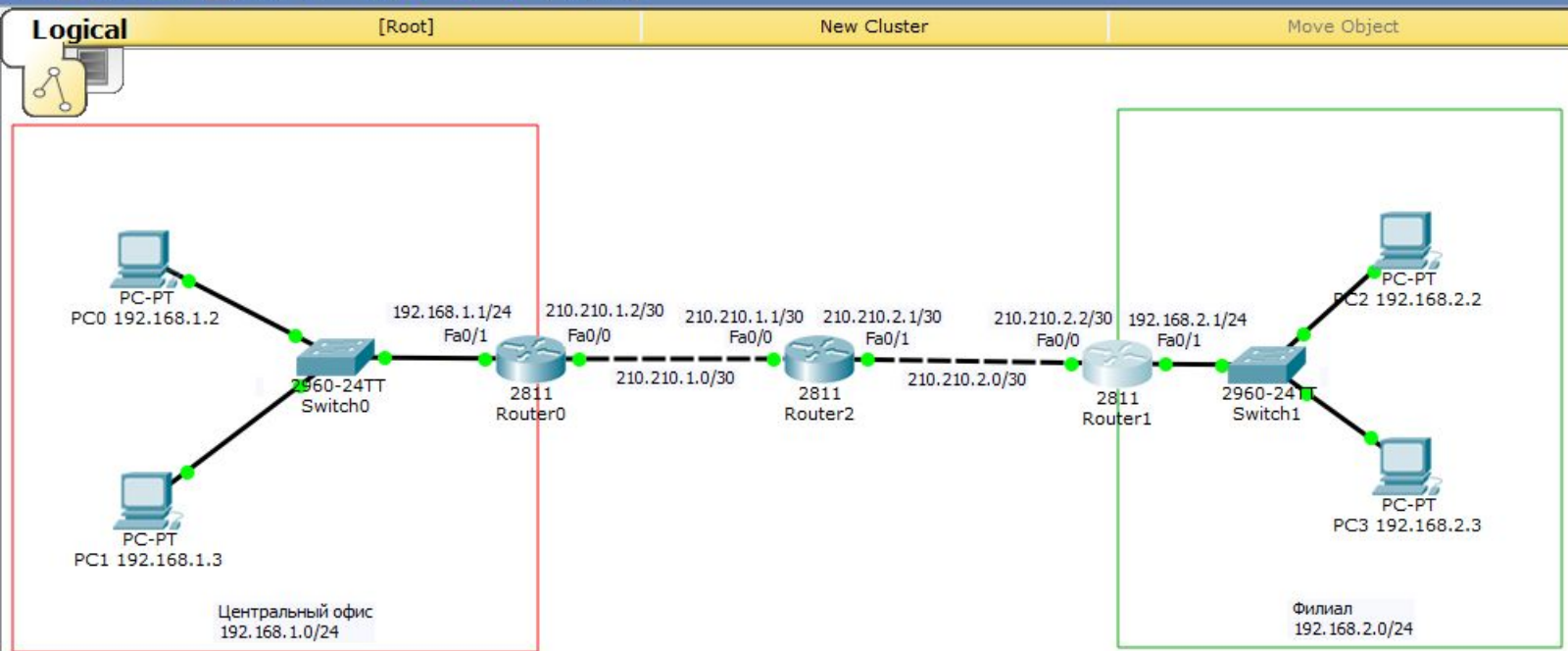
Scenario 0

New Delete

Toggle PDU List Window

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





Router1

Physical Config CLI

IOS Command Line Interface

```
ip access-list extended FOR-VPN
permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
ip access-list extended FOR-NAT
deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
permit ip 192.168.2.0 0.0.0.255 any
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
Router#
```

Copy Paste

Наберём команду:

«show run».

Видим, что Access List *применился*.

