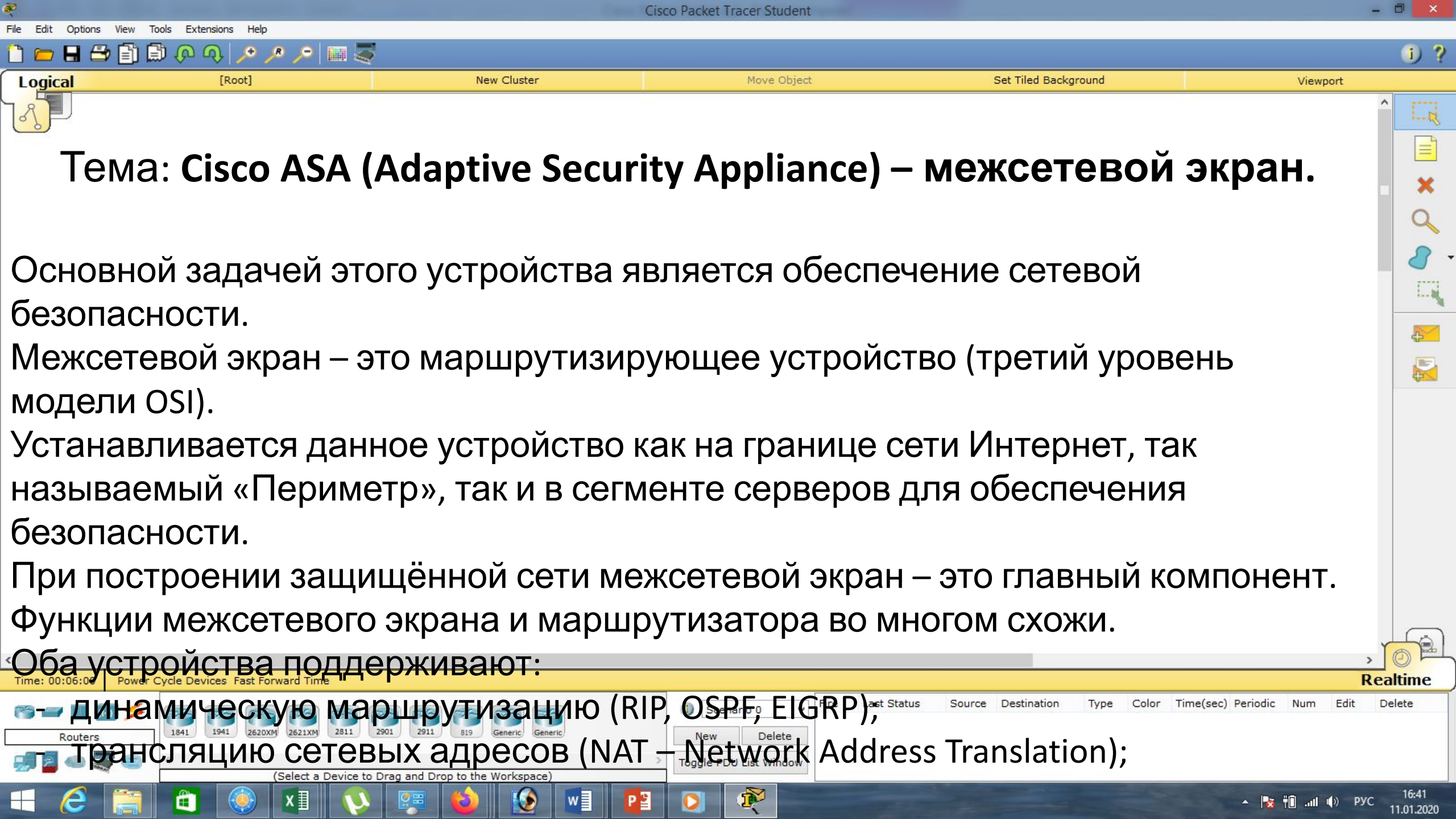


МДК.01.01
Организация, принципы
построения и функционирования
компьютерных сетей
3-курс

Практические занятия

Занятие 14



Тема: Cisco ASA (Adaptive Security Appliance) – межсетевой экран.

Основной задачей этого устройства является обеспечение сетевой безопасности.

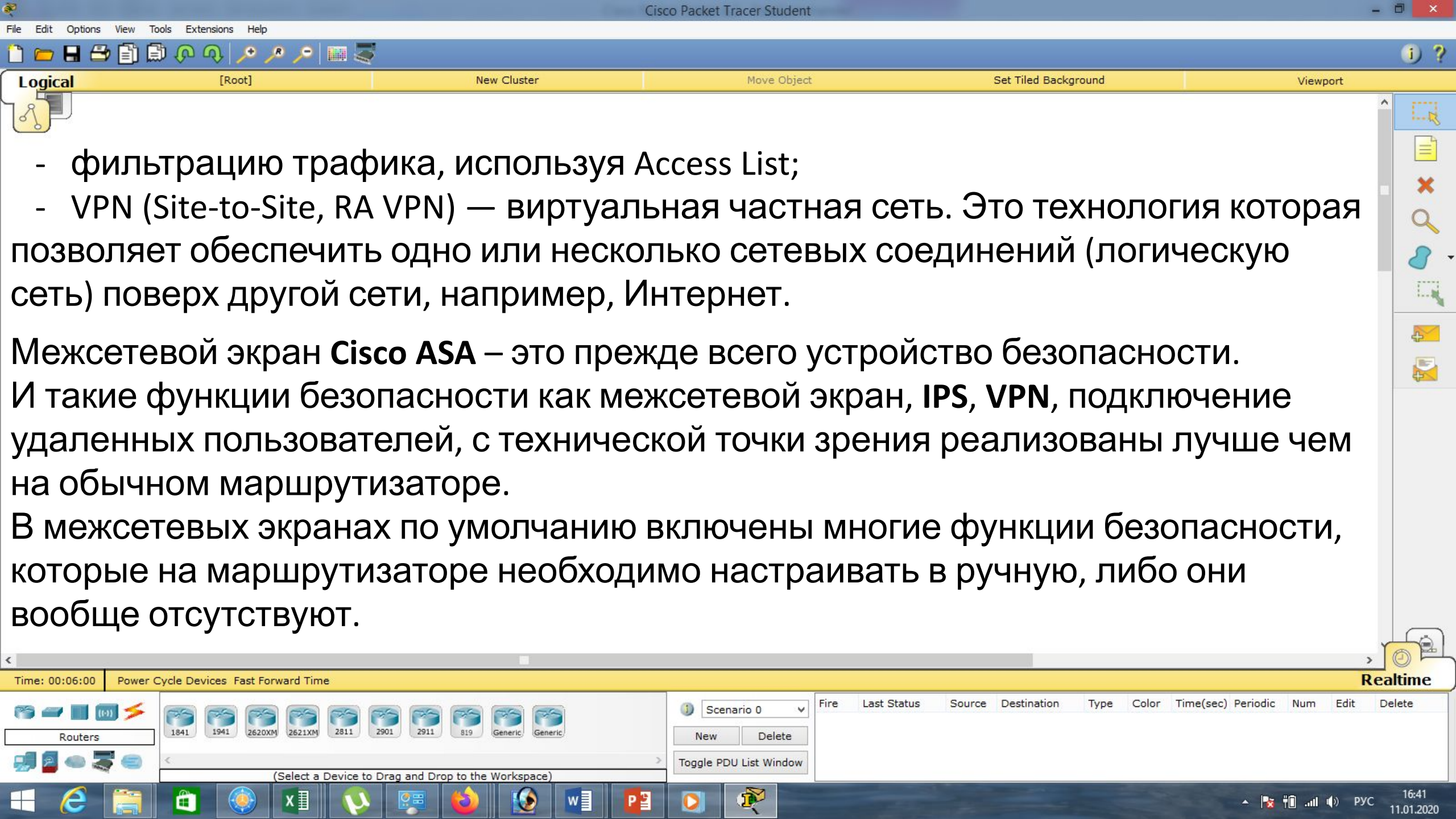
Межсетевой экран – это маршрутизирующее устройство (третий уровень модели OSI).

Устанавливается данное устройство как на границе сети Интернет, так называемый «Периметр», так и в сегменте серверов для обеспечения безопасности.

При построении защищённой сети межсетевой экран – это главный компонент. Функции межсетевого экрана и маршрутизатора во многом схожи.

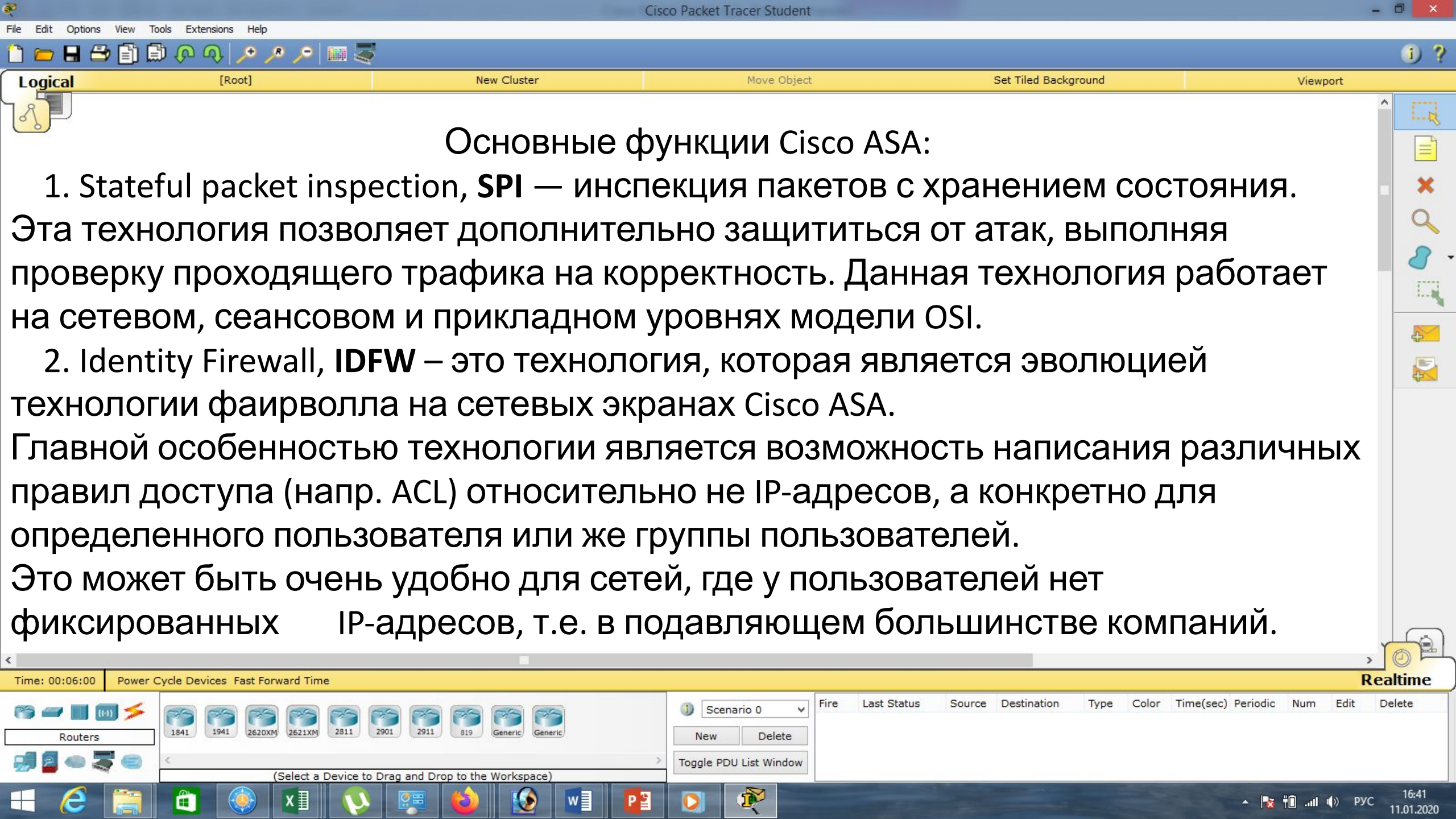
Оба устройства поддерживают:

- динамическую маршрутизацию (RIP, OSPF, EIGRP);
- трансляцию сетевых адресов (NAT – Network Address Translation);



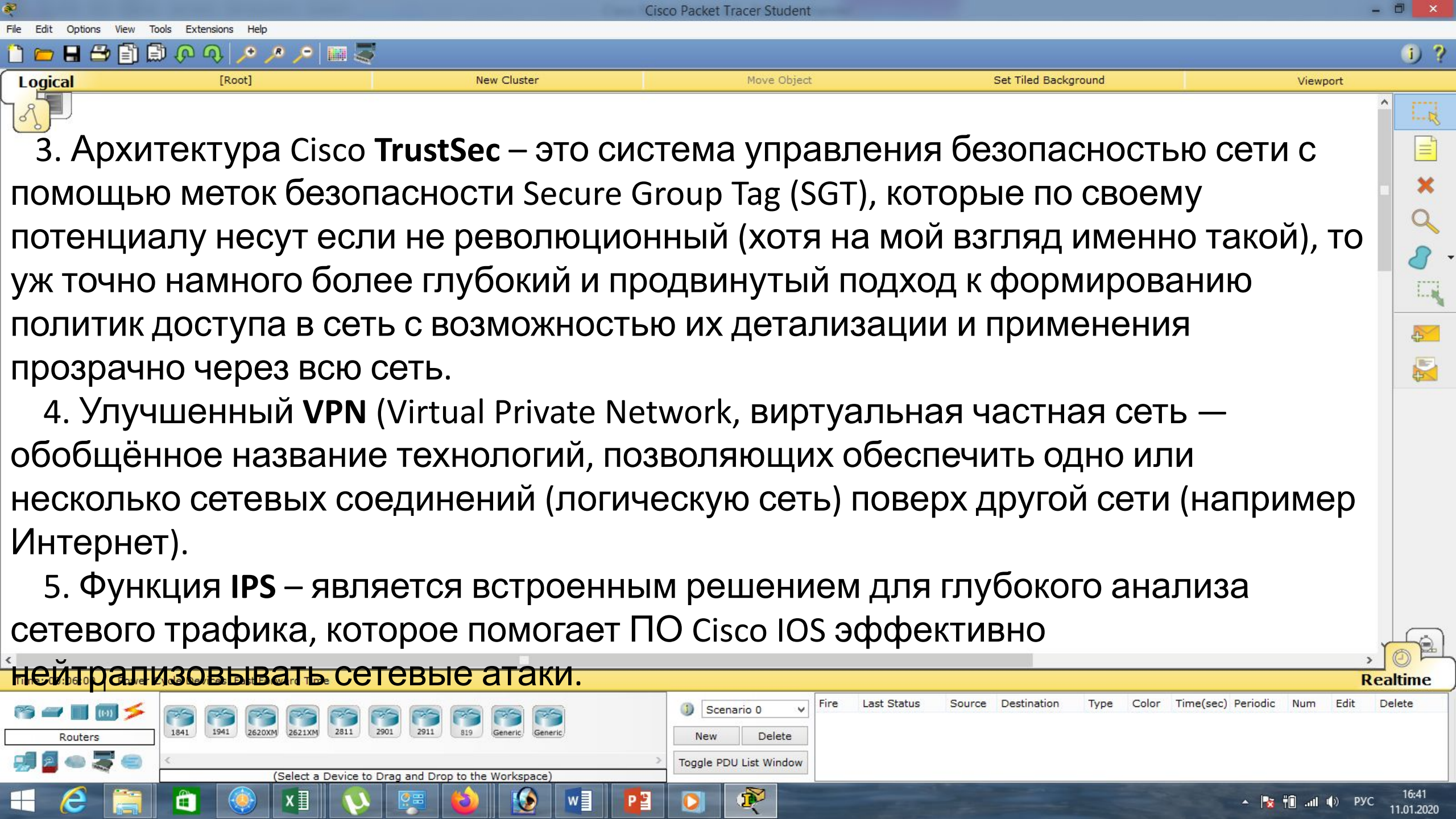
- фильтрацию трафика, используя Access List;
- VPN (Site-to-Site, RA VPN) — виртуальная частная сеть. Это технология которая позволяет обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети, например, Интернет.

Межсетевой экран **Cisco ASA** – это прежде всего устройство безопасности. И такие функции безопасности как межсетевой экран, **IPS**, **VPN**, подключение удаленных пользователей, с технической точки зрения реализованы лучше чем на обычном маршрутизаторе. В межсетевых экранах по умолчанию включены многие функции безопасности, которые на маршрутизаторе необходимо настраивать в ручную, либо они вообще отсутствуют.



Основные функции Cisco ASA:

1. Stateful packet inspection, **SPI** — инспекция пакетов с хранением состояния. Эта технология позволяет дополнительно защититься от атак, выполняя проверку проходящего трафика на корректность. Данная технология работает на сетевом, сеансовом и прикладном уровнях модели OSI.
2. Identity Firewall, **IDFW** – это технология, которая является эволюцией технологии фаирволла на сетевых экранах Cisco ASA. Главной особенностью технологии является возможность написания различных правил доступа (напр. ACL) относительно не IP-адресов, а конкретно для определенного пользователя или же группы пользователей. Это может быть очень удобно для сетей, где у пользователей нет фиксированных IP-адресов, т.е. в подавляющем большинстве компаний.



3. Архитектура Cisco **TrustSec** – это система управления безопасностью сети с помощью меток безопасности Secure Group Tag (SGT), которые по своему потенциалу несут если не революционный (хотя на мой взгляд именно такой), то уж точно намного более глубокий и продвинутый подход к формированию политик доступа в сеть с возможностью их детализации и применения прозрачно через всю сеть.

4. Улучшенный **VPN** (Virtual Private Network, виртуальная частная сеть — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например Интернет).

5. Функция **IPS** – является встроенным решением для глубокого анализа сетевого трафика, которое помогает ПО Cisco IOS эффективно нейтрализовать сетевые атаки.



Routers



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

Scenario 0

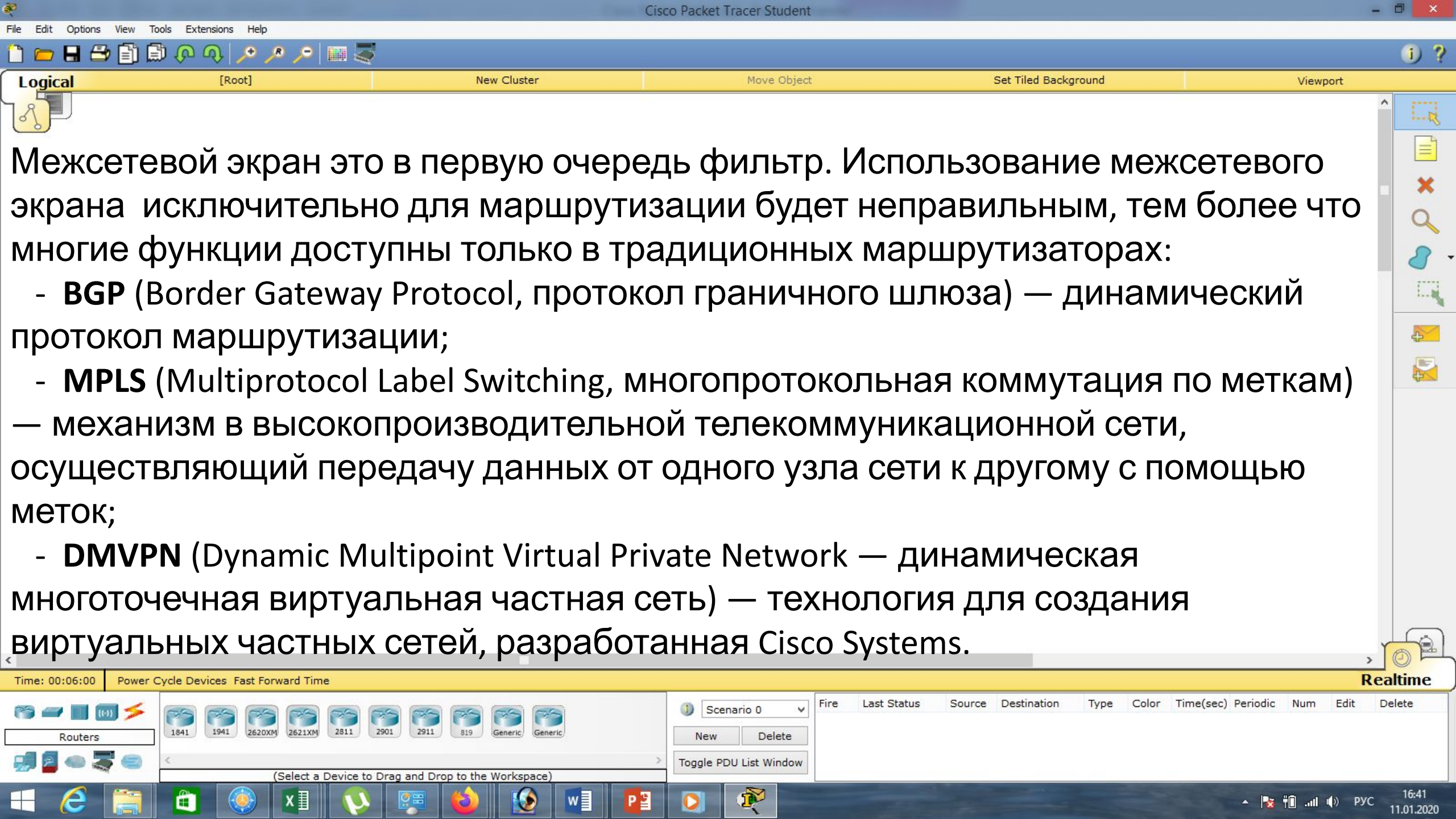
New Delete

Toggle PDU List Window

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

Realtime





Межсетевой экран это в первую очередь фильтр. Использование межсетевого экрана исключительно для маршрутизации будет неправильным, тем более что многие функции доступны только в традиционных маршрутизаторах:

- **BGP** (Border Gateway Protocol, протокол граничного шлюза) — динамический протокол маршрутизации;
- **MPLS** (Multiprotocol Label Switching, многопротокольная коммутация по меткам) — механизм в высокопроизводительной телекоммуникационной сети, осуществляющий передачу данных от одного узла сети к другому с помощью меток;
- **DMVPN** (Dynamic Multipoint Virtual Private Network — динамическая многоточечная виртуальная частная сеть) — технология для создания виртуальных частных сетей, разработанная Cisco Systems.



