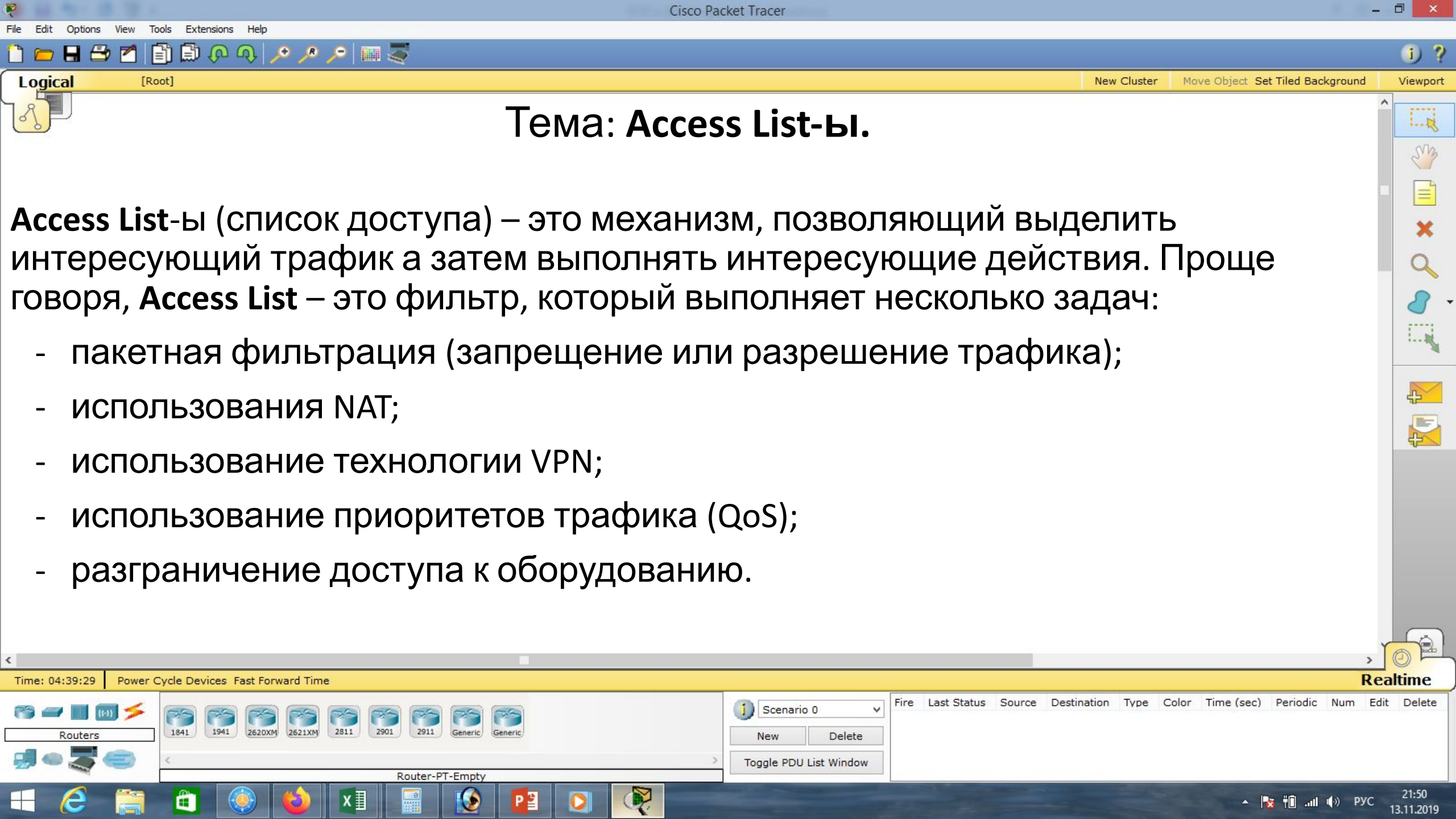
МДК.01.01

Организация, принципы построения и функционирования компьютерных сетей

3-курс

Практические занятия

Занятие 13


Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical [Root]
New Cluster Move Object Set Tiled Background Viewport
Тема: Access List-ы.
Access List-ы (список доступа) – это механизм, позволяющий выделить интересующий трафик а затем выполнять интересующие действия. Проще говоря, Access List – это фильтр, который выполняет несколько задач:
- пакетная фильтрация (запрещение или разрешение трафика);
- использования NAT;
- использование технологии VPN;
- использование приоритетов трафика (QoS);
- разграничение доступа к оборудованию.
Time: 04:39:29 Power Cycle Devices Fast Forward Time
Realtime
Routers
1841 1941 2620XM 2621XM 2811 2901 2911 Generic Generic
Router-PT-Empty
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time (sec) Periodic Num Edit Delete
РУС 21:50 13.11.2019

Cisco Packet Tracer

File Edit Options View Tools Extensions Help

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

Подробно рассмотрим пакетную фильтрацию, то есть задачу с запрещением или разрешением трафика.

Access List-ы бывают следующих видов:

- стандартные;
- расширенные;
- динамические;
- рефлексивные;
- временные.

Подробно рассмотрим стандартные и расширенные Access List-ы.

Time: 04:39:29 Power Cycle Devices Fast Forward Time Realtime

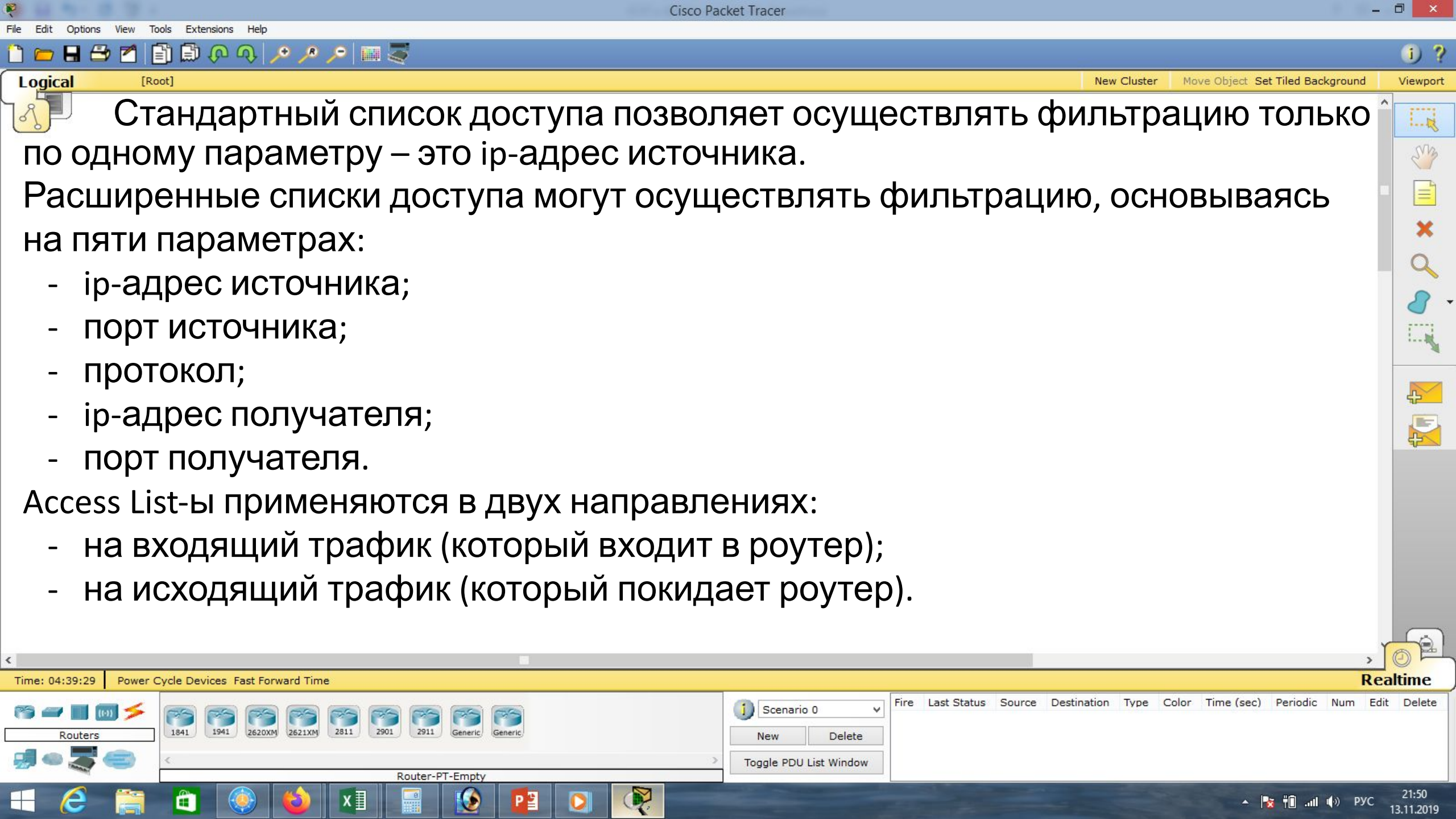
Routers 1841 1941 2620XM 2621XM 2811 2901 2911 Generic Generic