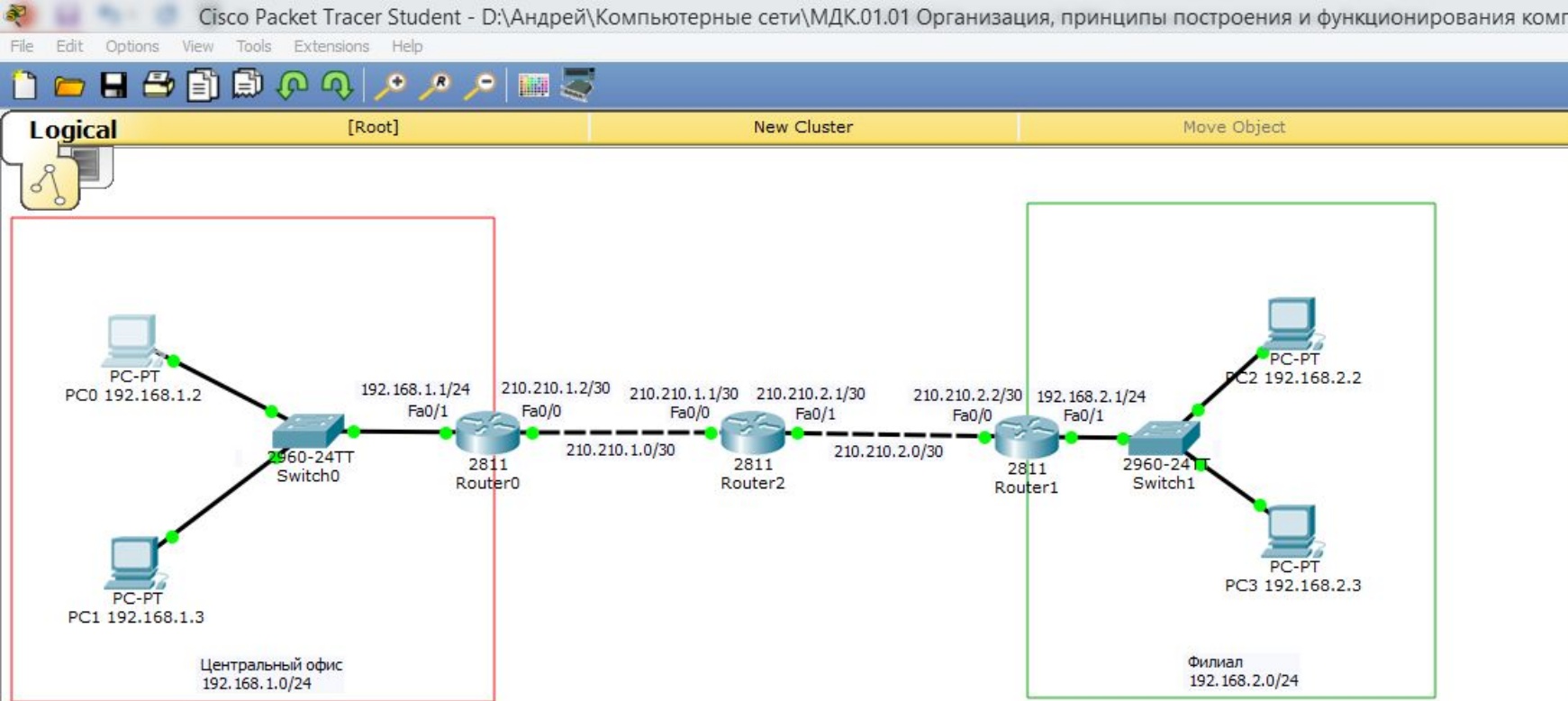
Scenario 0

New Delete

Toggle PDU List Window

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

2901



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

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

Scenario 0

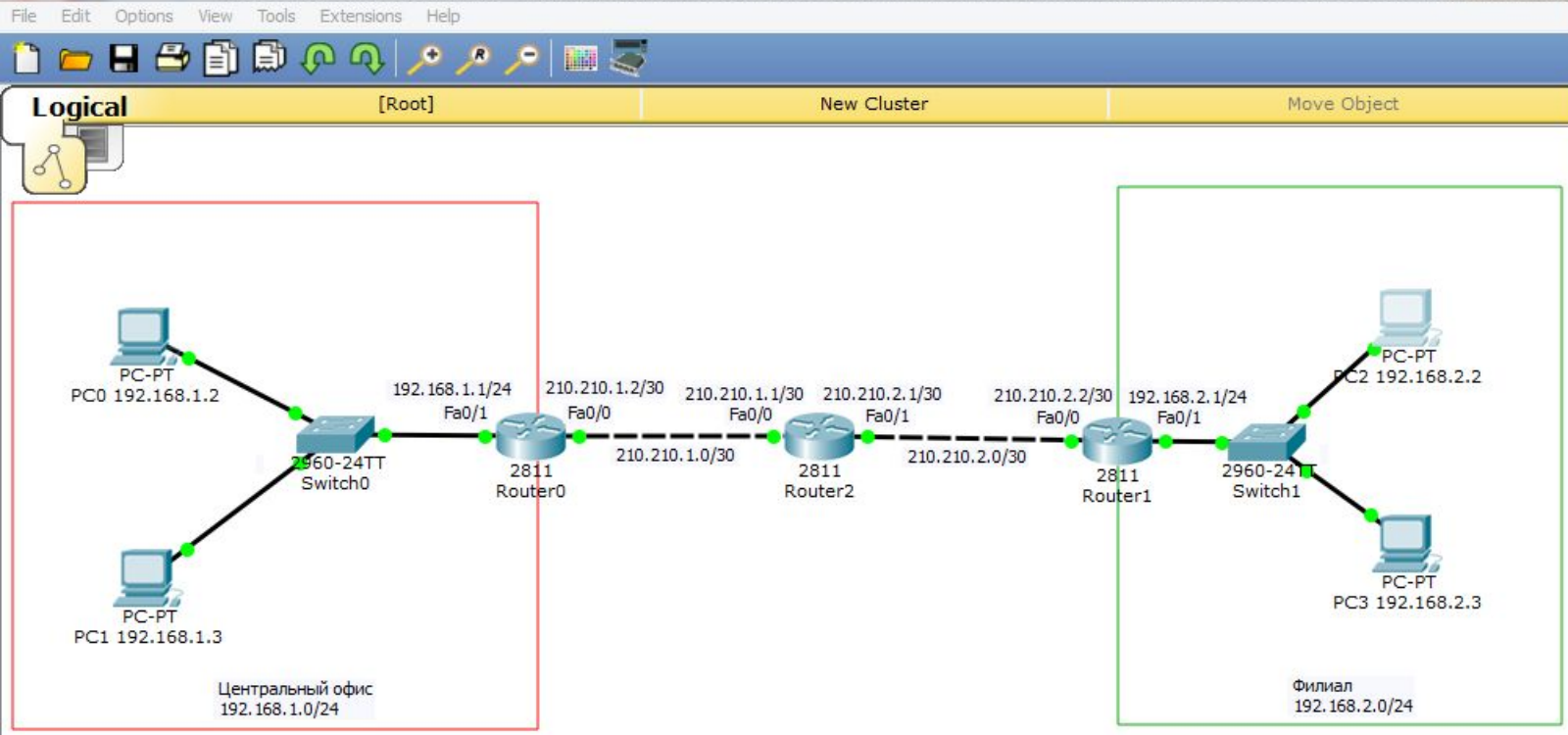
New Delete

Toggle PDU List Window

2911

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

Windows taskbar: 1:33 19.01.2020



PC2 192.168.2.2

Physical Config Desktop Custom Interface

Command Prompt

```
Reply from 192.168.1.2: bytes=32 time=13ms TTL=126
Reply from 192.168.1.2: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 13ms, Average = 11ms

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=11ms TTL=126
Reply from 192.168.1.2: bytes=32 time=12ms TTL=126
Reply from 192.168.1.2: bytes=32 time=13ms TTL=126
Reply from 192.168.1.2: bytes=32 time=14ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 14ms, Average = 12ms

PC>
```

На всякий случай проверим связь одного из компьютеров филиала с компьютером Центрального офиса: «ping 192.168.1.2».
Связь тоже есть!!!