Routers



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

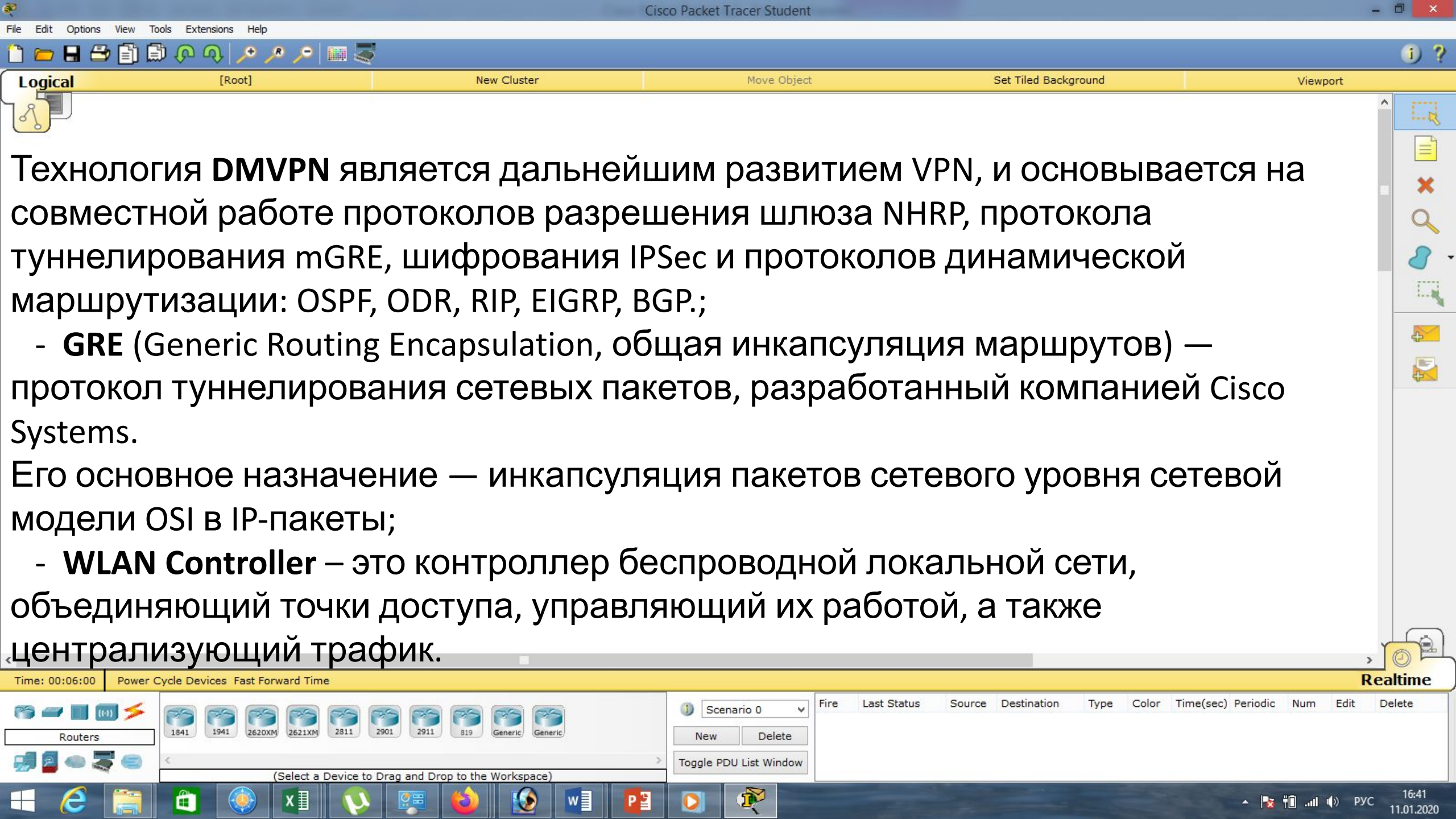
Scenario 0

New Delete

Toggle PDU List Window

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



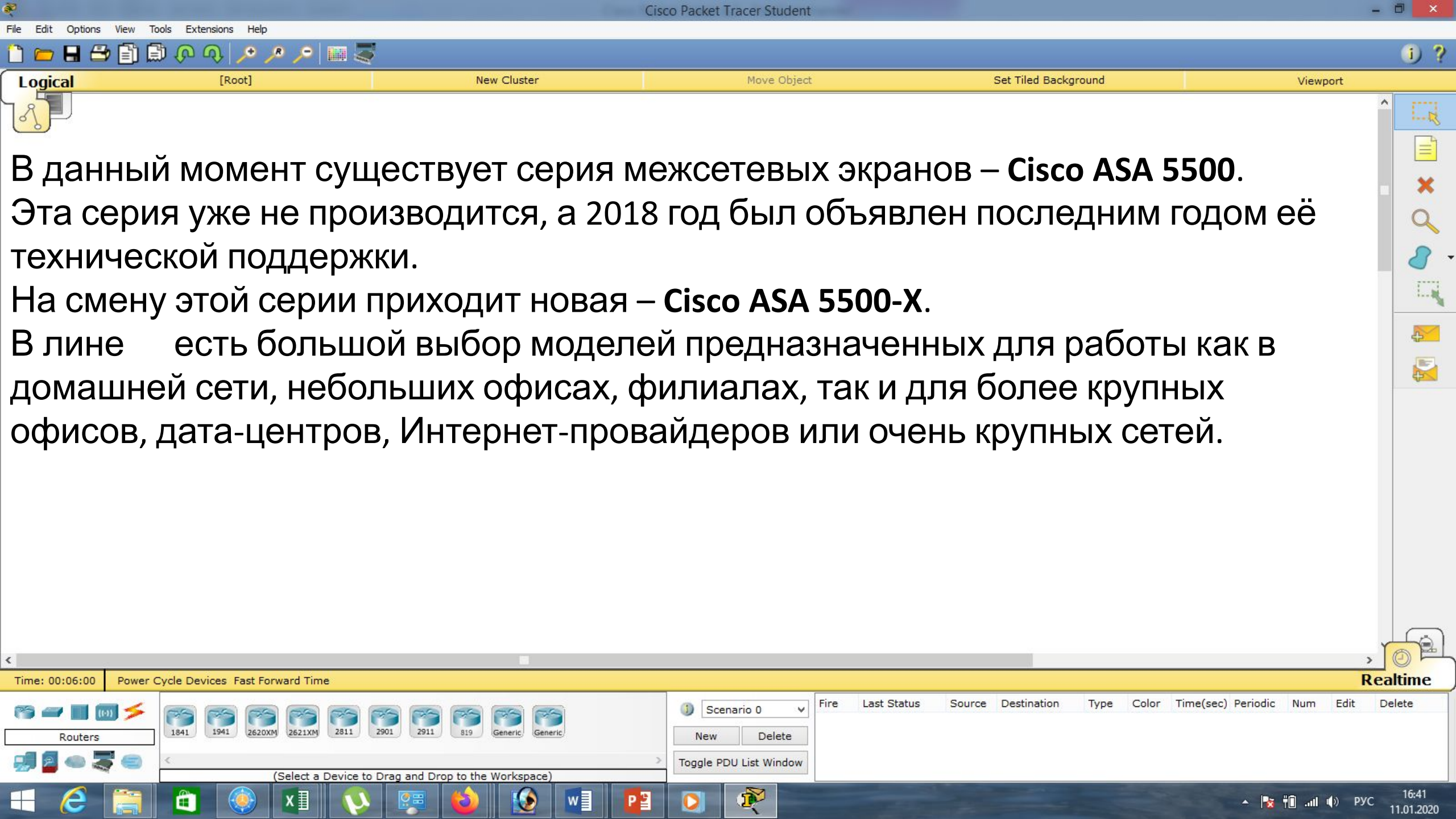


Технология **DMVPN** является дальнейшим развитием VPN, и основывается на совместной работе протоколов разрешения шлюза NHRP, протокола туннелирования mGRE, шифрования IPSec и протоколов динамической маршрутизации: OSPF, ODR, RIP, EIGRP, BGP.;

- **GRE** (Generic Routing Encapsulation, общая инкапсуляция маршрутов) — протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems.

Его основное назначение — инкапсуляция пакетов сетевого уровня сетевой модели OSI в IP-пакеты;

- **WLAN Controller** – это контроллер беспроводной локальной сети, объединяющий точки доступа, управляющий их работой, а также централизующий трафик.



Logical

[Root]

New Cluster

Move Object

Set Tiled Background

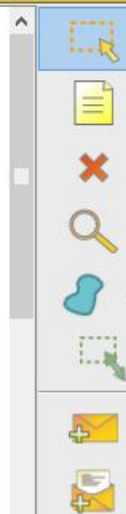
Viewport



В данный момент существует серия межсетевых экранов – **Cisco ASA 5500**. Эта серия уже не производится, а 2018 год был объявлен последним годом её технической поддержки.

На смену этой серии приходит новая – **Cisco ASA 5500-X**.

В линейке есть большой выбор моделей предназначенных для работы как в домашней сети, небольших офисах, филиалах, так и для более крупных офисов, дата-центров, Интернет-провайдеров или очень крупных сетей.



Time: 00:06:00 Power Cycle Devices Fast Forward Time

Realtime



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
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

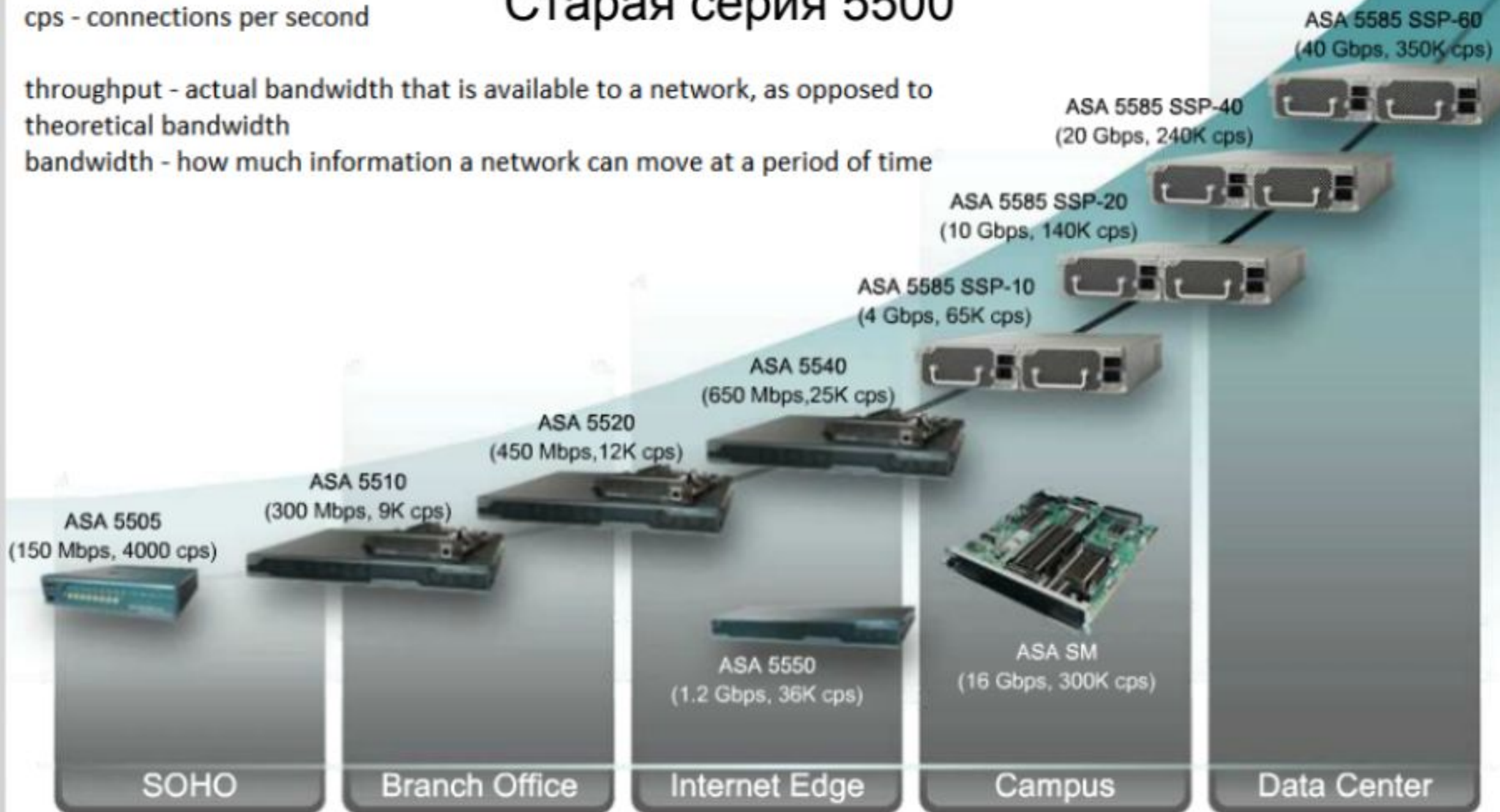


Mbps/Gbps - max throughput
cps - connections per second

Старая серия 5500

throughput - actual bandwidth that is available to a network, as opposed to theoretical bandwidth

bandwidth - how much information a network can move at a period of time



Вид спереди

Новая серия 5500-X



ASA 5512-X

ASA 5515-X

ASA 5525-X

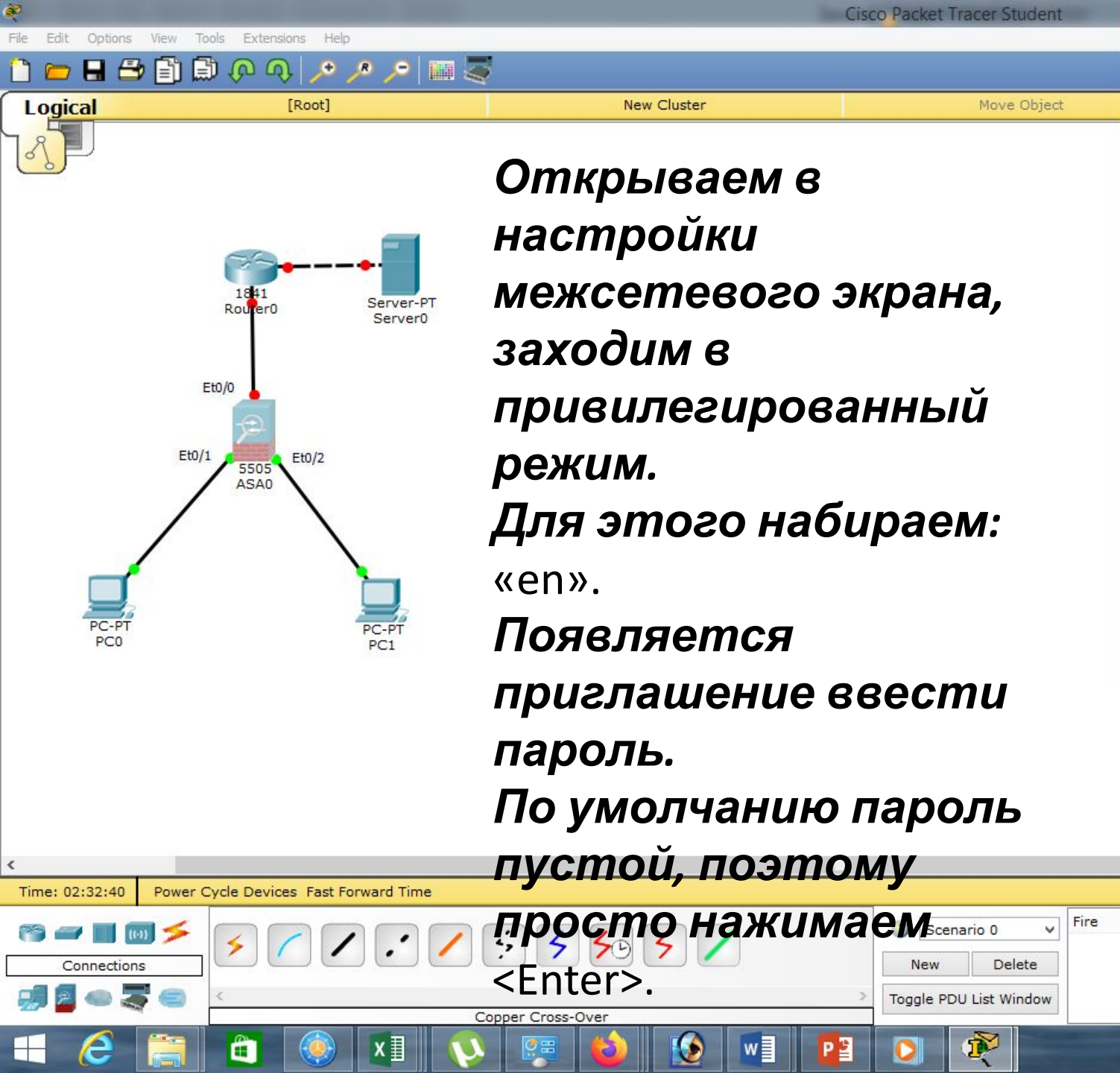
ASA 5545-X

ASA 5555-X



© 2011 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Устройство ASA 5500	Эквивалентное устройство ASA 5500-X
ASA 5510	ASA 5512-X
ASA 5510 Security Plus license	ASA 5515 или ASA 5512 Security Plus license
ASA 5520	ASA 5525-X
ASA 5540	ASA 5545-X
ASA 5550	ASA 5555-X



**Открываем в
настройки
межсетевого экрана,
заходим в
привилегированный
режим.
Для этого набираем:
«en».
Появляется
приглашение ввести
пароль.
По умолчанию пароль
пустой, поэтому
просто нажимаем
<Enter>.**

ASA0

Physical Config CLI

ASA Command Line Interface

```
sending email to export@cisco.com.
***** Warning *****

Copyright (c) 1996-2011 by Cisco Systems, Inc.

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Reading from flash...
!

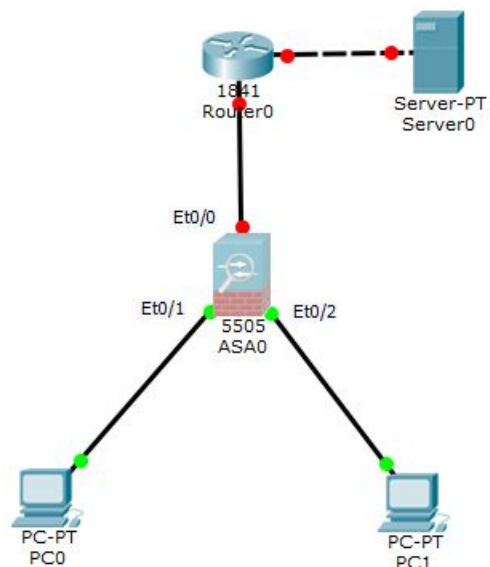
Type help or '?' for a list of available commands.

ciscoasa>en
Password:
ciscoasa#
```

Copy Paste

Realtime

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



**Для проверки
возможностей
межсетевого экрана
модели ASA 5505
набираем:
«show version».**

ASA0

Physical Config CLI

ASA Command Line Interface

Copyright (c) 1996-2011 by Cisco Systems, Inc.

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Reading from flash...
!

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

```
ciscoasa>en
Password:
ciscoasa#
ciscoasa#show ver
ciscoasa#show version
```

Copy Paste



Copper Cross-Over

Scenario 0

New Delete

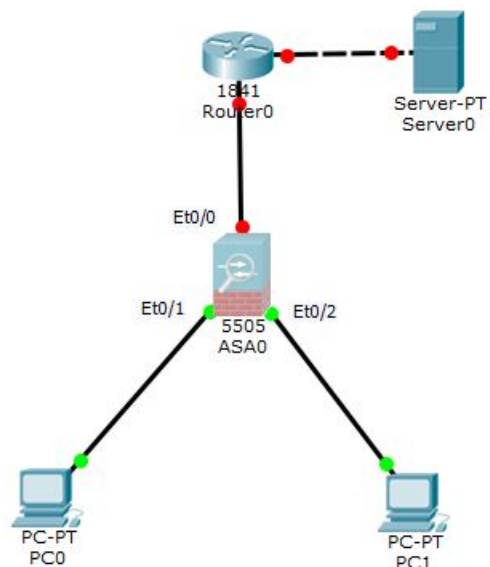
Toggle PDU List Window

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





**Видим версію
прошивки.**



ASA0

Physical Config CLI

ASA Command Line Interface

```
Cisco Adaptive Security Appliance Software Version 8.4(2)
Device Manager Version 6.4(5)

Compiled on Wed 16-Jun-11 18:17 by mnnguyen
System image file is "disk0:/asa842-k8.bin"
Config file at boot was "startup-config"

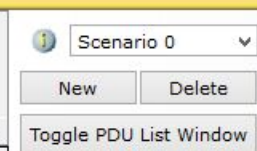
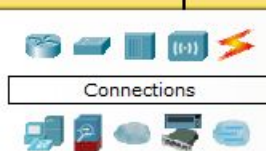
ciscoasa up 23 minutes 56 seconds

Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xffff00000, 2048KB

Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                                Boot microcode       : CN1000-MC-BOOT-2.00
                                SSL/IKE microcode      : CNLite-MC-SSLm-PLUS-2.03
                                IPSec microcode        : CNLite-MC-IPSECm-MAIN-2.06
                                Number of accelerators: 1

0: Int: Internal-Data0/0      : address is 44d3.caef.1e22, irq 11
1: Ext: Ethernet0/0          : address is 00E0.F9D9.1101, irq 255
2: Ext: Ethernet0/1          : address is 00E0.F9D9.1102, irq 255
3: Ext: Ethernet0/2          : address is 00E0.F9D9.1103, irq 255
4: Ext: Ethernet0/3          : address is 00E0.F9D9.1104, irq 255
5: Ext: Ethernet0/4          : address is 00E0.F9D9.1105, irq 255
6: Ext: Ethernet0/5          : address is 00E0.F9D9.1106, irq 255
7: Ext: Ethernet0/6          : address is 00E0.F9D9.1107, irq 255
8: Ext: Ethernet0/7          : address is 00E0.F9D9.1108, irq 255
9: Int: Internal-Data0/1      : address is 0000.0003.0002, irq 255
```

Copy Paste

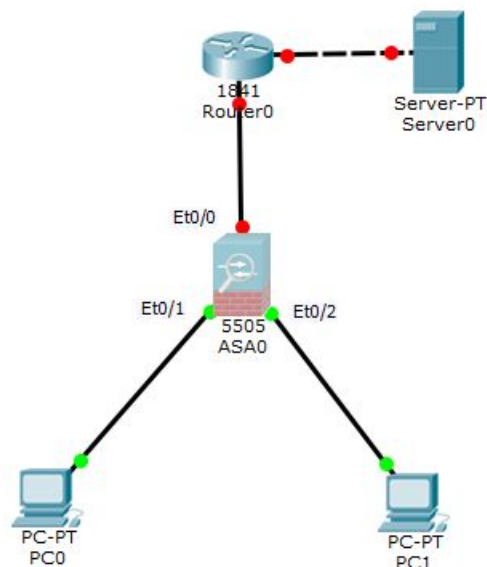


Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete





Чуть ниже видим файл прошивки.



