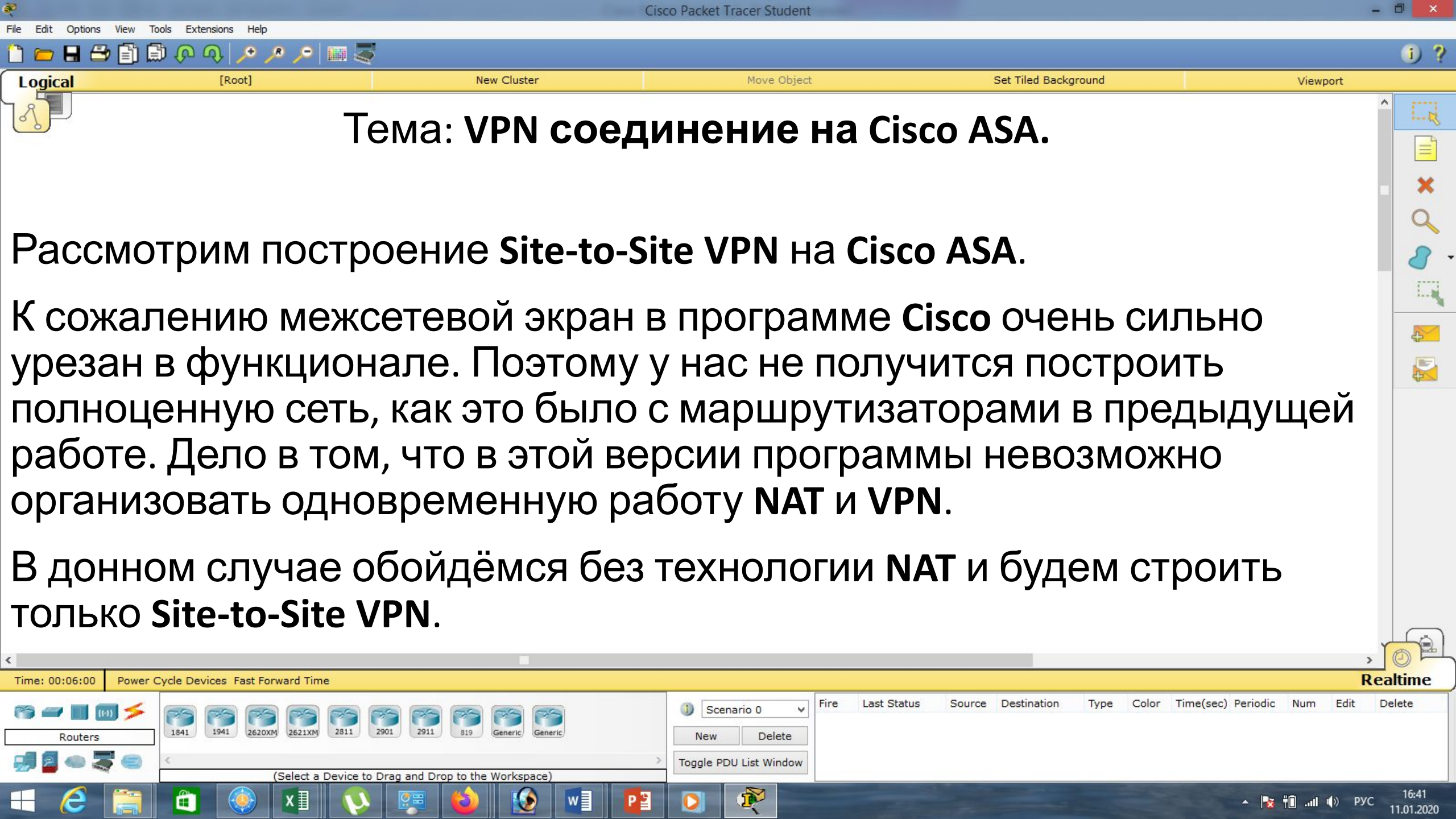
МДК.01.01

Организация, принципы построения и функционирования компьютерных сетей

3-курс

Практические занятия

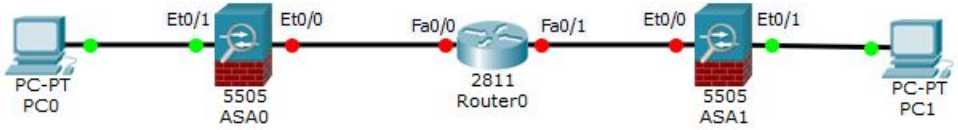
Занятие 17


Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
Тема: VPN соединение на Cisco ASA.
Рассмотрим построение Site-to-Site VPN на Cisco ASA.
К сожалению межсетевой экран в программе Cisco очень сильно урезан в функционале. Поэтому у нас не получится построить полноценную сеть, как это было с маршрутизаторами в предыдущей работе. Дело в том, что в этой версии программы невозможно организовать одновременную работу NAT и VPN.
В донном случае обойдёмся без технологии NAT и будем строить только Site-to-Site VPN.
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



Построим схему, показанную на рисунке.
Подробно рассмотрим настройки Cisco ASA***.***

Time: 00:04:49 | Power Cycle Devices | Fast Forward Time | Realtime

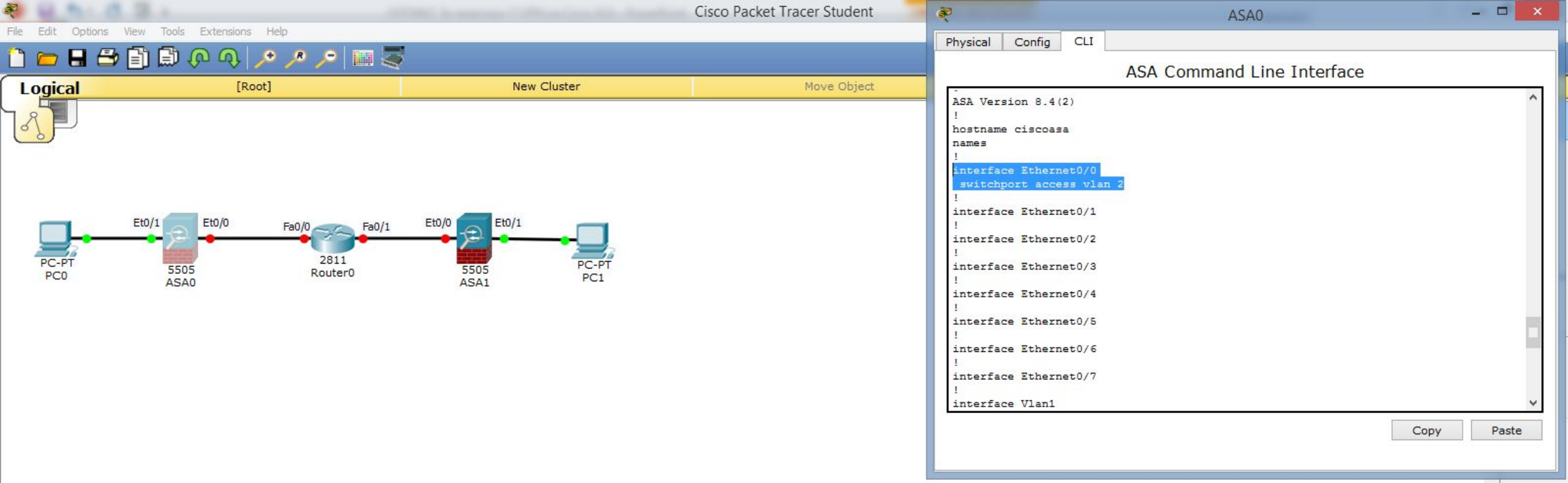
Connections

Copper Straight-Through

Scenario 0 | New | Delete | Toggle PDU List Window

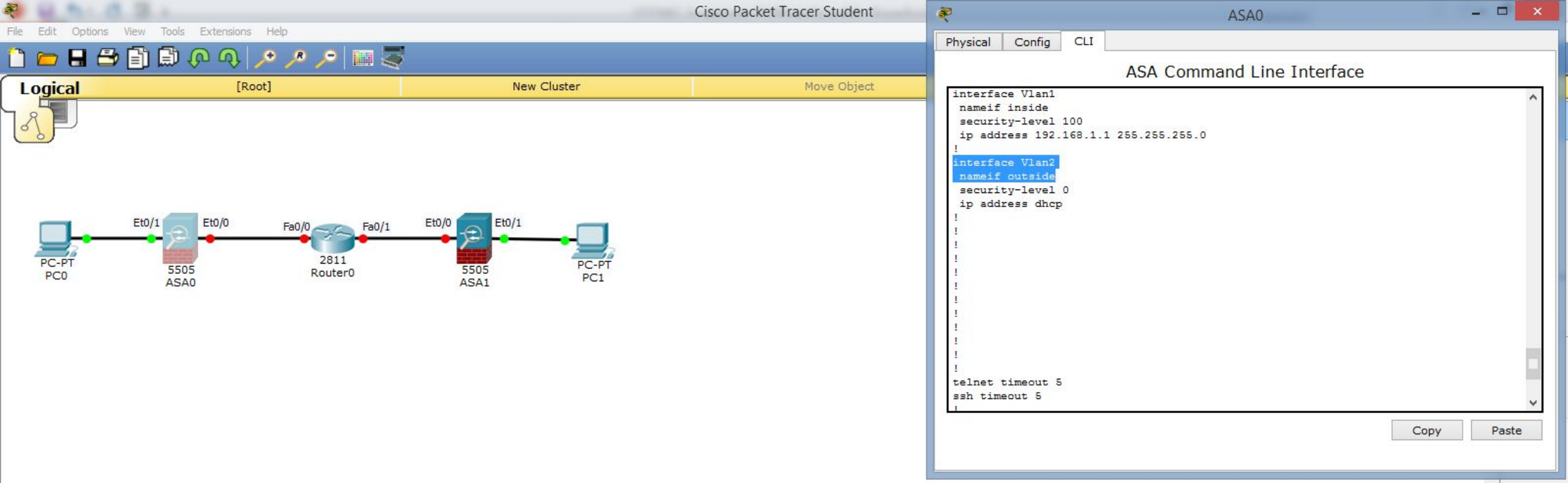
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete

ENG 20:57 23.01.2020

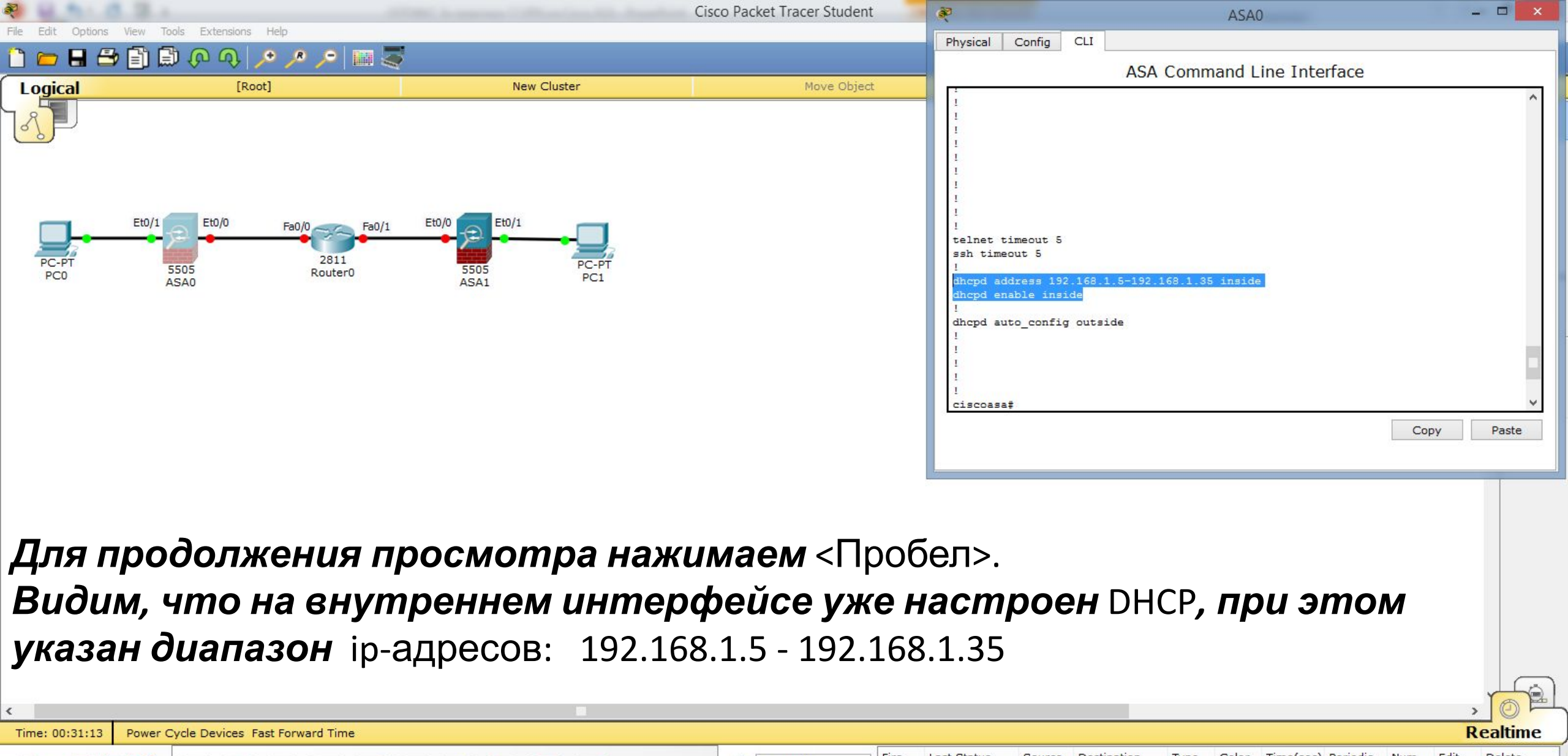


Зайдём в настройки ASA0***:*** «en», ***пароль*** пустой***, поэтому просто нажимаем*** <Enter>, ***далее посмотрим заводские настройки:*** «show run», ***для продолжения просмотра нажимаем*** <Пробел>.

Видим, что Ethernet0/0 ***уже настроен во*** vlan 2.

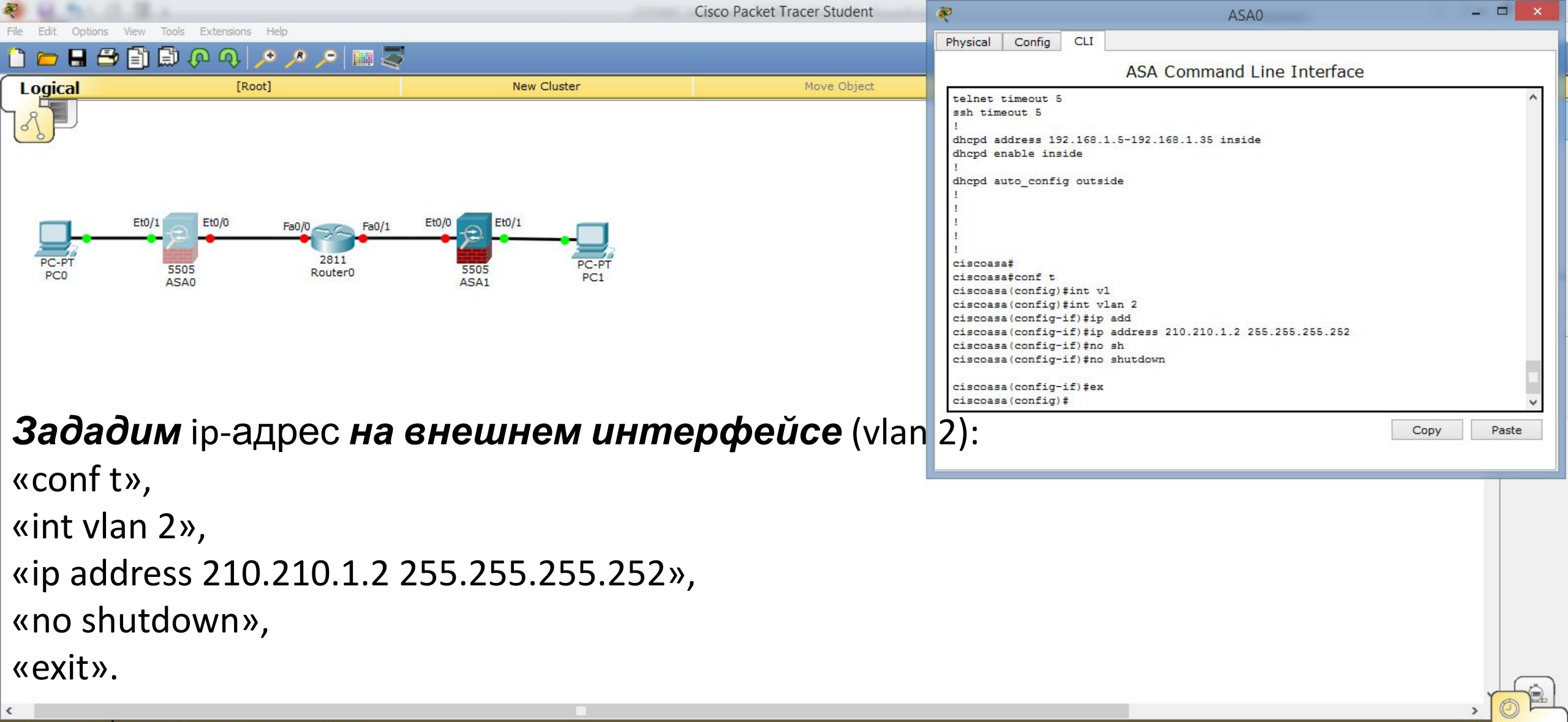


Для продолжения просмотра нажимаем <Пробел>.
Видим, что interface Vlan2 ***является внешним интерфейсом*** (outside), ip-адрес ***ему не назначен. А*** interface Vlan1 ***является внутренним интерфейсом*** (inside) ***с уже назначенным*** шлюзом***. Его*** ip-адрес: 192.168.1.1 255.255.255.0



Для продолжения просмотра нажимаем <Пробел>.