Time: 31:17:53 Power Cycle Devices Fast Forward Time

Realtime

Scenario 0

New Delete

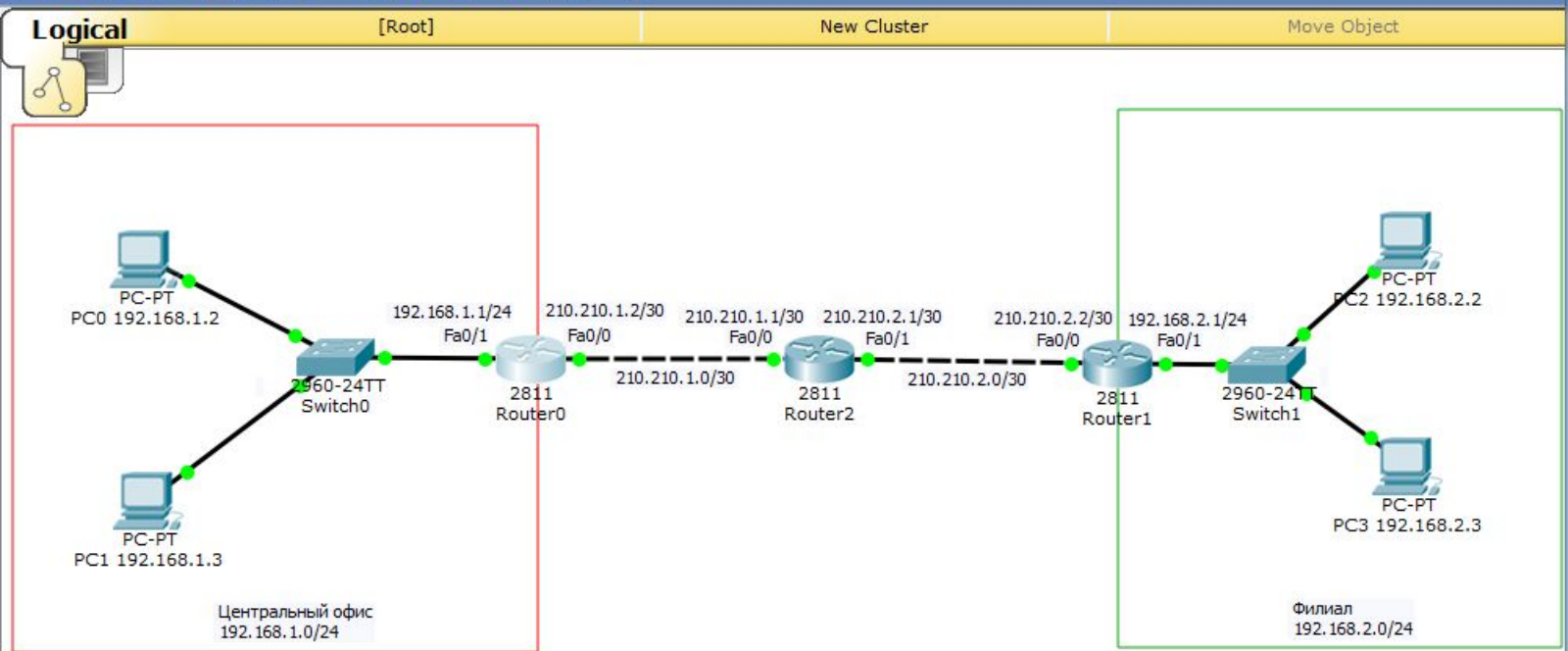
Toggle PDU List Window

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

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

2621XM

Windows taskbar: 1:39 19.01.2020



Router0

Physical Config CLI

IOS Command Line Interface

```
Router#show crypto ip
Router#show crypto ipsec sa

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

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer 210.210.2.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 0
#pkts decaps: 21, #pkts decrypt: 21, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 210.210.1.2, remote crypto endpt.: 210.210.2.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x0(0)

inbound esp sas:
```

Copy Paste

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.