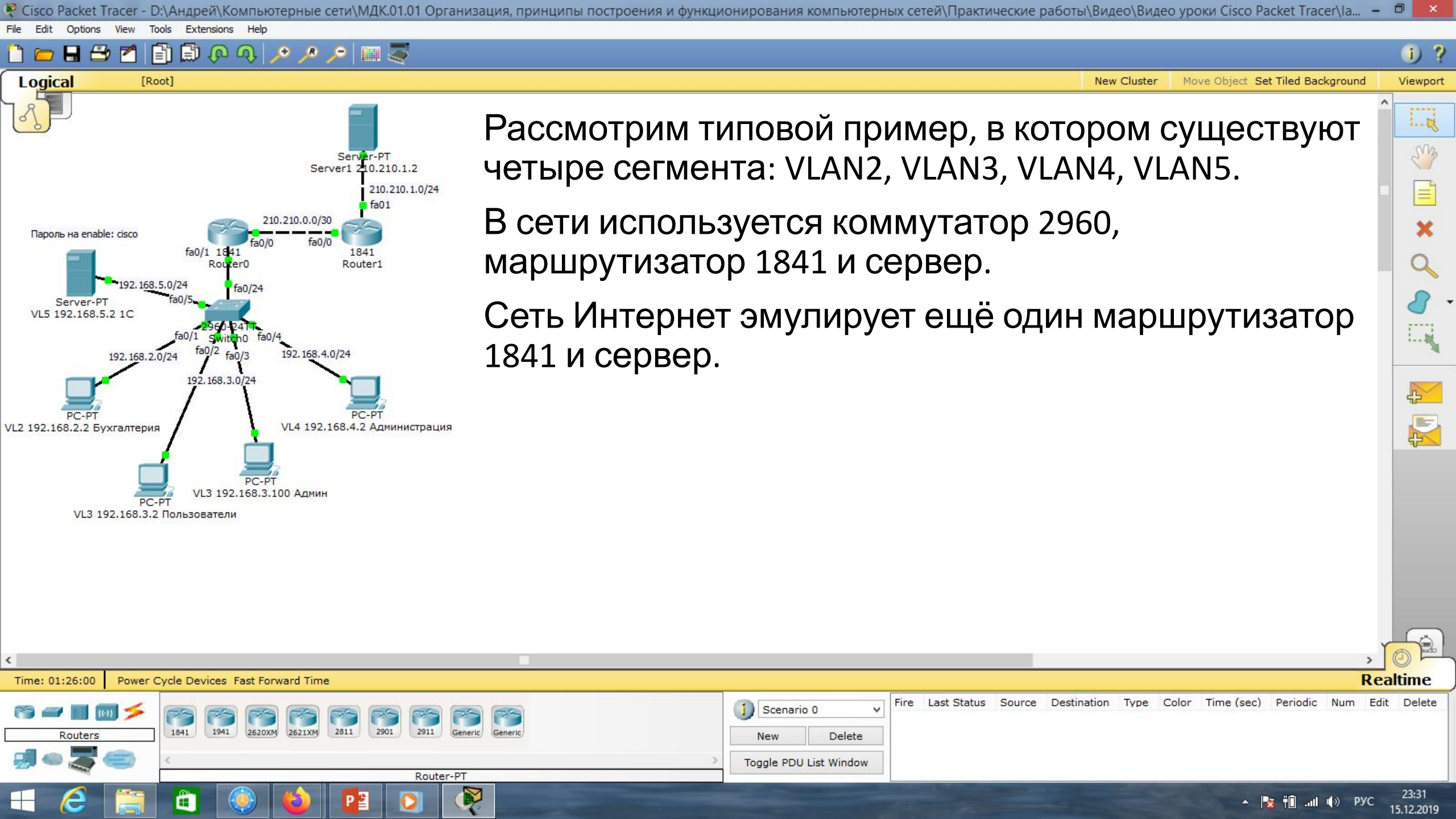
Router-PT-Empty

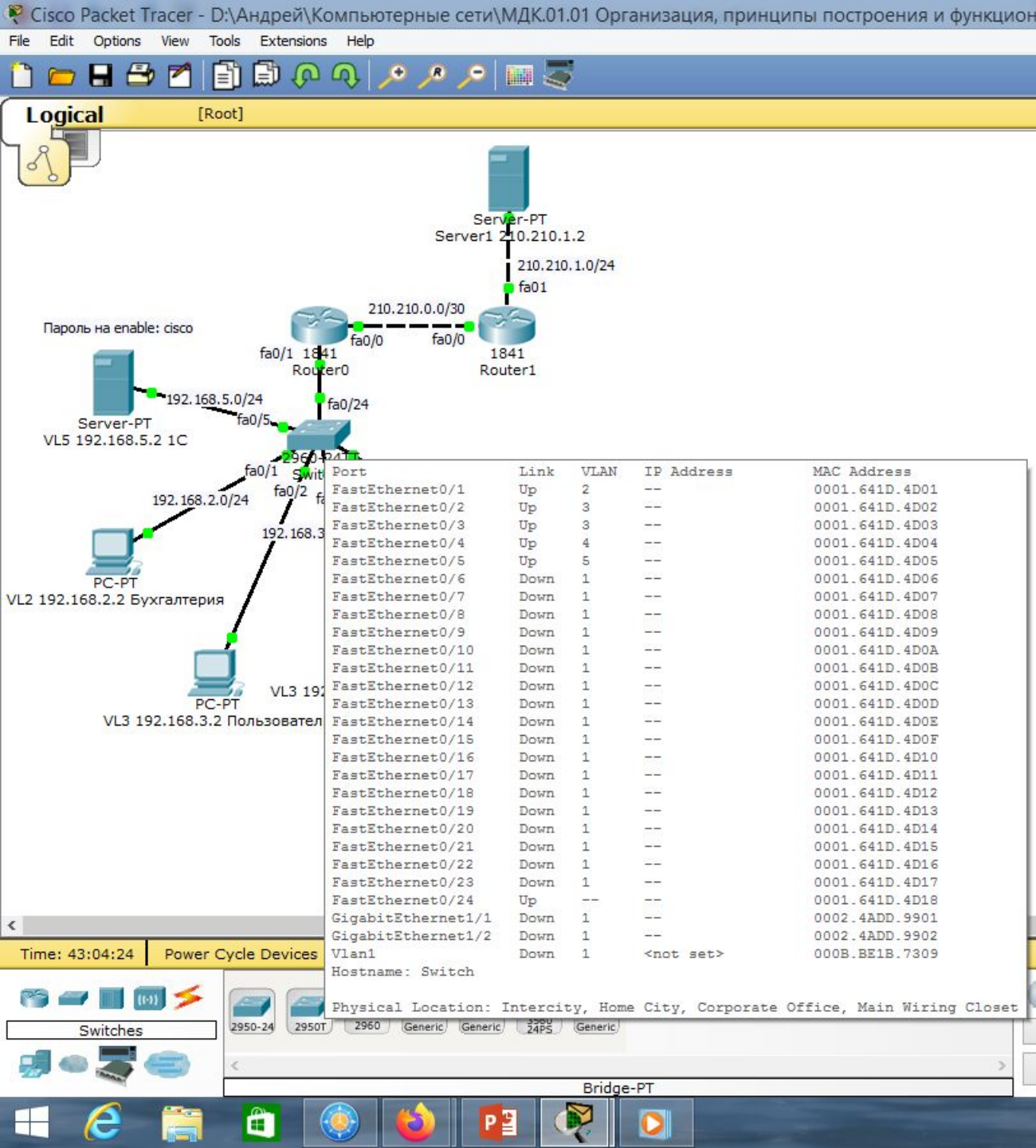
Scenario 0 New Delete Toggle PDU List Window

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

РУС 21:50 13.11.2019


Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical [Root]
New Cluster Move Object Set Tiled Background Viewport
Стандартный список доступа позволяет осуществлять фильтрацию только по одному параметру – это ip-адрес источника.
Расширенные списки доступа могут осуществлять фильтрацию, основываясь на пяти параметрах:
- ip-адрес источника;
- порт источника;
- протокол;
- ip-адрес получателя;
- порт получателя.
Access List-ы применяются в двух направлениях:
- на входящий трафик (который входит в роутер);
- на исходящий трафик (который покидает роутер).
Time: 04:39:29 Power Cycle Devices Fast Forward Time
Realtime
Routers
1841 1941 2620XM 2621XM 2811 2901 2911 Generic Generic
Router-PT-Empty
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time (sec) Periodic Num Edit Delete
РУС 21:50 13.11.2019