Видим, что на внутреннем интерфейсе уже настроен DHCP***, при этом указан диапазон*** ip-адресов: 192.168.1.5 - 192.168.1.35



Зададим ip-адрес ***на внешнем интерфейсе*** (vlan 2):

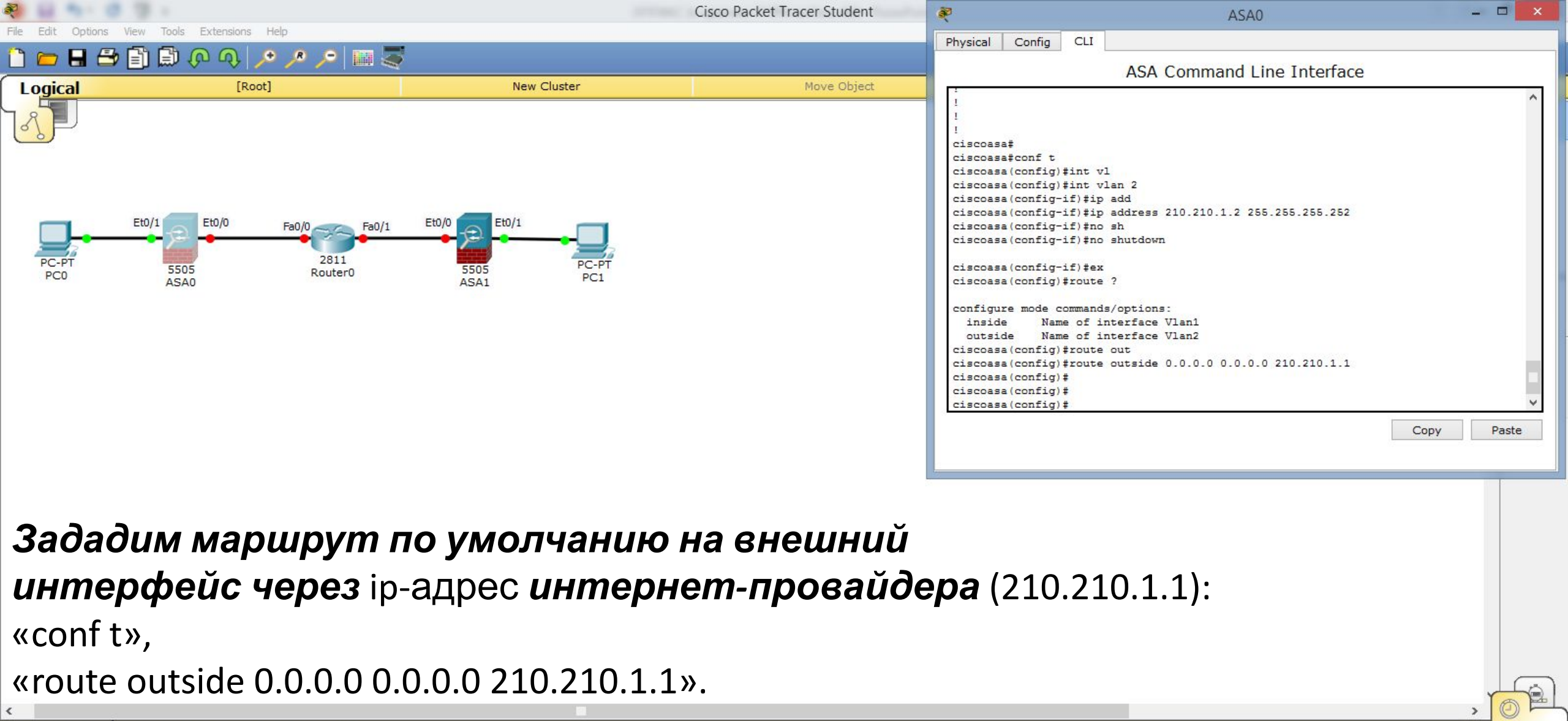
«conf t»,

«int vlan 2»,

«ip address 210.210.1.2 255.255.255.252»,

«no shutdown»,

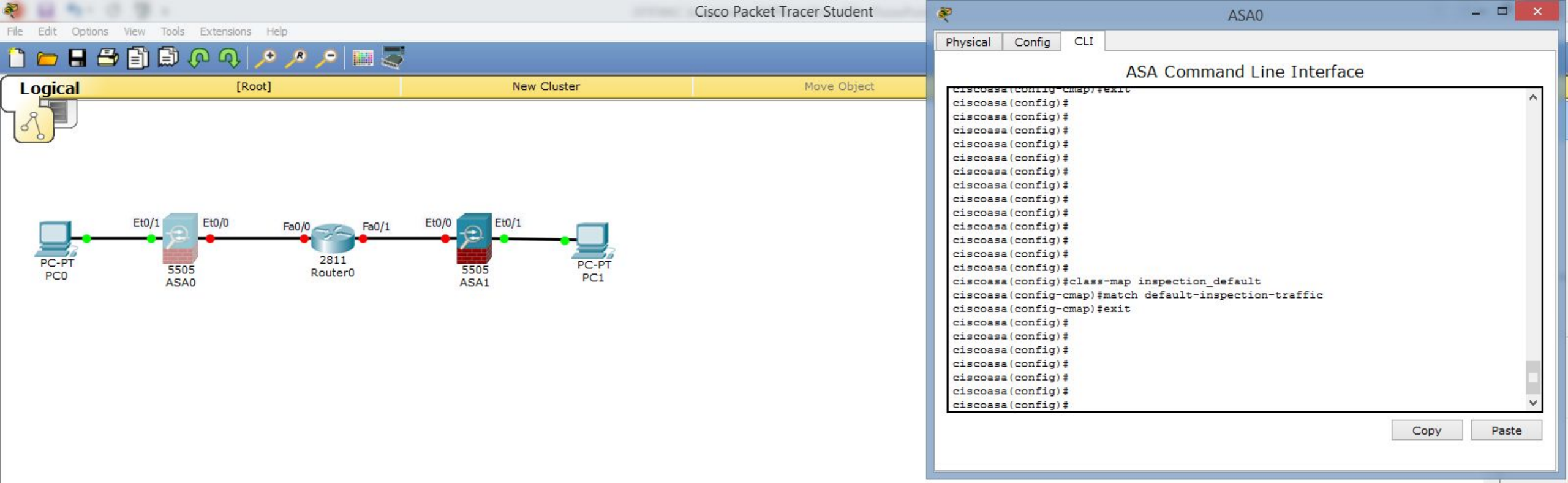
«exit».



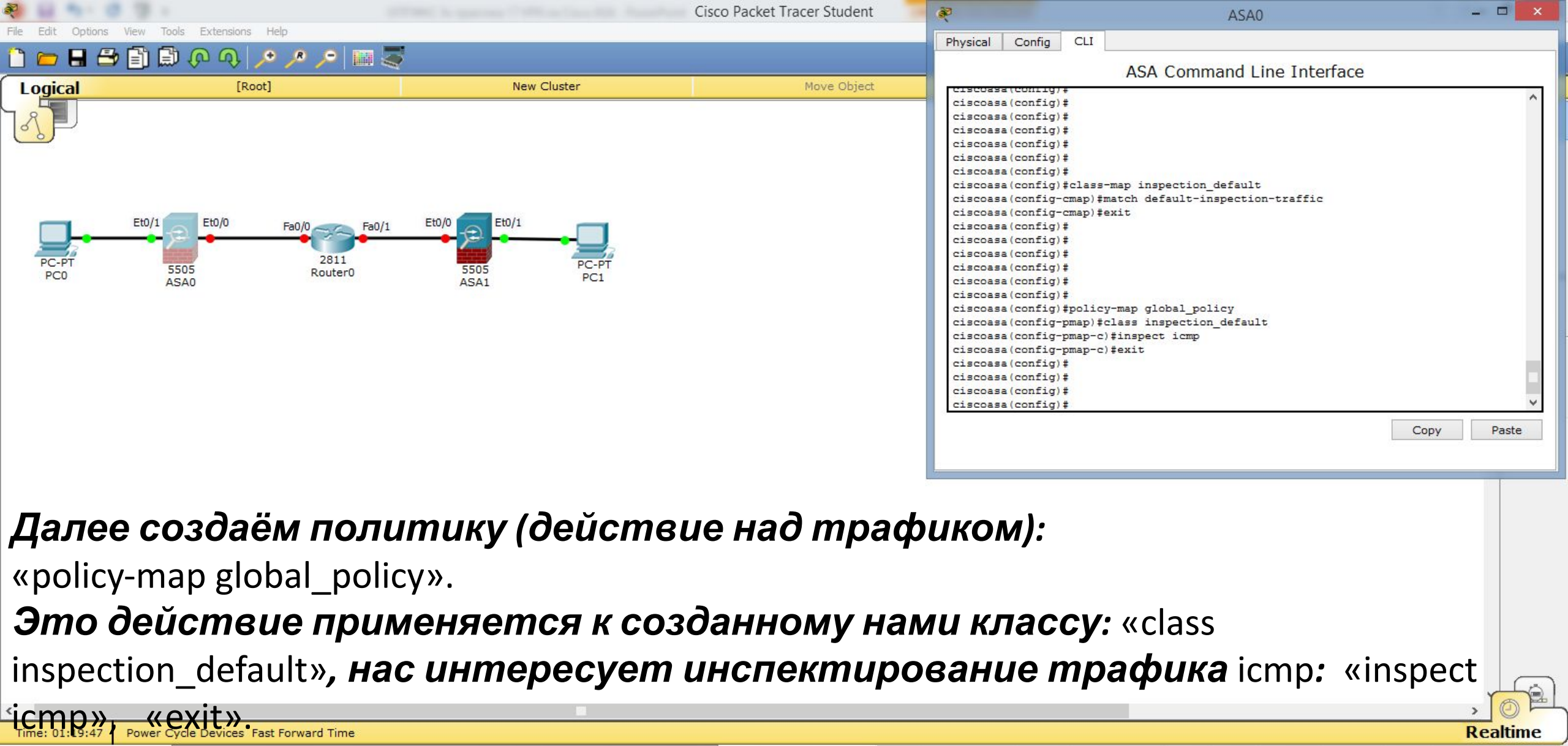
Зададим маршрут по умолчанию на внешний интерфейс через ip-адрес ***интернет-провайдера*** (210.210.1.1):

«conf t»,

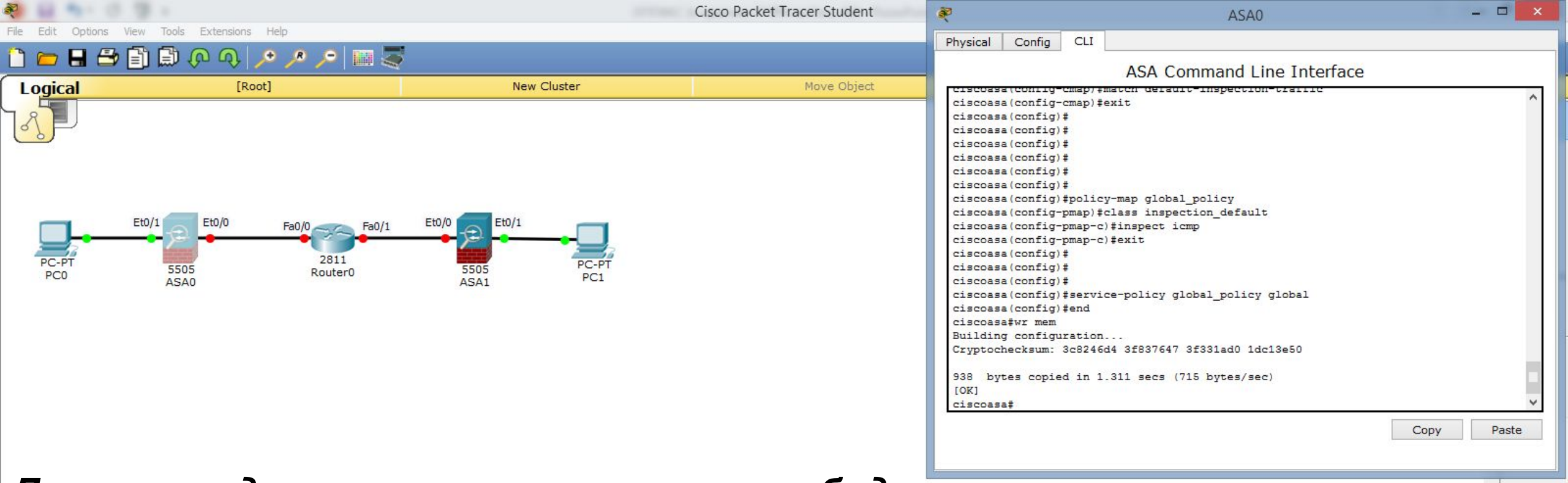
«route outside 0.0.0.0 0.0.0.0 210.210.1.1».



Далее нужно настроить инспектирование трафика.
Сначала определяем тип трафика, который хотим инспектировать:
«class-map inspection_default», ***указываем весь трафик:***
«match default-inspection-traffic», «exit».



Далее создаём политику (действие над трафиком):
«policy-map global_policy».
Это действие применяется к созданному нами классу: «class inspection_default»***, нас интересует инспектирование трафика*** icmp***:*** «inspect icmp», «exit».

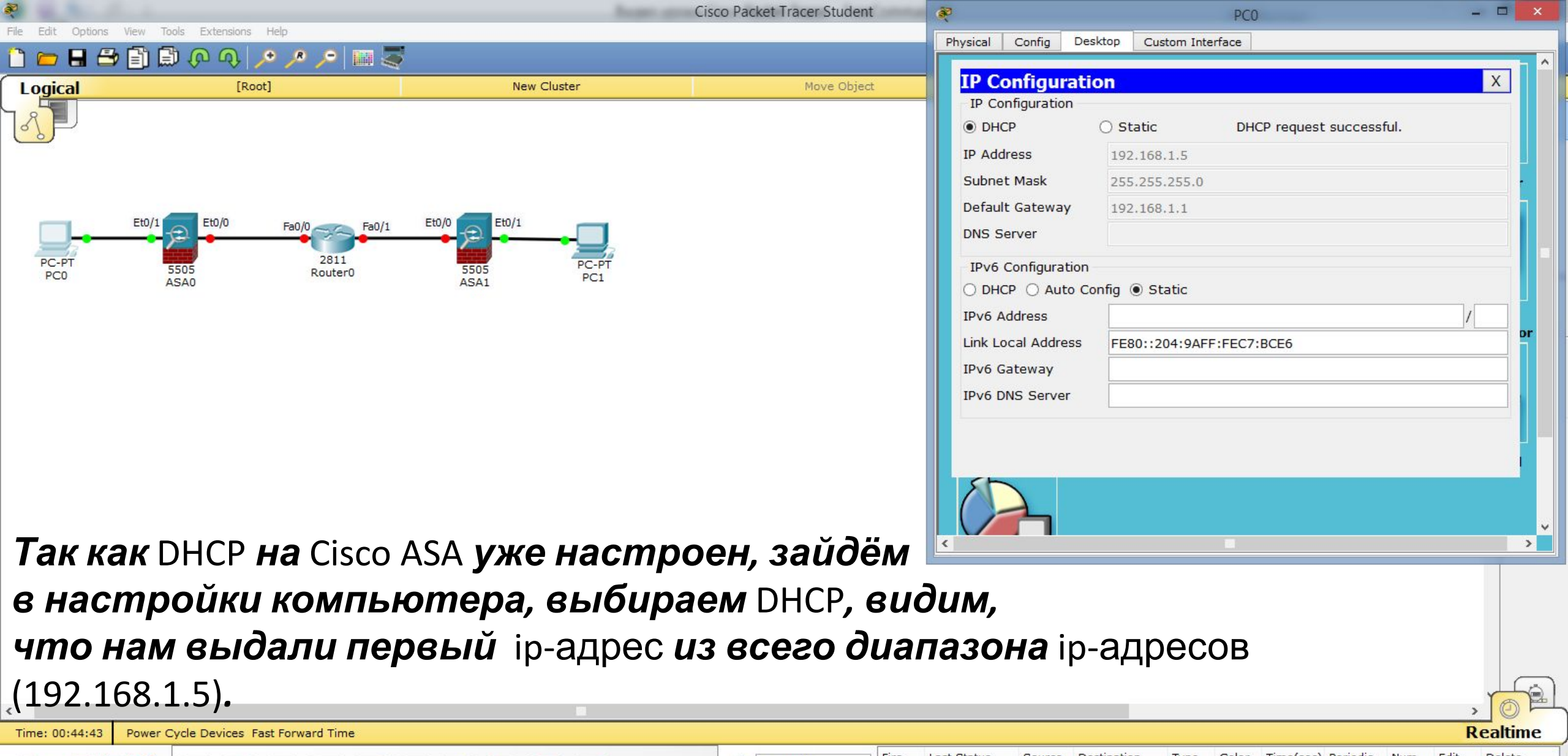


Далее определяем, в каком направлении будем использовать политику инспектирования трафика. В нашем случае во всех направлениях:

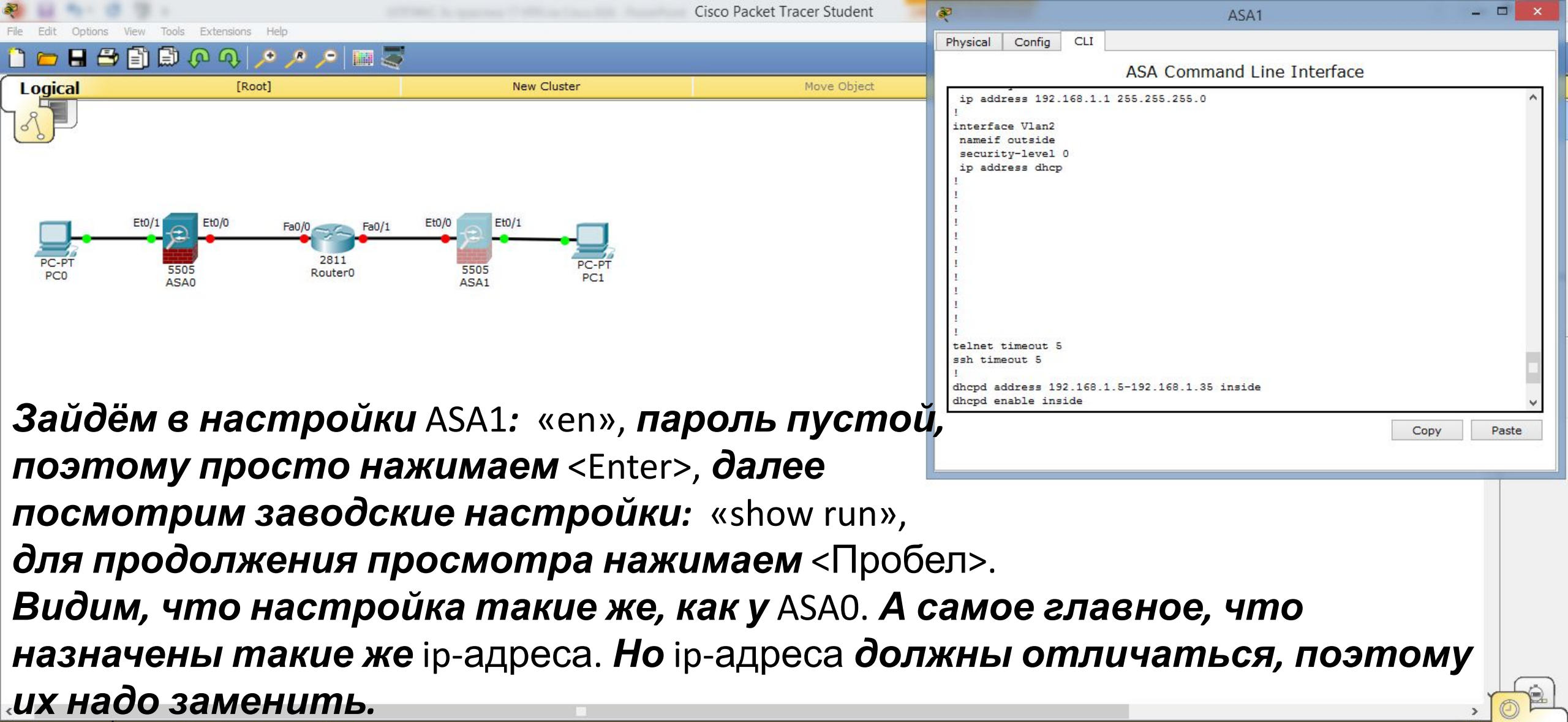
«service-policy global_policy global»,

«end»,

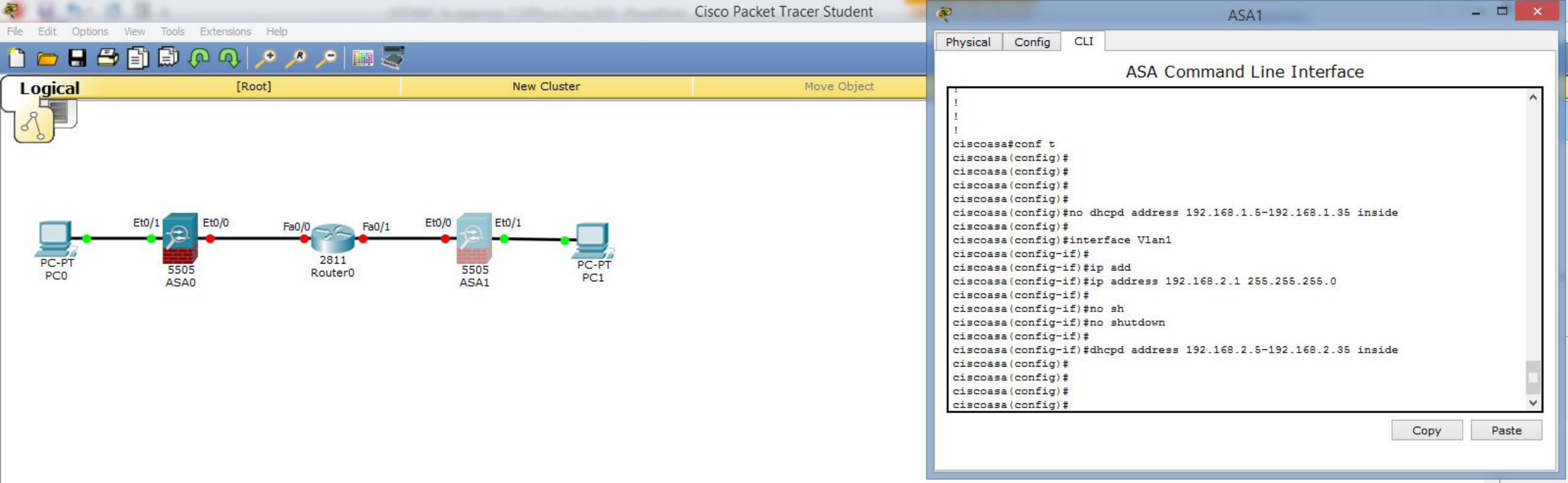
«wr mem».