ASA0

Physical Config CLI

ASA Command Line Interface

```
Cisco Adaptive Security Appliance Software Version 8.4(2)
Device Manager Version 6.4(5)

Compiled on Wed 16-Jun-11 18:17 by mnguyen
System image file is "disk0:/asa842-k8.bin"
Config file at boot was "startup-config"

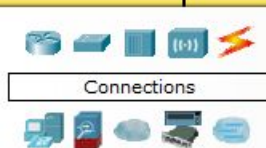
ciscoasa up 23 minutes 56 seconds

Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xffff00000, 2048KB

Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                                Boot microcode       : CN1000-MC-BOOT-2.00
                                SSL/IKE microcode      : CNLite-MC-SSLm-PLUS-2.03
                                IPSec microcode         : CNLite-MC-IPSECm-MAIN-2.06
                                Number of accelerators: 1

0: Int: Internal-Data0/0   : address is 44d3.caef.1e22, irq 11
1: Ext: Ethernet0/0        : address is 00E0.F9D9.1101, irq 255
2: Ext: Ethernet0/1        : address is 00E0.F9D9.1102, irq 255
3: Ext: Ethernet0/2        : address is 00E0.F9D9.1103, irq 255
4: Ext: Ethernet0/3        : address is 00E0.F9D9.1104, irq 255
5: Ext: Ethernet0/4        : address is 00E0.F9D9.1105, irq 255
6: Ext: Ethernet0/5        : address is 00E0.F9D9.1106, irq 255
7: Ext: Ethernet0/6        : address is 00E0.F9D9.1107, irq 255
8: Ext: Ethernet0/7        : address is 00E0.F9D9.1108, irq 255
9: Int: Internal-Data0/1   : address is 0000.0003.0002, irq 255
```

Copy Paste



Copper Cross-Over

Scenario 0

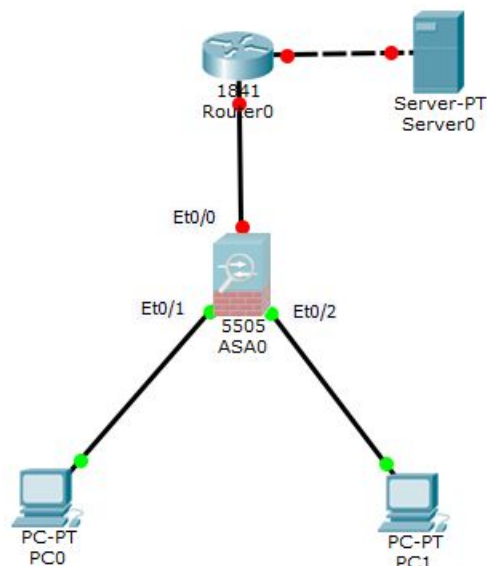
New Delete

Toggle PDU List Window

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



**Далее находим
основные параметры
прошивки
ниже – порты.**



ASA0

Physical Config CLI

ASA Command Line Interface

```
Cisco Adaptive Security Appliance Software Version 8.4(2)
Device Manager Version 6.4(5)

Compiled on Wed 16-Jun-11 18:17 by mnguyen
System image file is "disk0:/asa842-k8.bin"
Config file at boot was "startup-config"

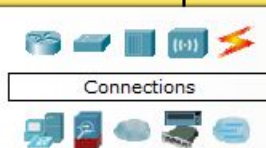
ciscoasa up 23 minutes 56 seconds

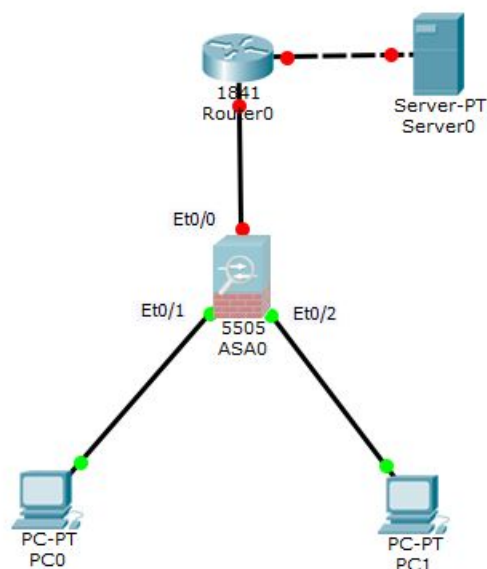
Hardware: ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xffff00000, 2048KB

Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
Boot microcode : CN1000-MC-BOOT-2.00
SSL/IKE microcode : CNLite-MC-SSLm-PLUS-2.03
IPSec microcode : CNLite-MC-IPSECm-MAIN-2.06
Number of accelerators: 1

0: Int: Internal-Data0/0 : address is 44d3.caef.1e22, irq 11
1: Ext: Ethernet0/0 : address is 00E0.F9D9.1101, irq 255
2: Ext: Ethernet0/1 : address is 00E0.F9D9.1102, irq 255
3: Ext: Ethernet0/2 : address is 00E0.F9D9.1103, irq 255
4: Ext: Ethernet0/3 : address is 00E0.F9D9.1104, irq 255
5: Ext: Ethernet0/4 : address is 00E0.F9D9.1105, irq 255
6: Ext: Ethernet0/5 : address is 00E0.F9D9.1106, irq 255
7: Ext: Ethernet0/6 : address is 00E0.F9D9.1107, irq 255
8: Ext: Ethernet0/7 : address is 00E0.F9D9.1108, irq 255
9: Int: Internal-Data0/1 : address is 0000.0003.0002, irq 255
```

Copy Paste





Перемещаемся в самый низ.
Видим, что установлена базовая лицензия.
На данный момент сменить её невозможно.

ASA0

Physical Config CLI

ASA Command Line Interface

Licensed features for this platform:

Maximum Physical Interfaces	: 8	perpetual
VLANs	: 3	DMZ Restricted
Dual ISPs	: Disabled	perpetual
VLAN Trunk Ports	: 0	perpetual
Inside Hosts	: 10	perpetual
Failover	: Disabled	perpetual
VPN-DES	: Enabled	perpetual
VPN-3DES-AES	: Enabled	perpetual
AnyConnect Premium Peers	: 2	perpetual
AnyConnect Essentials	: Disabled	perpetual
Other VPN Peers	: 10	perpetual
Total VPN Peers	: 25	perpetual
Shared License	: Disabled	perpetual
AnyConnect for Mobile	: Disabled	perpetual
AnyConnect for Cisco VPN Phone	: Disabled	perpetual
Advanced Endpoint Assessment	: Disabled	perpetual
UC Phone Proxy Sessions	: 2	perpetual
Total UC Proxy Sessions	: 2	perpetual
Botnet Traffic Filter	: Disabled	perpetual
Intercompany Media Engine	: Disabled	perpetual

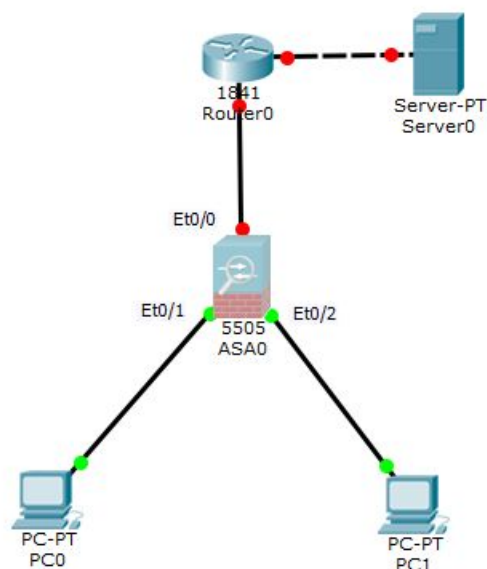
This platform has a Base license.

Serial Number: JMX1536T2F9
Running Permanent Activation Key: 0x8L39GM6H 0xPGAES72H 0xI74W8T07 0xVMQRVKB5 0x72F1UL61
Configuration register is 0x1
Configuration has not been modified since last system restart.

ciscoasa#

Copy Paste





Максимальное количество VLANs равно трём. Причём один из них (DNZ), как правило ограниченный.

ASA0

Physical Config CLI

ASA Command Line Interface

Licensed features for this platform:

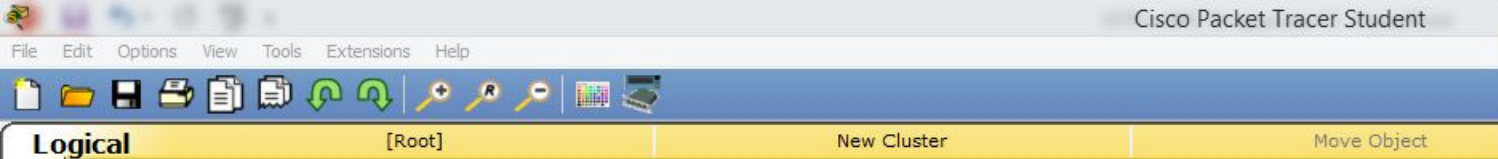
Maximum Physical Interfaces	: 8	perpetual
VLANs	: 3	DMZ Restricted
Dual ISPs	: Disabled	perpetual
VLAN Trunk Ports	: 0	perpetual
Inside Hosts	: 10	perpetual
Failover	: Disabled	perpetual
VPN-DES	: Enabled	perpetual
VPN-3DES-AES	: Enabled	perpetual
AnyConnect Premium Peers	: 2	perpetual
AnyConnect Essentials	: Disabled	perpetual
Other VPN Peers	: 10	perpetual
Total VPN Peers	: 25	perpetual
Shared License	: Disabled	perpetual
AnyConnect for Mobile	: Disabled	perpetual
AnyConnect for Cisco VPN Phone	: Disabled	perpetual
Advanced Endpoint Assessment	: Disabled	perpetual
UC Phone Proxy Sessions	: 2	perpetual
Total UC Proxy Sessions	: 2	perpetual
Botnet Traffic Filter	: Disabled	perpetual
Intercompany Media Engine	: Disabled	perpetual

This platform has a Base license.

Serial Number: JMX1536T2F9
 Running Permanent Activation Key: 0x8L39GM6H 0xPGAES72H 0xI74W8T07 0xVMQRVKB5 0x72F1UL61
 Configuration register is 0x1
 Configuration has not been modified since last system restart.

ciscoasa#

Copy Paste



Также видим, что у нас нет возможности использовать Trunk Ports. Это делает макетирование в Cisco Packet Tracer **весьма неудобным. Будем ждать новые версии, а пока придётся работать с тем, что есть.**

ASA0

Physical Config CLI

ASA Command Line Interface

Licensed features for this platform:

Maximum Physical Interfaces	: 8	perpetual
VLANs	: 3	DMZ Restricted
Dual ISPs	: Disabled	perpetual
VLAN Trunk Ports	: 0	perpetual
Inside Hosts	: 10	perpetual
Failover	: Disabled	perpetual
VPN-DES	: Enabled	perpetual
VPN-3DES-AES	: Enabled	perpetual
AnyConnect Premium Peers	: 2	perpetual
AnyConnect Essentials	: Disabled	perpetual
Other VPN Peers	: 10	perpetual
Total VPN Peers	: 25	perpetual
Shared License	: Disabled	perpetual
AnyConnect for Mobile	: Disabled	perpetual
AnyConnect for Cisco VPN Phone	: Disabled	perpetual
Advanced Endpoint Assessment	: Disabled	perpetual
UC Phone Proxy Sessions	: 2	perpetual
Total UC Proxy Sessions	: 2	perpetual
Botnet Traffic Filter	: Disabled	perpetual
Intercompany Media Engine	: Disabled	perpetual

This platform has a Base license.

Serial Number: JMX1536T2F9
Running Permanent Activation Key: 0x8L39GM6H 0xPGAES72H 0xI74W8T07 0xVMQRVKB5 0x72F1UL61
Configuration register is 0x1
Configuration has not been modified since last system restart.

ciscoasa#

Copy Paste

Time: 02:52:02 Power Cycle Devices Fast Forward Time

Connections

Scenario 0

New Delete

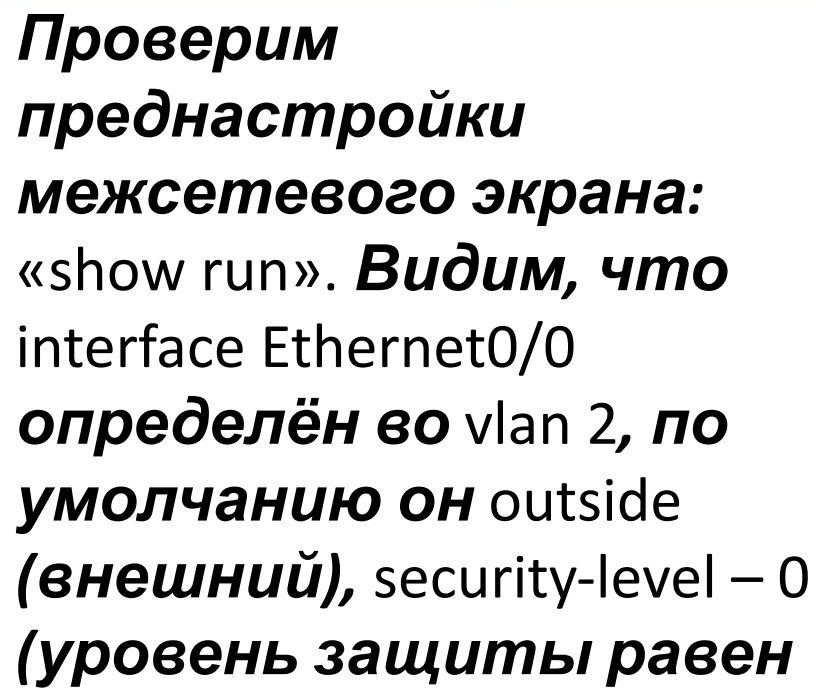
Toggle PDU List Window

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

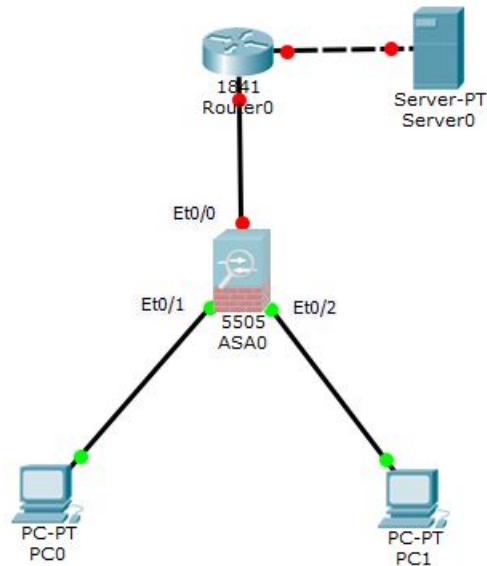
Copper Cross-Over

Realtime

19:27 11.01.2020



0) и включен дисс-клиент.



Опускаемся ещё ниже и видим, что по умолчанию настроен dhcp-сервер на внутреннем интерфейсе. Это значит, он будет раздавать ip-адреса подключенным компьютерам.

Physical	Config	CLI
----------	--------	-----

ASA Command Line Interface

```

!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp
!
!
!
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd address 192.168.1.5-192.168.1.35 inside
dhcpd enable inside
!
dhcpd auto_config outside
!
!
!
!
!
!
ciscoasa#

```

Copy

Paste

Time: 03:28:35	Power Cycle Devices Fast Forward Time
----------------	---------------------------------------

Realtime



Connections



Scenario 0

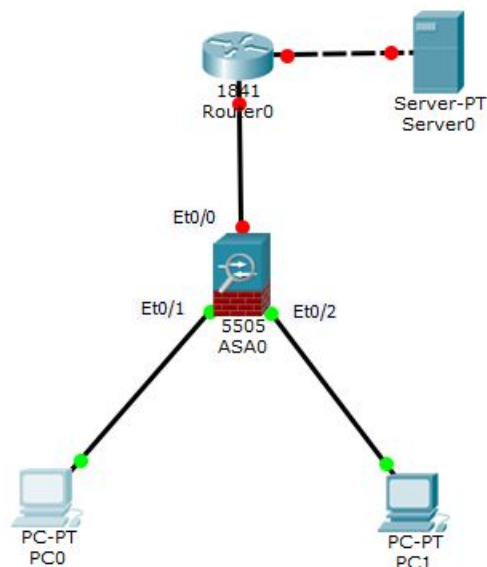
New Delete

Toggle PDU List Window

[illegible]



**Если это верно,
получим ip-адрес для
компьютера PC0.
Сработало, ip-адрес
получен.**



PC0

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IP Address 192.168.1.5

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server

IPv6 Configuration

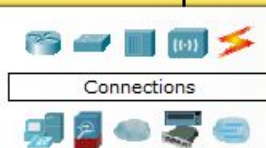
☐ DHCP ☐ Auto Config ☒ Static

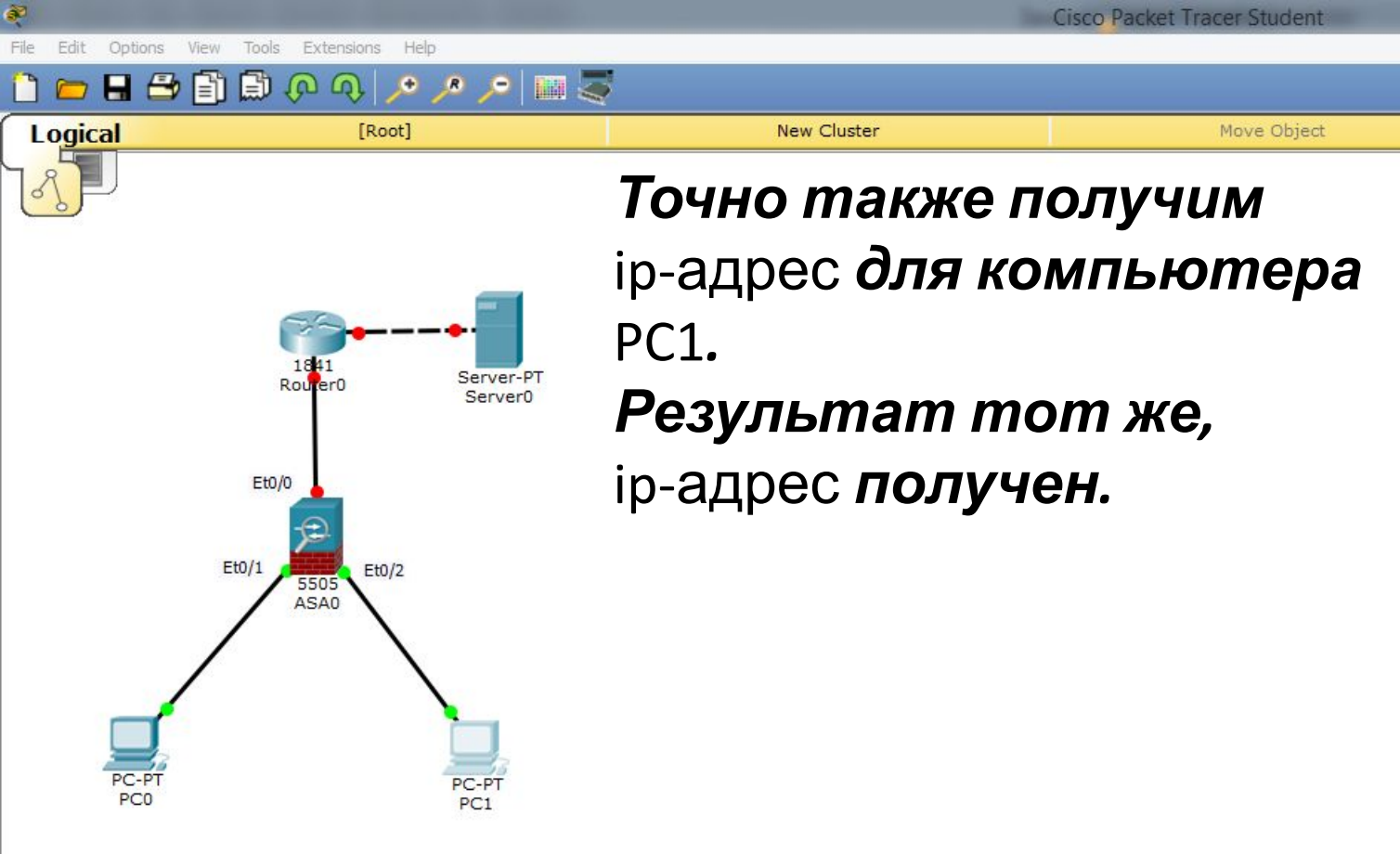
IPv6 Address /

Link Local Address FE80::206:2AFF:FE7E:4634

IPv6 Gateway

IPv6 DNS Server





**Точно также получим
ip-адрес для компьютера
PC1.
Результат тот же,
ip-адрес получен.**

PC1

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IP Address 192.168.1.6

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /

Link Local Address FE80::20D:BDFF:FEC0:13DA

IPv6 Gateway

IPv6 DNS Server

Time: 03:36:37 Power Cycle Devices Fast Forward Time

Connections

Copper Cross-Over

Scenario 0

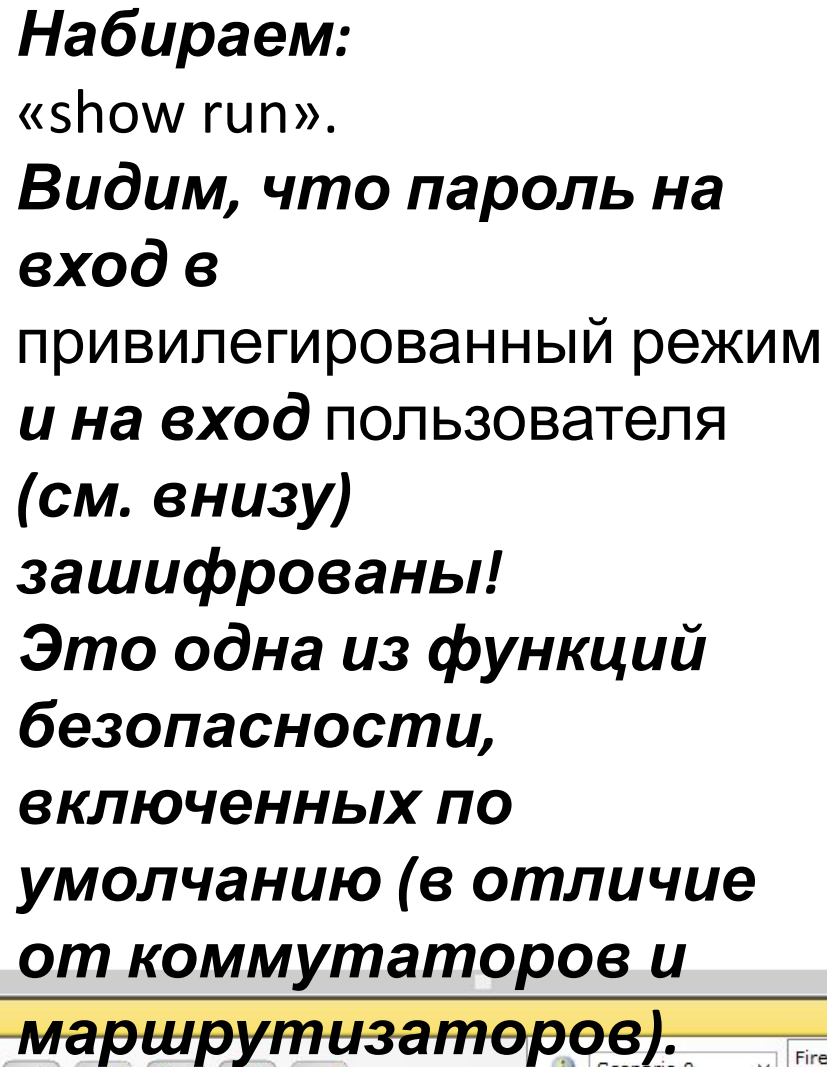
New Delete

Toggle PDU List Window

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

Realtime

20:12 11.01.2020

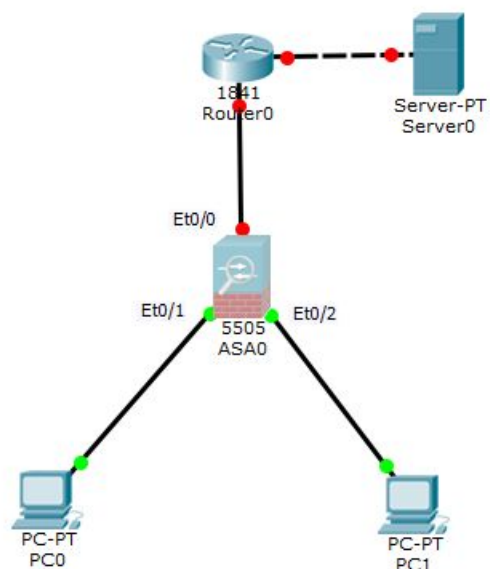


Набираем:
«show run».