Cisco Packet Tracer - D:\Андрей\Компьютерные сети\МДК.01.01 Организация, принципы построения и функционирования компьютерных сетей\Практические работы\Видео\Видео уроки Cisco Packet Tracer\Ia...
File Edit Options View Tools Extensions Help
Logical [Root]
New Cluster Move Object Set Tiled Background Viewport
Server-PT
Server1 210.210.1.2
210.210.1.0/24
fa01
210.210.0.0/30
Пароль на enable: cisco
fa0/1 1841
Router0
fa0/0
fa0/0
1841
Router1
192.168.5.0/24
fa0/24
Server-PT
VL5 192.168.5.2 1C
fa0/5
2960-24TT
Switch0
fa0/1
fa0/2
fa0/3
fa0/4
192.168.2.0/24
192.168.3.0/24
192.168.4.0/24
PC-PT
VL2 192.168.2.2 Бухгалтерия
PC-PT
VL4 192.168.4.2 Администрация
PC-PT
VL3 192.168.3.100 Админ
PC-PT
VL3 192.168.3.2 Пользователи
Рассмотрим типовой пример, в котором существуют четыре сегмента: VLAN2, VLAN3, VLAN4, VLAN5.
В сети используется коммутатор 2960, маршрутизатор 1841 и сервер.
Сеть Интернет эмулирует ещё один маршрутизатор 1841 и сервер.
Time: 01:26:00 Power Cycle Devices Fast Forward Time
Realtime
Routers
1841 1941 2620XM 2621XM 2811 2901 2911 Generic Generic
Router-PT
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time (sec) Periodic Num Edit Delete
РУС
23:31
15.12.2019



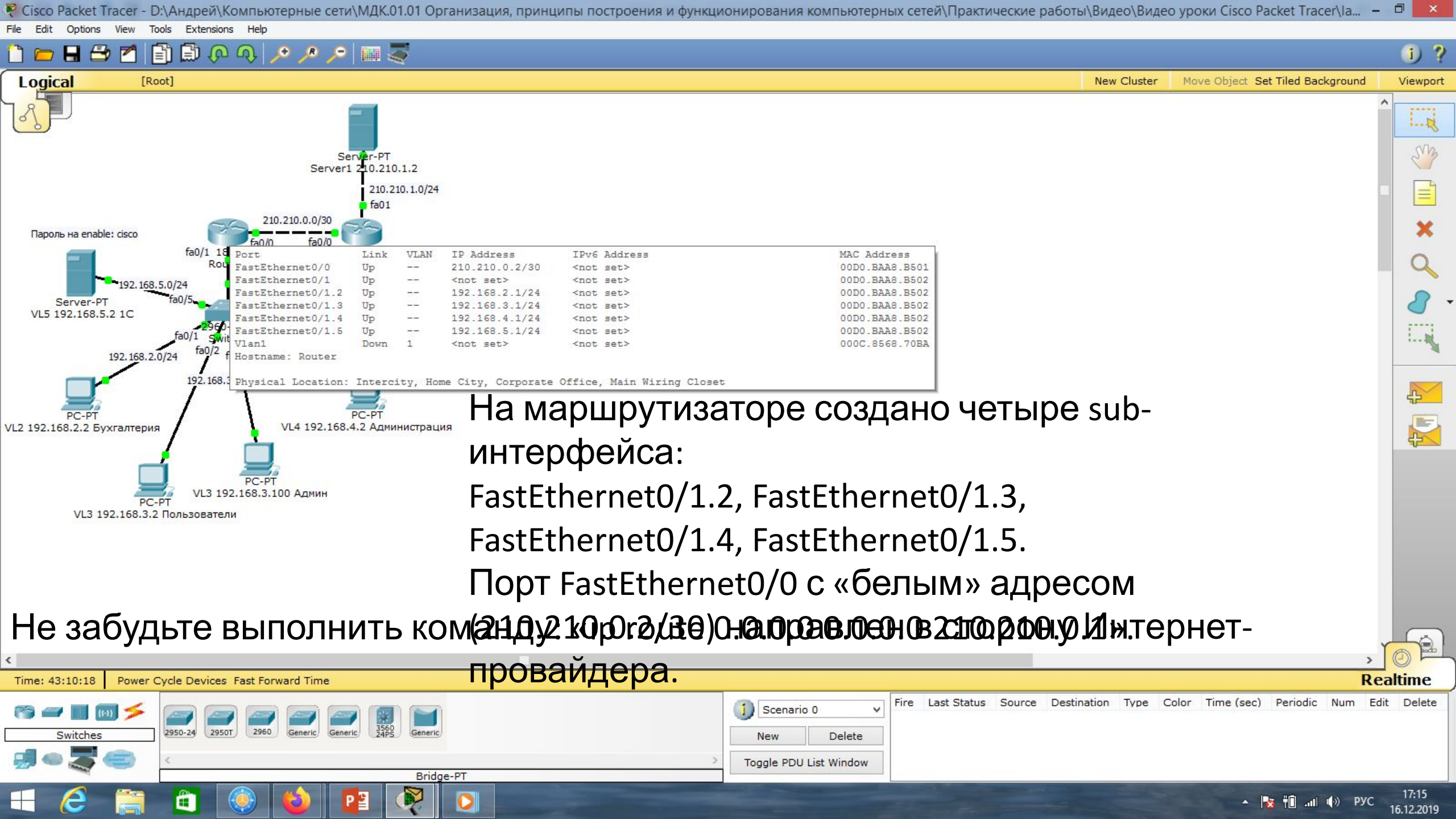
На коммутаторе используются порты:

FastEthernet0/1, FastEthernet0/2,

FastEthernet0/3, FastEthernet0/4,

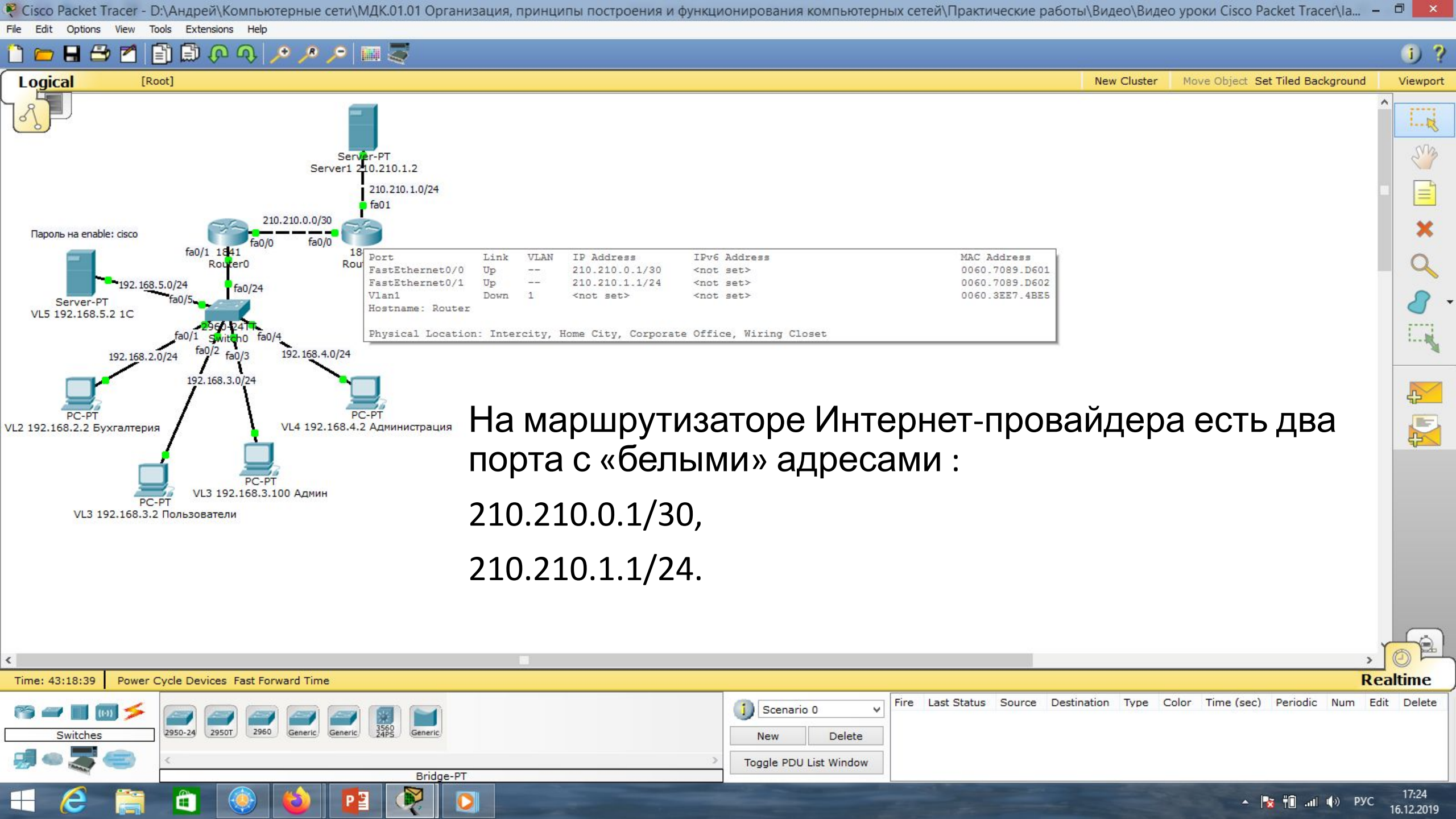
FastEthernet0/5, FastEthernet0/24.