Так как DHCP ***на*** Cisco ASA ***уже настроен, зайдём в настройки компьютера, выбираем*** DHCP***, видим, что нам выдали первый*** ip-адрес ***из всего диапазона*** ip-адресов (192.168.1.5)**.**

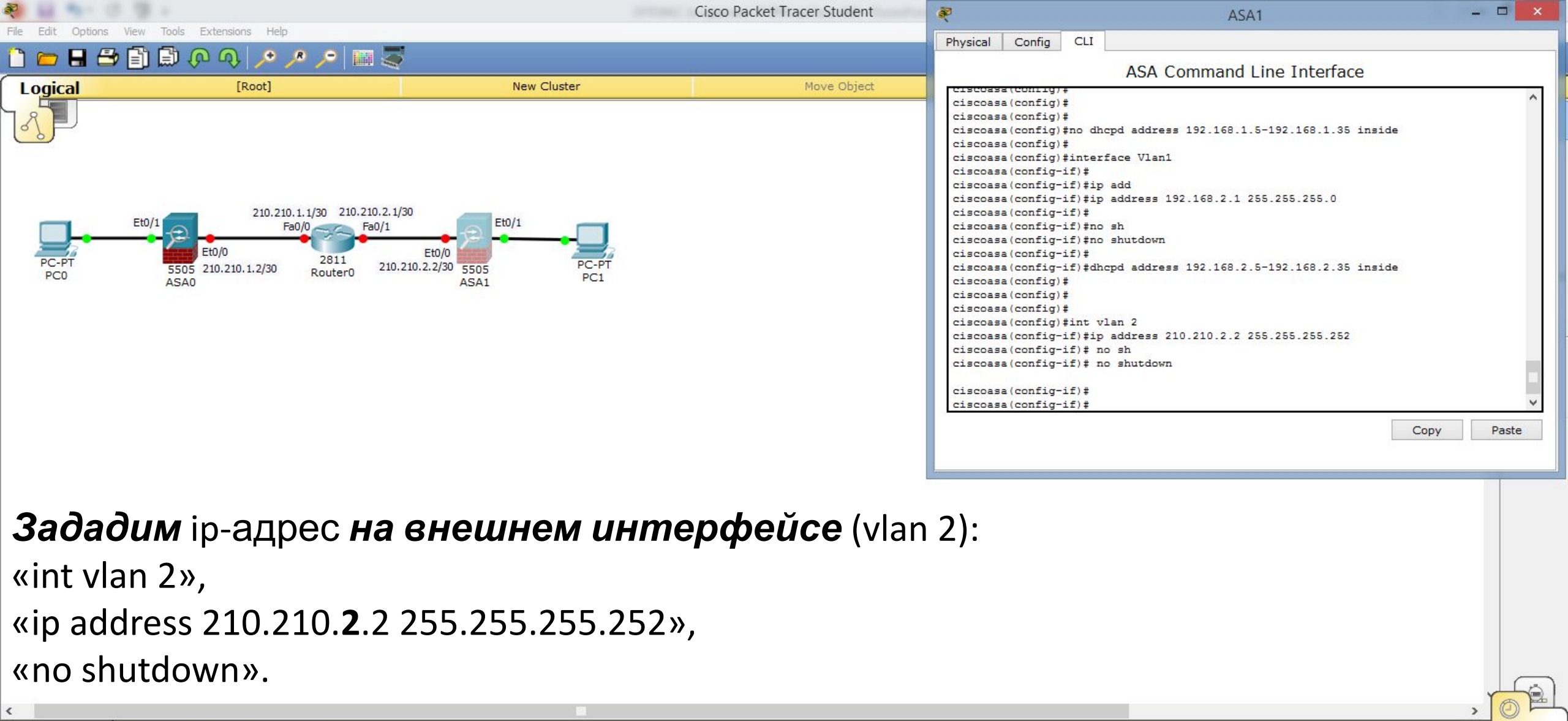


Зайдём в настройки ASA1***:*** «en», ***пароль пустой, поэтому просто нажимаем*** <Enter>, ***далее посмотрим заводские настройки:*** «show run», ***для продолжения просмотра нажимаем*** <Пробел>. ***Видим, что настройка такие же, как у*** ASA0. ***А самое главное, что назначены такие же*** ip-адреса. ***Но*** ip-адреса ***должны отличаться, поэтому их надо заменить.***



Для этого удалим pool ip-адресов DHCP ***и исправим*** ip-адрес ***на внутреннем интерфейсе*** (vlan 1)***:*** «conf t», «no dhcpd address 192.168.1.5-192.168.1.35 inside», «interface Vlan1», «ip address 192.168.**2**.1 255.255.255.0», «no shutdown».

Добавим новый pool***:*** «dhcpd address 192.168.2.5-192.168.2.35 inside».

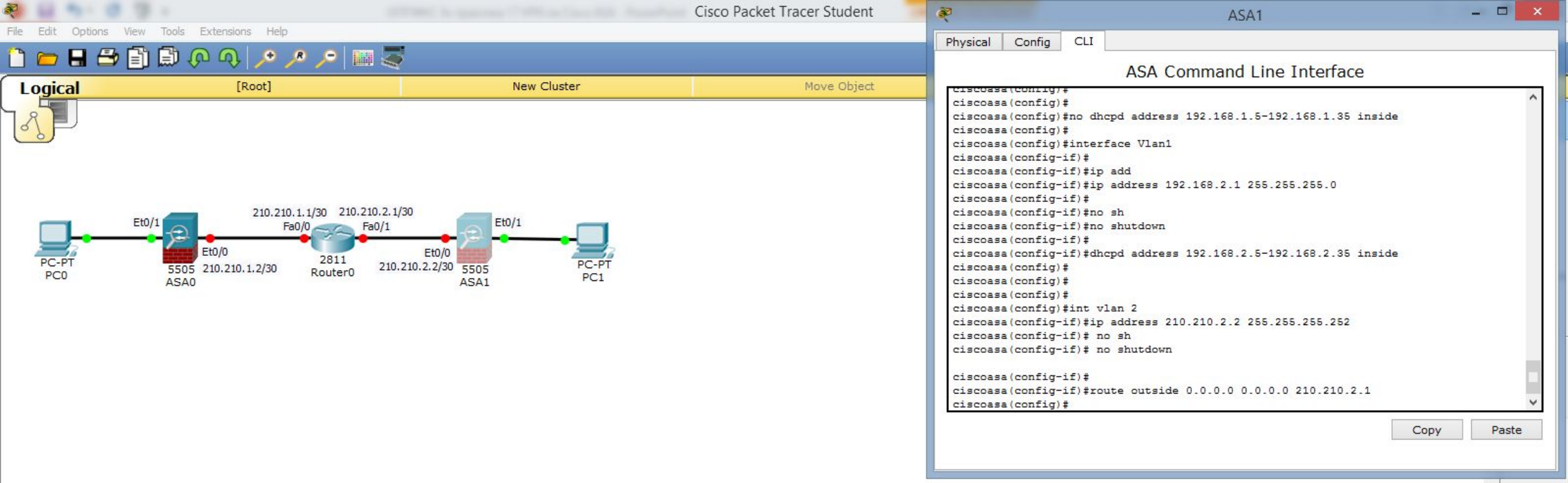


Зададим ip-адрес ***на внешнем интерфейсе*** (vlan 2):

«int vlan 2»,

«ip address 210.210.**2**.2 255.255.255.252»,

«no shutdown».



Зададим маршрут по умолчанию на внешний интерфейс через ip-адрес ***интернет-провайдера*** (210.210.**2**.1):

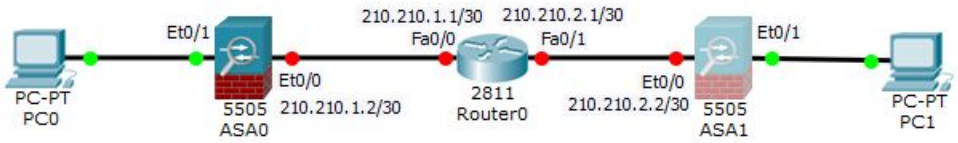
«conf t»,

«route outside 0.0.0.0 0.0.0.0 210.210.**2**.1».

Cisco Packet Tracer Student

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object



ASA1

Physical Config CLI

ASA Command Line Interface

```
ciscoasa(config-if)#no sh
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#
ciscoasa(config-if)#dhcpd address 192.168.2.5-192.168.2.35 inside
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip address 210.210.2.2 255.255.255.252
ciscoasa(config-if)# no sh
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)#
ciscoasa(config-if)#route outside 0.0.0.0 0.0.0.0 210.210.2.1
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#
ciscoasa(config-cmap)#exit
ciscoasa(config)#
ciscoasa(config)#
```

Copy Paste

Далее нужно настроить инспектирование трафика.
Сначала определяем тип трафика, который хотим инспектировать:
«class-map inspection_default», ***указываем весь трафик:***
«match default-inspection-traffic», «exit».

Time: 02:16:14 Power Cycle Devices Fast Forward Time Realtime

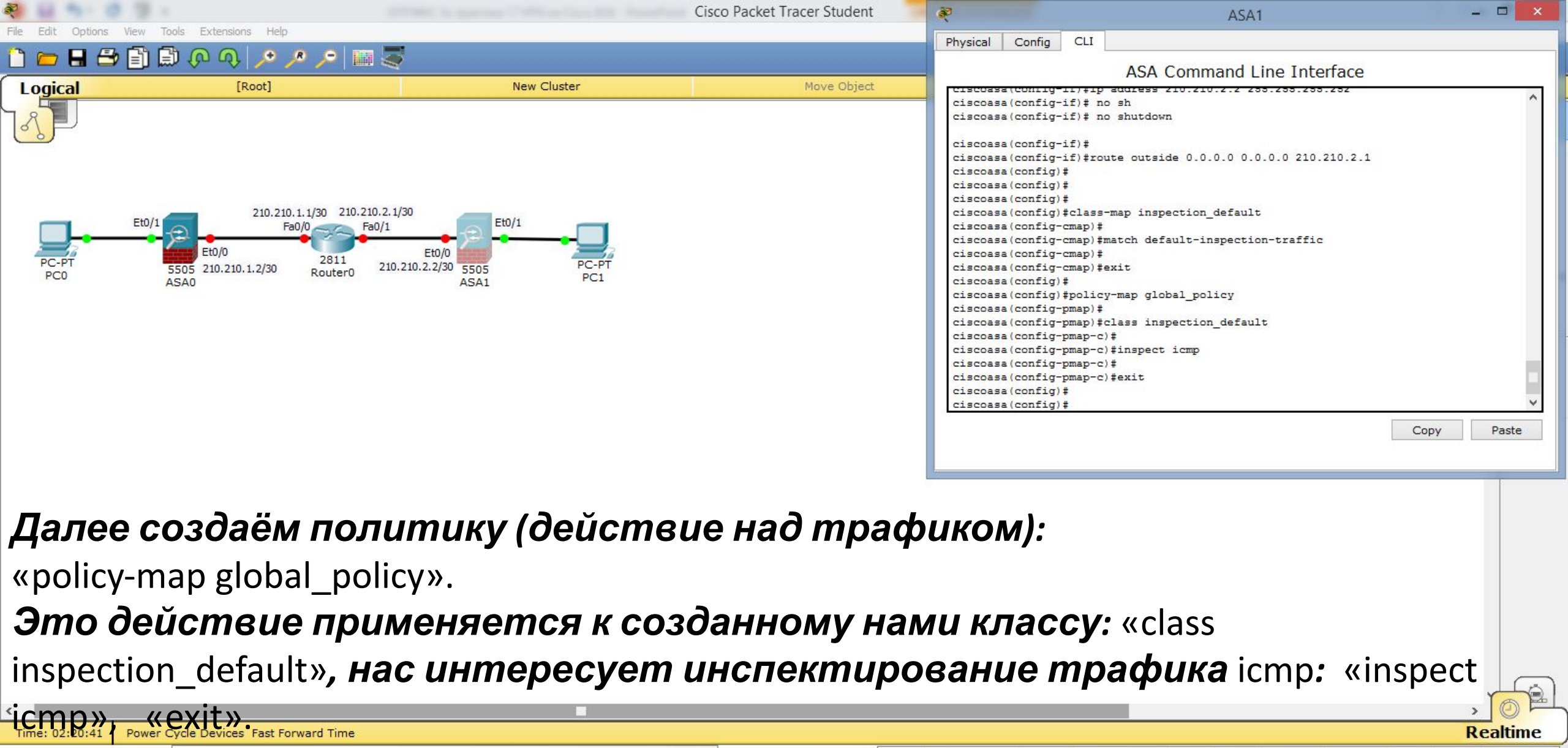
Connections

Copper Straight-Through

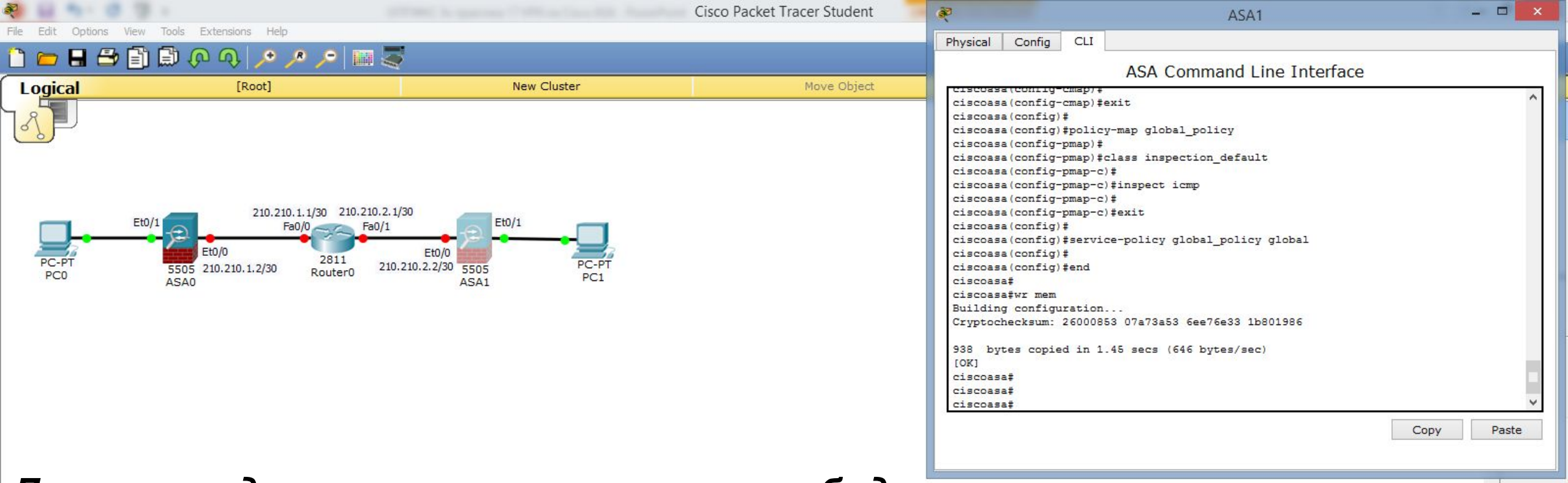
Scenario 0 New Delete Toggle PDU List Window

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

ENG 23:09 23.01.2020



Далее создаём политику (действие над трафиком):
«policy-map global_policy».
Это действие применяется к созданному нами классу: «class inspection_default»***, нас интересует инспектирование трафика*** icmp***:*** «inspect icmp», «exit».

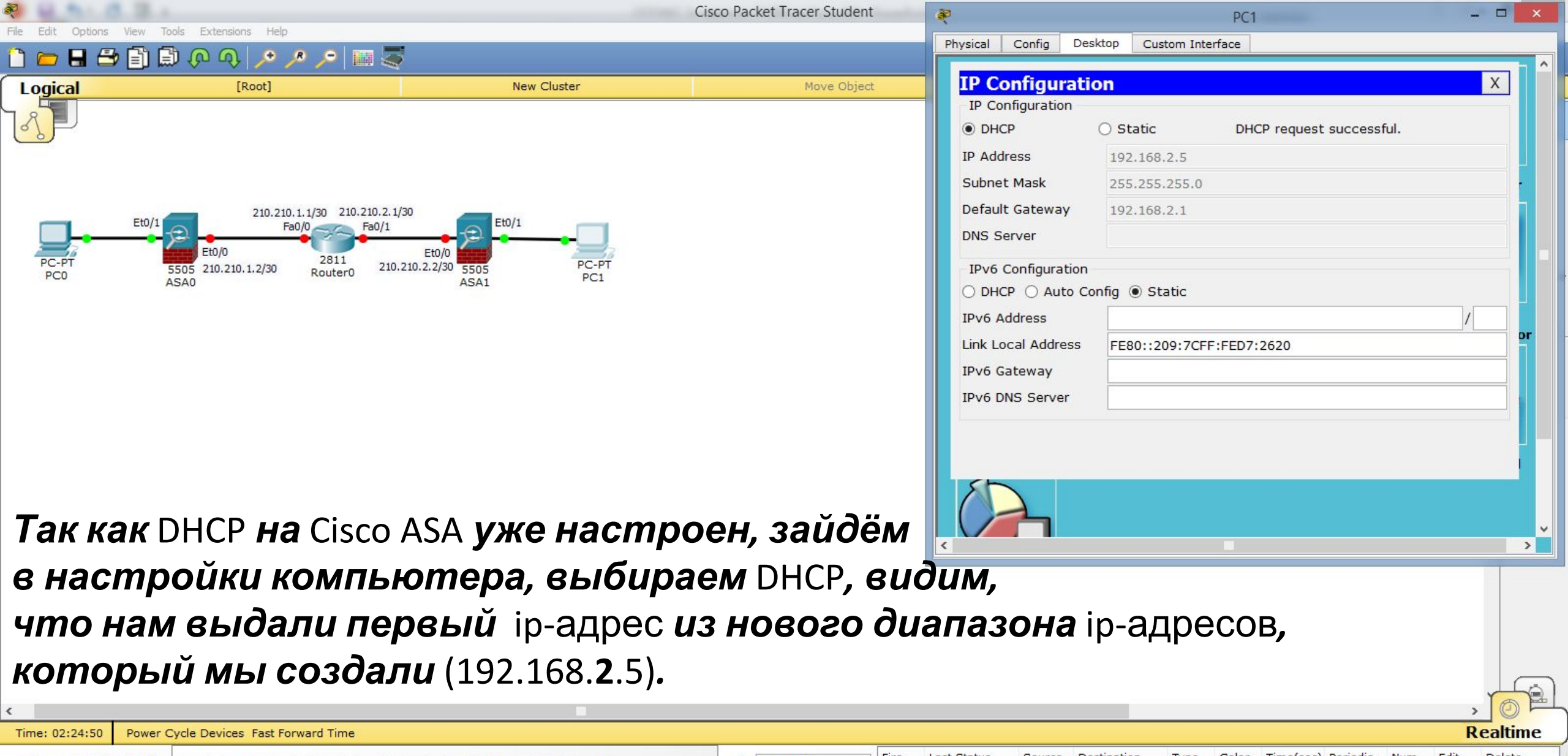


Далее определяем, в каком направлении будем использовать политику инспектирования трафика. В нашем случае во всех направлениях:

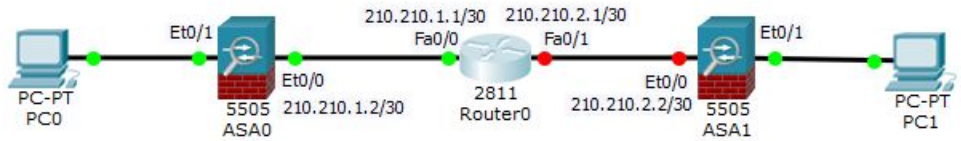
«service-policy global_policy global»,

«end»,

«wr mem».