Видим, что пароль на вход в привилегированный режим и на вход пользователя (см. внизу) зашифрованы!

Это одна из функций безопасности, включенных по умолчанию (в отличие от коммутаторов и маршрутизаторов).

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



Выберем протокол SSH, по которому будем осуществлять удалённый доступ, указываем ip-адрес сети и интерфейс. Так как команда длинная, для просмотра вариантов пользуемся знаком «?»: «ssh 192.168.1.0 255.255.255.0 inside».

ASA0

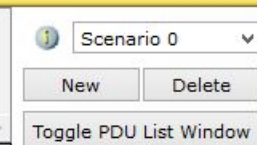
Physical Config CLI

ASA Command Line Interface

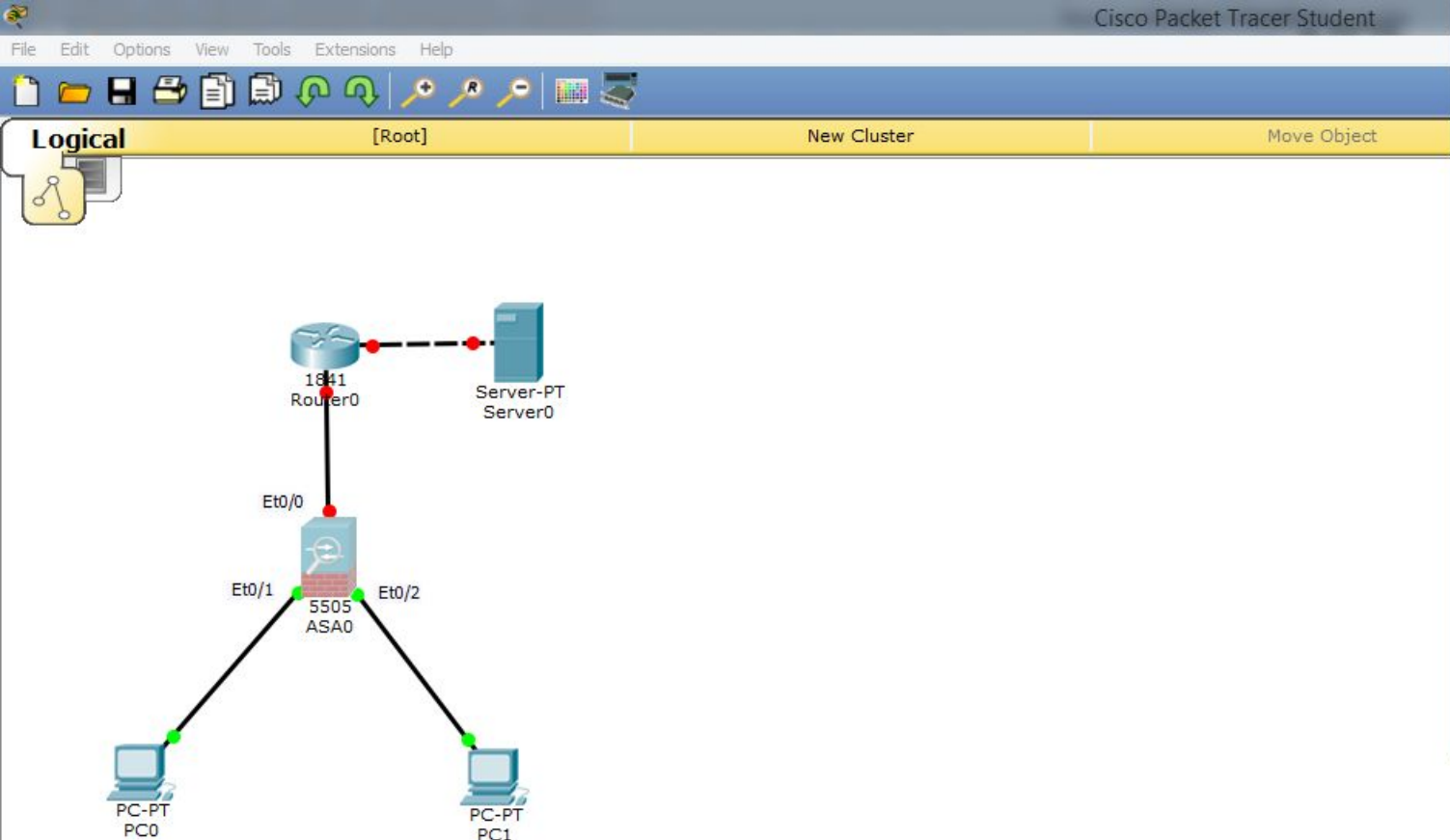
```
!
telnet timeout 5
ssh timeout 5
!
dhcpd address 192.168.1.5-192.168.1.35 inside
dhcpd enable inside
!
dhcpd auto_config outside
!
!
!
!
!
!
!
!
!
!
ciscoasa(config)#ssh ?

configure mode commands/options:
WORD                               The IP address of the host and/or network authorized to
                                login to the system
X:X:X:X::X/<0-128>                 IPv6 address/prefix authorized to login to the system
timeout                           Configure ssh idle timeout
ciscoasa(config)#ssh 192.168.1.0 255.255.255.0 ins
ciscoasa(config)#ssh 192.168.1.0 255.255.255.0 inside
ciscoasa(config)#
```

Copy Paste



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



ASA0

Physical Config CLI

ASA Command Line Interface

```
X.X.X.X.X/0-128/ Ifve address/prefix authorized to login to the system
timeout          Configure ssh idle timeout
ciscoasa(config)#ssh 192.168.1.0 255.255.255.0 ins
ciscoasa(config)#ssh 192.168.1.0 255.255.255.0 inside
ciscoasa(config)#
ciscoasa(config)#aaa aut
ciscoasa(config)#aaa authentication ?

configure mode commands/options:
  ssh      SSH
  telnet   Telnet
ciscoasa(config)#aaa authentication ssh ?

configure mode commands/options:
  console Specify this keyword to identify a server group for administrative
           authentication
ciscoasa(config)#aaa authentication ssh co
ciscoasa(config)#aaa authentication ssh console ?

configure mode commands/options:
  LOCAL   Predefined server tag for AAA protocol 'local'
ciscoasa(config)#aaa authentication ssh console L
ciscoasa(config)#aaa authentication ssh console LOCAL
ciscoasa(config)#
```

Copy Paste

Далее задаём параметры аутентификации пользователя. Так как команда длинная, для просмотра вариантов пользуемся знаком «?»:
«aaa authentication ssh console LOCAL».

Time: 04:16:47 Power Cycle Devices Fast Forward Time

Connections

Scenario 0

New Delete

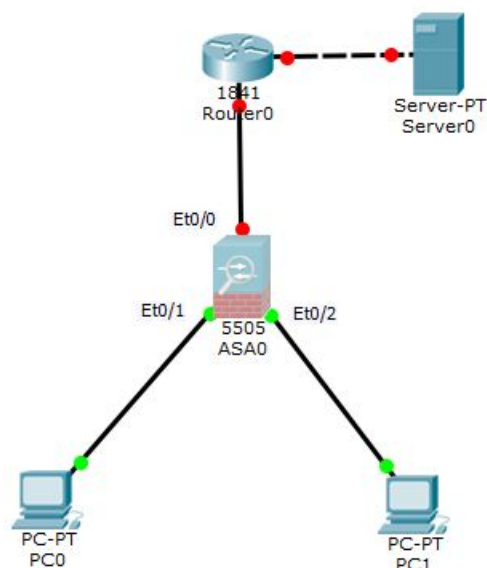
Toggle PDU List Window

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

Copper Cross-Over

Realtime

20:52 11.01.2020



Наберём команду:
«show run».

На этом устройстве
она доступна в любой
момент (не так как на
коммутаторах и
маршрутизаторах).

ASA0

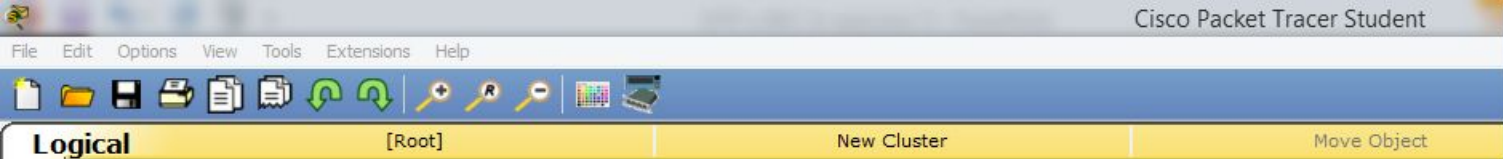
Physical Config CLI

ASA Command Line Interface

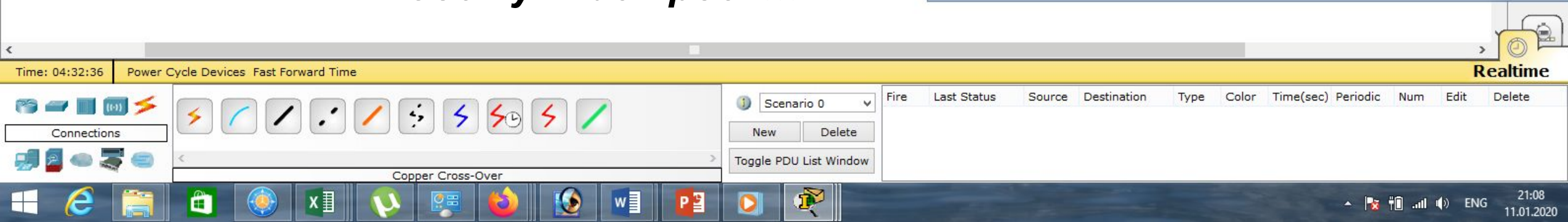
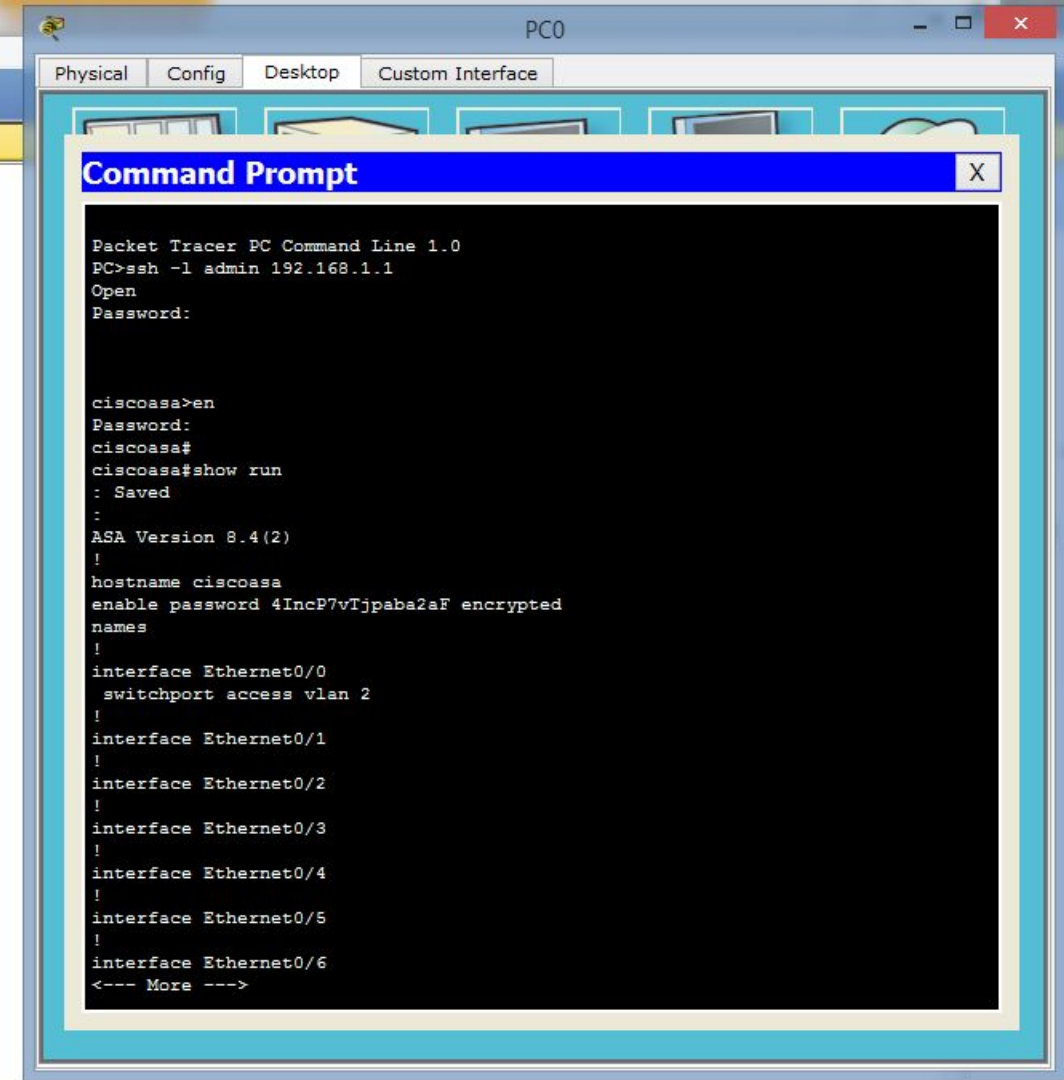
```
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#show run
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
enable password 4IncP7vTjpaba2aF encrypted
names
!
interface Ethernet0/0
  switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
  nameif outside
  security-level 0
  ip address dhcp
!
```

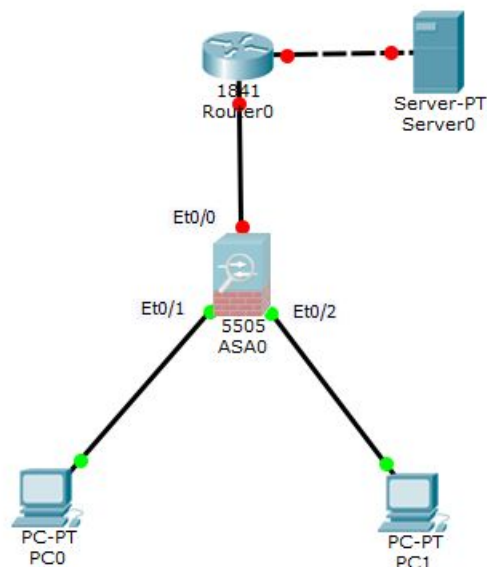
Copy Paste





**Попробуем удалённо
подключиться к
межсетевому экрану с
компьютера PC0:
«ssh -l admin 192.168.1.1»,
пароль: cisco.
Входим в
привилегированный
режим: «en», пароль: cisco,
далее: «show run».
Видим, что удалённый
доступ настроен!!!**





**Уровень доверия к
интерфейсу Security Level
можно легко изменить,
например, на 95.**

**Для этого в режиме
глобального
конфигурирования
набираем:**

«int vlan 1»,
«security-level 95»,
«end»,
«show run».

ASA0

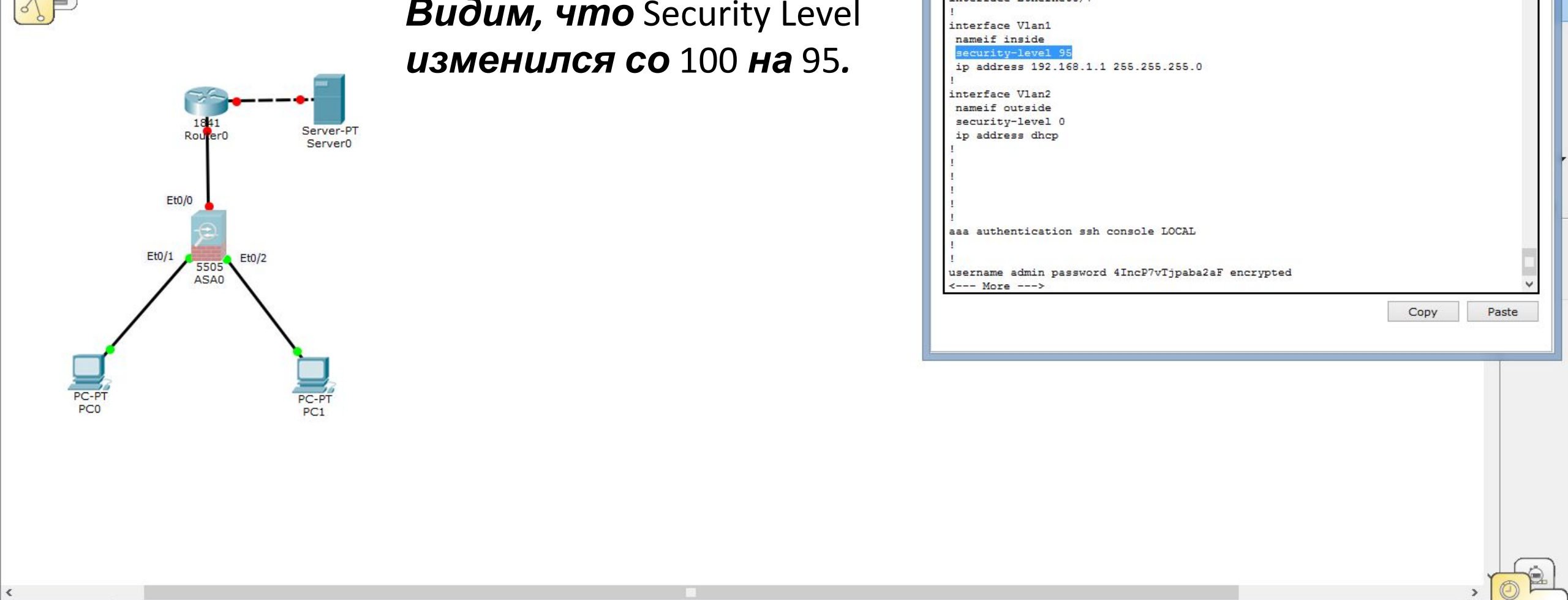
Physical Config CLI

ASA Command Line Interface

```
!
!
!
telnet timeout 5
ssh 192.168.1.0 255.255.255.0 inside
ssh timeout 5
!
dhcpd address 192.168.1.5-192.168.1.35 inside
dhcpd enable inside
!
dhcpd auto_config outside
!
!
!
!
!
!
ciscoasa(config)#int vlan 1
ciscoasa(config-if)#sec
ciscoasa(config-if)#security-level 95
ciscoasa(config-if)#end
ciscoasa#
ciscoasa#
ciscoasa#show run
```

Copy Paste





Видим, что Security Level изменился со 100 на 95.