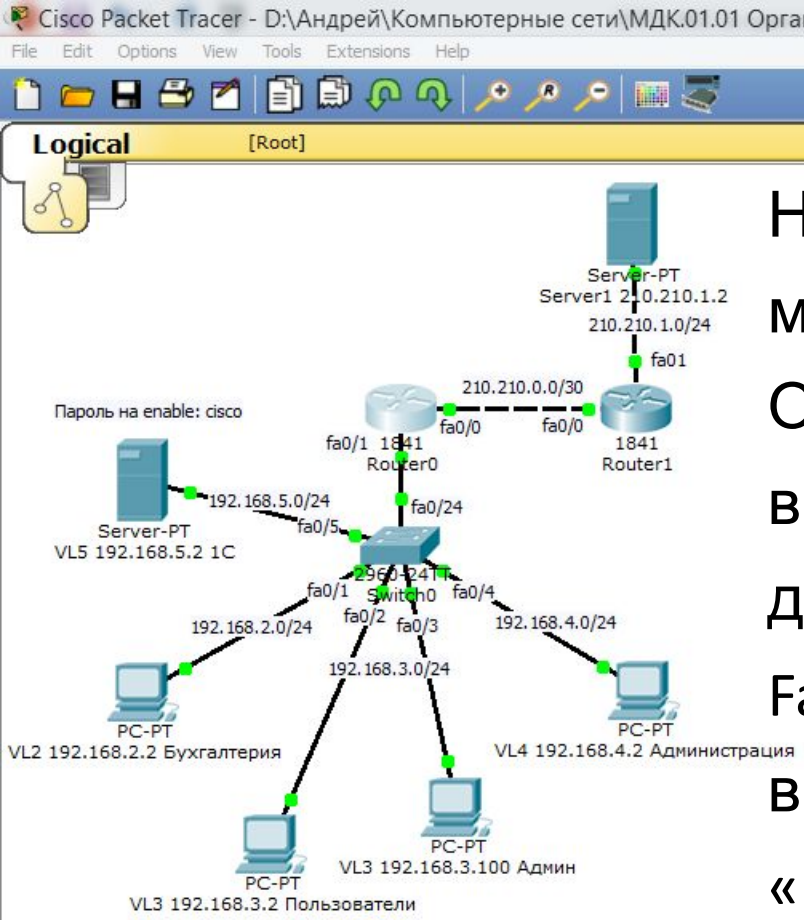
Порт FastEthernet0/24 используется как транк-порт, прокинутый до маршрутизатора.



На маршрутизаторе создано четыре sub-интерфейса:
FastEthernet0/1.2, FastEthernet0/1.3,
FastEthernet0/1.4, FastEthernet0/1.5.
Порт FastEthernet0/0 с «белым» адресом (210.210.0.2/30) направлен в сторону Интернет-провайдера.

Не забудьте выполнить команду ip nat inside source list 1 interface fa0/0 overload.

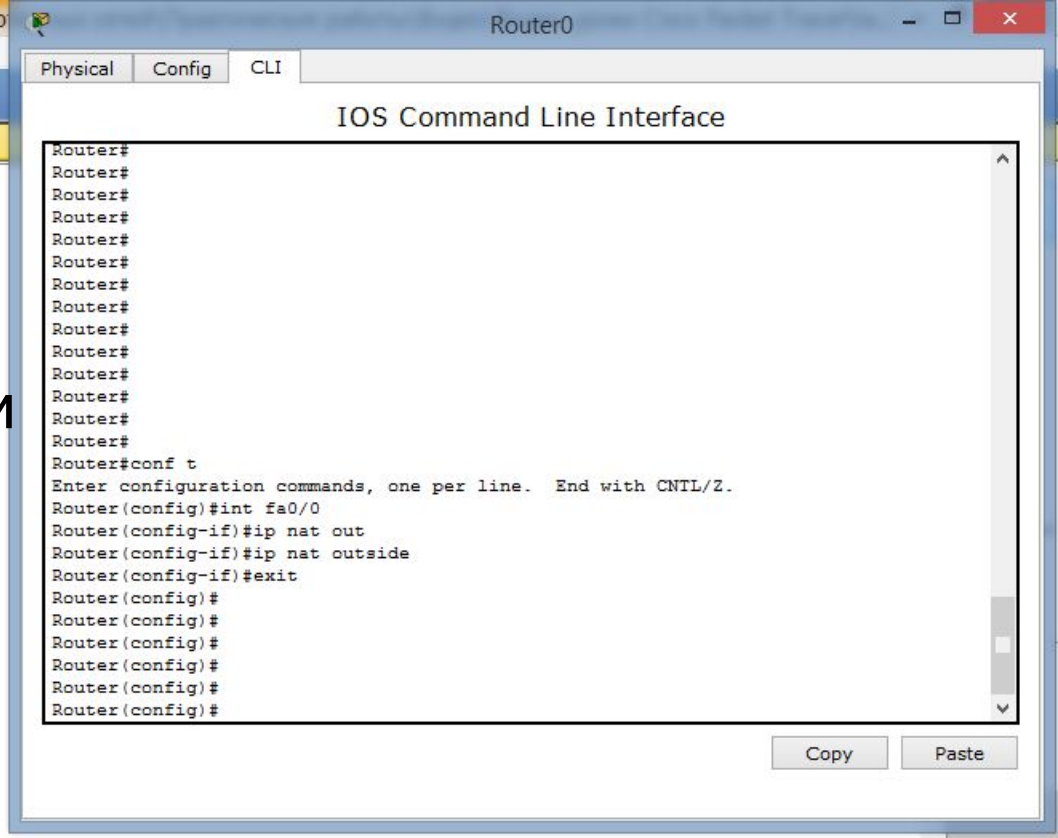

Cisco Packet Tracer - D:\Андрей\Компьютерные сети\МДК.01.01 Организация, принципы построения и функционирования компьютерных сетей\Практические работы\Видео\Видео уроки Cisco Packet Tracer\Ia...
File Edit Options View Tools Extensions Help
Logical [Root]
New Cluster Move Object Set Tiled Background Viewport
Server-PT
Server1 210.210.1.2
210.210.1.0/24
fa01
210.210.0.0/30
Пароль на enable: cisco
fa0/1 1841
Router0
fa0/0
fa0/0
Port Link VLAN IP Address IPv6 Address MAC Address
FastEthernet0/0 Up -- 210.210.0.1/30 <not set> 0060.7089.D601
FastEthernet0/1 Up -- 210.210.1.1/24 <not set> 0060.7089.D602
Vlan1 Down 1 <not set> <not set> 0060.3EE7.4BE5
Hostname: Router
Physical Location: Intercity, Home City, Corporate Office, Wiring Closet
192.168.5.0/24
fa0/5
fa0/24
Server-PT
VL5 192.168.5.2 1C
2960-24TT
Switch0
fa0/1
fa0/2
fa0/3
fa0/4
192.168.2.0/24
192.168.3.0/24
192.168.4.0/24
PC-PT
VL2 192.168.2.2 Бухгалтерия
PC-PT
VL4 192.168.4.2 Администрация
PC-PT
VL3 192.168.3.100 Админ
PC-PT
VL3 192.168.3.2 Пользователи
На маршрутизаторе Интернет-провайдера есть два порта с «белыми» адресами :
210.210.0.1/30,
210.210.1.1/24.
Time: 43:18:39 Power Cycle Devices Fast Forward Time
Realtime
Switches
2950-24 2950T 2960 Generic Generic 3560 24PS Generic
Bridge-PT
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time (sec) Periodic Num Edit Delete
РУС 17:24 16.12.2019