Так как DHCP ***на*** Cisco ASA ***уже настроен, зайдём в настройки компьютера, выбираем*** DHCP***, видим, что нам выдали первый*** ip-адрес ***из нового диапазона*** ip-адресов***, который мы создали*** (192.168.**2**.5)***.***



Настроим ip-адреса ***на маршрутизаторе интернет-провайдера*** (Router0)***:***

«n»,

«en»,

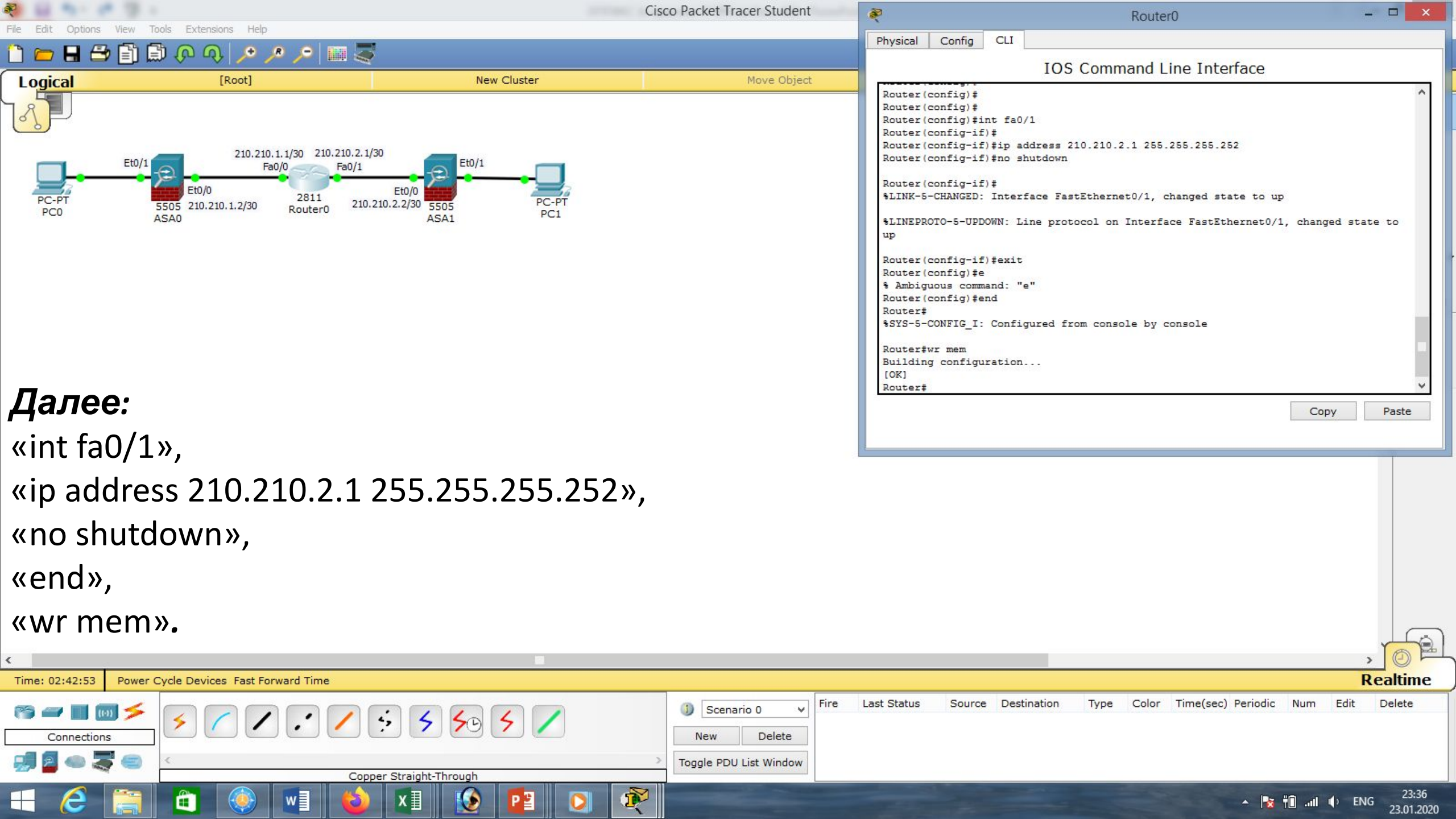
«conf t»,

«int fa0/0»,

«ip address 210.210.1.1 255.255.255.252»,

«no shutdown»,

«exit».



Далее:

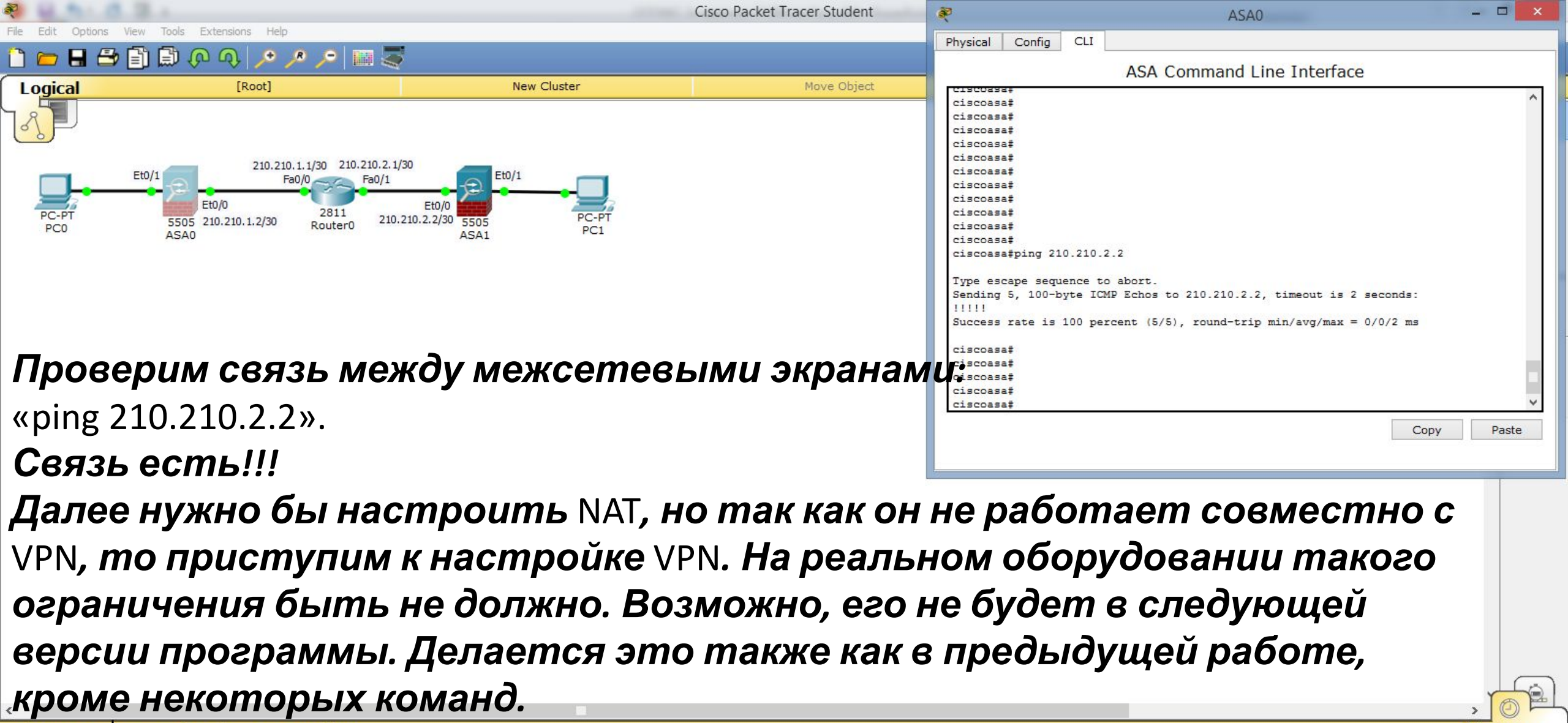
«int fa0/1»,

«ip address 210.210.2.1 255.255.255.252»,

«no shutdown»,

«end»,

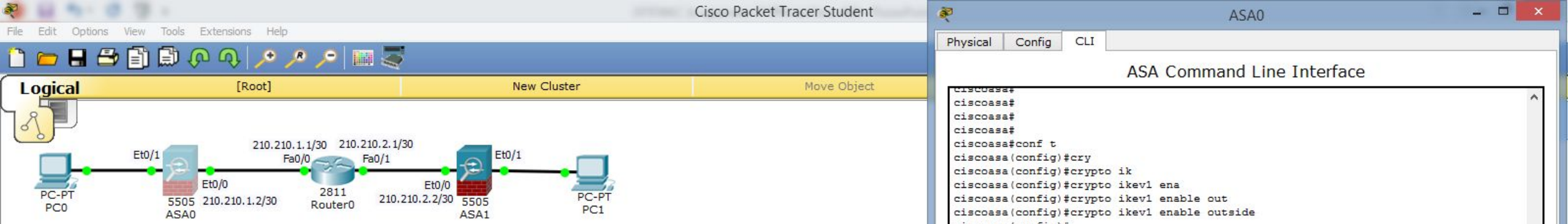
«wr mem».

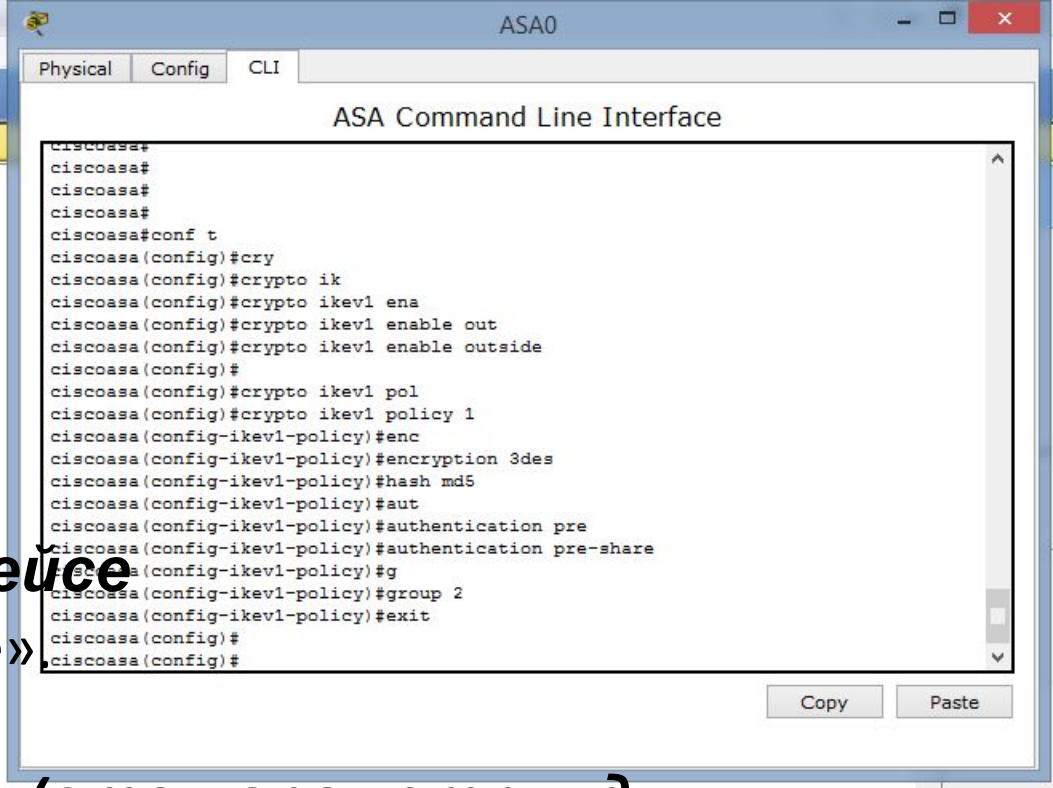


Проверим связь между межсетевыми экранами: «ping 210.210.2.2».

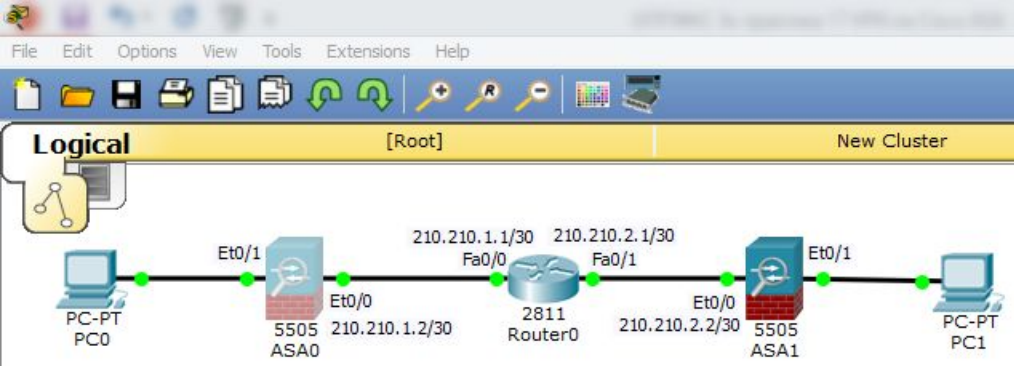
Связь есть!!!

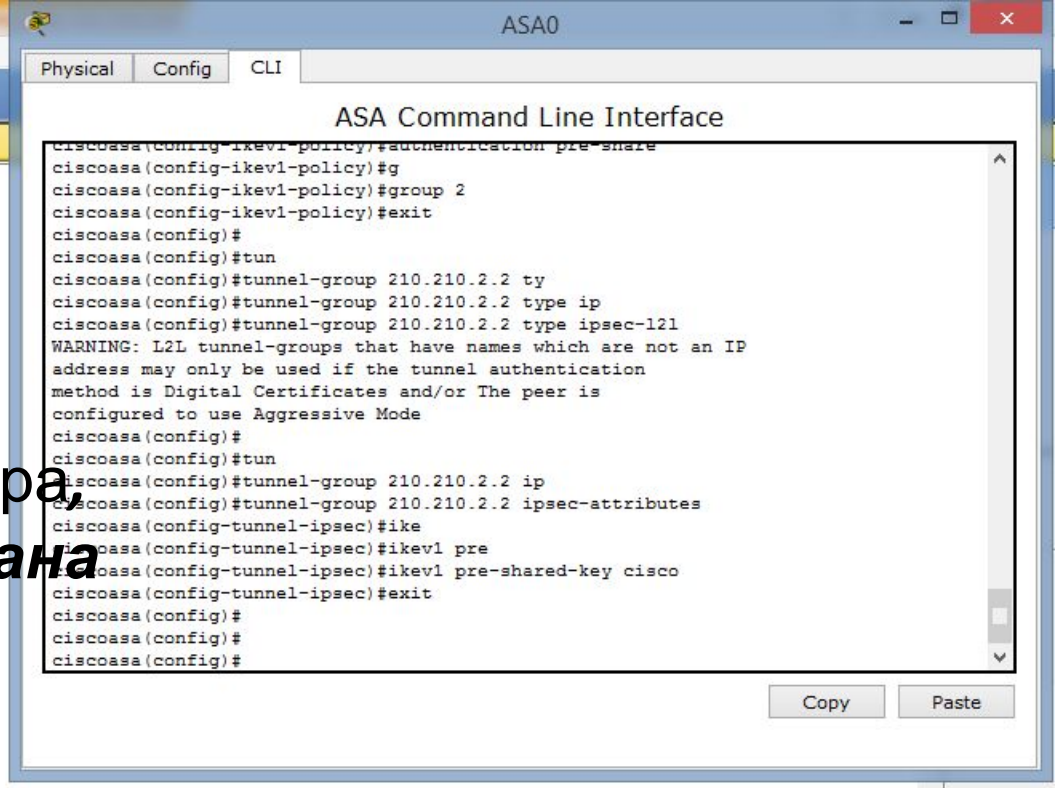
Далее нужно бы настроить NAT***, но так как он не работает совместно с*** VPN***, то приступим к настройке*** VPN***. На реальном оборудовании такого ограничения быть не должно. Возможно, его не будет в следующей версии программы. Делается это также как в предыдущей работе, кроме некоторых команд.***





Начнём с маршрутизатора центрального офиса Router0***. Для начала нам необходимо настроить*** первую фазу***. На внешнем интерфейсе включим протокол*** ike***:*** «crypto ikev1 enable outside». ***Далее создаётся*** политика***:*** «crypto ikev1 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 ***межсетевого экрана*** ASA1***, с которым будем строить*** VPN***:***

«tunnel-group 210.210.2.2 type ipsec-l2l».

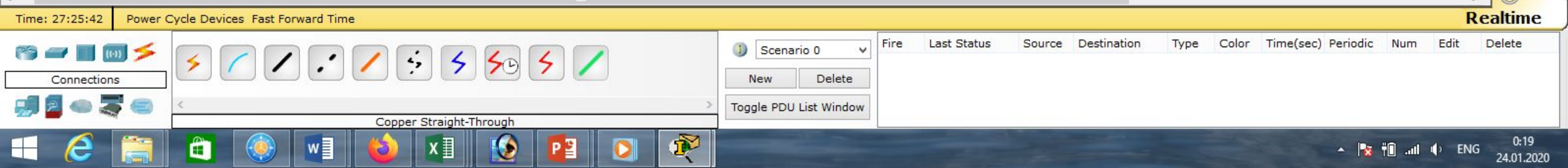
Зададим атрибуты ipsec***:***

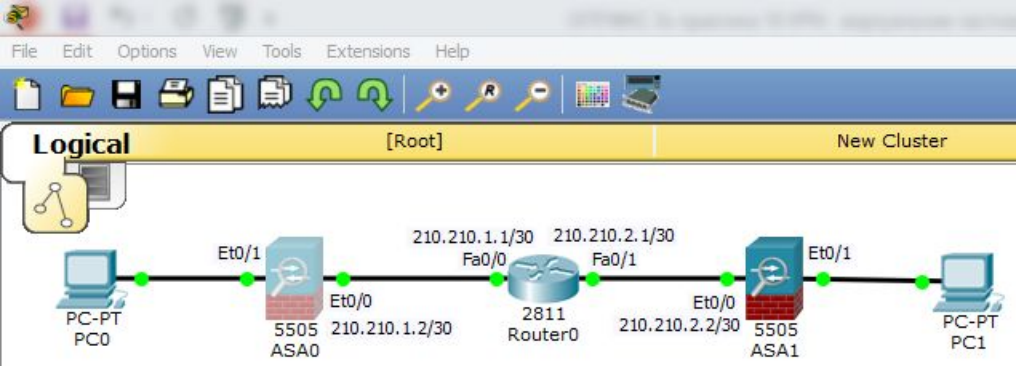
«tunnel-group 210.210.2.2 ipsec-attributes»,

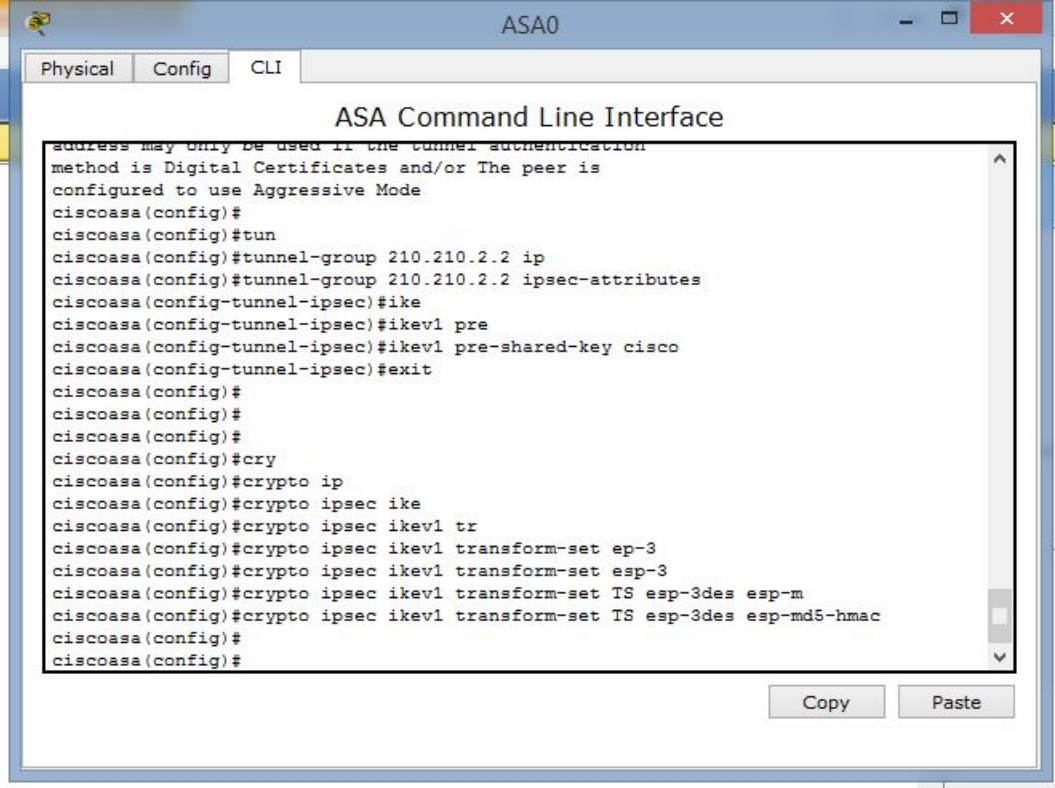
«ikev1 pre-shared-key cisco», «exit».

Мы настроили параметры, необходимые для первой фазы.

Переходим ко второй фазе.