The network diagram shows a central ASA device (ASA0) with three interfaces. Interface Et0/0 is connected to Router0 (1841). Router0 is further connected to Server-PT (Server0). Interface Et0/1 of ASA0 is connected to PC-PT (PC0), and interface Et0/2 is connected to PC-PT (PC1).

```
!
interface Vlan1
 nameif inside
 security-level 95
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp
!
!
!
!
!
!
!
aaa authentication ssh console LOCAL
!
!
username admin password 4IncP7vTjpaba2aF encrypted
<--- More --->
```

Copy

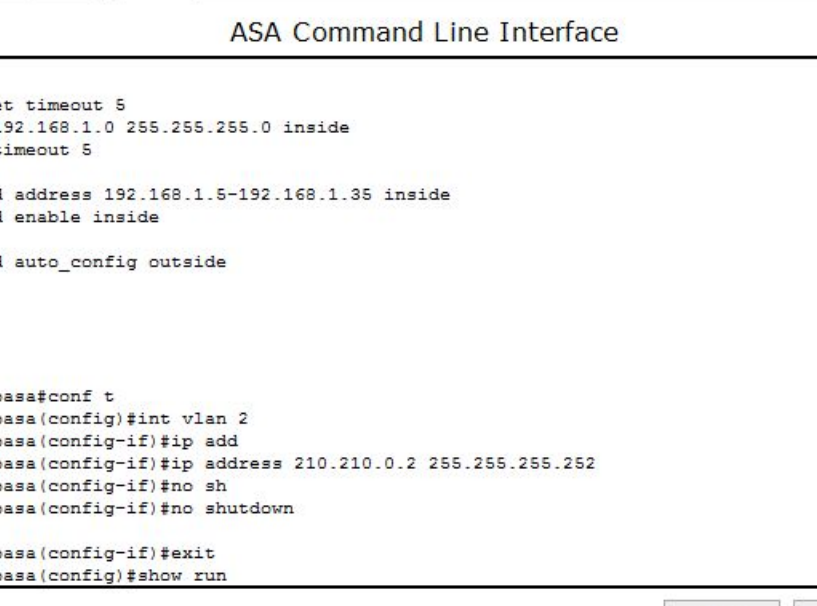
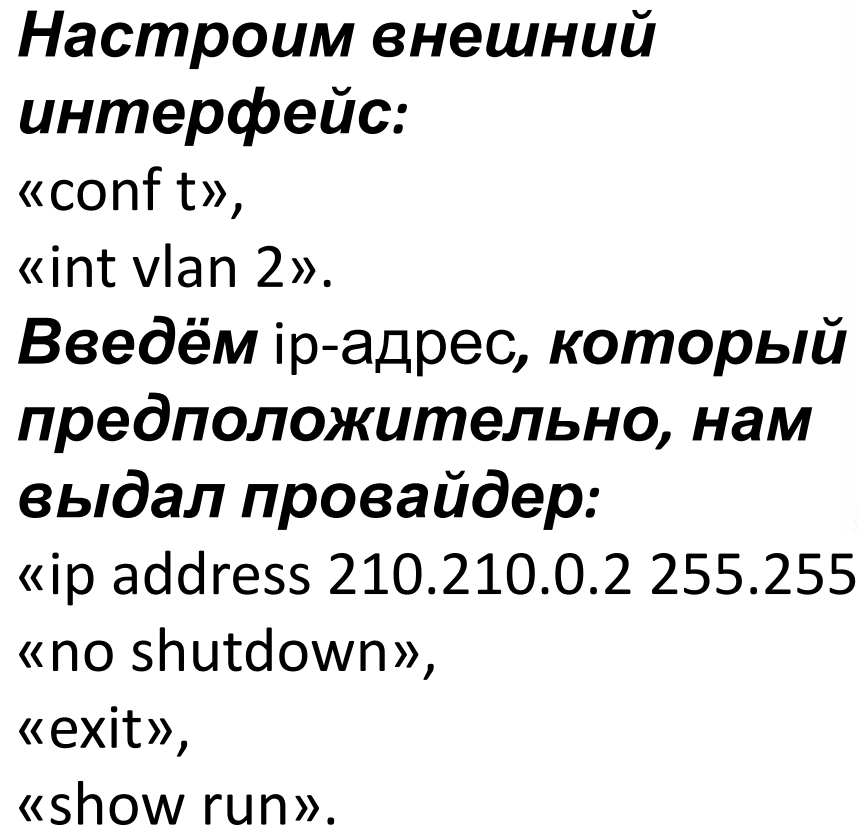
Paste

Time: 05:07:44

Power Cycle Devices Fast Forward Time

Realtime

[illegible]



The screenshot displays the ASA0 Command Line Interface (CLI) window. The window has a title bar with 'ASA0' and standard window controls. Below the title bar are three tabs: 'Physical', 'Config', and 'CLI', with 'CLI' being the active tab. The main area of the window is titled 'ASA Command Line Interface' and contains a text area with the following commands:

```
!
!
telnet timeout 5
ssh 192.168.1.0 255.255.255.0 inside
ssh timeout 5
!
dhcpd address 192.168.1.5-192.168.1.35 inside
dhcpd enable inside
!
dhcpd auto_config outside
!
!
!
!
!
!
ciscoasa#conf t
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip add
ciscoasa(config-if)#ip address 210.210.0.2 255.255.255.252
ciscoasa(config-if)#no sh
ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#exit
ciscoasa(config)#show run
```

At the bottom right of the window, there are two buttons: 'Copy' and 'Paste'.

[Root]

New Cluster

Move Object



Config

CLI

```
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 95
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 210.210.0.2 255.255.255.252
!
!
!
!
!
!
aaa authentication ssh console LOCAL
!
```

Copy

Paste

Time: 05:22:26	Power Cycle Devices Fast Forward Time
----------------	---------------------------------------

[illegible]

Copper Cross-Over

Scenario 0

New

Delete

Toggle PDU List Window

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

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object

210.210.1.1 255.255.255.0 Et0/1
210.210.0.1 255.255.255.252 Et0/0
1841 Router0
Server-PT Server0
Et0/0
5505 ASA0
Et0/1 Et0/2
PC-PT PC0
PC-PT PC1

Time: 05:33:46 Power Cycle Devices Fast Forward Time

Connections

Copper Cross-Over

Scenario 0 New Delete Toggle PDU List Window

Настроим маршрутизатор провайдера:

«n», «en»,
«int fa0/0»,
«ip address 210.210.0.1
255.255.255.252»,
«no shutdown»,
«exit»,
«int fa0/1»,
«ip address 210.210.1.1 255.255.255.0»,
«no shutdown»,
«end», «wr mem».

Router0

Physical Config CLI

IOS Command Line Interface

```
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

--- System Configuration Dialog ---

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

Press RETURN to get started!

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip add
Router(config-if)#ip address 210.210.0.1 255.255.255.252
Router(config-if)#no sh
Router(config-if)#no shutdown

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

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

Router(config-if)#exit
Router(config)#int fa0/1
Router(config-if)#ip address 210.210.1.1 255.255.255.0
Router(config-if)#no shutdown

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

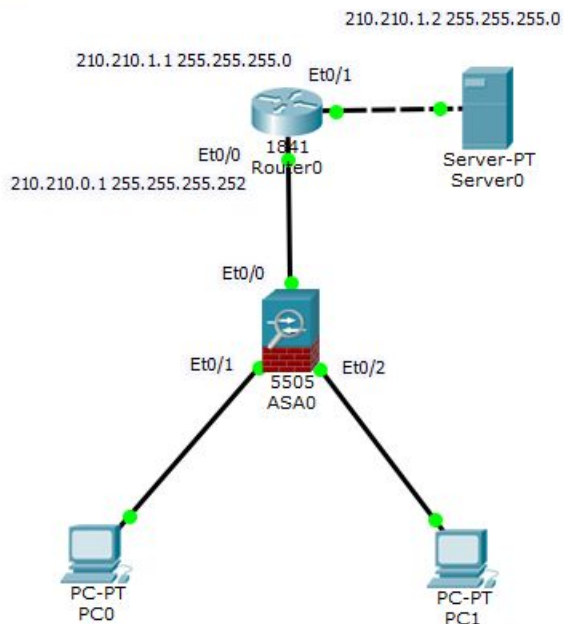
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

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

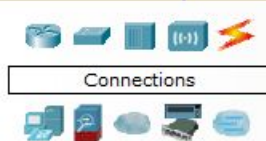
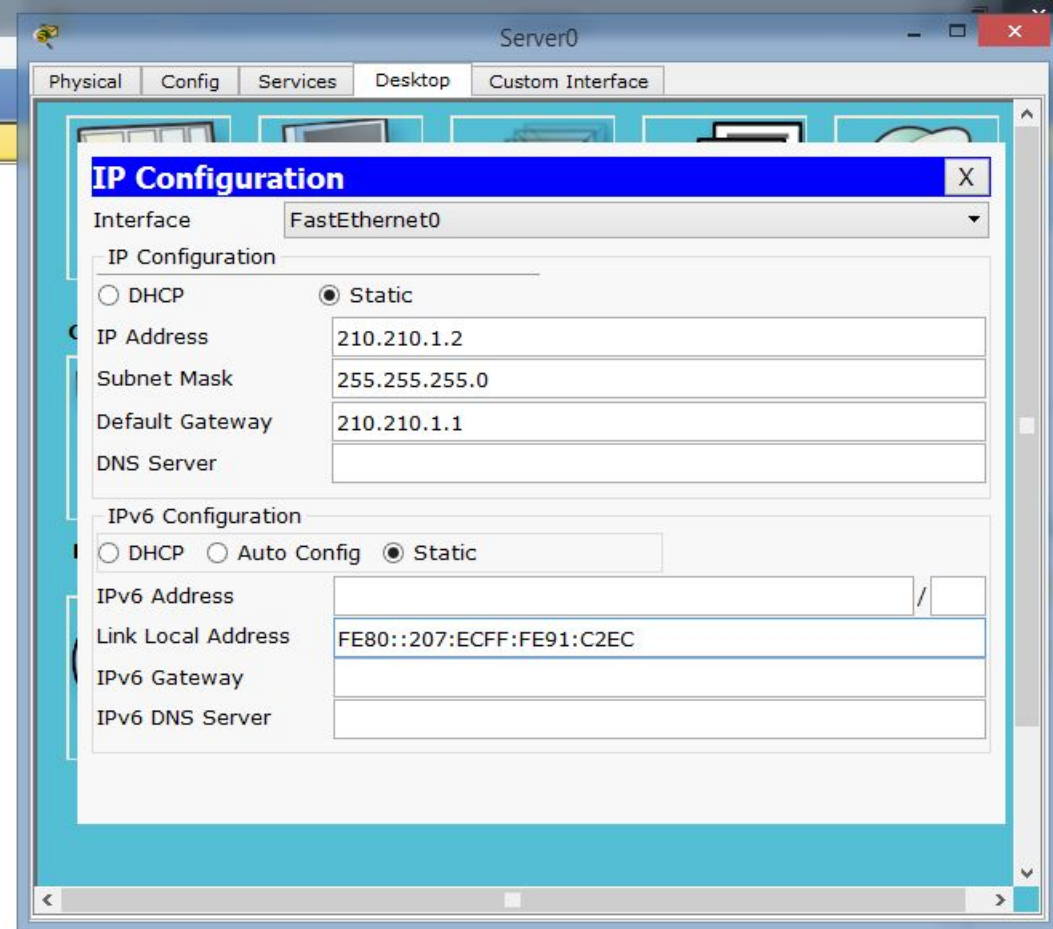
Router#wr mem
Building configuration...
[OK]
Router#
```

Copy Paste

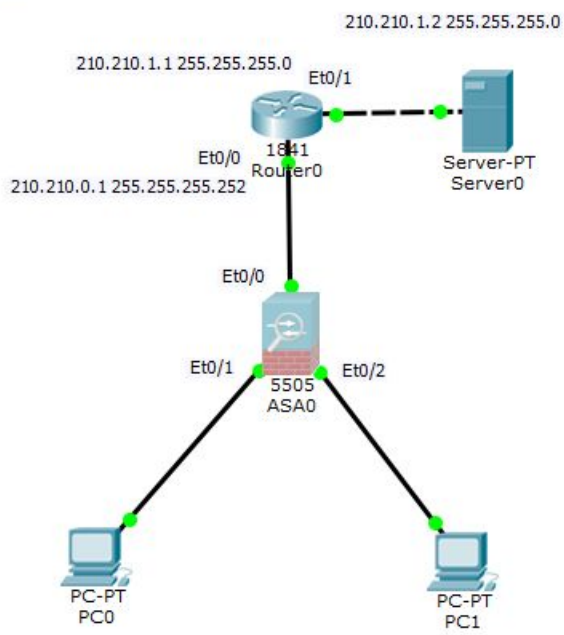
22:10 11.01.2020



Настроим сервер.
Введём ip-адрес,:
«210.210.1.2»,
маску:
«255.255.255.0» и
шлюз по умолчанию:
«210.210.1.1».



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



**Проверим связь с
межсетевого экрана на
маршрутизатор:
«ping 210.210.0.1».
Видим, что связь есть!**

ASA0

Physical Config CLI

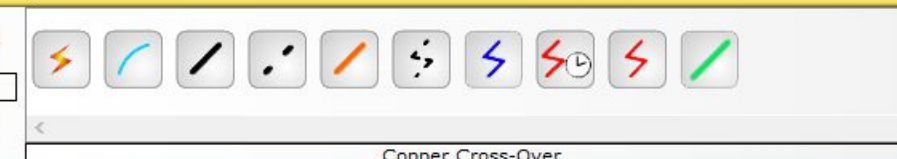
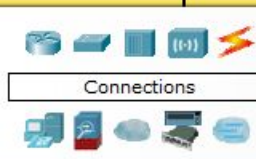
ASA Command Line Interface

```
telnet timeout 5
ssh 192.168.1.0 255.255.255.0 inside
ssh timeout 5
!
dhcpd address 192.168.1.5-192.168.1.35 inside
dhcpd enable inside
!
dhcpd auto_config outside
!
!
!
!
!
ciscoasa(config)#
ciscoasa(config)#ping 210.210.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 210.210.0.1, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/3 ms

ciscoasa(config)#
ciscoasa(config)#
```

Copy Paste



Scenario 0

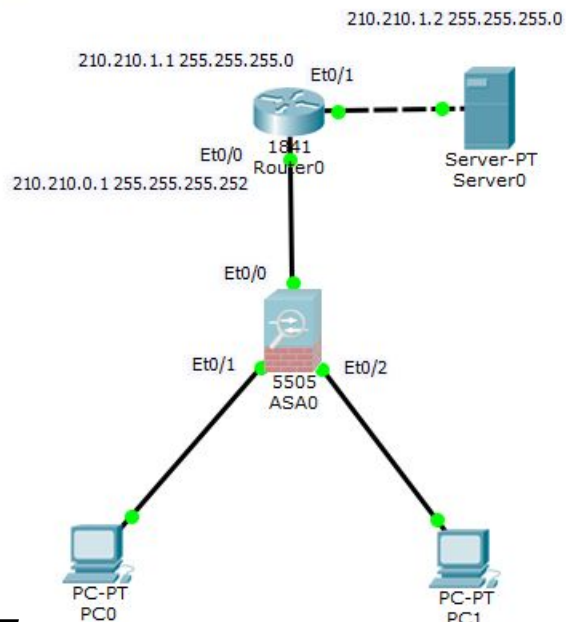
New Delete

Toggle PDU List Window

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



Logical [Root] New Cluster Move Object



ASA0

Physical Config CLI

ASA Command Line Interface

```
ciscoasa(config)#ping 210.210.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 210.210.0.1, timeout is 2 seconds:
..!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/3 ms

ciscoasa(config)#
ciscoasa(config)#route ?

configure mode commands/options:
  inside      Name of interface Vlan1
  outside     Name of interface Vlan2
ciscoasa(config)#route o
ciscoasa(config)#route outside ?

configure mode commands/options:
  Hostname or A.B.C.D The foreign network for this route, 0 means default
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 ?

configure mode commands/options:
  Hostname or A.B.C.D The address of the gateway by which the foreign network
                      is reached.
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 210.210.0.1
ciscoasa(config)#end
ciscoasa#
ciscoasa#
```

Copy Paste

Пропишем маршрут по умолчанию. Так как команда длинная, для просмотра вариантов пользуемся знаком «?»:
«route outside 0.0.0.0 0.0.0.0 210.210.0.1»,
«end».

Time: 05:56:46 Power Cycle Devices Fast Forward Time

Realtime



Copper Cross-Over

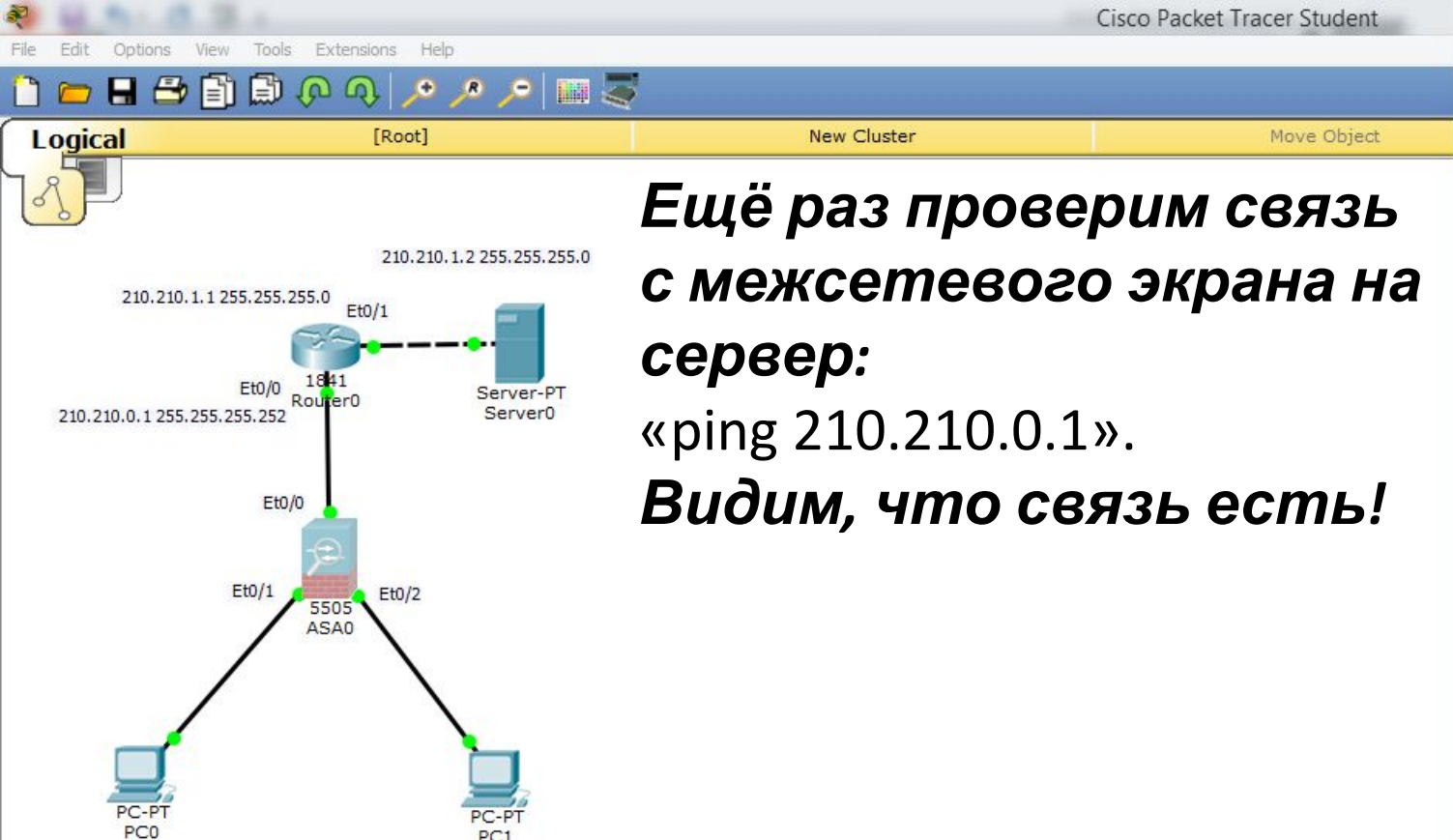
Scenario 0

New Delete

Toggle PDU List Window

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





**Ещё раз проверим связь
с межсетевого экрана на
сервер:
«ping 210.210.0.1».
Видим, что связь есть!**

ASA0

Physical Config CLI

ASA Command Line Interface

```
ciscoasa(config)#route 0
ciscoasa(config)#route outside ?

configure mode commands/options:
  Hostname or A.B.C.D The foreign network for this route, 0 means default
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 ?

configure mode commands/options:
  Hostname or A.B.C.D The address of the gateway by which the foreign network
  is reached.
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 210.210.0.1
ciscoasa(config)#end
ciscoasa#
ciscoasa#ping 210.210.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 210.210.1.2, timeout is 2 seconds:
...!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/1/3 ms

ciscoasa#ping 210.210.1.2

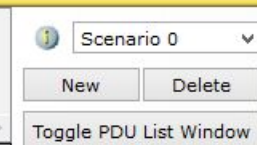
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 210.210.1.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

ciscoasa#
```

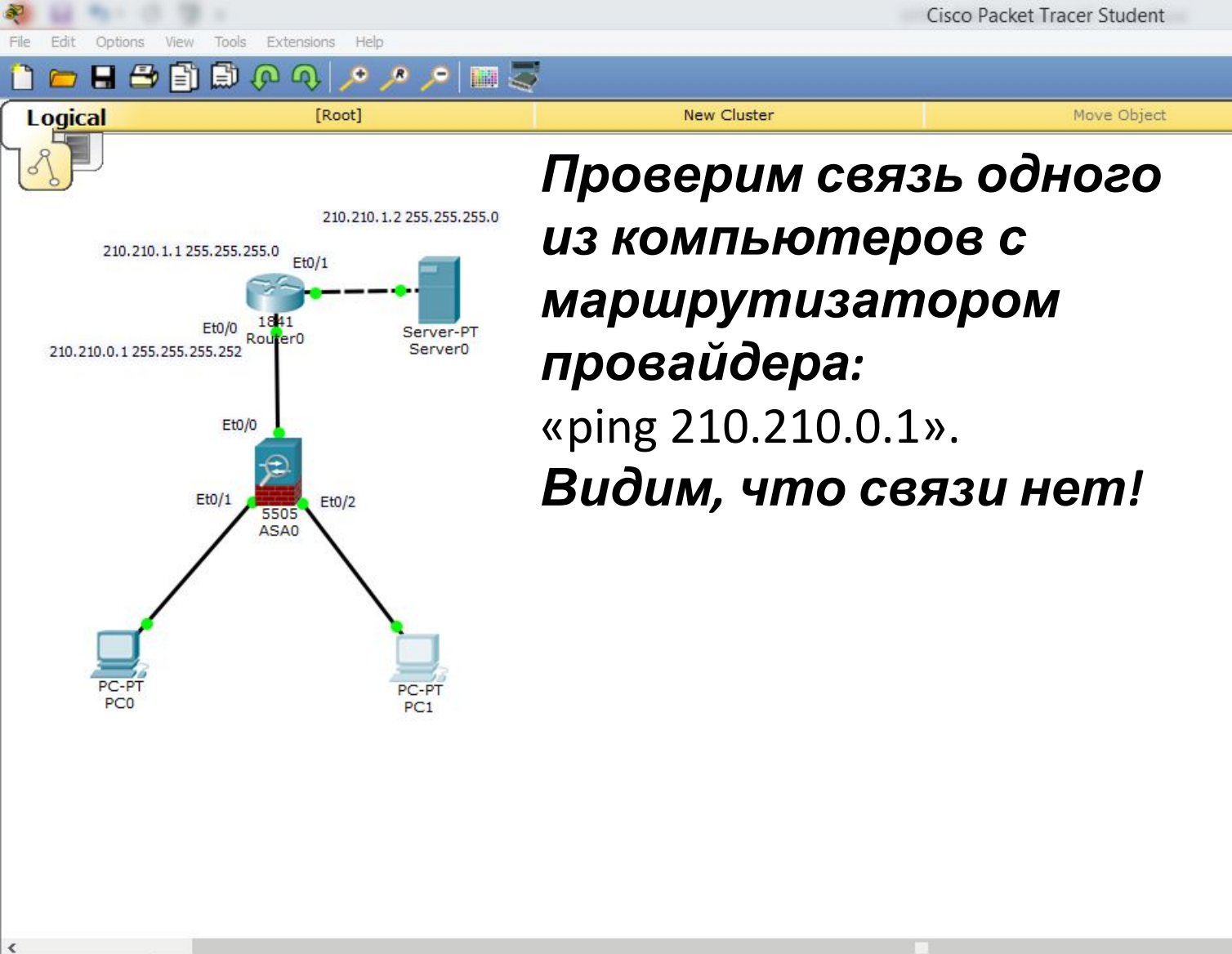
Copy Paste

Time: 06:18:07 Power Cycle Devices Fast Forward Time

Realtime



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



Проверим связь одного из компьютеров с маршрутизатором провайдера:
«ping 210.210.0.1».
Видим, что связи нет!