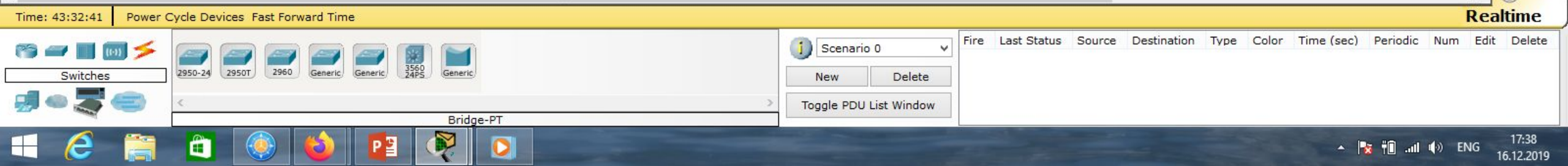


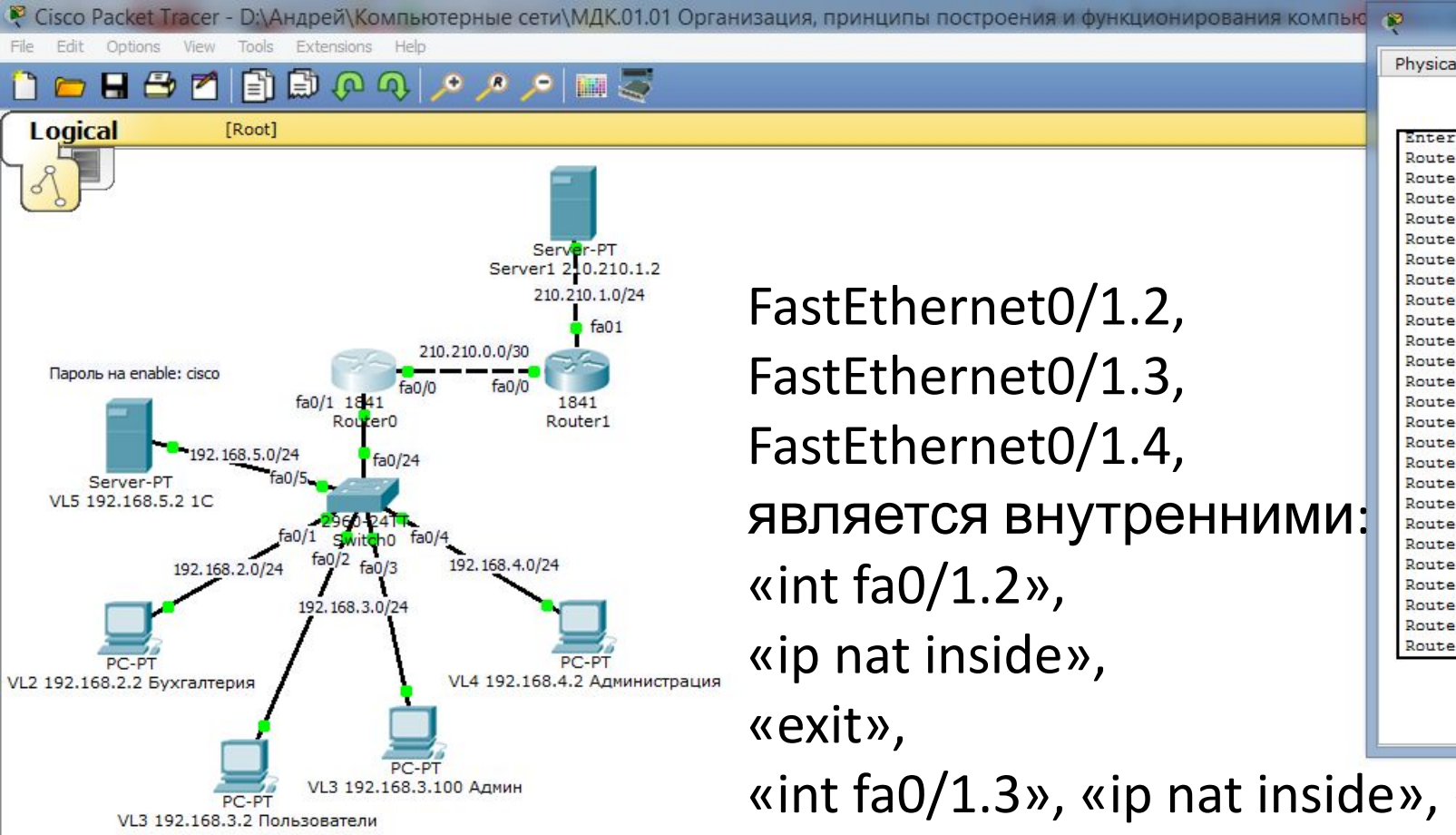
Настроим NAT на маршрутизаторе.

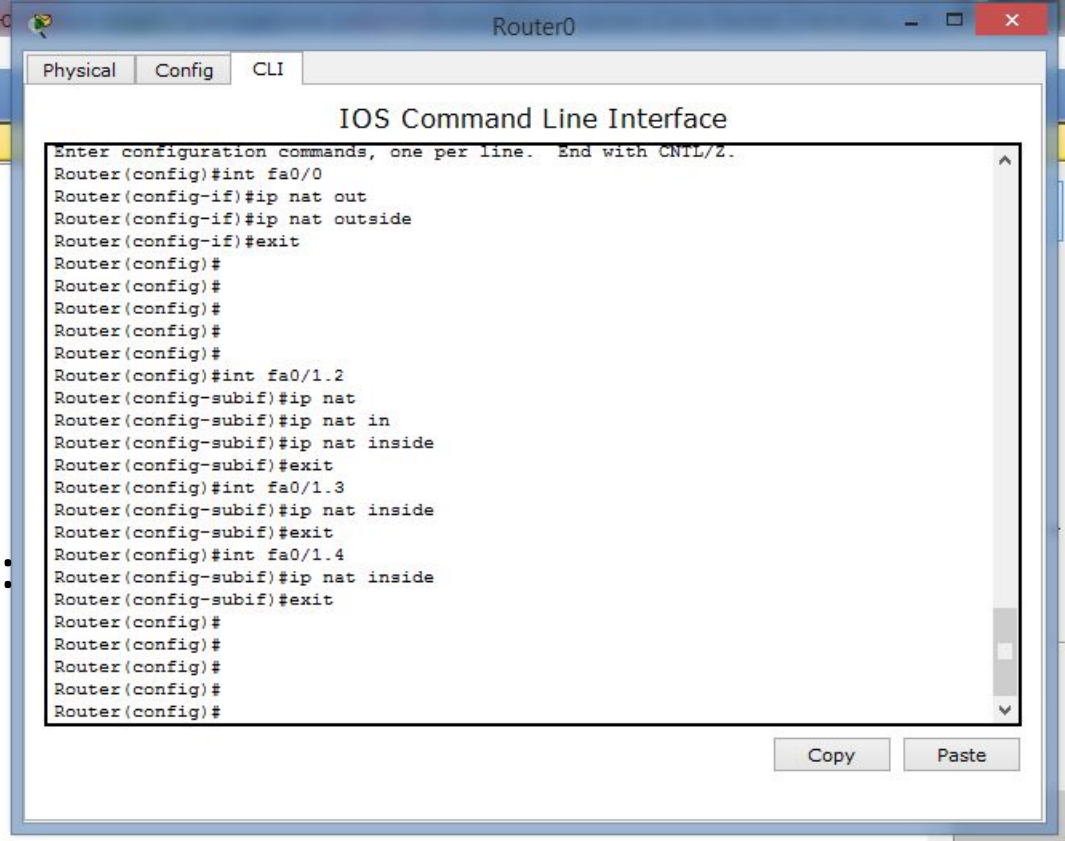
Определим внутренние и внешние интерфейсы для NAT.

FastEthernet0/0 является внешним: «en», «conf t», «int fa0/0», «ip nat outside», «exit».