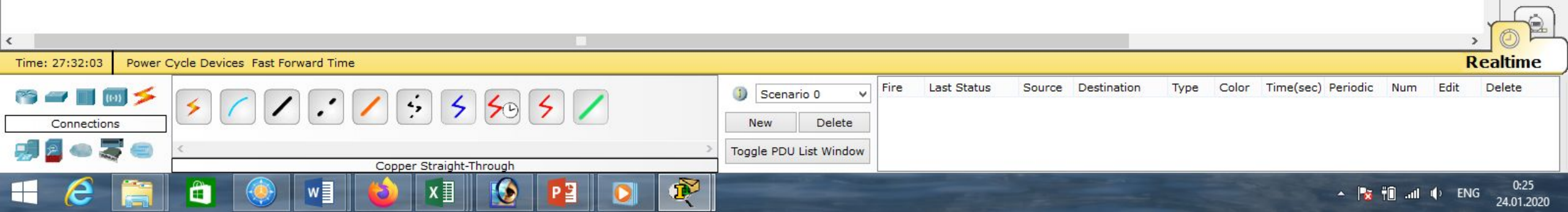


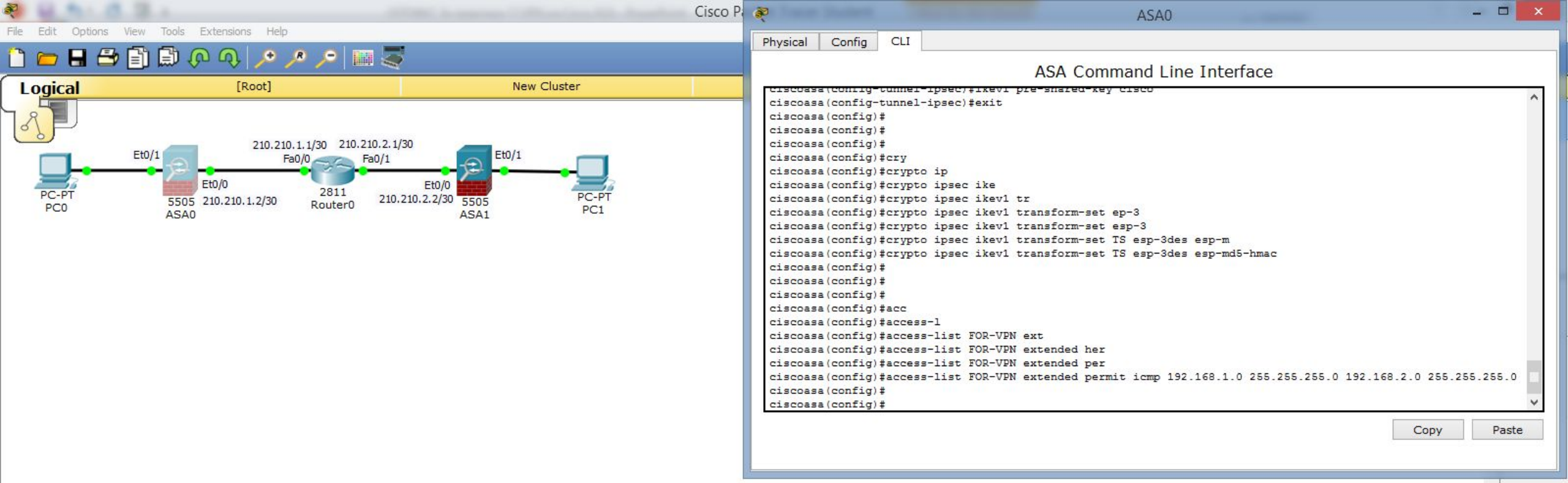




Указываем параметры для построения ipsec-***туннеля с именем*** TS***, далее указываем алгоритм шифрования и хэширования:***

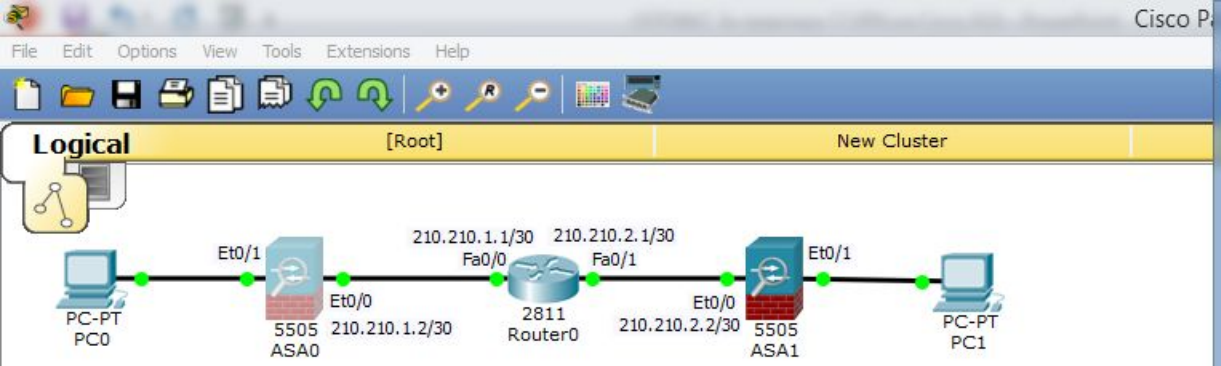
«crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac».

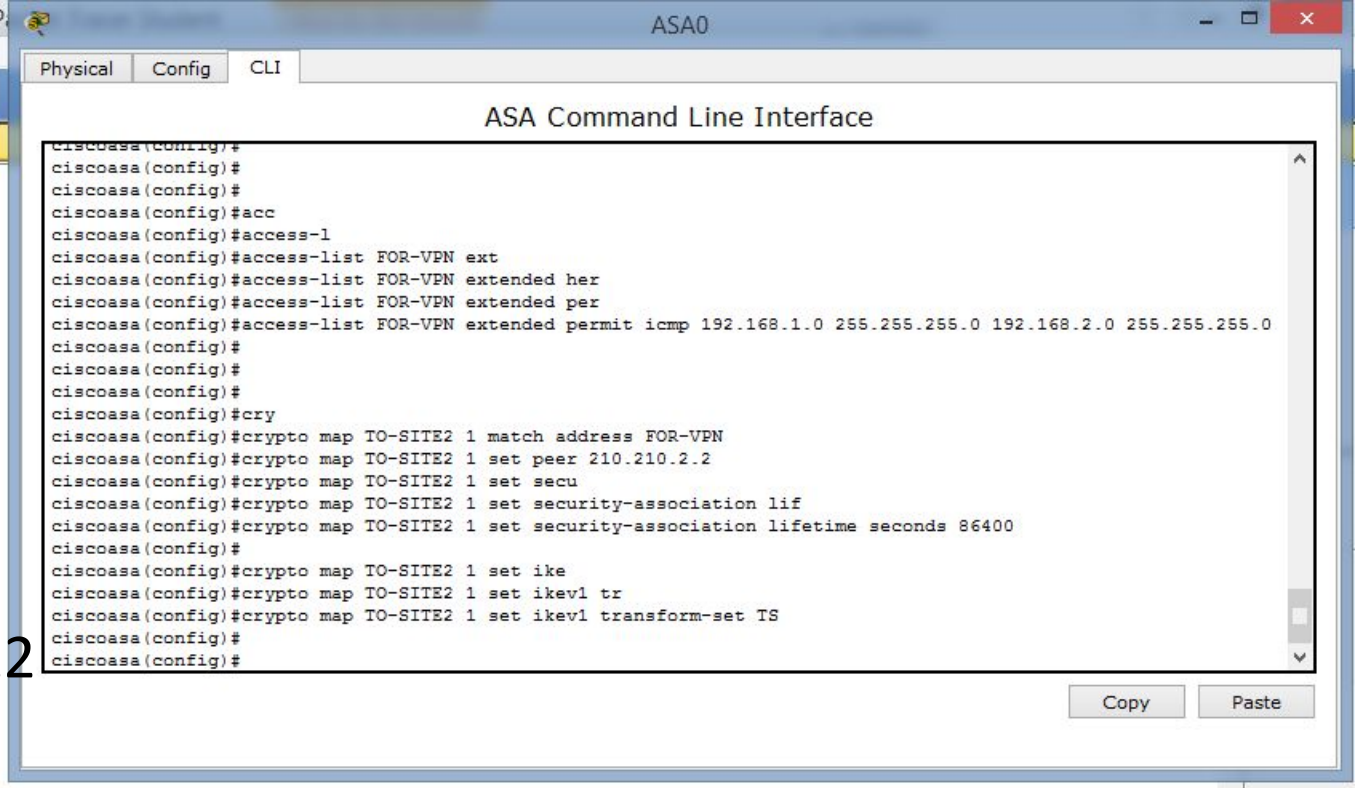




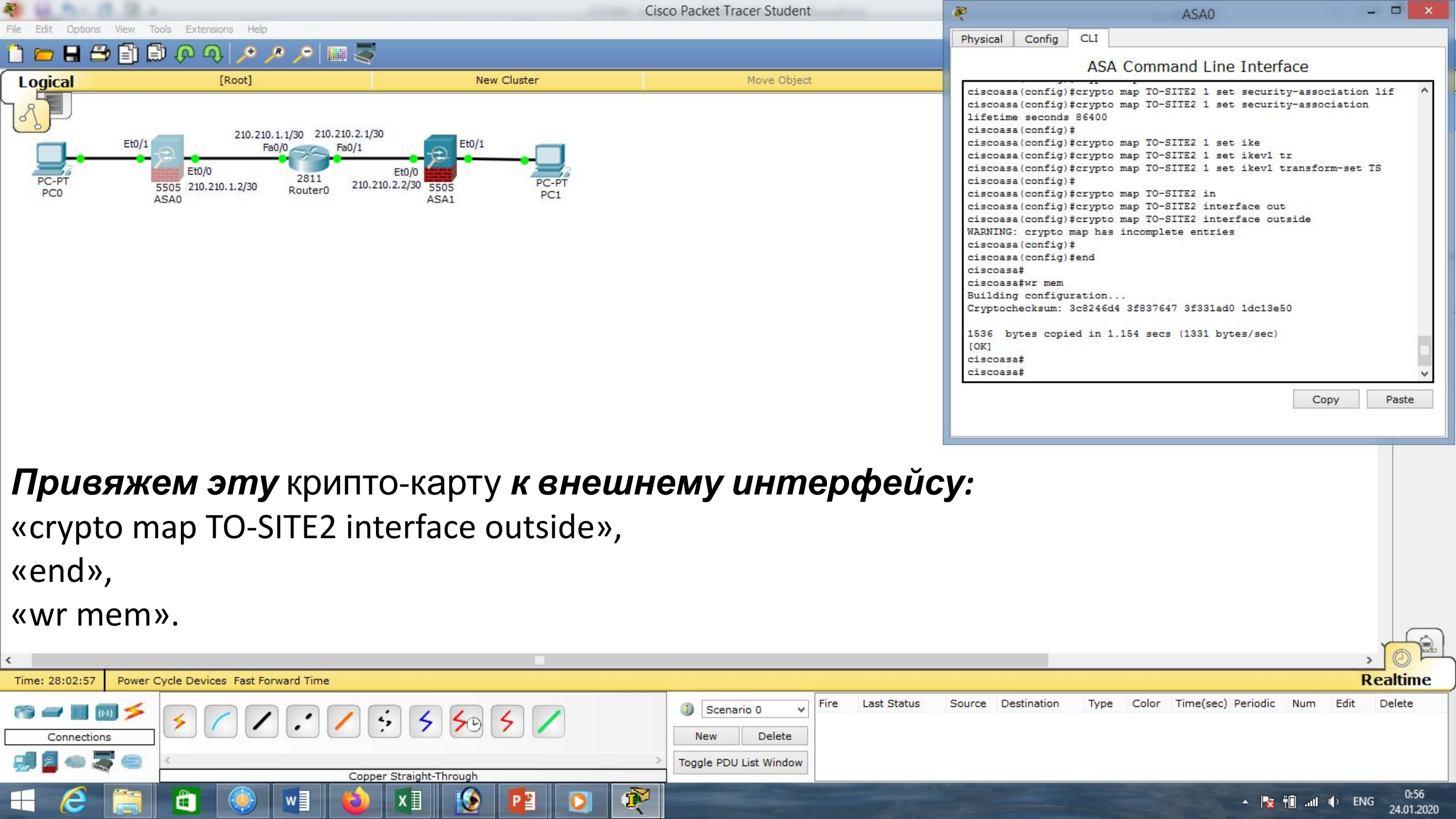
Далее мы должны создать Access List ***с именем*** FOR-VPN***, то есть определить, какой трафик мы будем направлять в*** VPN ***-туннель:***

«access-list FOR-VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0».





Создаём крипто-карту ***с именем*** TO-SITE2 ***под номером*** 1***:***
«crypto map TO-SITE2 1 match address FOR-VPN»,
указываем пир, то есть внешний ip-адрес ***межсетевого экрана*** ASA1***:***
«crypto map TO-SITE2 1 set peer 210.210.2.2»***, и указываем*** lifetime ***туннеля в секундах:*** «crypto map TO-SITE2 1 set security-association lifetime seconds 86400».
Привязываем transform-set TS***:*** «crypto map TO-SITE2 1 set ikev1 transform-set TS».

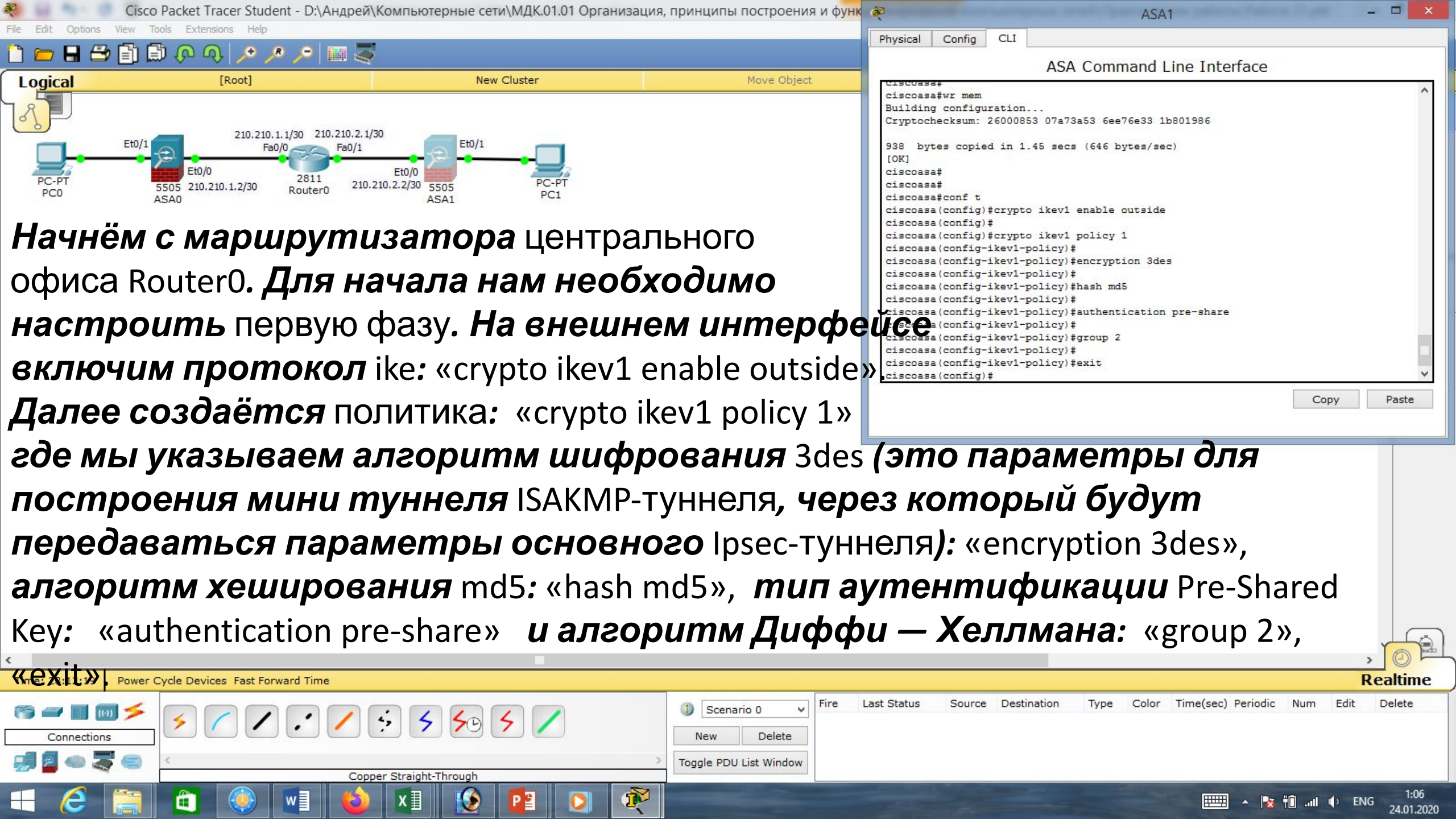


Привяжем эту крипто-карту ***к внешнему интерфейсу:***

«crypto map TO-SITE2 interface outside»,

«end»,

«wr mem».

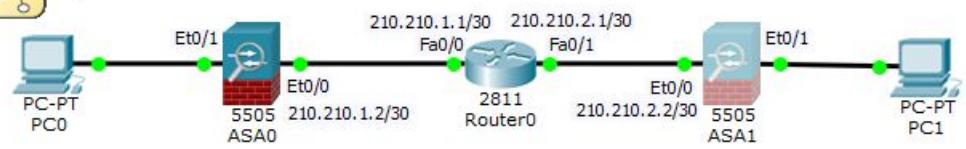


Начнём с маршрутизатора центрального офиса Router0***. Для начала нам необходимо настроить*** первую фазу***. На внешнем интерфейсе включим протокол*** ike***:*** «crypto ikev1 enable outside». ***Далее создаётся*** политика***:*** «crypto ikev1 policy 1» ***где мы указываем алгоритм шифрования*** 3des ***(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».

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

File Edit Options View Tools Extensions Help

Logical | [Root] | New Cluster | Move Object



Настроим ключ аутентификации и адреса пира, ***то есть внешнего*** ip-адреса ***межсетевого экрана*** ASA0***, с которым будем строить*** VPN***:***

«tunnel-group 210.210.**1**.2 type ipsec-l2l».

Зададим атрибуты ipsec***:***

«tunnel-group 210.210.**1**.2 ipsec-attributes»,

«ikev1 pre-shared-key cisco», «exit».

Мы настроили параметры, необходимые для первой фазы.

Переходим ко второй фазе.