Time: 31:30:56 Power Cycle Devices Fast Forward Time

Realtime

Scenario 0

New Delete

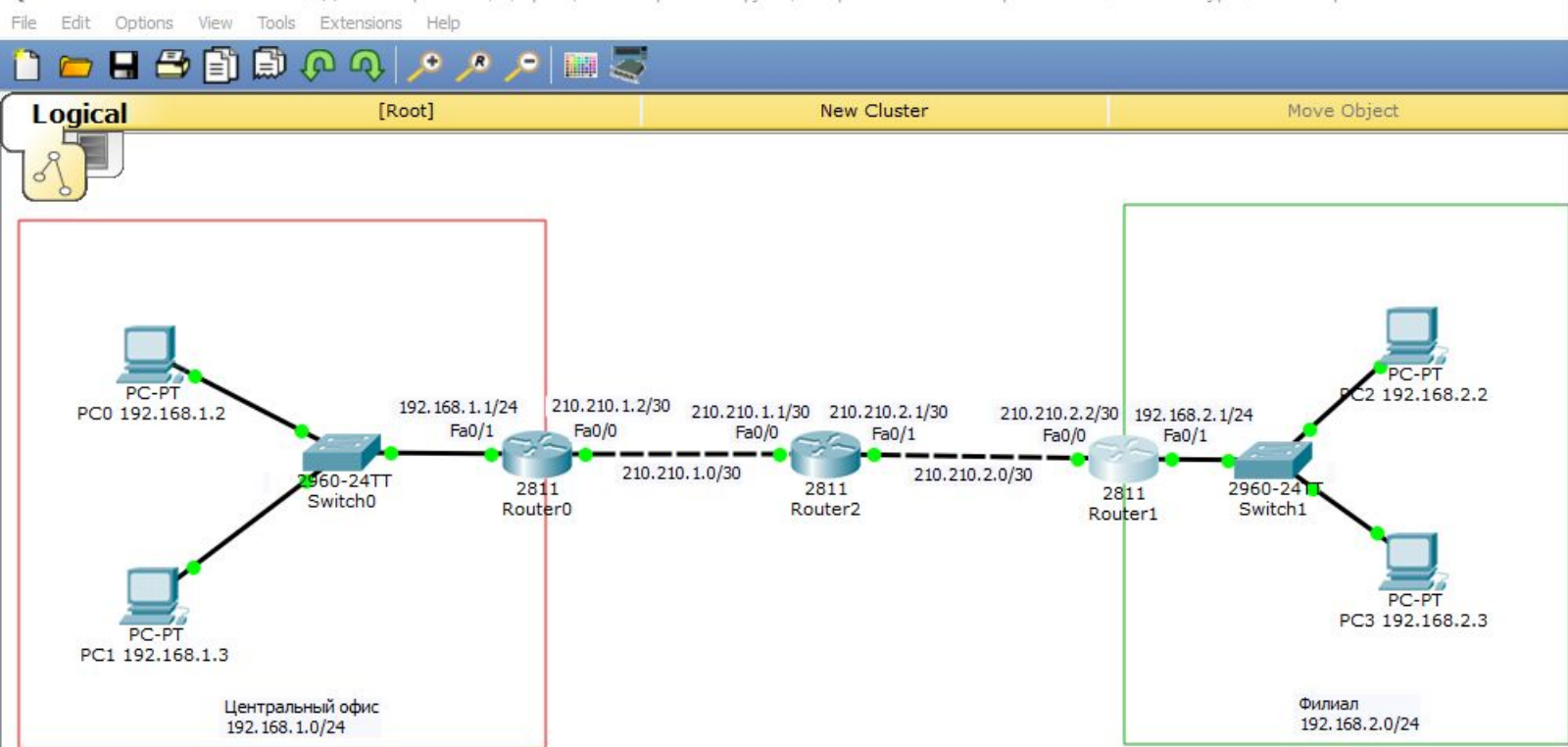
Toggle PDU List Window

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

Router-PT

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

Windows Taskbar: 1:52 19.01.2020



Router1

Physical Config CLI

IOS Command Line Interface

```
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state      conn-id slot status
210.210.1.2  210.210.2.2  QM_IDLE   1069     0  ACTIVE

IPv6 Crypto ISAKMP SA

Router#
Router#
Router#
Router#
```

Copy Paste

На маршрутизаторе филиала посмотрим, построился ли тот самый технологический туннель: «show crypto isakmp sa».
Видим, что туннель есть.