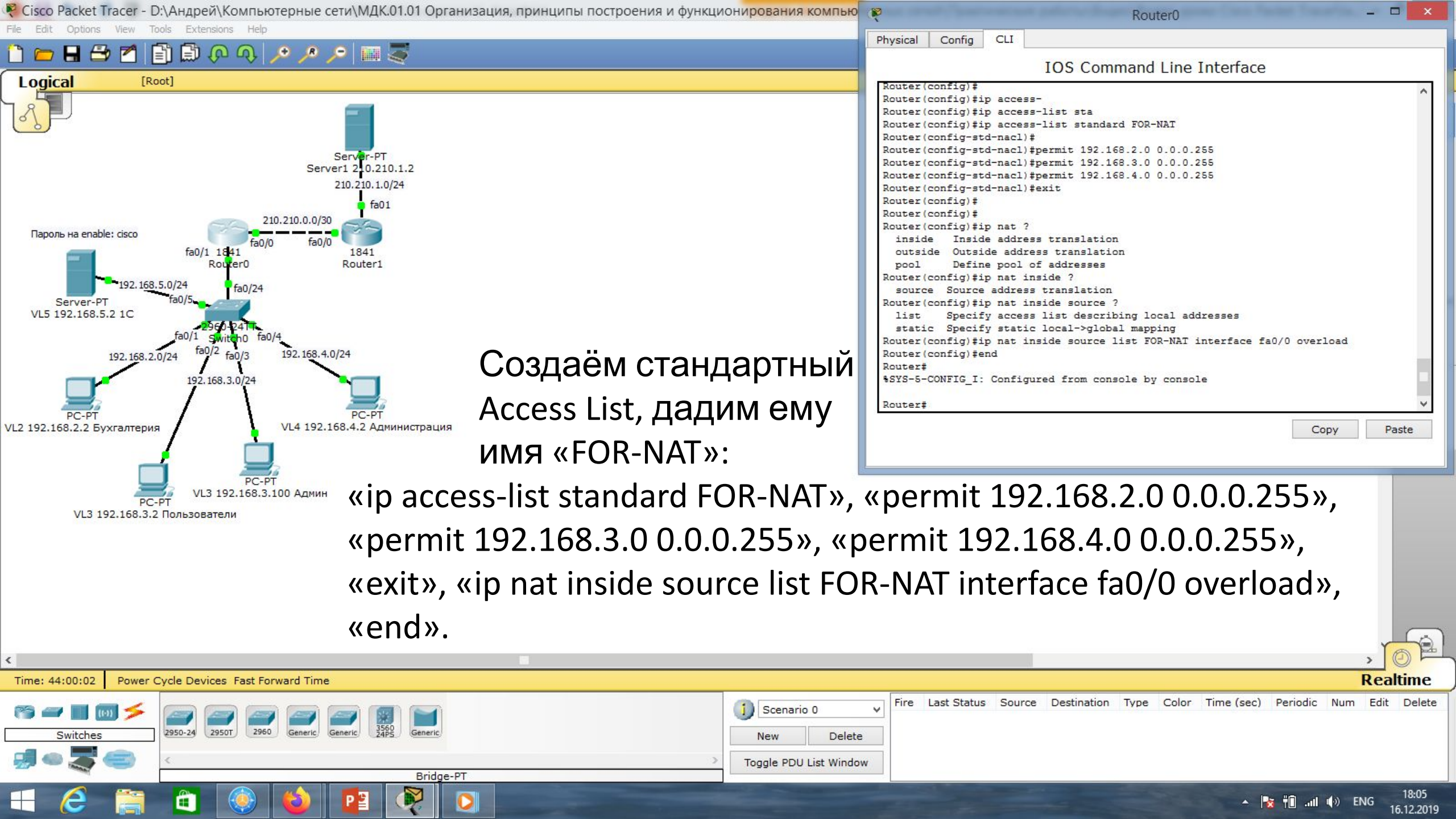






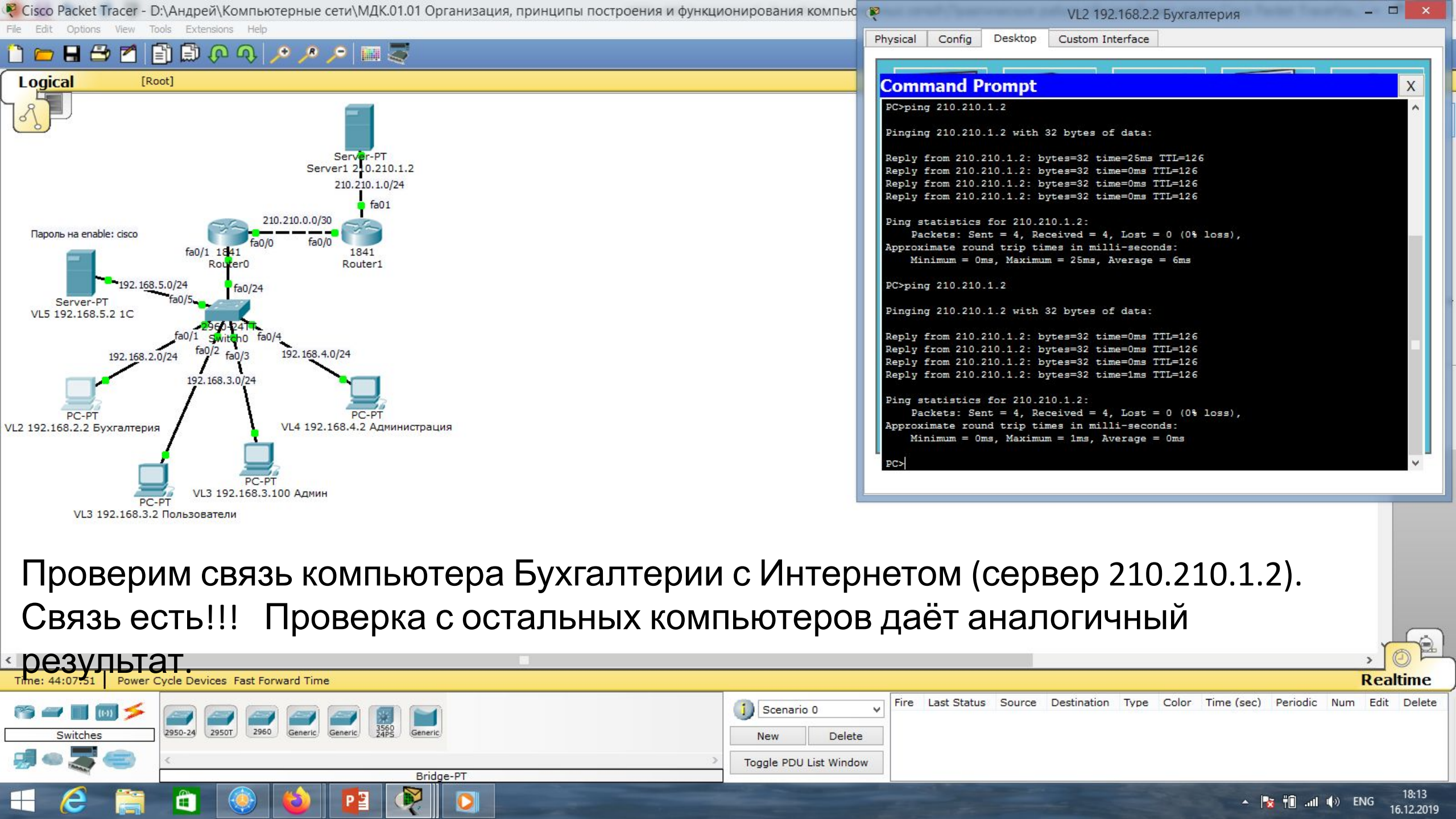


FastEthernet0/1.2,
FastEthernet0/1.3,
FastEthernet0/1.4,
является внутренними:
«int fa0/1.2»,
«ip nat inside»,
«exit»,
«int fa0/1.3», «ip nat inside», «exit»,
«int fa0/1.4», «ip nat inside», «exit».
Интерфейс FastEthernet0/1.5 (к «серверу 1С») не трогаем, чтобы исключить доступ «сервера 1С» в Интернет.

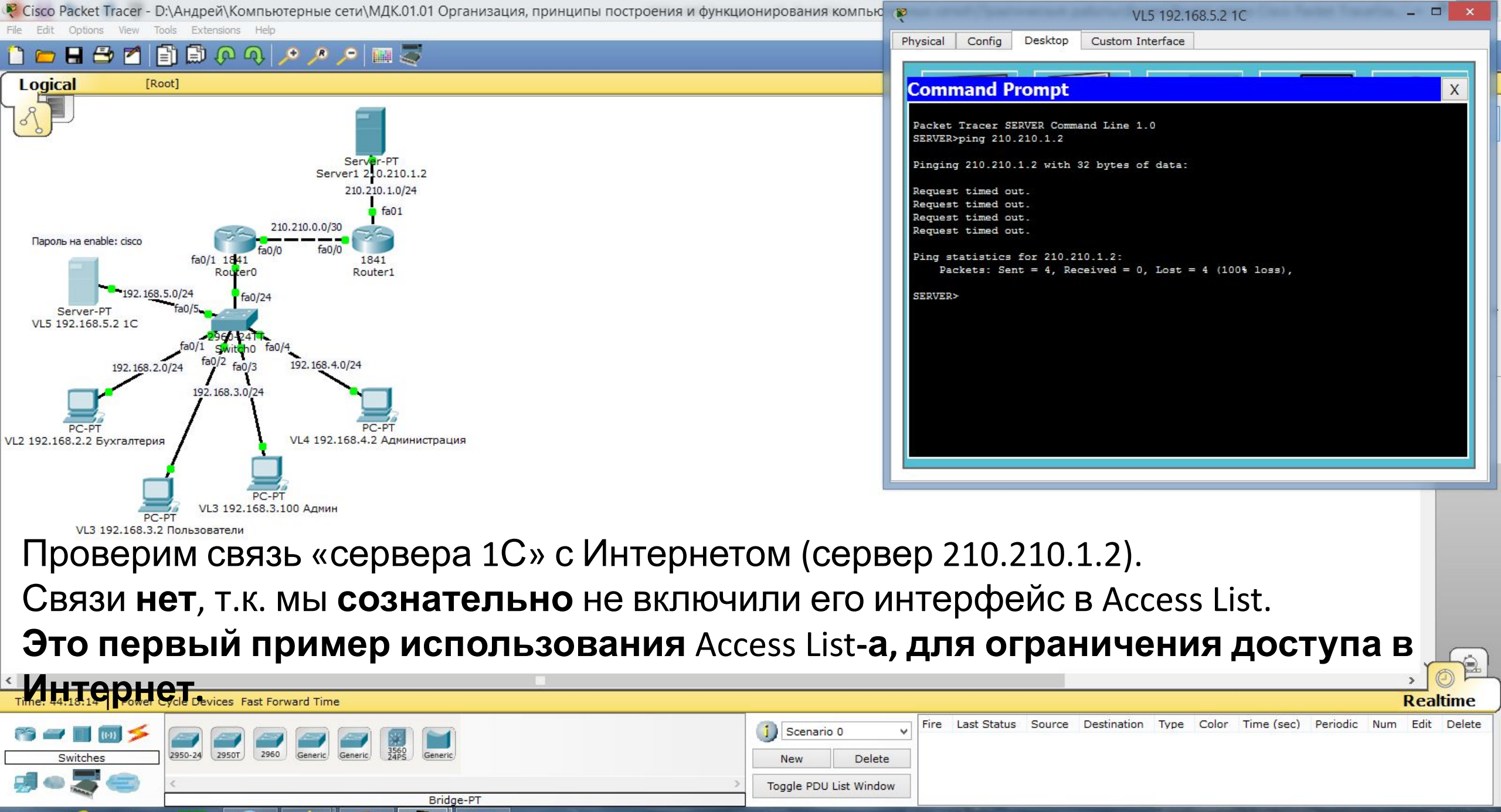


Создаём стандартный Access List, дадим ему имя «FOR-NAT»:

«ip access-list standard FOR-NAT», «permit 192.168.2.0 0.0.0.255», «permit 192.168.3.0 0.0.0.255», «permit 192.168.4.0 0.0.0.255», «exit», «ip nat inside source list FOR-NAT interface fa0/0 overload», «end».