PC1

Physical Config Desktop Custom Interface

Command Prompt

```
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>ping 210.210.0.1

Pinging 210.210.0.1 with 32 bytes of data:

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

Ping statistics for 210.210.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
PC>
PC>
PC>
PC>
PC>
```

Time: 06:28:16 Power Cycle Devices Fast Forward Time

Connections

Copper Cross-Over

Scenario 0

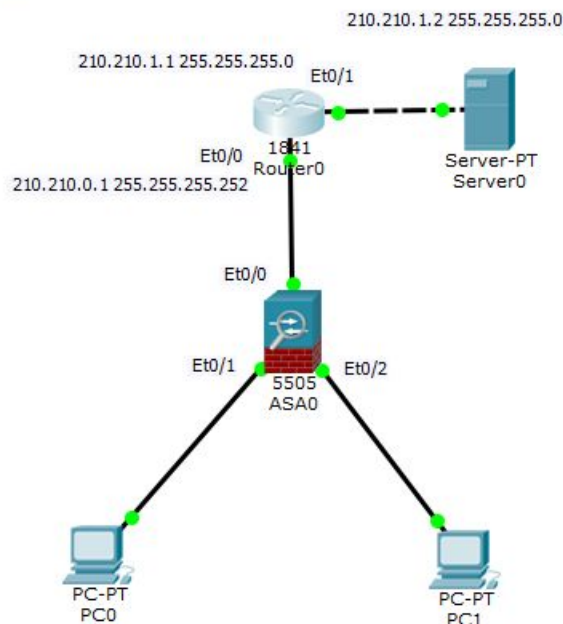
New Delete

Toggle PDU List Window

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

Realtime

23:04 11.01.2020



**Чтобы связь появилась,
необходимо прописать
маршрут на
маршрутизаторе
провайдера в нашу
локальную сеть
(192.168.0.1 255.255.255.0)
через ip-адрес межсетевого
экрана (210.210.0.2):**

«en»,

«conf t»,

«ip route 192.168.1.0 255.255.255.0 210.210.0.2»,

«end», «wr mem».

Router0

Physical Config CLI

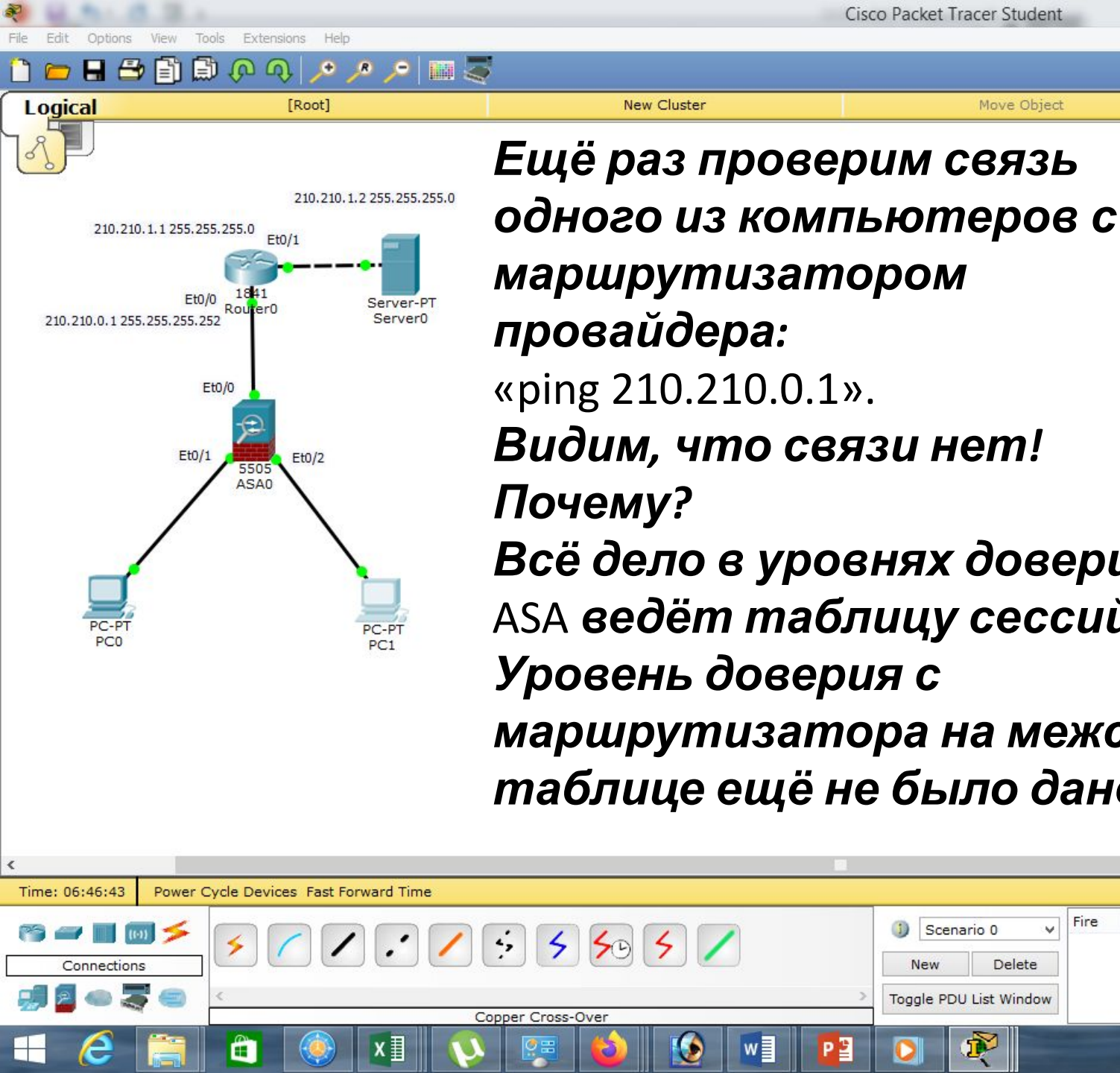
IOS Command Line Interface

```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 192.168.1.0 255.255.255.0 210.210.0.2
Router(config)#
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

Copy Paste





**Ещё раз проверим связь
одного из компьютеров с
маршрутизатором
провайдера:**

«ping 210.210.0.1».

Видим, что связи нет!

Почему?

Всё дело в уровнях доверия.

ASA ведёт таблицу сессий.

Уровень доверия с

**маршрутизатора на межсетевой экран низкий и в
таблице ещё не было дано ни одного разрешения.**

PC1

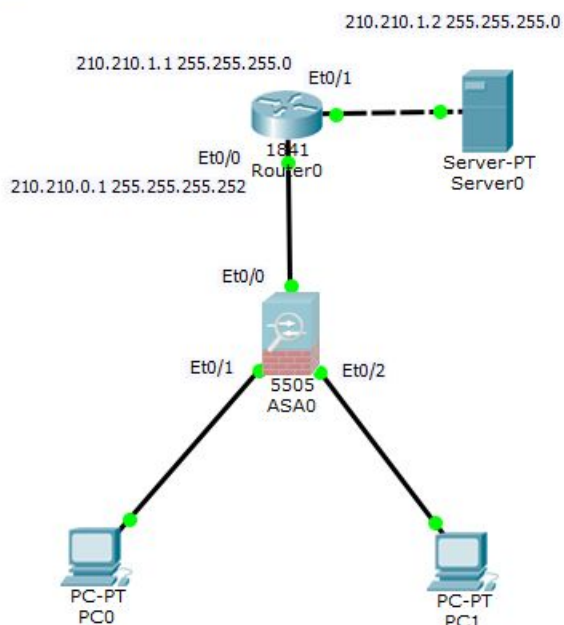
Physical Config Desktop Custom Interface

Command Prompt

```
Pinging 210.210.0.1 with 32 bytes of data:  
  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 210.210.0.1:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
PC>  
PC>  
PC>  
PC>  
PC>  
PC>ping 210.210.0.1  
  
Pinging 210.210.0.1 with 32 bytes of data:  
  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 210.210.0.1:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
PC>
```

Realtime

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



По умолчанию на ASA инспектирование трафика не настроено. Сделаем это. Сначала определяем тип трафика, который хотим инспектировать: «conf t», «class-map inspection_default», указываем весь трафик: «match default-inspection-traffic», «exit».

ASA0

Physical Config CLI

ASA Command Line Interface

```
Hostname or A.B.C.D The foreign network for this route, 0 means default
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 ?

configure mode commands/options:
  Hostname or A.B.C.D The address of the gateway by which the foreign network
                        is reached.
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 210.210.0.1
ciscoasa(config)#end
ciscoasa#
ciscoasa#ping 210.210.1.2

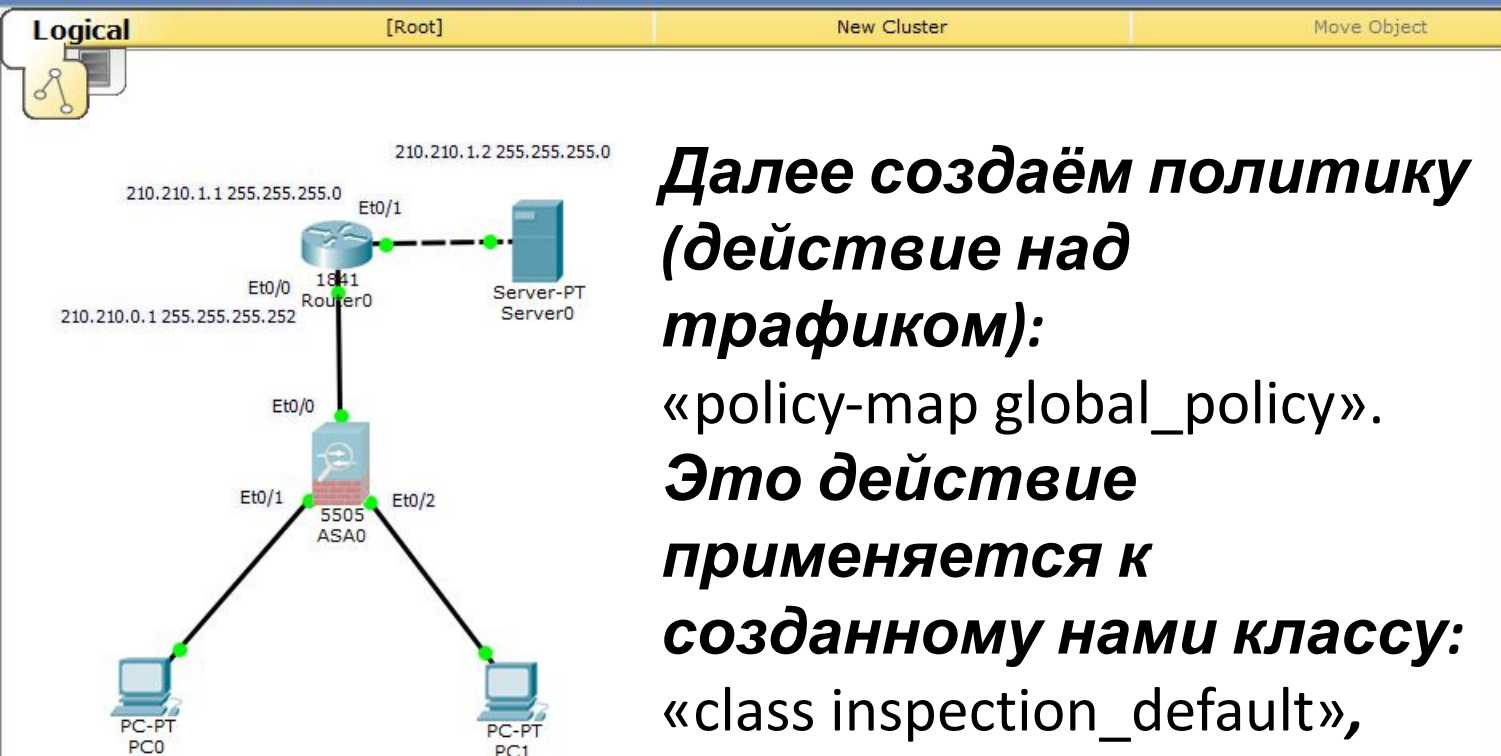
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 210.210.1.2, timeout is 2 seconds:
.....
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/1/3 ms

ciscoasa#ping 210.210.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 210.210.1.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

ciscoasa#conf t
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#exit
ciscoasa(config)#
```

Copy Paste



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».

ASA0

Physical Config CLI

ASA Command Line Interface

```
.....
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/1/3 ms

ciscoasa#ping 210.210.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 210.210.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

ciscoasa#conf t
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#ciscoasa(config-pmap-c)#class inspection_default
^
% Invalid input detected at '^' marker.

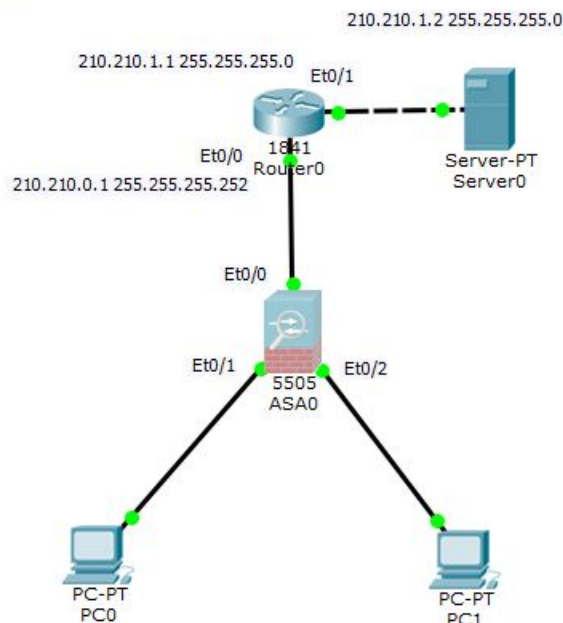
ciscoasa(config-pmap-c)#ciscoasa(config-pmap-c)#inspect icmp
^
% Invalid input detected at '^' marker.

ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#
ciscoasa(config-pmap-c)#exit
ciscoasa(config)#
```

Copy Paste



Logical [Root] New Cluster Move Object



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

«service-policy global_policy global»,
«end»,
«wr mem».

ASA0

Physical Config CLI

ASA Command Line Interface

```
ciscoasa(config-pmap-c)#ciscoasa(config-pmap)#class inspection_default
^
% Invalid input detected at '^' marker.

ciscoasa(config-pmap-c)#ciscoasa(config-pmap-c)#inspect icmp
^
% Invalid input detected at '^' marker.

ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#
ciscoasa(config-pmap-c)#exit
ciscoasa(config)#ciscoasa(config-pmap-c)#exit
ciscoasa(config)#
^
% Invalid input detected at '^' marker.

ciscoasa(config)#service-policy global_policy global
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#end
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 058c285f 55e0062d 00ad1335 5d2a0add

1101 bytes copied in 2.714 secs (405 bytes/sec)
[OK]
ciscoasa#
ciscoasa#
```

Copy Paste

Time: 31:29:36 Power Cycle Devices Fast Forward Time

Realtime



Copper Cross-Over

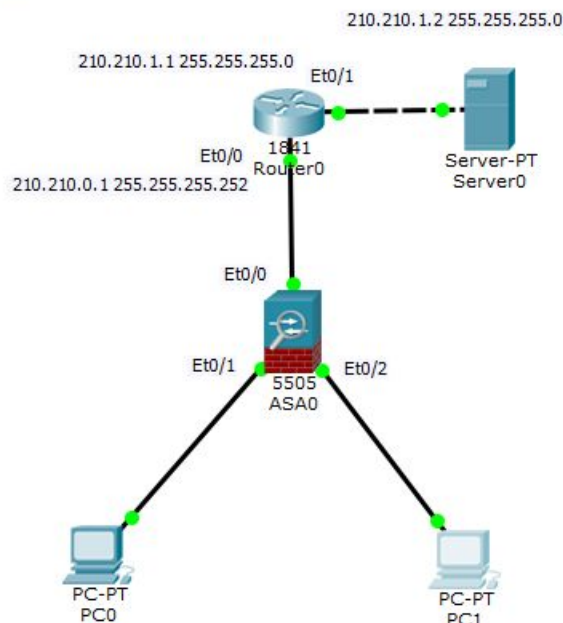
Scenario 0

New Delete

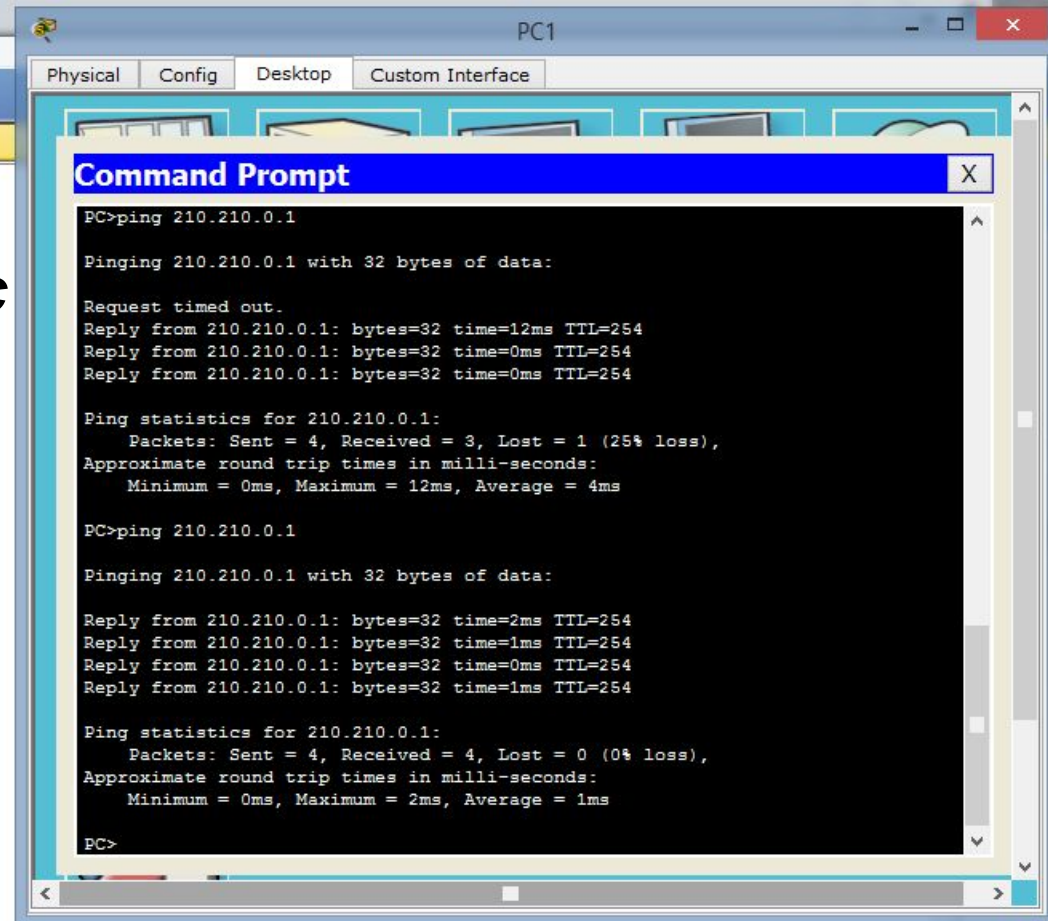
Toggle PDU List Window

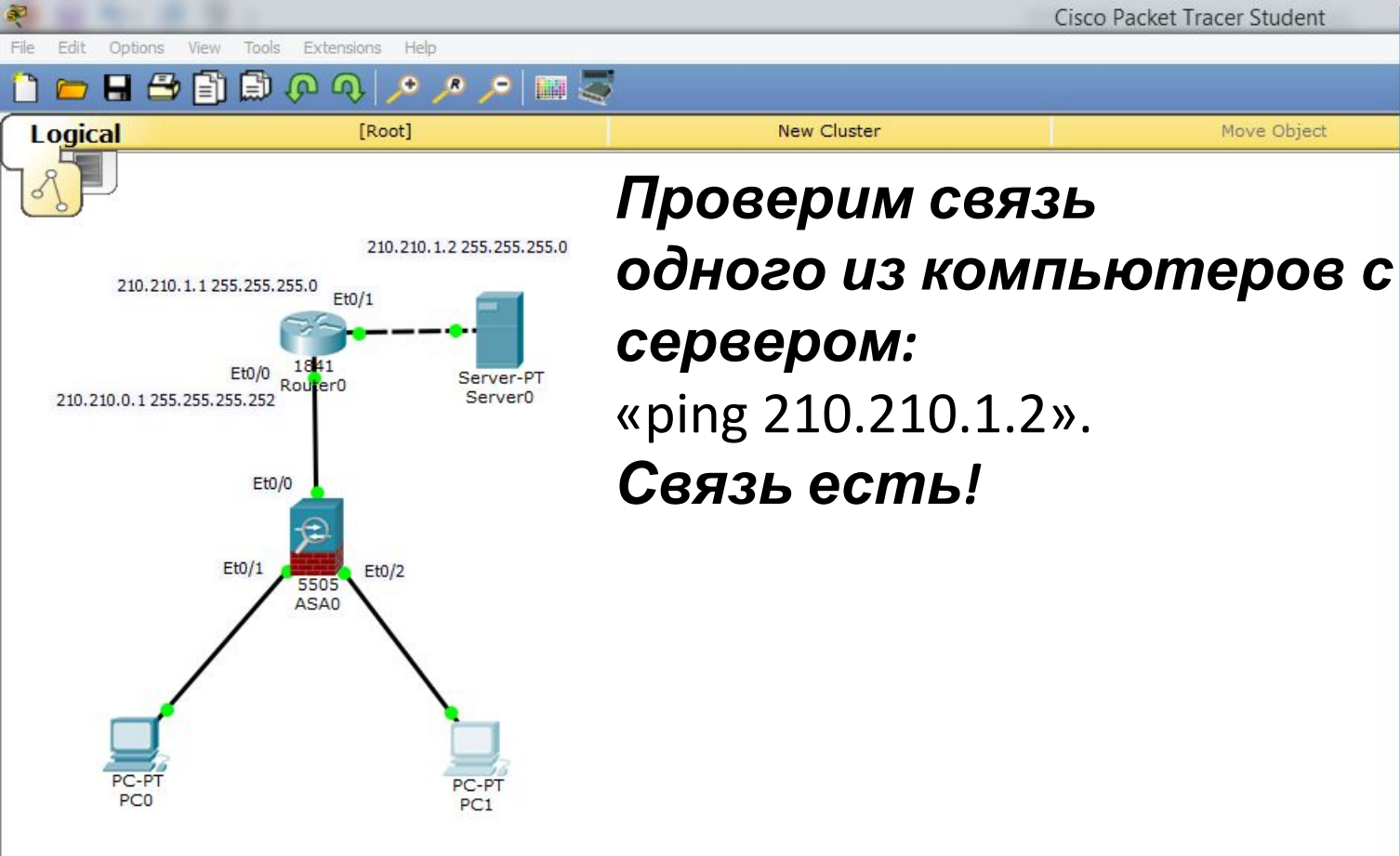
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------





**Ещё раз проверим связь
одного из компьютеров с
маршрутизатором
провайдера:
«ping 210.210.0.1».
Связь есть!**





PC1

Physical Config Desktop Custom Interface

Command Prompt