Time: 00:08:04 Power Cycle Devices Fast Forward Time Realtime

Scenario 0

New Delete

Toggle PDU List Window

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

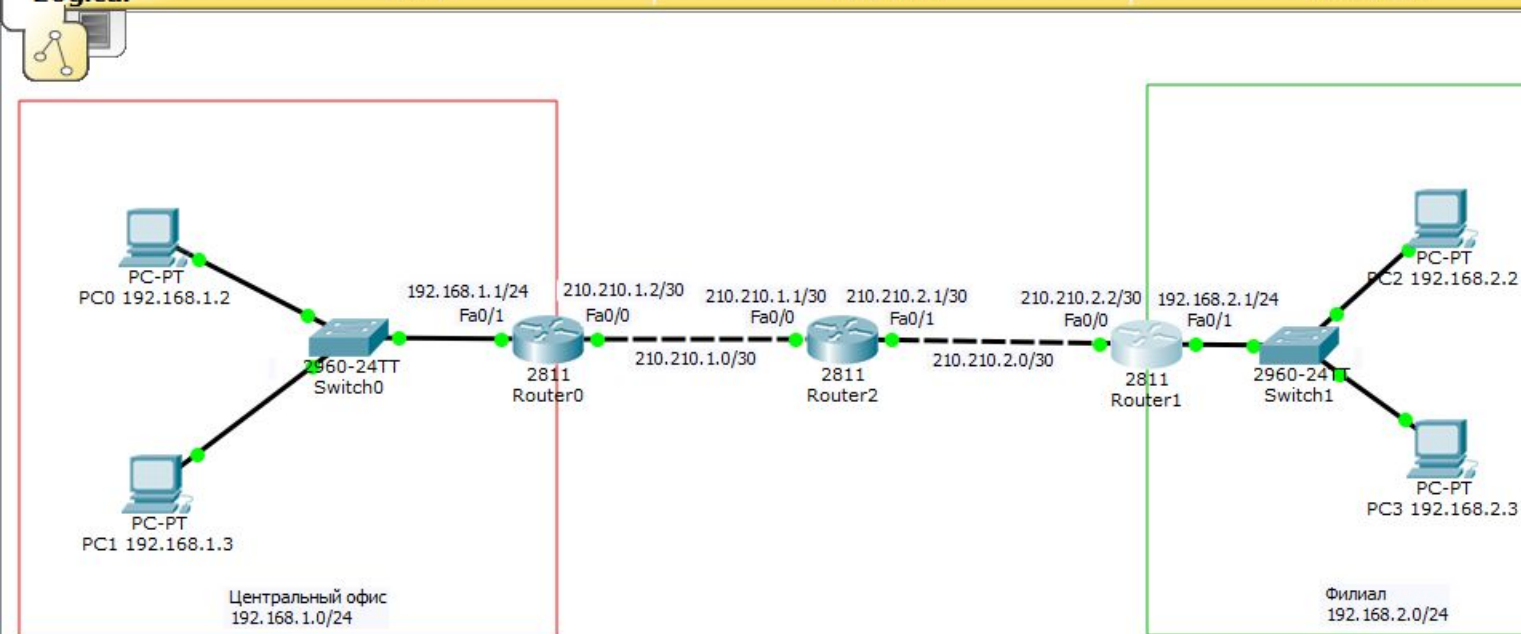
Router-PT-Empty

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

Windows Taskbar: 14:04 24.01.2020



Logical [Root] New Cluster Move Object



Router1

Physical Config CLI

IOS Command Line Interface

```
Router#
Router#show crypto ipsec sa

interface: FastEthernet0/0
  Crypto map tag: CMAP, local addr 210.210.2.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 210.210.1.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 0
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 210.210.2.2, remote crypto endpt.: 210.210.1.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x0E9F1AFF(245308159)

inbound esp sas:
  spi: 0x0A2B6D10(170618128)
--More--
```

Copy Paste

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!!!

Time: 00:09:47 Power Cycle Devices Fast Forward Time

Realtime

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

Scenario 0

New Delete

Toggle PDU List Window

Router-PT

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

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, Санкт-Петербург, 2016.
3. Компьютерные сети. Э. Таненбаум, 4-е издание, «Питер», Москва, Санкт-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