ASA1

Physical | Config | CLI

ASA Command Line Interface

```
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#tunnel-group 210.210.1.2 type ipsec-l2l
WARNING: L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode
ciscoasa(config)#tunnel-group 210.210.1.2 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#
ciscoasa(config-tunnel-ipsec)#ikev1 pre-shared-key cisco
ciscoasa(config-tunnel-ipsec)#
ciscoasa(config-tunnel-ipsec)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
```

Copy Paste

Time: 28:18:10 | Power Cycle Devices | Fast Forward Time | Realtime

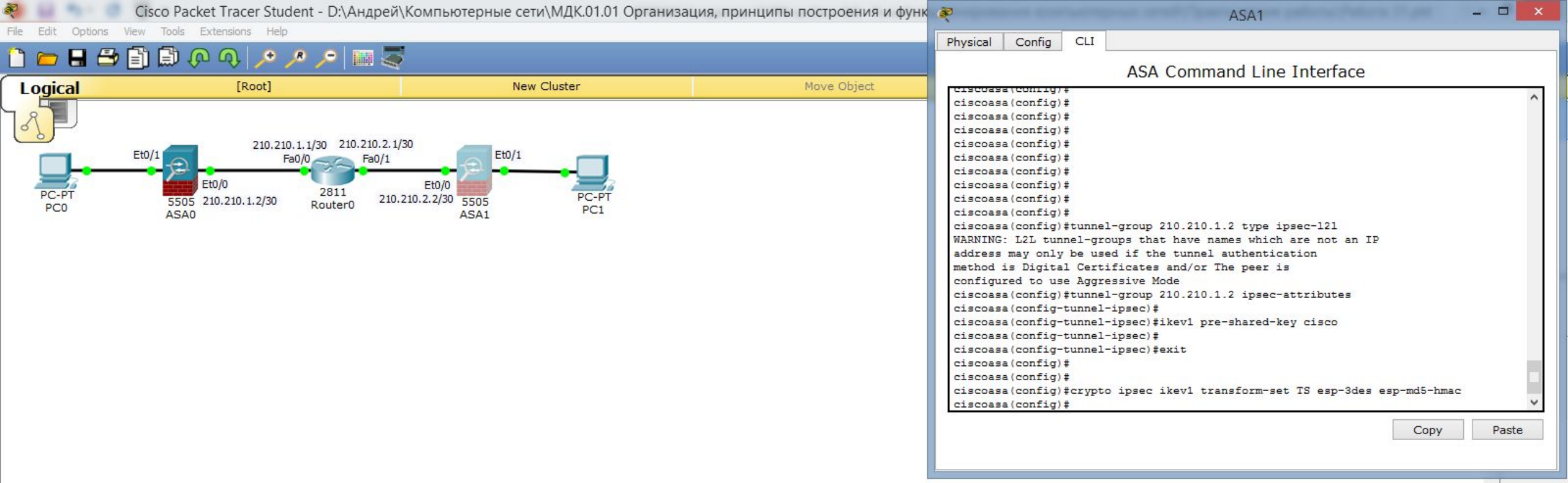
Connections

Copper Straight-Through

Scenario 0 | New | Delete | Toggle PDU List Window

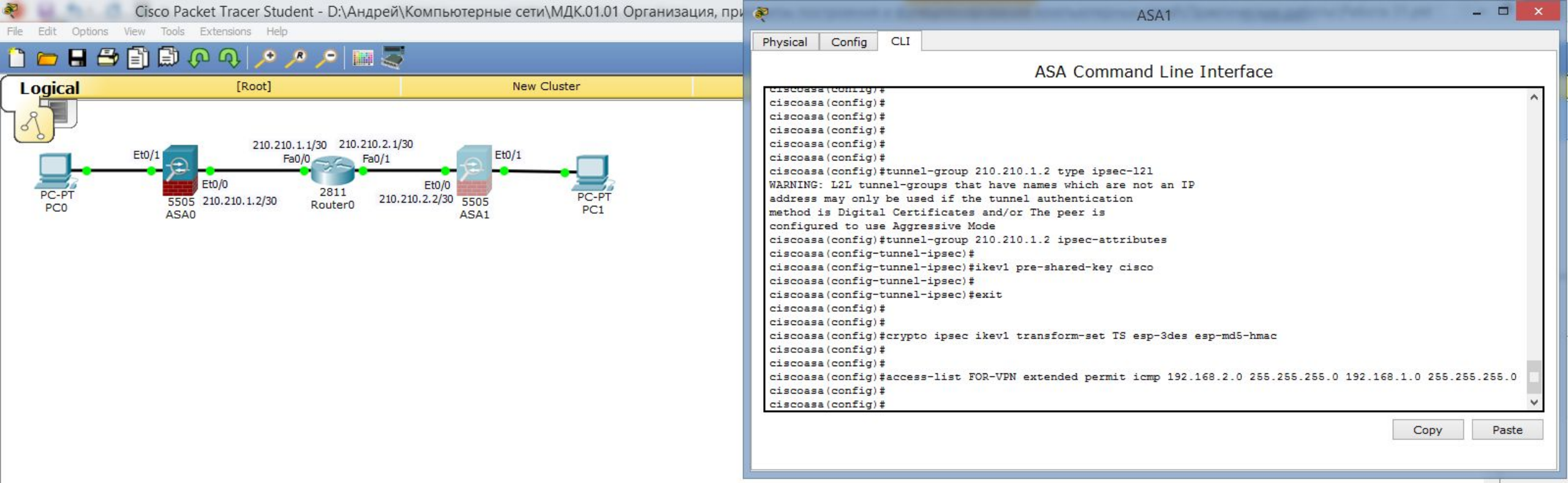
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete

ENG 1:11 24.01.2020



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

«crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac».



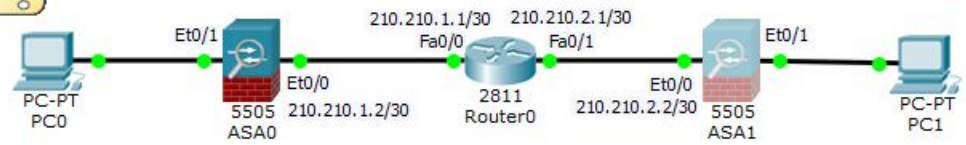
Далее мы должны создать Access List ***с именем*** FOR-VPN***, то есть определить, какой трафик мы будем направлять в*** VPN ***-туннель:***

«access-list FOR-VPN extended permit icmp 192.168.**2**.0 255.255.255.0 192.168.**1**.0 255.255.255.0».

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

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object



ASA1

Physical Config CLI

ASA Command Line Interface

```
ciscoasa(config-tunnel-ipsec)#
ciscoasa(config-tunnel-ipsec)#ikev1 pre-shared-key cisco
ciscoasa(config-tunnel-ipsec)#
ciscoasa(config-tunnel-ipsec)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#access-list FOR-VPN extended permit icmp 192.168.2.0 255.255.255.0
192.168.1.0 255.255.255.0
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#crypto map TO-SITE1 1 match address FOR-VPN
ciscoasa(config)#
ciscoasa(config)#crypto map TO-SITE1 1 set peer 210.210.1.2
ciscoasa(config)#
ciscoasa(config)#crypto map TO-SITE1 1 set security-association lifetime seconds 86400
ciscoasa(config)#
ciscoasa(config)#crypto map TO-SITE1 1 set ikev1 transform-set TS
ciscoasa(config)#
ciscoasa(config)#
```

Copy Paste

Создаём крипто-карту ***с именем*** TO-SITE2 ***под номером*** 1***:***

«crypto map TO-SITE**1** 1 match address FOR-VPN»,

указываем пир, то есть внешний ip-адрес ***межсетевого экрана*** ASA1***:***

«crypto map TO-SITE**1** 1 set peer 210.210.**1**.2»***, и указываем*** lifetime ***туннеля в секундах:*** «crypto map TO-SITE**1** 1 set security-association lifetime seconds 86400».

Привязываем transform-set TS***:*** «crypto map TO-SITE**1** 1 set ikev1 transform-set TS».

Time: 28:28:44 Power Cycle Devices Fast Forward Time Realtime

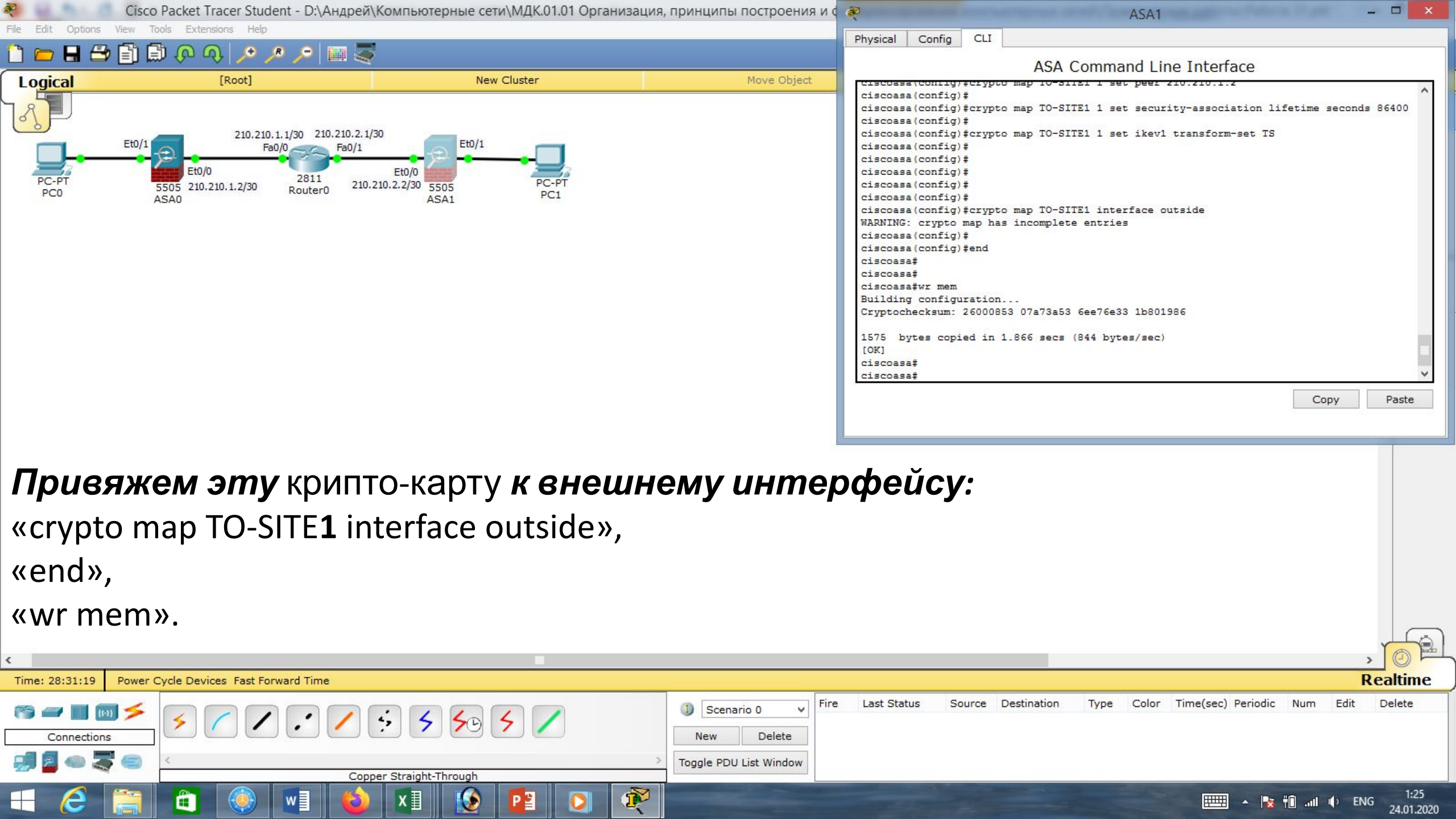
Connections

Copper Straight-Through

Scenario 0 New Delete Toggle PDU List Window

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

ENG 1:22 24.01.2020



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

«crypto map TO-SITE**1** interface outside»,

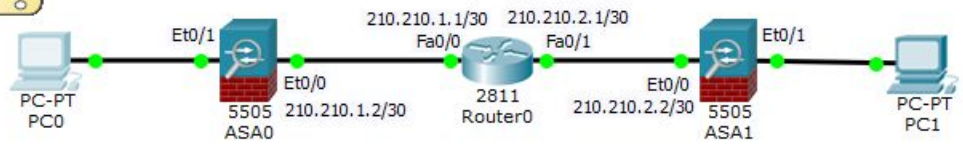
«end»,

«wr mem».

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

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object



PC0

Physical Config Desktop Custom Interface

Command Prompt X

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.2.5

Pinging 192.168.2.5 with 32 bytes of data:

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

Ping statistics for 192.168.2.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Проверим связь между компьютерами из центрального офиса и филиала:

«ping 192.168.2.5».

Связи нет ☹

Time: 48:59:04 Power Cycle Devices Fast Forward Time Realtime

Connections

Copper Straight-Through

Scenario 0 New Delete Toggle PDU List Window

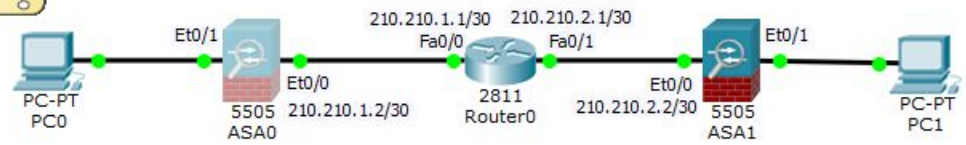
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete

ENG 21:53 24.01.2020

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

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object



ASA0

Physical Config CLI

ASA Command Line Interface

```
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 3c8246d4 3f837647 3f331ad0 1dc13e50

1536  bytes copied in 1.154 secs (1331 bytes/sec)
[OK]
ciscoasa#
ciscoasa#show cry
ciscoasa#show crypto isa
ciscoasa#show crypto isakmp sa

IKEv1 SAs:

   Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 1
1   IKE Peer: 210.210.2.2
    Type    : L2L             Role    : Initiator
    Rekey   : no              State   : MM_NO_STATE

There are no IKEv2 SAs
ciscoasa#
```

Copy Paste

Зайдём на ASA0***. Посмотрим, строится ли туннель:***

«show crypto isakmp sa».

Видим, что технологический туннель построен.

Time: 49:04:17 Power Cycle Devices Fast Forward Time

Realtime

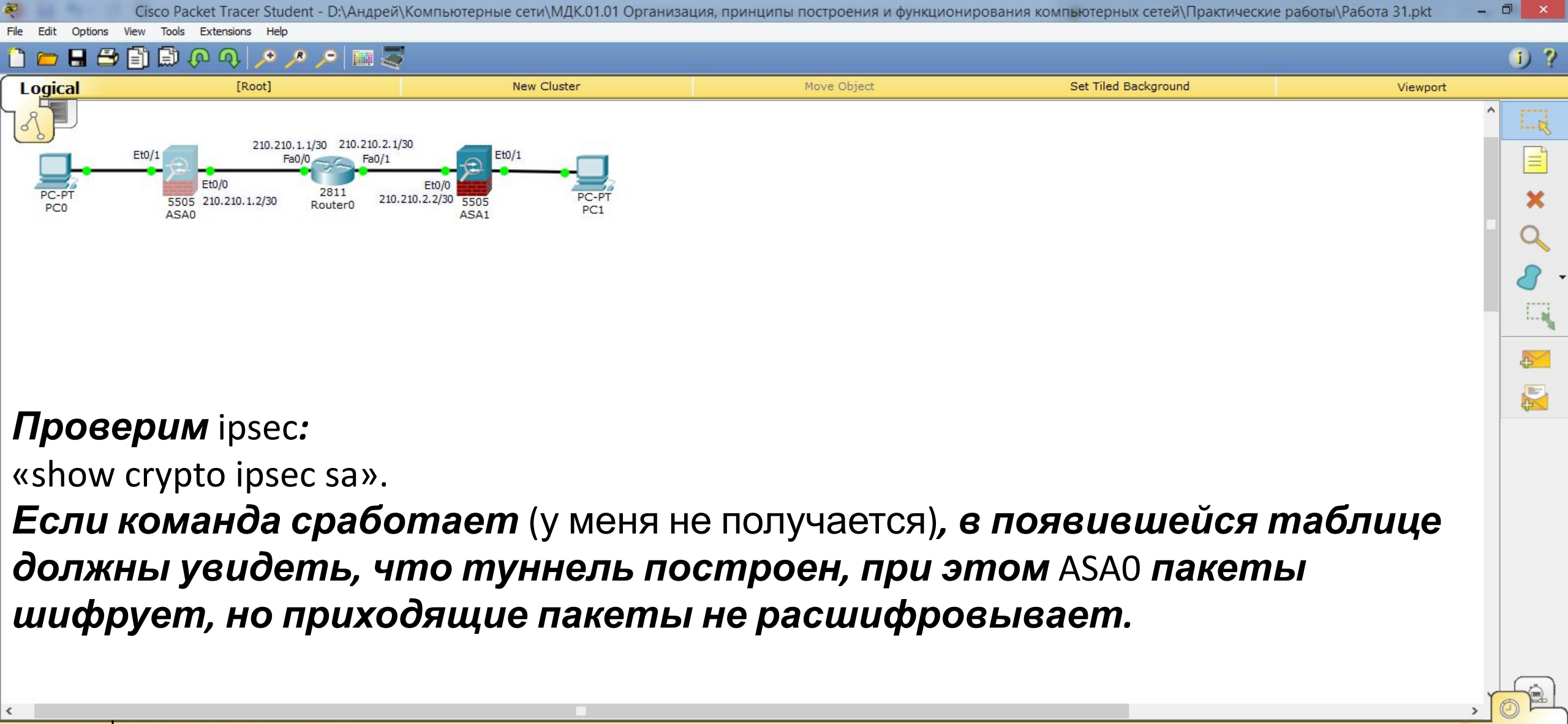
Connections

Copper Straight-Through

Scenario 0 New Delete Toggle PDU List Window

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

ENG 21:58 24.01.2020



Проверим ipsec***:***

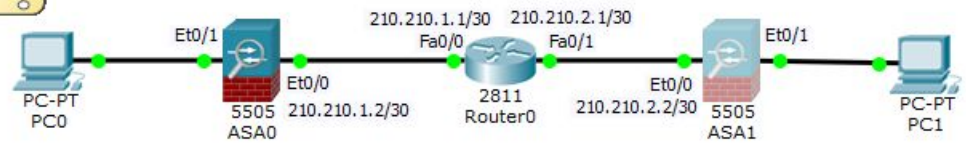
«show crypto ipsec sa».

Если команда сработает (у меня не получается)***, в появившейся таблице должны увидеть, что туннель построен, при этом*** ASA0 ***пакеты шифрует, но приходящие пакеты не расшифровывает.***

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

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object



ASA1

Physical Config CLI

ASA Command Line Interface

```
ciscoasa#show ip
ciscoasa#show ip cry
ciscoasa#show ip cryp
ciscoasa#show cryp
ciscoasa#show crypto ip
ciscoasa#show crypto ipsec sa

There are no ipsec sas
ciscoasa#show crypto isakmp sa

IKEv1 SAs:

  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 1
1   IKE Peer: 210.210.1.2
    Type    : L2L             Role    : responder
    Rekey   : no              State   : QM_IDLE

There are no IKEv2 SAs
ciscoasa#
ciscoasa#
ciscoasa#
```

Copy Paste

Зайдём на ASA1***. Посмотрим, строится ли туннель:***

«show crypto isakmp sa».

Видим, что технологический туннель построен.

Time: 49:24:06 Power Cycle Devices Fast Forward Time Realtime

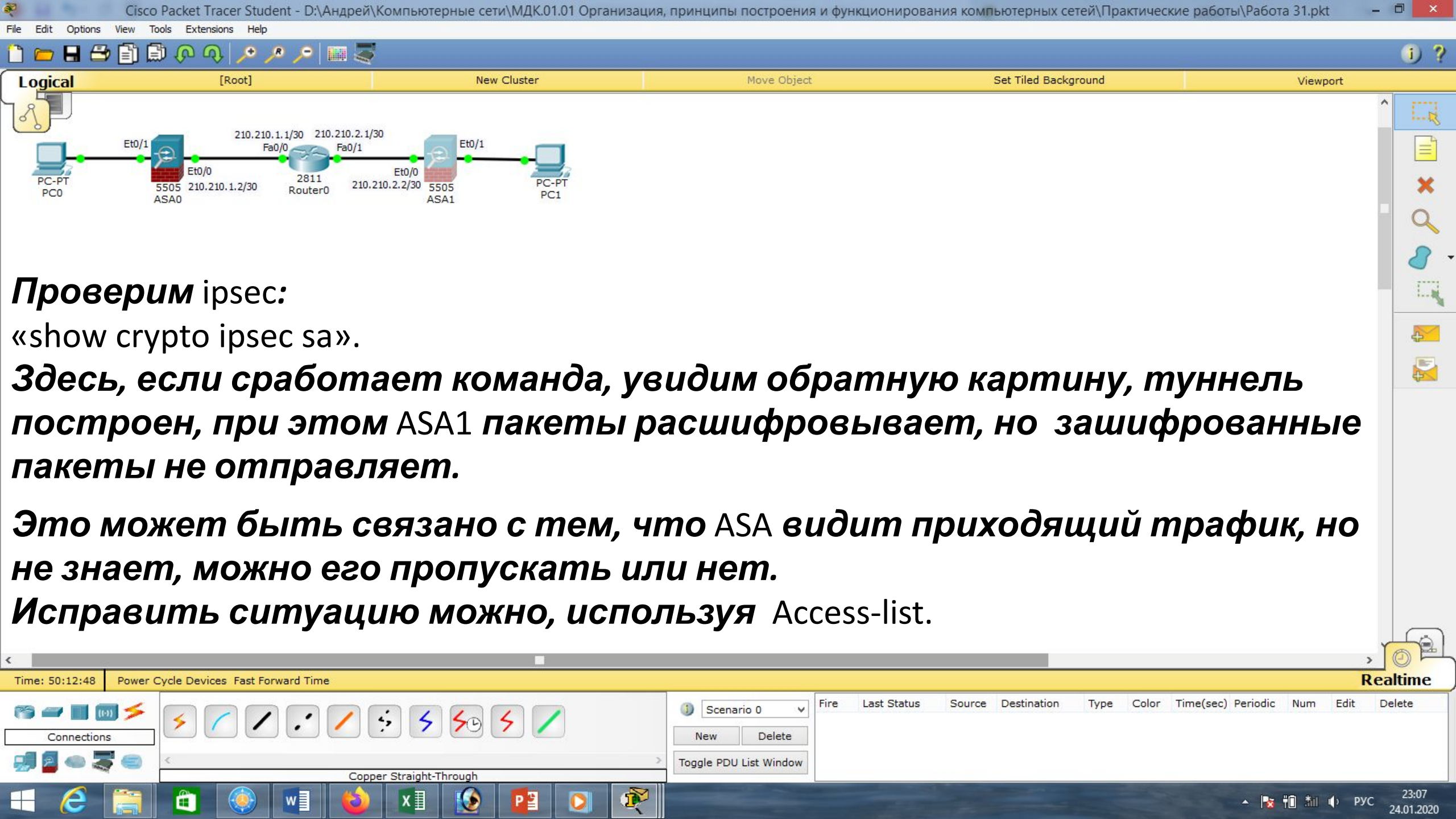
Connections

Copper Straight-Through

Scenario 0 New Delete Toggle PDU List Window

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

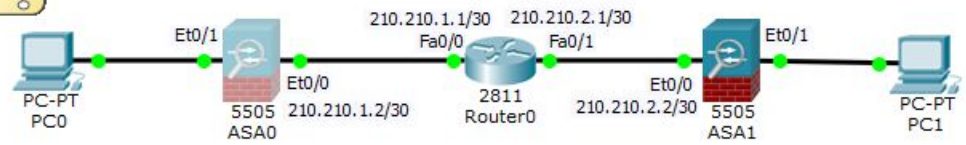
РУС 22:18 24.01.2020


Cisco Packet Tracer Student - D:\Андрей\Компьютерные сети\МДК.01.01 Организация, принципы построения и функционирования компьютерных сетей\Практические работы\Работа 31.pkt
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
PC-PT PC0
Et0/1
5505 ASA0
Et0/0 210.210.1.2/30
210.210.1.1/30 Fa0/0
2811 Router0
210.210.2.1/30 Fa0/1
Et0/0 210.210.2.2/30
5505 ASA1
Et0/1
PC-PT PC1
Проверим ipsec:
«show crypto ipsec sa».
Здесь, если сработает команда, увидим обратную картину, туннель построен, при этом ASA1 пакеты расшифровывает, но зашифрованные пакеты не отправляет.
Это может быть связано с тем, что ASA видит приходящий трафик, но не знает, можно его пропускать или нет.
Исправить ситуацию можно, используя Access-list.
Time: 50:12:48 Power Cycle Devices Fast Forward Time
Realtime
Connections
Copper Straight-Through
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
РУС 23:07 24.01.2020

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

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster



Создадим такой Access-list ***на*** ASA0 ***с именем*** FROM-VPN ***и разрешим трафик из сети*** 192.168.2.0***, получателем будет сеть*** 192.168.1.0 ***:***

«access-list FROM-VPN permit icmp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0».