```
PC>ping 210.210.1.2

Pinging 210.210.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 210.210.1.2: bytes=32 time=0ms TTL=126
Reply from 210.210.1.2: bytes=32 time=0ms TTL=126

Ping statistics for 210.210.1.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 210.210.1.2

Pinging 210.210.1.2 with 32 bytes of data:

Reply from 210.210.1.2: bytes=32 time=2ms TTL=126
Reply from 210.210.1.2: bytes=32 time=4ms TTL=126
Reply from 210.210.1.2: bytes=32 time=1ms TTL=126
Reply from 210.210.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 210.210.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

PC>
```

Time: 31:38:37 Power Cycle Devices Fast Forward Time

Connections

Copper Cross-Over

Scenario 0

New Delete

Toggle PDU List Window

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

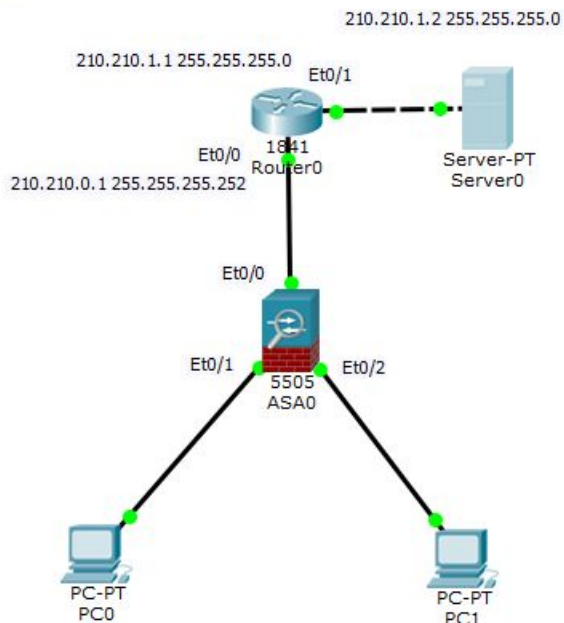
Realtime

0:15 12.01.2020



Logical [Root] New Cluster Move Object

**Проверим Web-сервер (HTTP).
Сервер включен.**



Server0

Physical Config Services Desktop Custom Interface

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP

HTTP

HTTP ☒ On ☐ Off

HTTPS ☒ On ☐ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x...		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

New File Import

Time: 31:40:53 Power Cycle Devices Fast Forward Time

Realtime



Copper Cross-Over

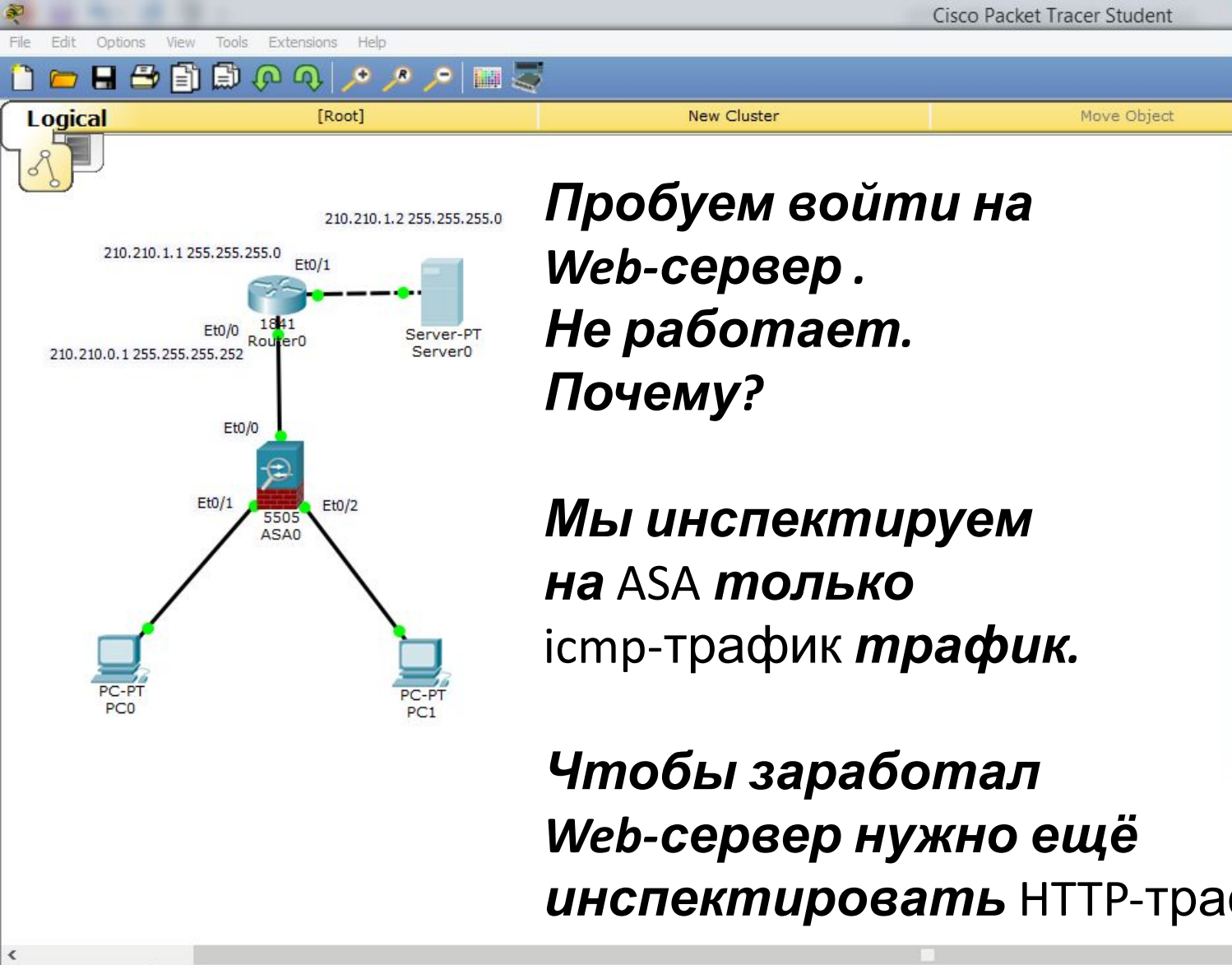
Scenario 0

New Delete

Toggle PDU List Window

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

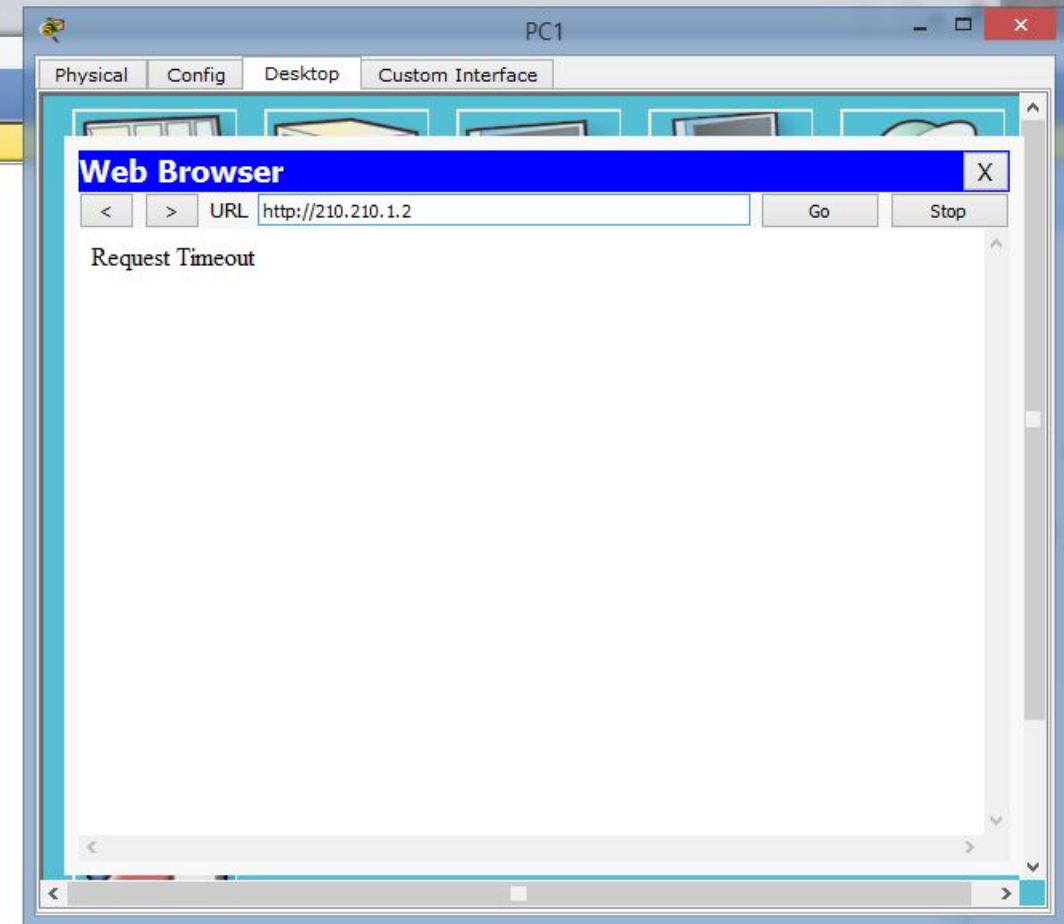




**Пробуем войти на Web-сервер.
Не работает.
Почему?**

**Мы инспектируем на ASA только
іstr-трафик *трафик*.**

**Чтобы заработал Web-сервер нужно ещё
инспектировать HTTP-трафик.**



Time: 31:46:19 Power Cycle Devices Fast Forward Time Realtime

Connections

Copper Cross-Over

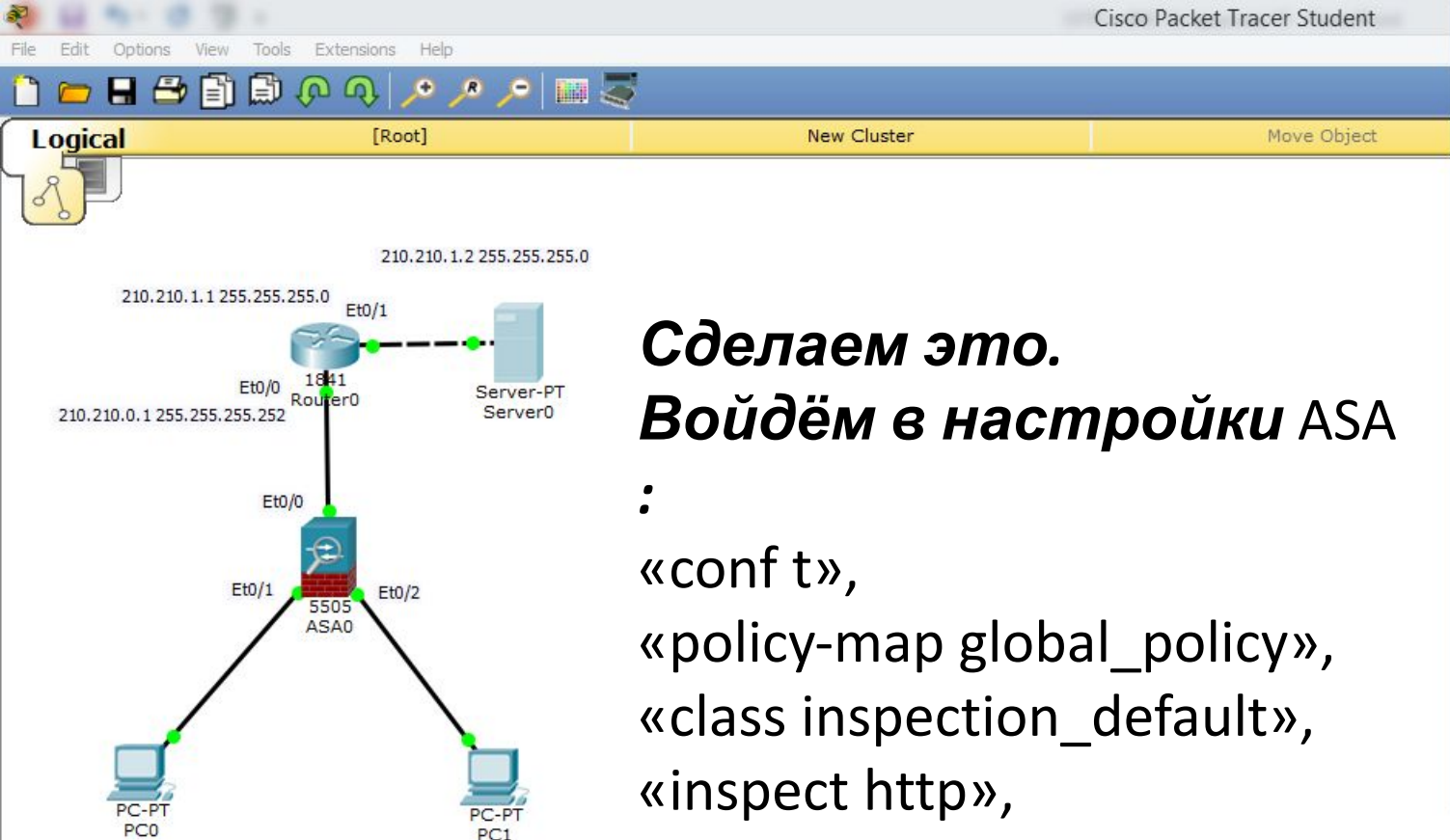
Scenario 0

New Delete

Toggle PDU List Window

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

Windows taskbar: 0:23 12.01.2020



Сделаем это.
Войдём в настройки ASA
:
«conf t»,
«policy-map global_policy»,
«class inspection_default»,
«inspect http»,
«end»,
«wr mem».

ASA0

Physical Config CLI

ASA Command Line Interface

```
ciscoasa(config)#
ciscoasa(config)#end
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 058c285f 55e0062d 00ad1335 5d2a0add

1101 bytes copied in 2.714 secs (405 bytes/sec)
[OK]
ciscoasa#
ciscoasa#conf t
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#
ciscoasa(config-pmap-c)#inspect http
ciscoasa(config-pmap-c)#
ciscoasa(config-pmap-c)#end
ciscoasa#
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 058c285f 55e0062d 00ad1335 5d2a0add

1116 bytes copied in 1.36 secs (820 bytes/sec)
[OK]
ciscoasa#
ciscoasa#
```

Copy Paste

Time: 31:55:48 Power Cycle Devices Fast Forward Time

Connections

Copper Cross-Over

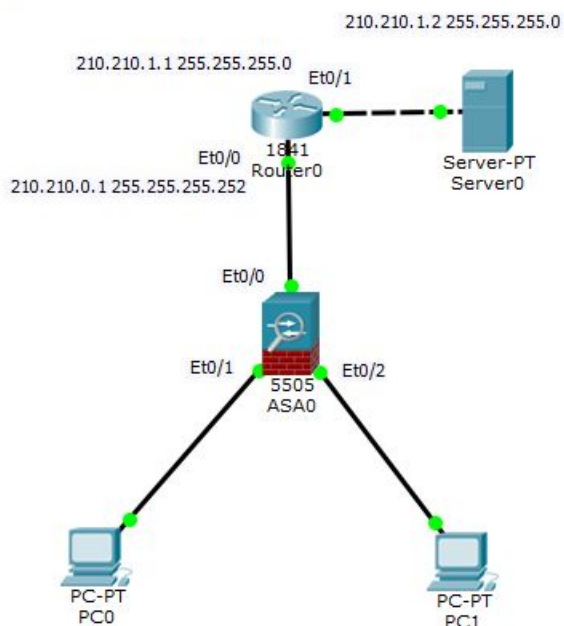
Scenario 0

New Delete

Toggle PDU List Window

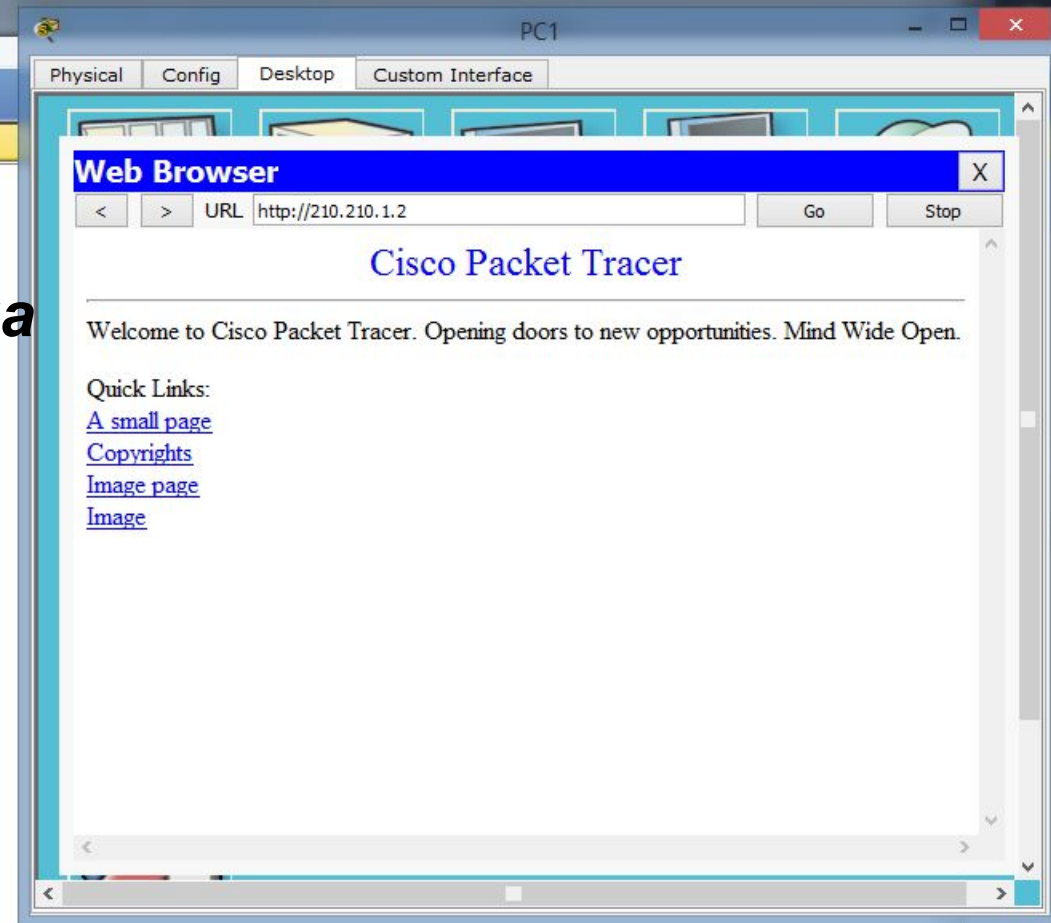
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

0:32 12.01.2020



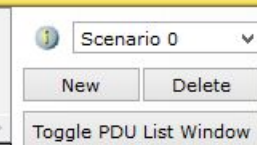
Ещё раз пробуем войти на Web-сервер.

Связь появилась!!!

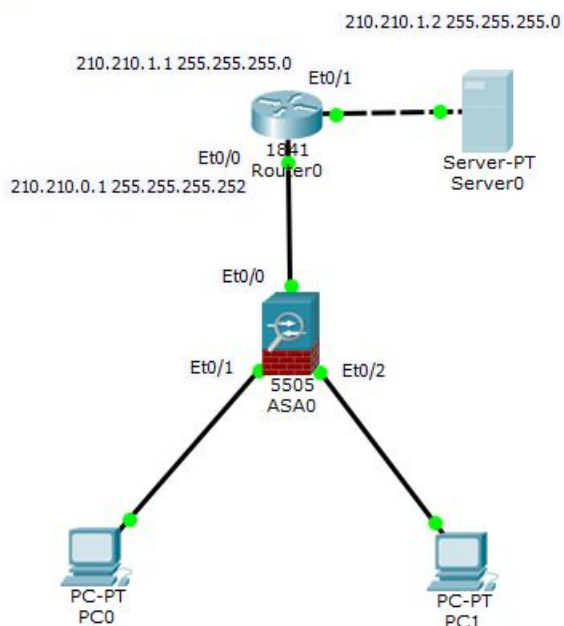


Time: 32:01:43 Power Cycle Devices Fast Forward Time

Realtime



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

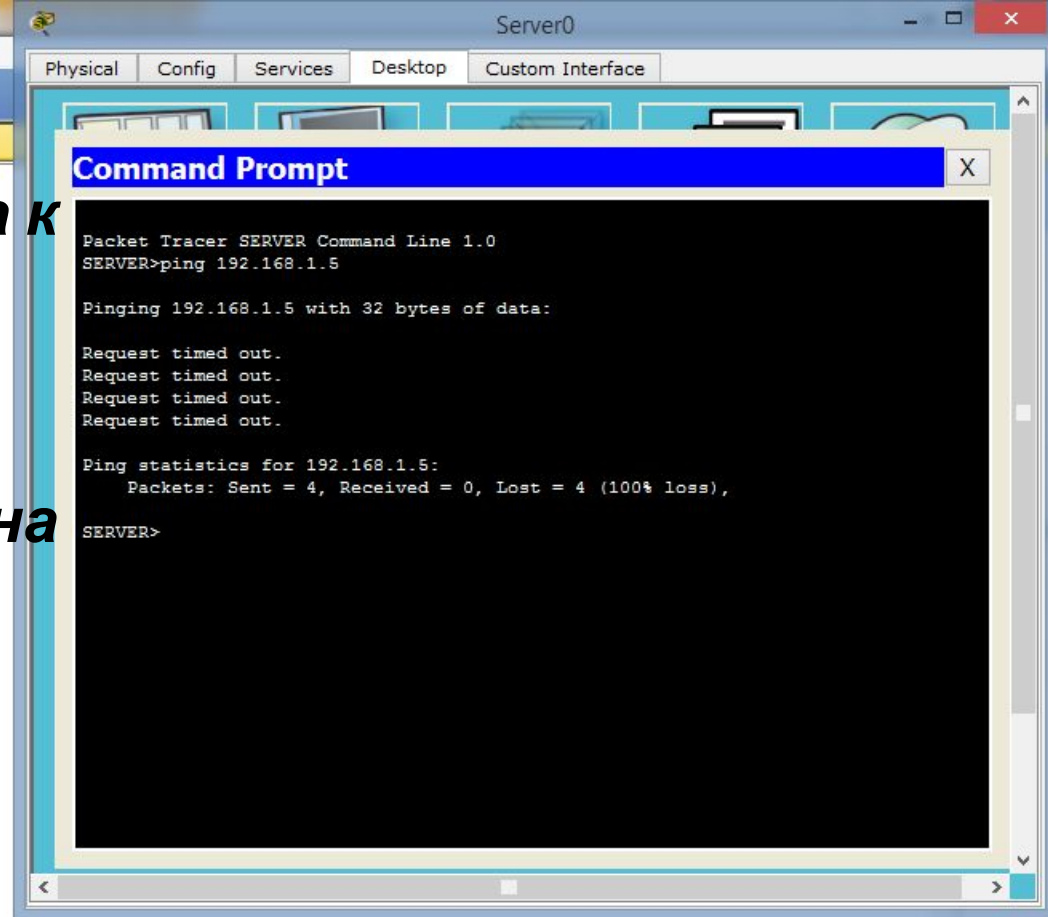


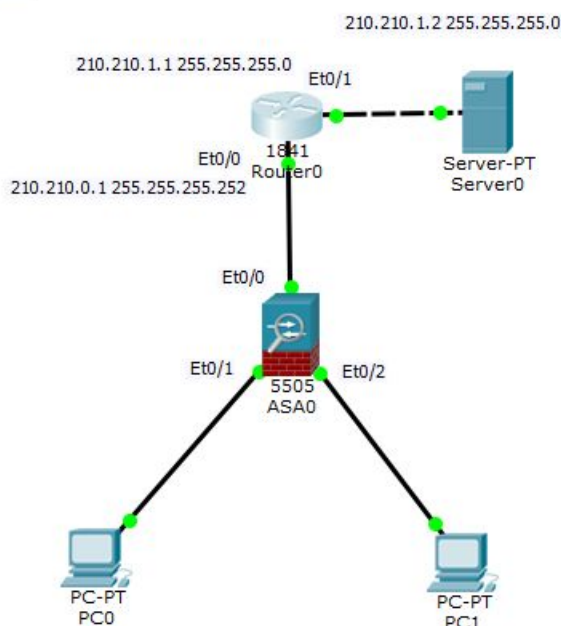
Проверим связь с сервера к одному из компьютеров:
«ping 192.168.1.5».

Связи нет и не будет, так как уровень доверия на вход извне в нашу сеть очень низкий.

ASA этот трафик не пропускает, если только мы не пропишем явный Access List.

Это одно из преимуществ сетевых экранов!!!





Рассмотрим настройку NAT на Cisco ASA. Она существенно отличается от настройки на маршрутизаторе. Для этого сначала мы удалим на маршрутизаторе провайдера, созданный ранее маршрут в нашу сеть:

«no ip route 192.168.1.0 255.255.255.0 210.210.0.2»,
«end»,
«wr mem».

Router0

Physical Config CLI

IOS Command Line Interface

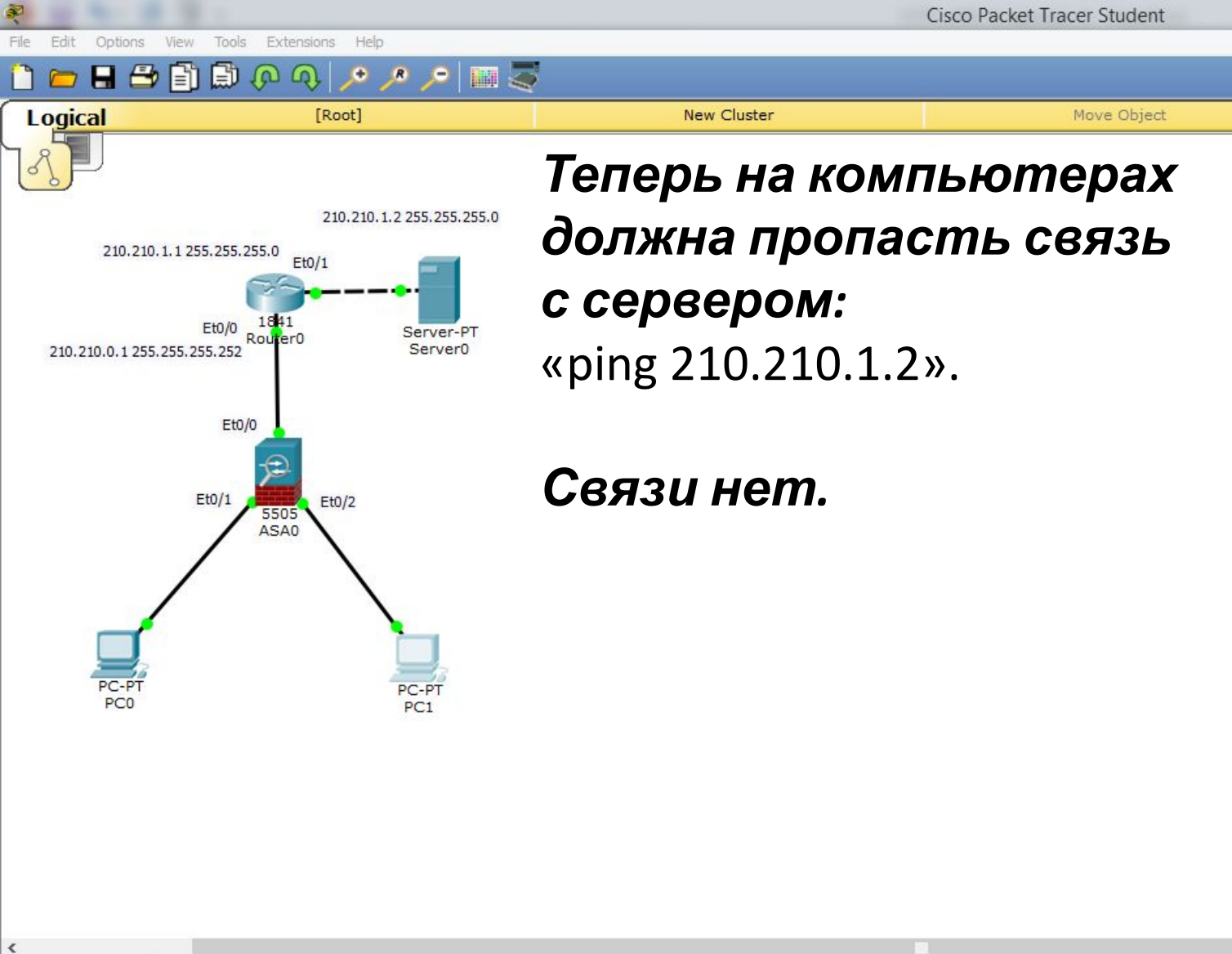
Press RETURN to get started.

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip route 192.168.1.0 255.255.255.0 210.210.0.2
Router(config)#
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

Copy Paste





**Теперь на компьютерах
должна пропасть связь
с сервером:
«ping 210.210.1.2».**

Связи нет.

PC1

Physical Config Desktop Custom Interface

Command Prompt

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 210.210.1.2

Pinging 210.210.1.2 with 32 bytes of data:

Reply from 210.210.1.2: bytes=32 time=2ms TTL=126
Reply from 210.210.1.2: bytes=32 time=4ms TTL=126
Reply from 210.210.1.2: bytes=32 time=1ms TTL=126
Reply from 210.210.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 210.210.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

PC>ping 210.210.1.2

Pinging 210.210.1.2 with 32 bytes of data:

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

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

PC>
```