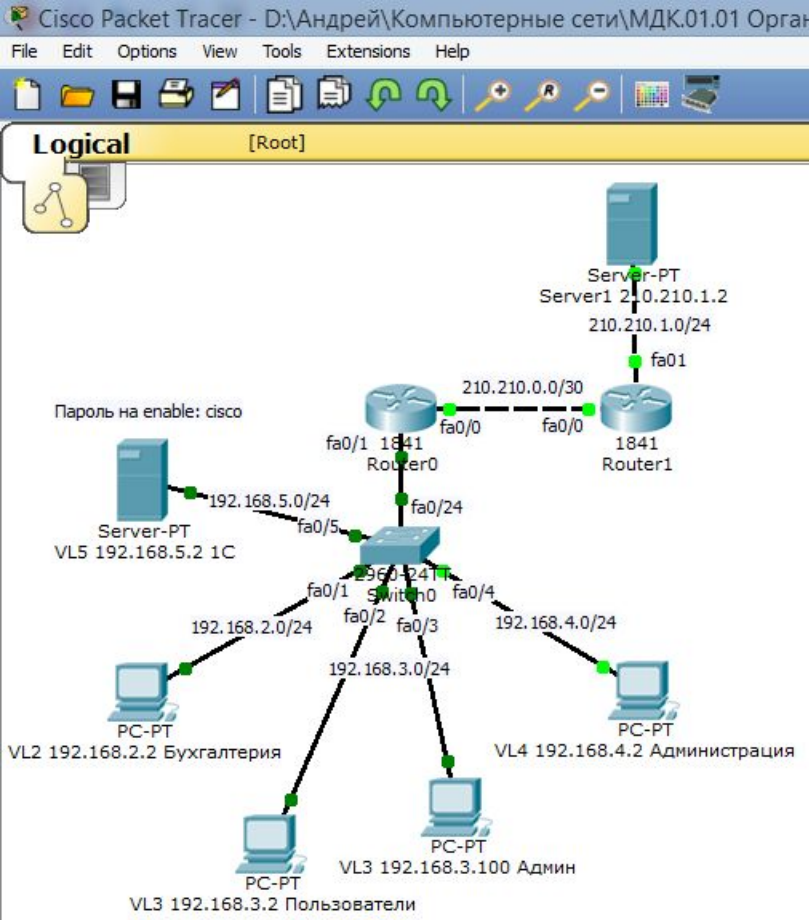
Проверим связь компьютера Бухгалтерии с Интернетом (сервер 210.210.1.2). Связь есть!!! Проверка с остальных компьютеров даёт аналогичный результат.



Проверим связь «сервера 1С» с Интернетом (сервер 210.210.1.2).

Связи **нет**, т.к. мы **сознательно** не включили его интерфейс в Access List.

Это первый пример использования Access List**-а, для ограничения доступа в Интернет.**



Используя NAT, получаем дополнительный уровень защиты т.к используем «серые» ip-адреса, которые не видны в сети Интернет.

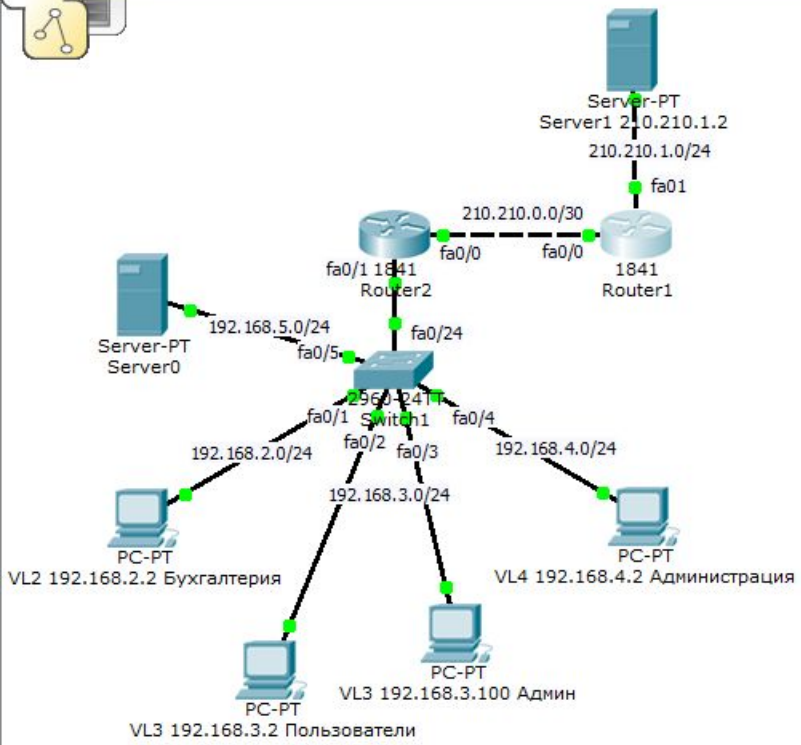
Однако, если злоумышленник взломал маршрутизатор провайдера, то он может прописать маршруты во внутренние сети, выбрав популярные адреса сетей, например, 192.168…, которые используются во многих организациях.

При этом он может получить доступ во внутреннюю сеть.

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

File Edit Options View Tools Extensions Help

Logical [Root]



Router1

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)#ip route 192.168.0.0 255.255.0.0 210.210.0.2
Router(config)#
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Copy Paste

Предположим, что злоумышленник взломал маршрутизатор провайдера и прописал маршруты в наши сети, указав большой диапазон:
«ip route 192.168.0.0 255.255.0.0 210.210.0.2», «end».

Time: 46:38:04 Power Cycle Devices Fast Forward Time

Realtime

Connections

Copper Straight-Through

Scenario 0

New Delete

Toggle PDU List Window

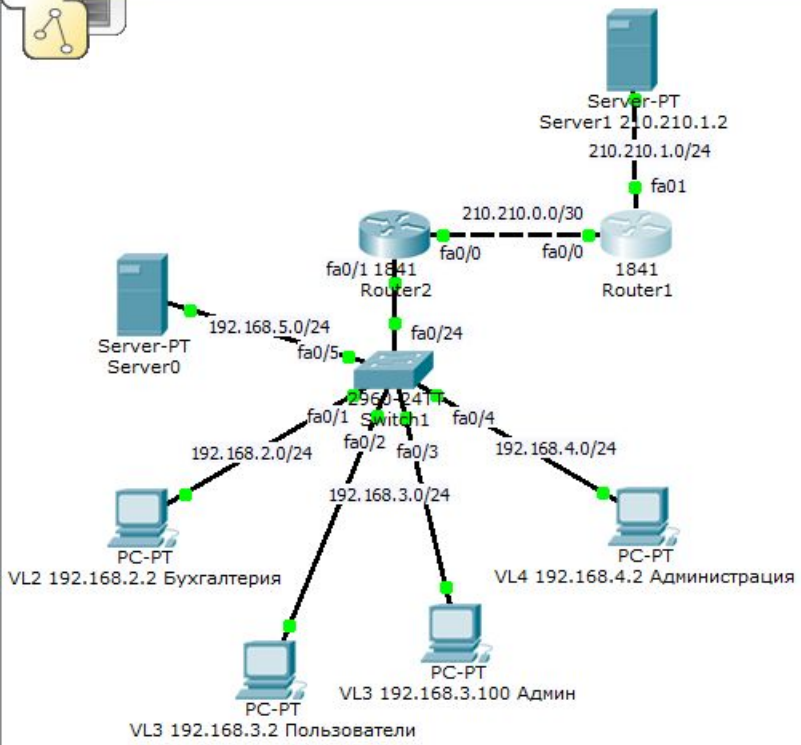
Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete

РУС 20:44 16.12.2019

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

File Edit Options View Tools Extensions Help

Logical [Root]



Router1

Physical Config CLI

IOS Command Line Interface

```
Router#ping
Protocol [ip]: 192.168.5.2
% Unknown protocol - "192.168.5.2", type "ping ?" for help

Router#ping 192.168.5.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Router#ping 192.168.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Router#ping 192.168.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Router#
```

Copy Paste

Проверим связь маршрутизатора провайдера с компьютерами нашей сети: «ping 192.168.5.2», «ping 192.168.2.2», «ping 192.168.3.2».

Связь есть! Злоумышленник получил доступ в нашу сеть!!!