Привяжем это Access-list ***на исходящий интерфейс*** ASA0***. Для трафика из сети*** 192.168.2.0 ***входящим в*** ASA0 ***будет интерфейс*** Et0/0***, а исходящим –*** Et0/1 ***(то есть, к компьютерам) :***

«access-group FROM-VPN out interface inside», «end», «wr mem».

ASA0

Physical Config CLI

ASA Command Line Interface

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/14 ms

ciscoasa(config)#acc
ciscoasa(config)#access
ciscoasa(config)#access-li
ciscoasa(config)#access-list FROM-VPN per
ciscoasa(config)#access-list FROM-VPN permit icmp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
ciscoasa(config)#
ciscoasa(config)#access-g
ciscoasa(config)#access-group FROM-VPN out in
ciscoasa(config)#access-group FROM-VPN out interface in
ciscoasa(config)#access-group FROM-VPN out interface inside
ciscoasa(config)#
ciscoasa(config)#end
ciscoasa#
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 3c8246d4 3f837647 3f331ad0 1dc13e50

1671  bytes copied in 1.18 secs (1416 bytes/sec)
[OK]
ciscoasa#
```

Copy Paste

Time: 50:39:55 Power Cycle Devices Fast Forward Time

Realtime

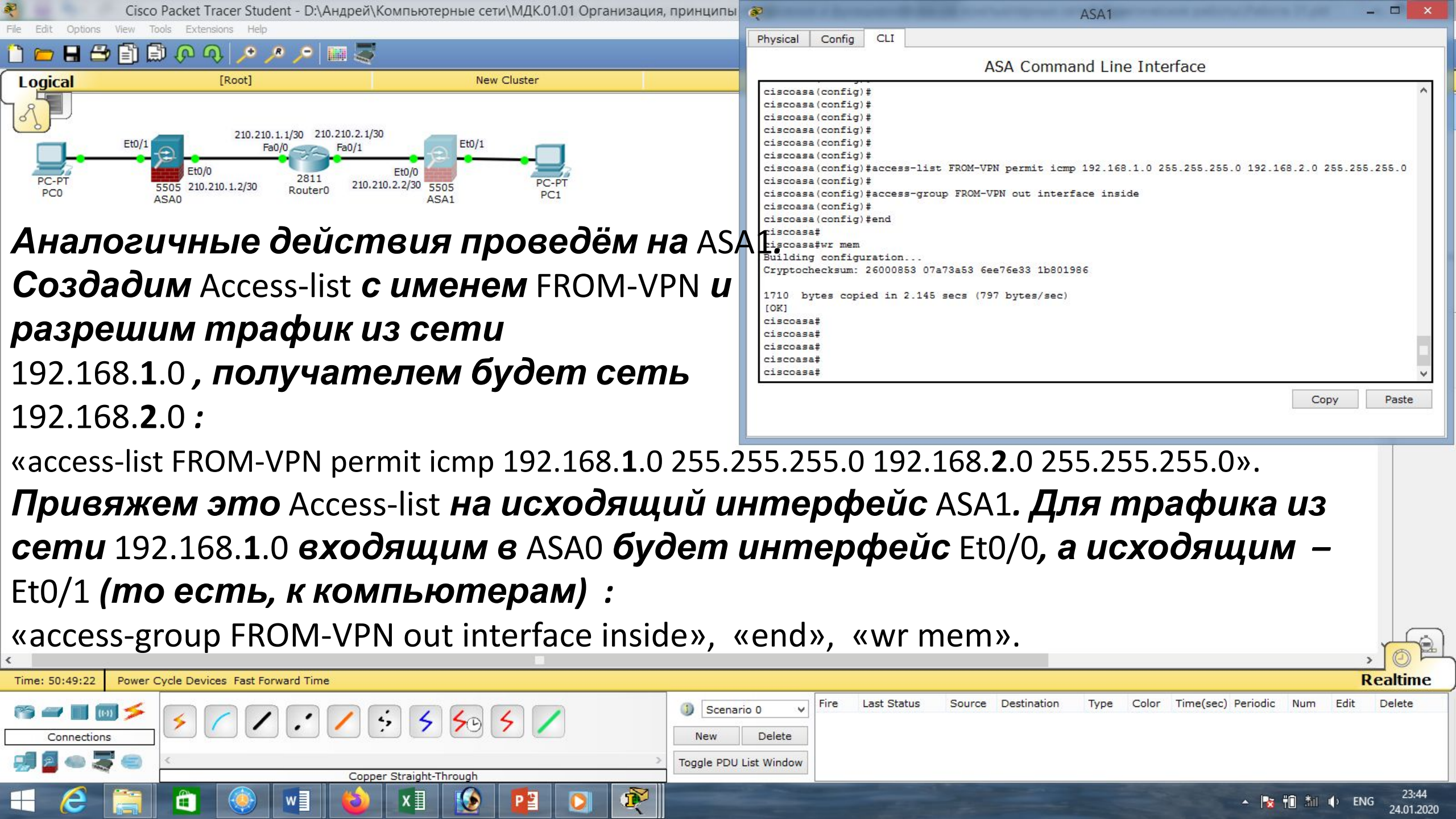
Connections

Copper Straight-Through

Scenario 0 New Delete Toggle PDU List Window

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

РУС 23:34 24.01.2020



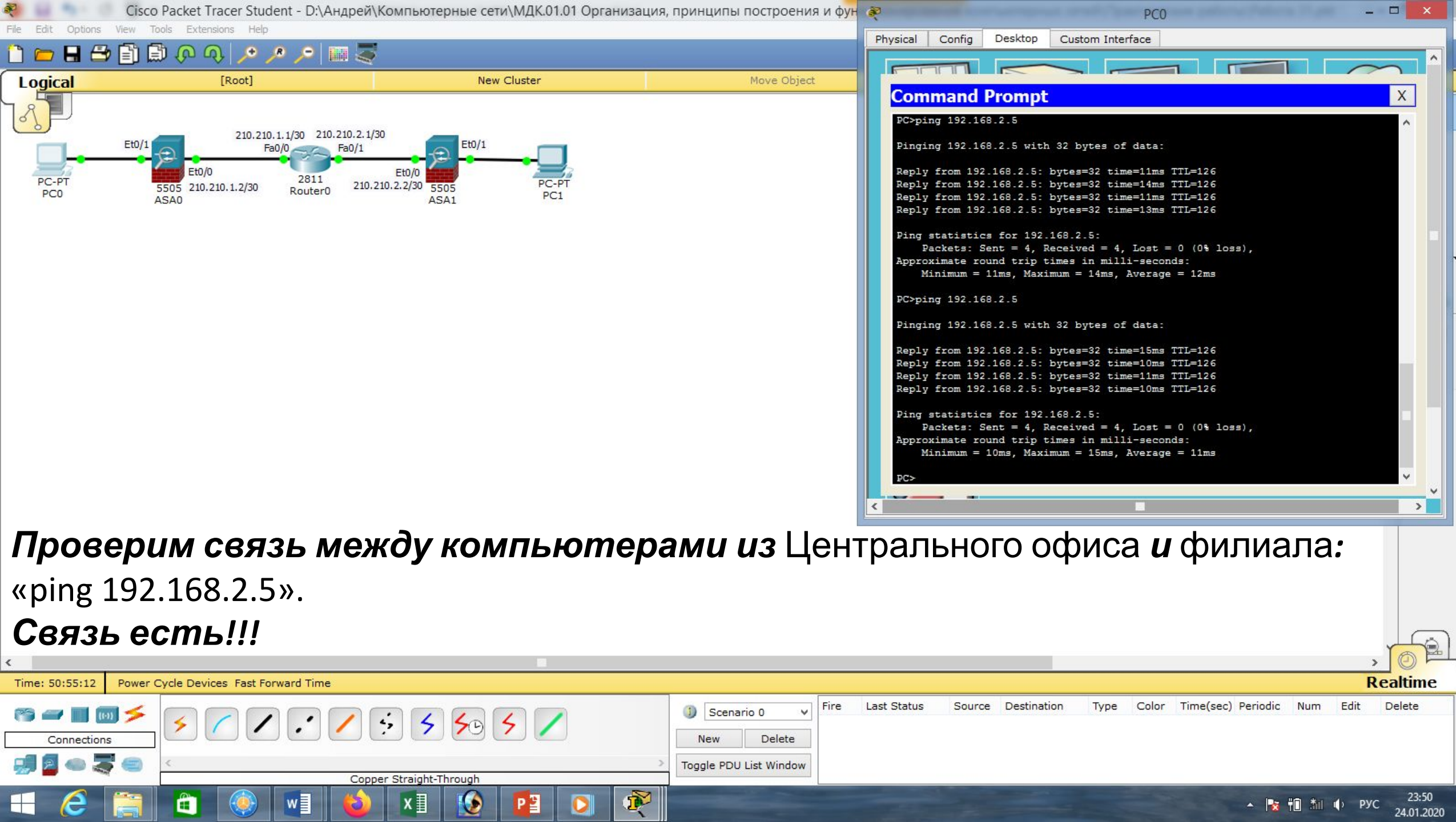
Аналогичные действия проведём на ASA1**.**

Создадим Access-list ***с именем*** FROM-VPN ***и разрешим трафик из сети*** 192.168.**1**.0 **,** ***получателем будет сеть*** 192.168.**2**.0 ***:***

«access-list FROM-VPN permit icmp 192.168.**1**.0 255.255.255.0 192.168.**2**.0 255.255.255.0».

Привяжем это Access-list ***на исходящий интерфейс*** ASA1**.** ***Для трафика из сети*** 192.168.**1**.0 ***входящим в*** ASA0 ***будет интерфейс*** Et0/0**,** ***а исходящим –*** Et0/1 ***(то есть, к компьютерам) :***

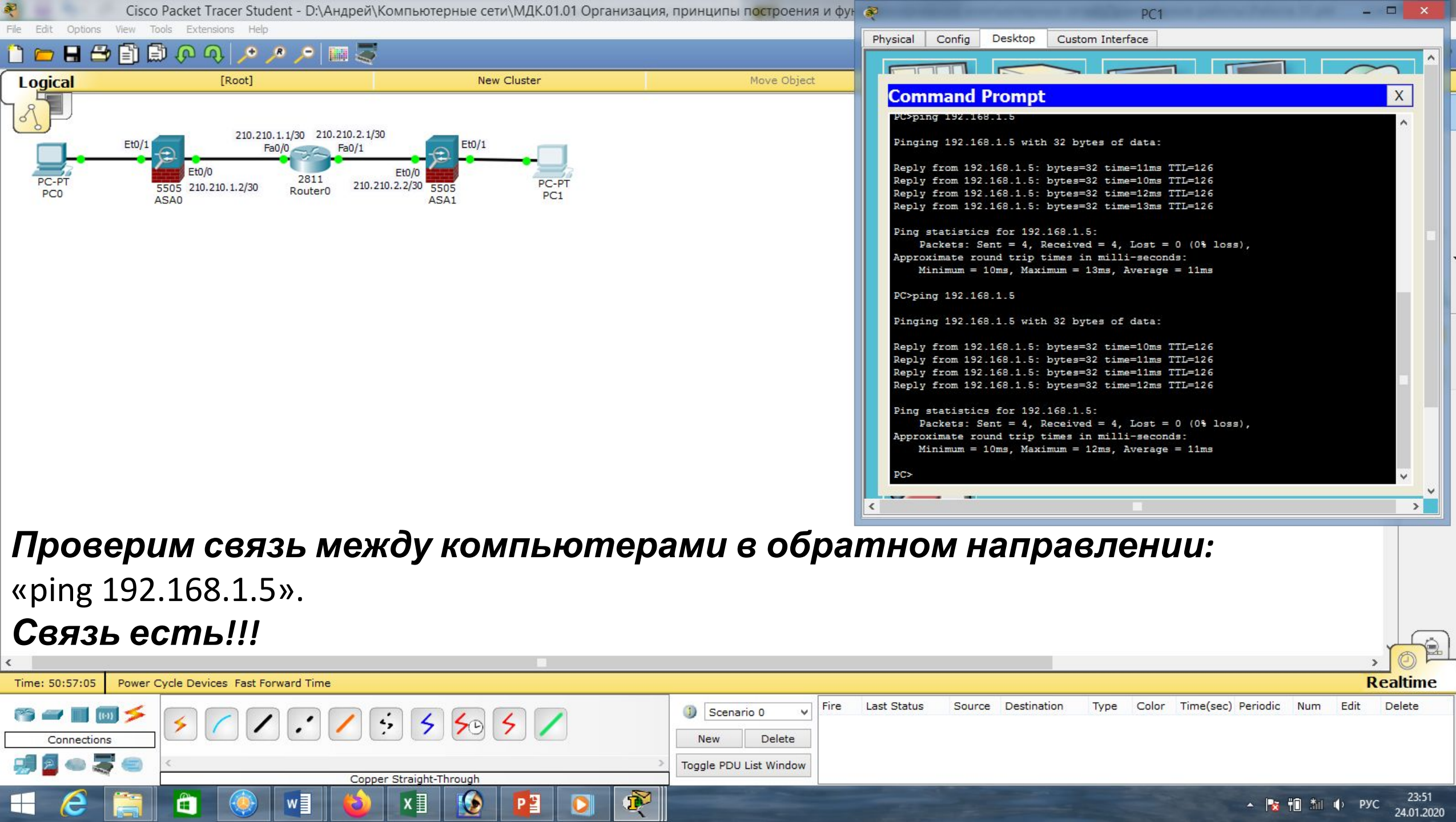
«access-group FROM-VPN out interface inside», «end», «wr mem».



Проверим связь между компьютерами из Центрального офиса ***и*** филиала***:***

«ping 192.168.2.5».

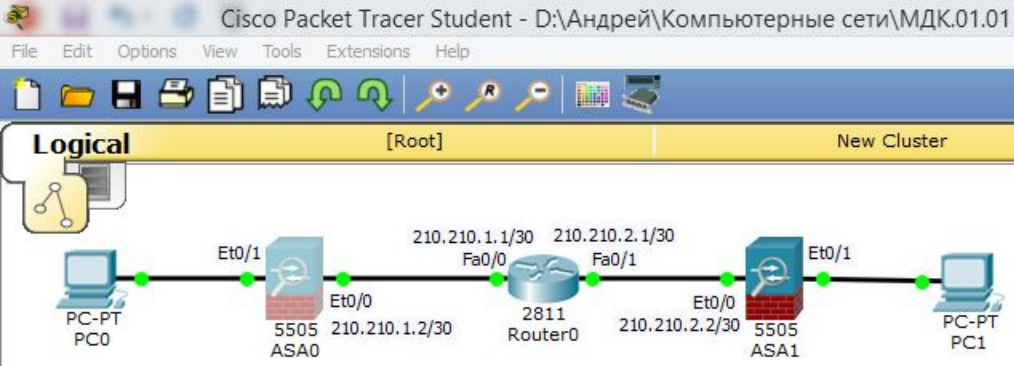
Связь есть!!!

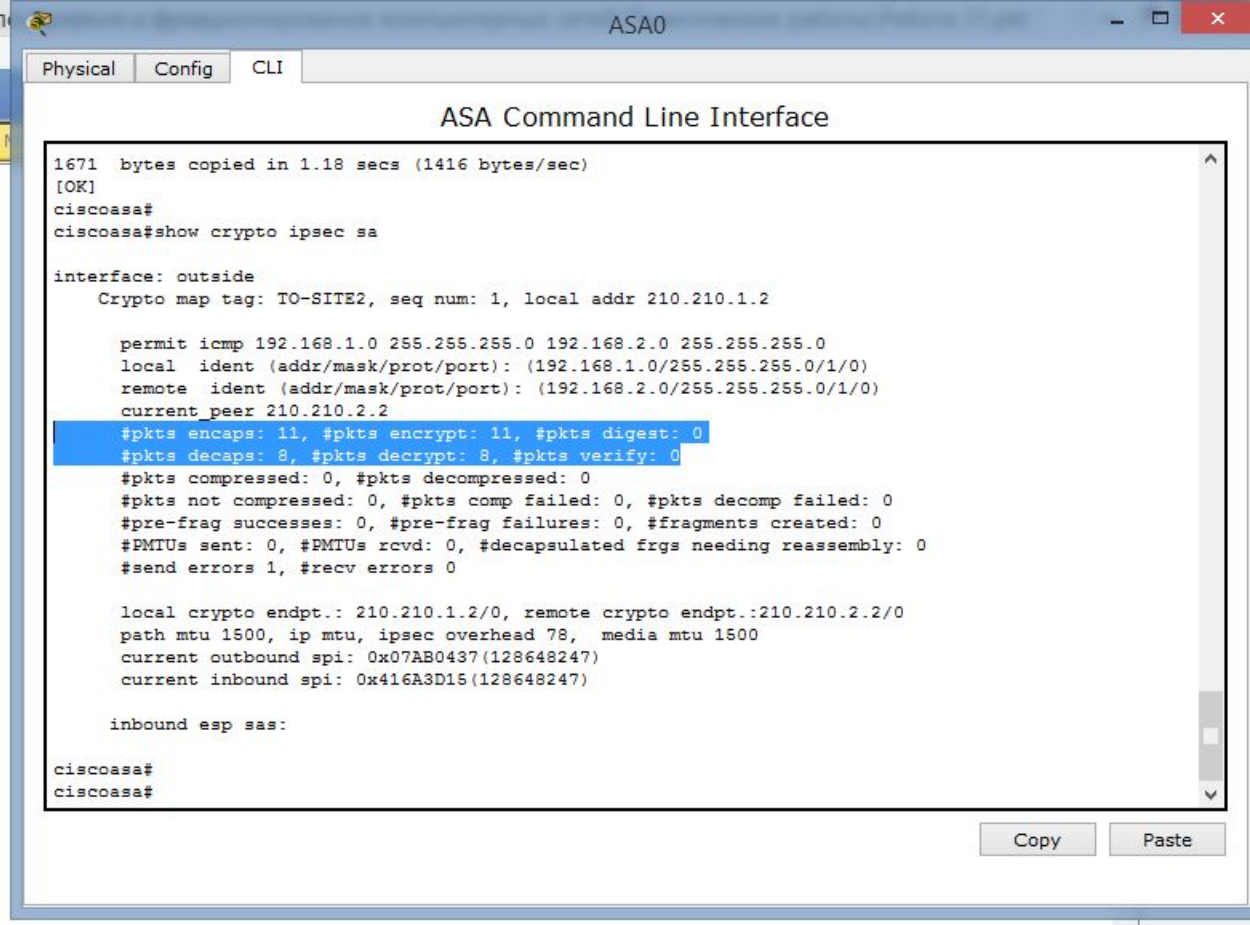


Проверим связь между компьютерами в обратном направлении:

«ping 192.168.1.5».

Связь есть!!!



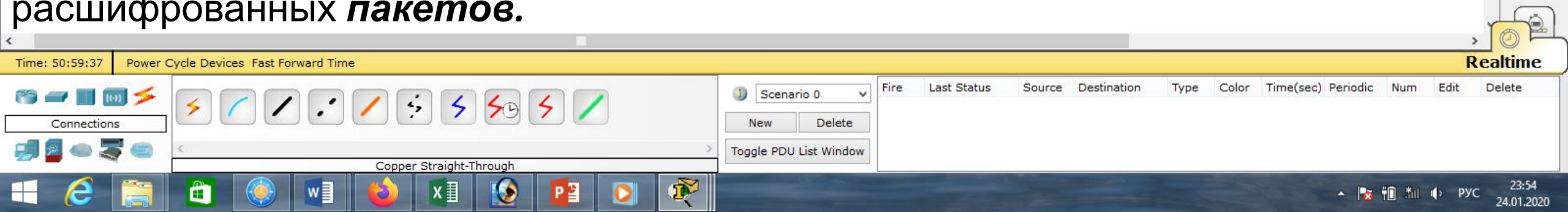


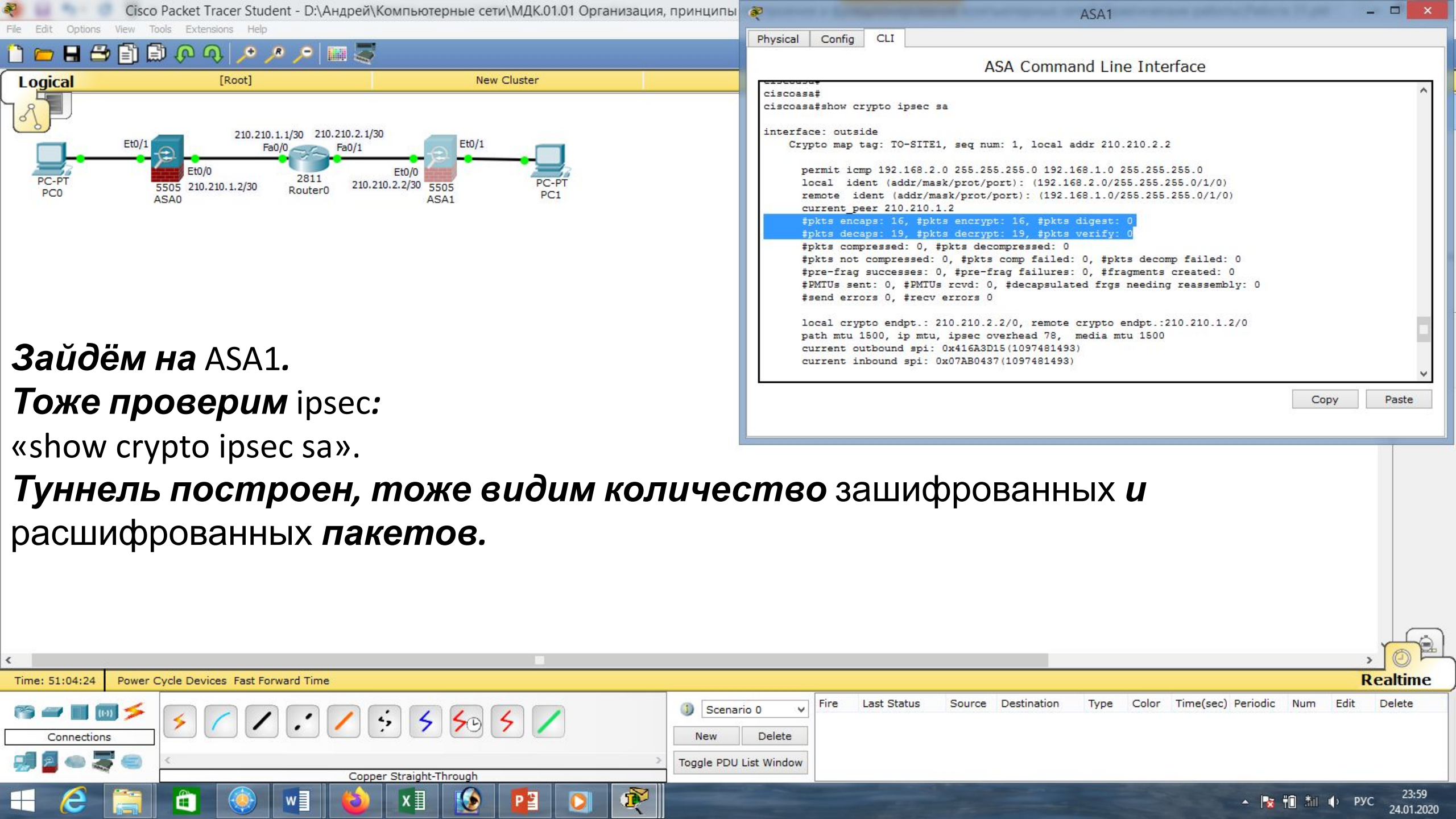
Зайдём на ASA0***.***

Ещё раз проверим ipsec***:***

«show crypto ipsec sa».

Туннель построен, при этом видим количество зашифрованных ***и*** расшифрованных ***пакетов.***



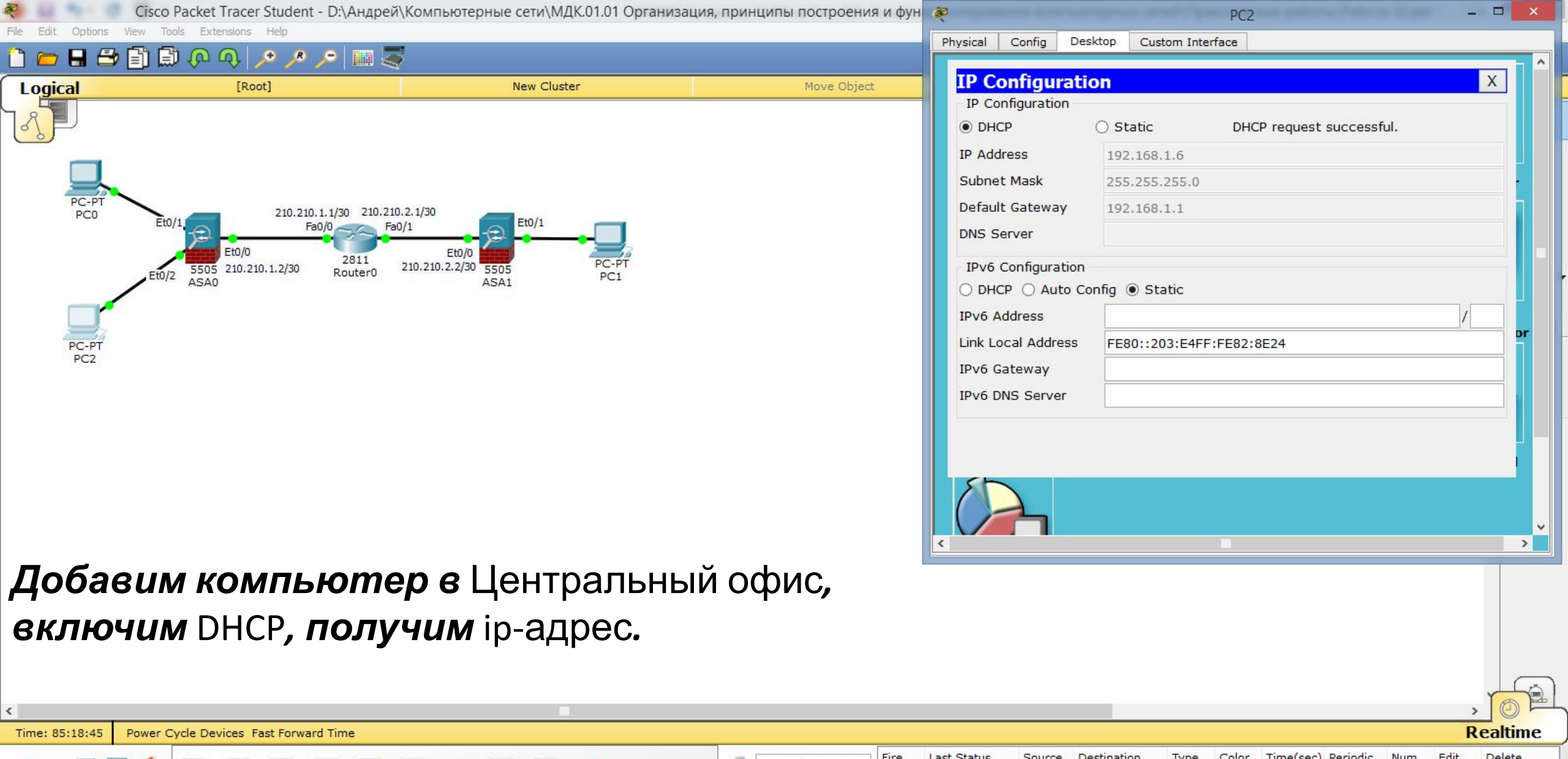


Зайдём на ASA1***.***

Тоже проверим ipsec***:***

«show crypto ipsec sa».

Туннель построен, тоже видим количество зашифрованных ***и*** расшифрованных ***пакетов.***

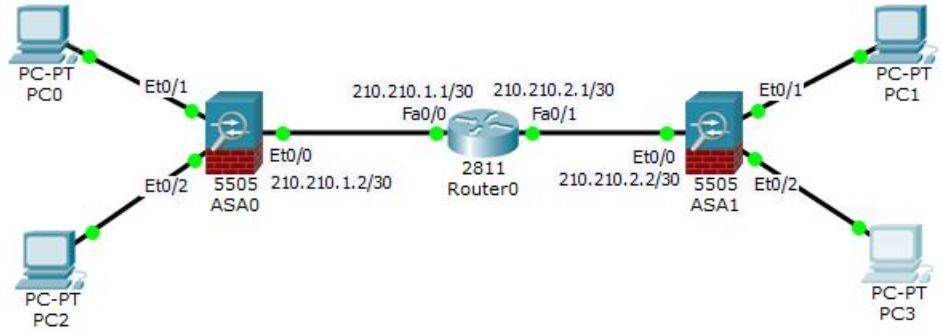


Добавим компьютер в Центральный офис***, включим*** DHCP***, получим*** ip-адрес***.***

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

File Edit Options View Tools Extensions Help

Logical | [Root] | New Cluster | Move Object



PC3

Physical | Config | Desktop | Custom Interface

IP Configuration

IP Configuration

DHCP Static DHCP request successful.

IP Address 192.168.2.6

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server

IPv6 Configuration

DHCP Auto Config Static

IPv6 Address /

Link Local Address FE80::2D0:BCFF:FE31:257E

IPv6 Gateway

IPv6 DNS Server

Добавим компьютер в филиал***, включим*** DHCP***, получим*** ip-адрес***.***