Time: 32:22:40 Power Cycle Devices Fast Forward Time

Connections

Copper Cross-Over

Scenario 0

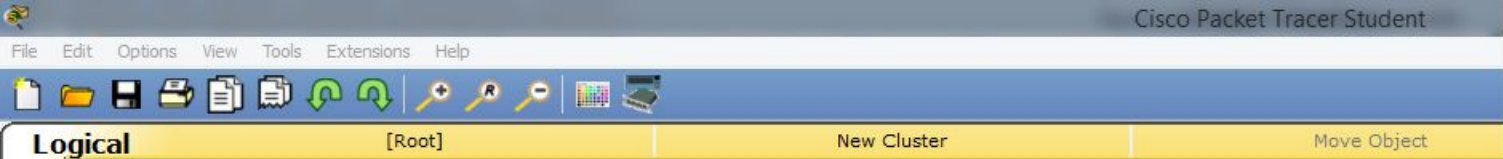
New Delete

Toggle PDU List Window

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

Realtime

0:59 12.01.2020



Настроим NAT на Cisco ASA.

Это делается с помощью создания объектов.

Создадим object network и дадим ему имя FOR-NAT:

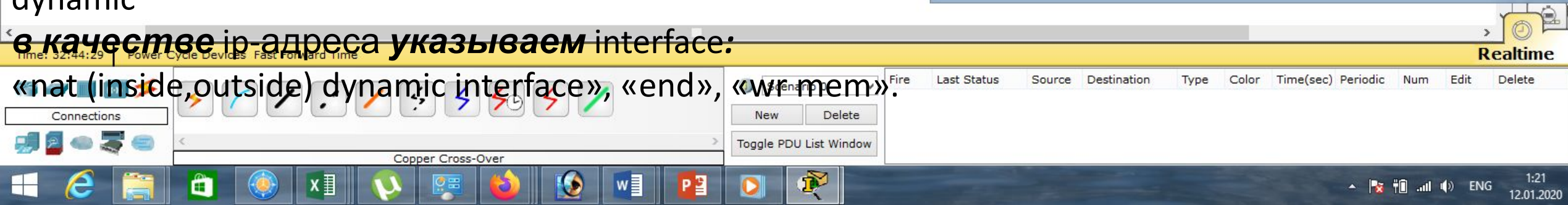
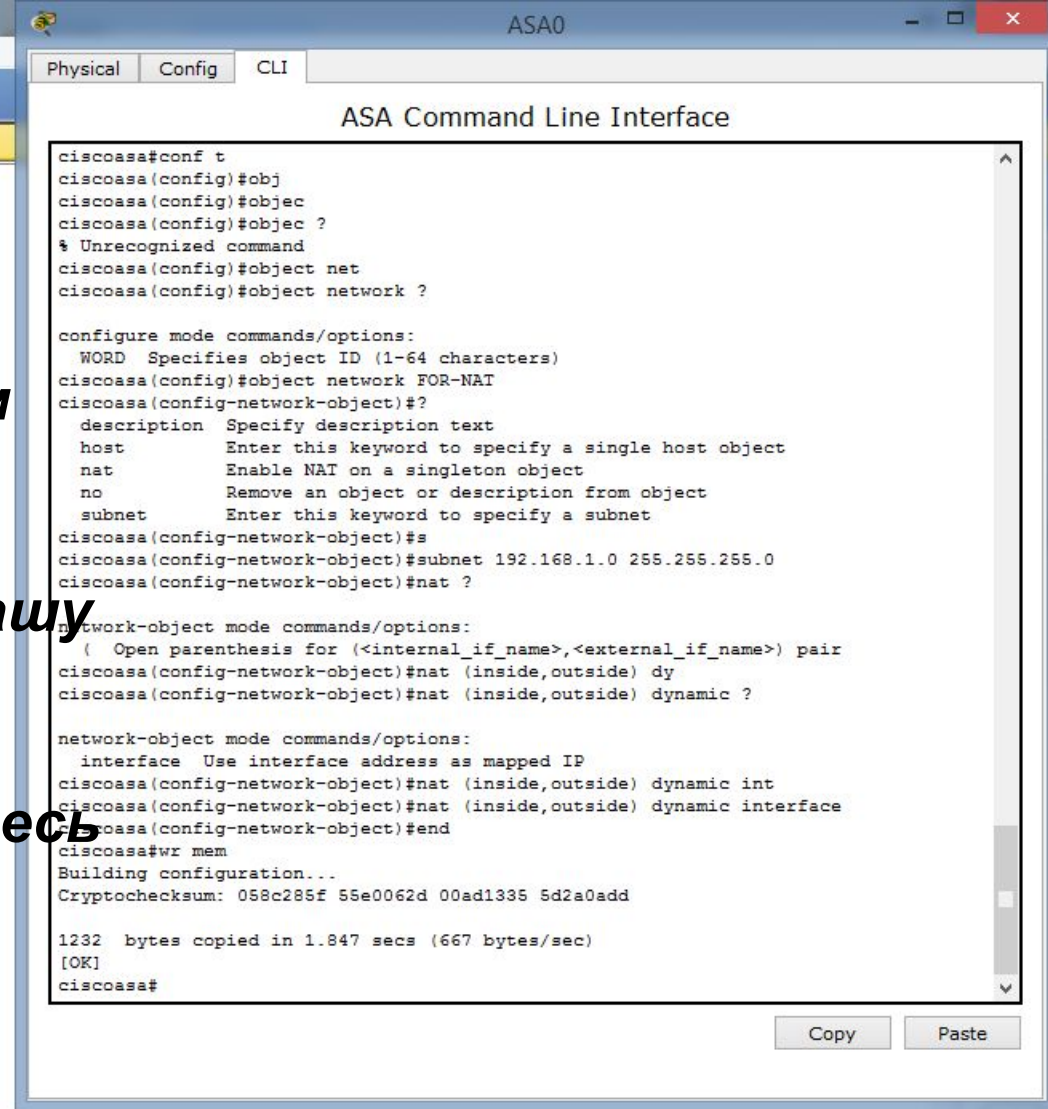
«object network FOR-NAT».

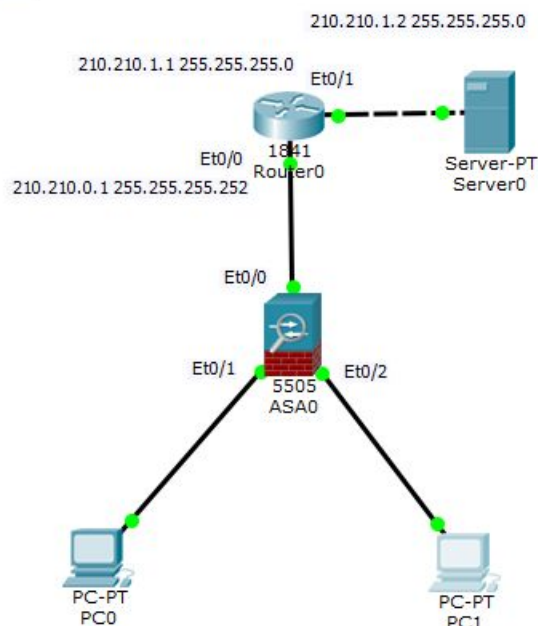
В этом объекте определим нашу сеть (пользуемся знаком «?»): «subnet 192.168.1.0 255.255.255.0», переходим к настройке NAT. Здесь

надо указать в скобках сначала внутренний интерфейс, а затем – внешний интерфейс, далее выбираем dynamic

в качестве ip-адреса указываем interface:

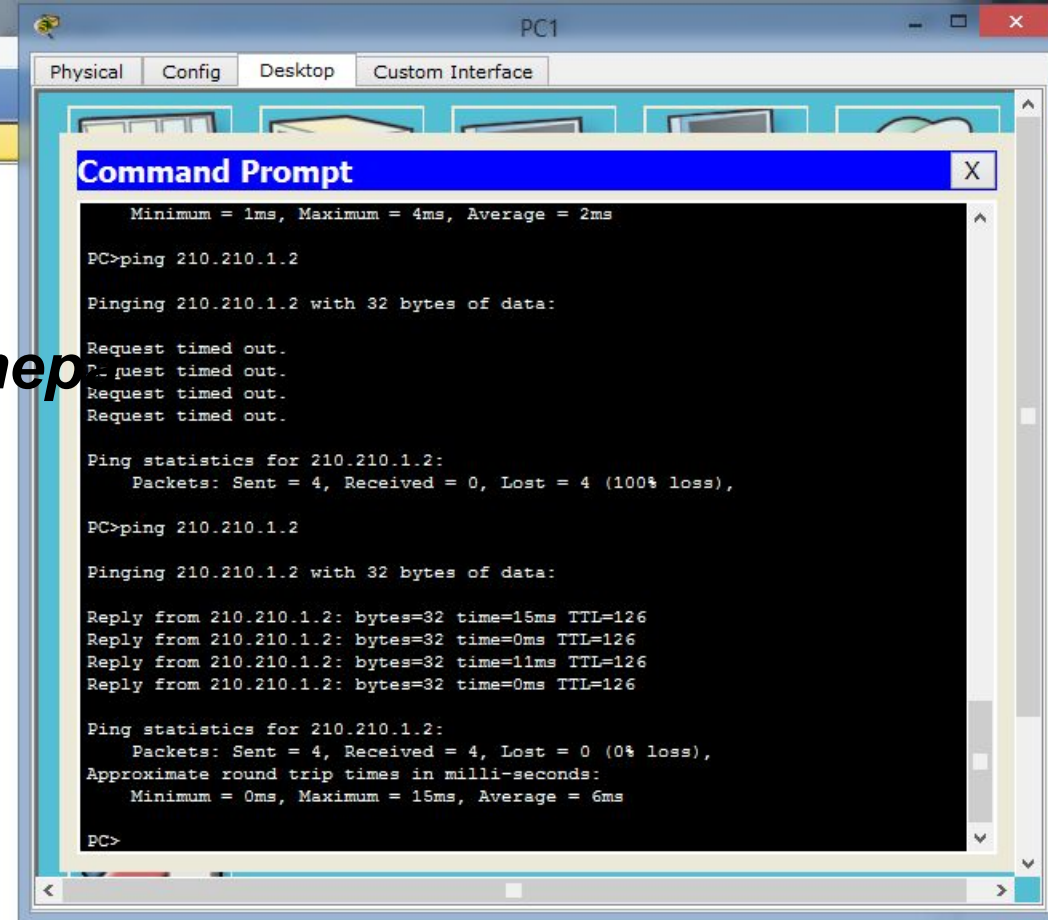
«nat (inside,outside) dynamic interface», «end», «wr mem».

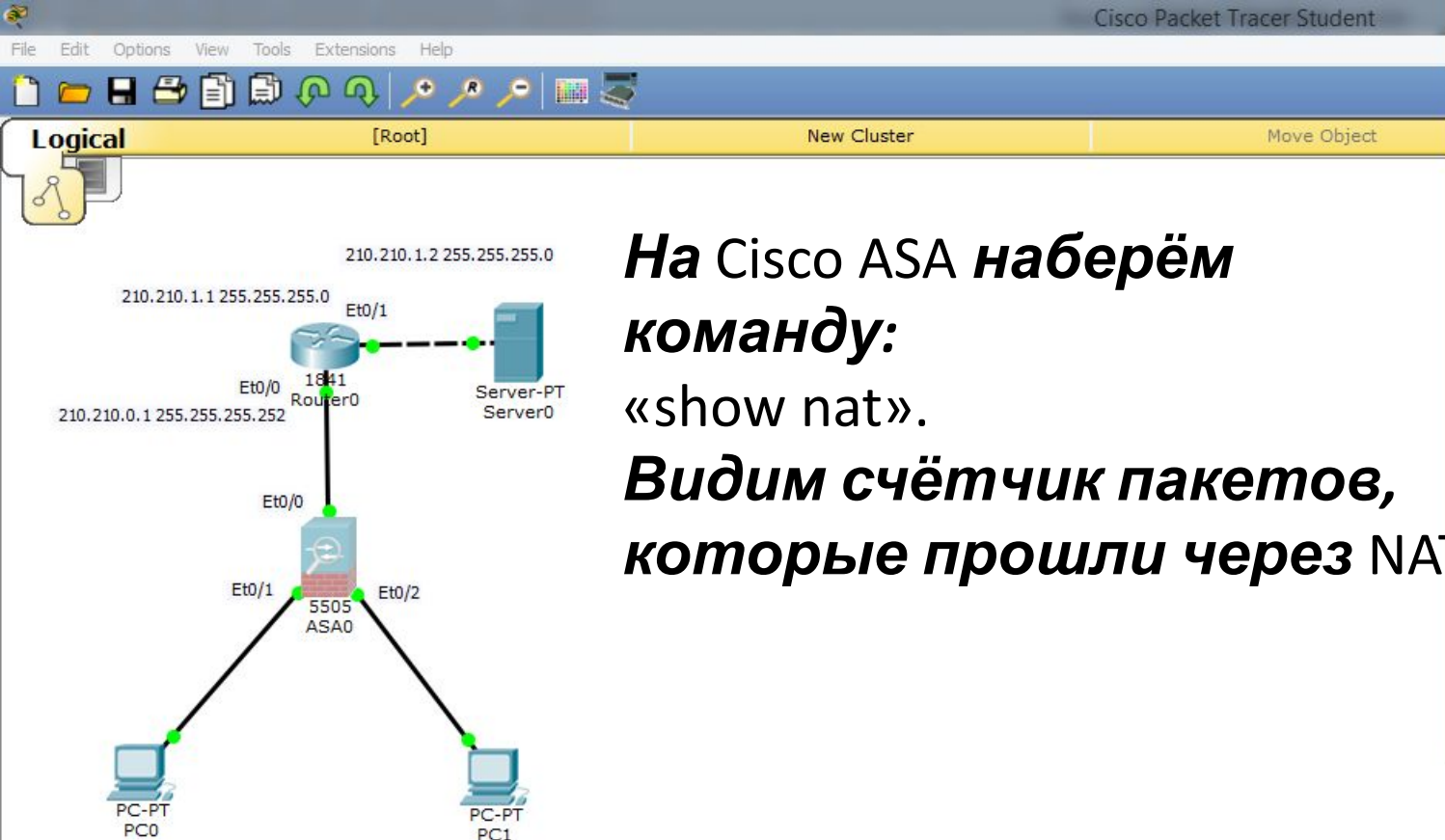




**На этом настройка NAT
Завершилась.
Проверим связь компьютер
с сервером:
«ping 210.210.1.2».**

Связь появилась!!!





На Cisco ASA наберём команду:
«show nat».
Видим счётчик пакетов, которые прошли через NAT.

ASA0

Physical Config CLI

ASA Command Line Interface

```
ciscoasa(config-network-object)#nat ?  
  
network-object mode commands/options:  
  ( Open parenthesis for (<internal_if_name>,<external_if_name>) pair  
ciscoasa(config-network-object)#nat (inside,outside) dy  
ciscoasa(config-network-object)#nat (inside,outside) dynamic ?  
  
network-object mode commands/options:  
  interface Use interface address as mapped IP  
ciscoasa(config-network-object)#nat (inside,outside) dynamic int  
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface  
ciscoasa(config-network-object)#end  
ciscoasa#wr mem  
Building configuration...  
Cryptochecksum: 058c285f 55e0062d 00ad1335 5d2a0add  
  
1232 bytes copied in 1.847 secs (667 bytes/sec)  
[OK]  
ciscoasa#show nat  
Auto NAT Policies (Section 2)  
1 (inside) to (outside) source dynamic FOR-NAT interface  
  translate_hits = 12, untranslate_hits = 12  
  
ciscoasa#
```

Copy Paste

На этом краткое знакомство с межсетевым экраном Cisco ASA закончено!

Time: 33:01:32 Power Cycle Devices Fast Forward Time

Connections

Copper Cross-Over

Scenario 0

New Delete

Toggle PDU List Window

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

Realtime

1:39 12.01.2020

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, 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