Time: 85:25:39 | Power Cycle Devices | Fast Forward Time

Realtime

WAN Emulation

Generic | Generic | DSL Modem | Cable Modem

Copper Straight-Through

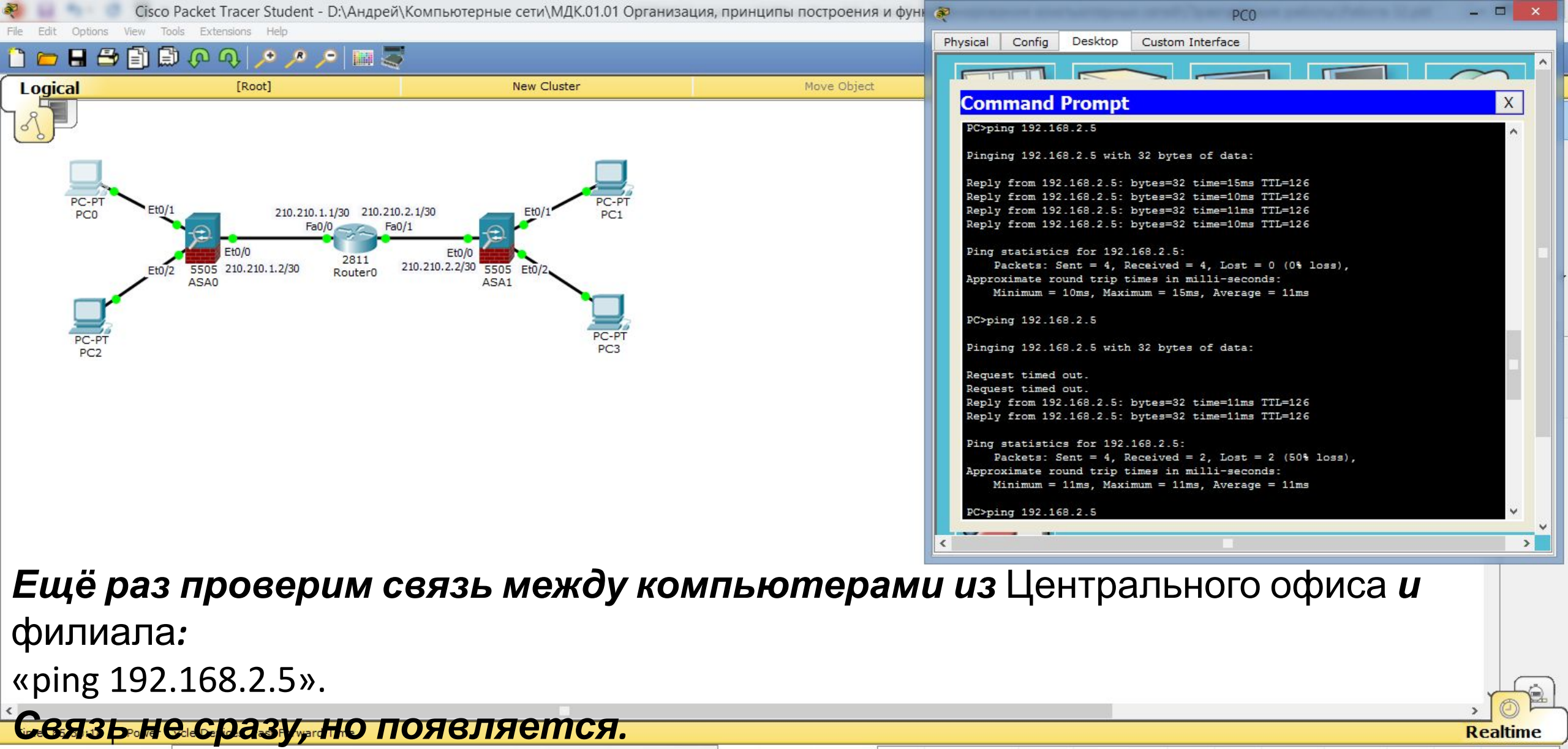
Scenario 0

New | Delete

Toggle PDU List Window

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

РУС 10:20 25.01.2020



Ещё раз проверим связь между компьютерами из Центрального офиса ***и*** филиала***:***

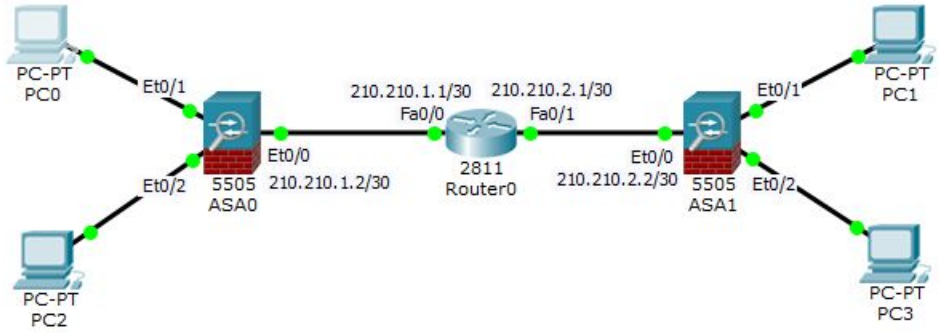
«ping 192.168.2.5».

Связь не сразу, но появляется.

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

File Edit Options View Tools Extensions Help

Logical | [Root] | New Cluster | Move Object



PC0

Physical | Config | Desktop | Custom Interface

Command Prompt

```
PC>ping 192.168.2.6

Pinging 192.168.2.6 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.6: bytes=32 time=11ms TTL=126
Reply from 192.168.2.6: bytes=32 time=10ms TTL=126
Reply from 192.168.2.6: bytes=32 time=14ms TTL=126

Ping statistics for 192.168.2.6:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 14ms, Average = 11ms

PC>ping 192.168.2.6

Pinging 192.168.2.6 with 32 bytes of data:

Reply from 192.168.2.6: bytes=32 time=11ms TTL=126
Reply from 192.168.2.6: bytes=32 time=12ms TTL=126
Reply from 192.168.2.6: bytes=32 time=11ms TTL=126
Reply from 192.168.2.6: bytes=32 time=24ms TTL=126

Ping statistics for 192.168.2.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 24ms, Average = 14ms

PC>
```

Проверим связь между компьютером из Центрального офиса ***и добавленным компьютером*** филиала***:*** «ping 192.168.2.**6**».

Связь есть!!!

Time: 85:33:10 | Power Cycle Devices | Fast Forward Time | Realtime

WAN Emulation

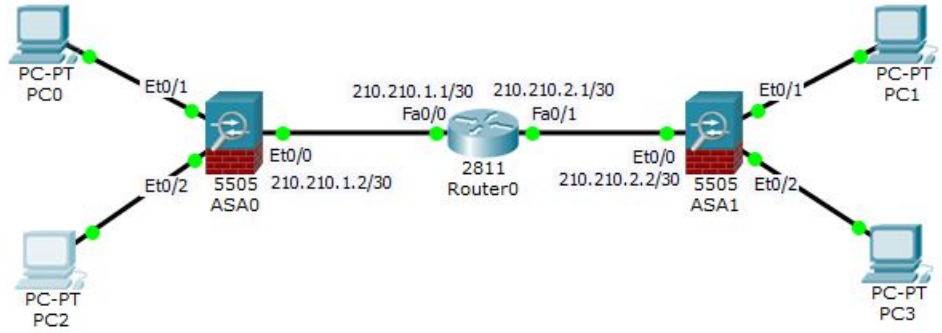
Generic | Generic | DSL Modem | Cable Modem

Copper Straight-Through

Scenario 0 | New | Delete | Toggle PDU List Window

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

РУС 10:28 25.01.2020



В заключении проверим связь между добавленными компьютерами из Центрального офиса ***и*** филиала***:*** «ping 192.168.2.6».
Связь есть!!!

Таким образом мы построили VPN-соединение***, используя*** Cisco ASA***!!!***

PC2

Physical | Config | Desktop | Custom Interface

Command Prompt

```
PC>ping 192.168.2.6

Pinging 192.168.2.6 with 32 bytes of data:

Reply from 192.168.2.6: bytes=32 time=16ms TTL=126
Reply from 192.168.2.6: bytes=32 time=13ms TTL=126
Reply from 192.168.2.6: bytes=32 time=10ms TTL=126
Reply from 192.168.2.6: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.2.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 16ms, Average = 13ms

PC>ping 192.168.2.6

Pinging 192.168.2.6 with 32 bytes of data:

Reply from 192.168.2.6: bytes=32 time=11ms TTL=126
Reply from 192.168.2.6: bytes=32 time=10ms TTL=126
Reply from 192.168.2.6: bytes=32 time=11ms TTL=126
Reply from 192.168.2.6: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.2.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 11ms, Average = 10ms

PC>
```

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

File Edit Options View Tools Extensions Help

Logical | [Root] | New Cluster | Move Object

Time: 85:35:15 | Power Cycle Devices | Fast Forward Time | Realtime

WAN Emulation | Generic | Generic | DSL Modem | Cable Modem | Copper Straight-Through

Scenario 0 | New | Delete | Toggle PDU List Window

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

РУС 10:30 25.01.2020

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