Time: 46:40:09 Power Cycle Devices Fast Forward Time

Realtime

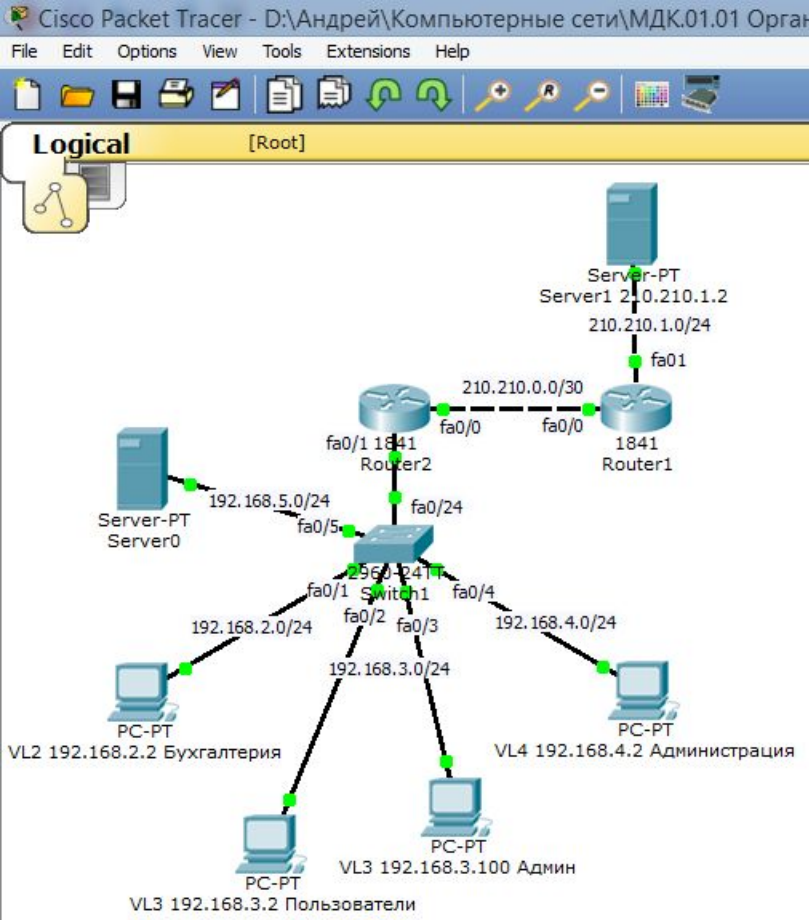
Connections

Copper Straight-Through

Scenario 0 New Delete Toggle PDU List Window

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

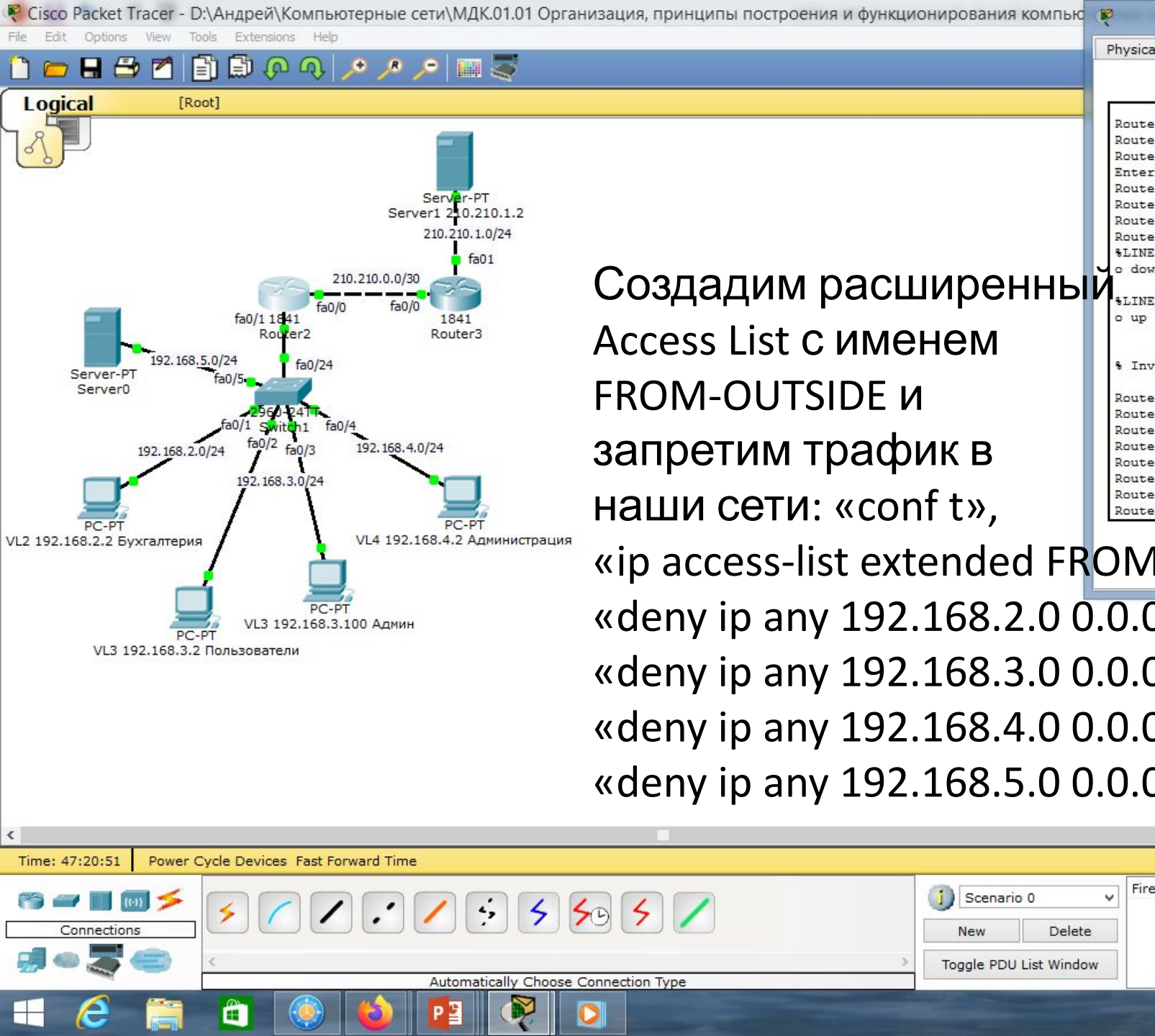
РУС 20:46 16.12.2019

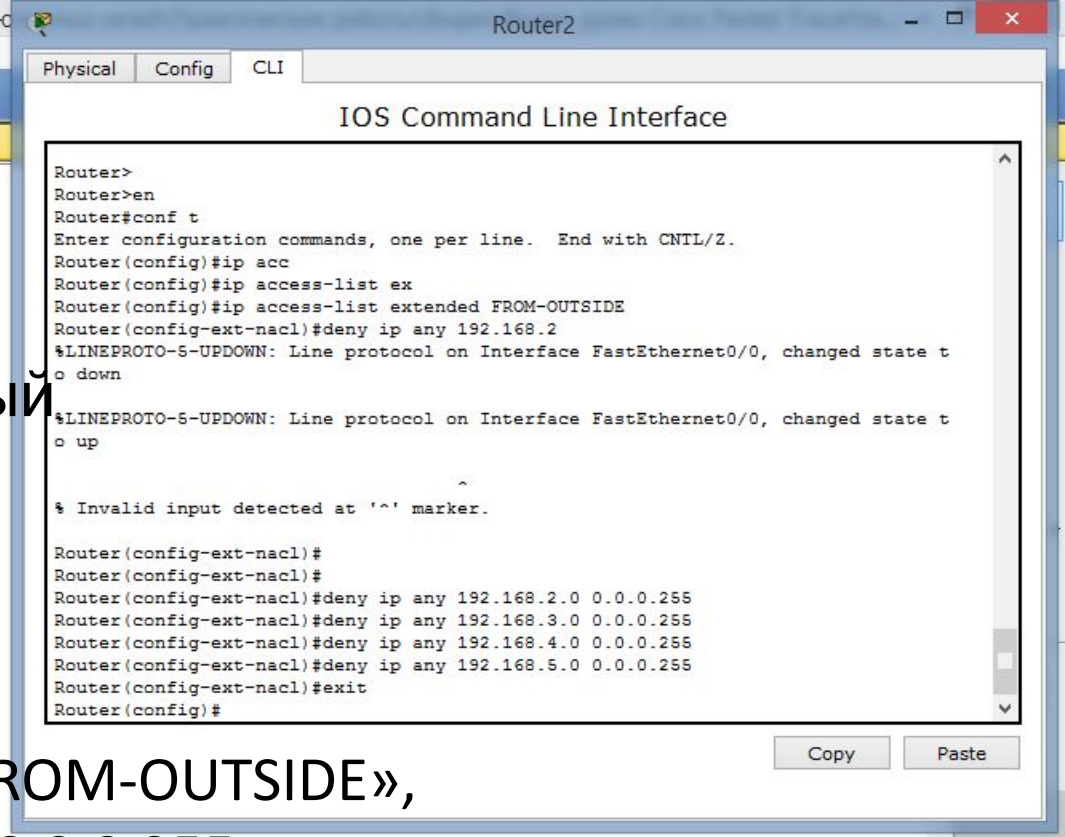


Чтобы ограничить доступ в наши сети, используем Access List-ы.

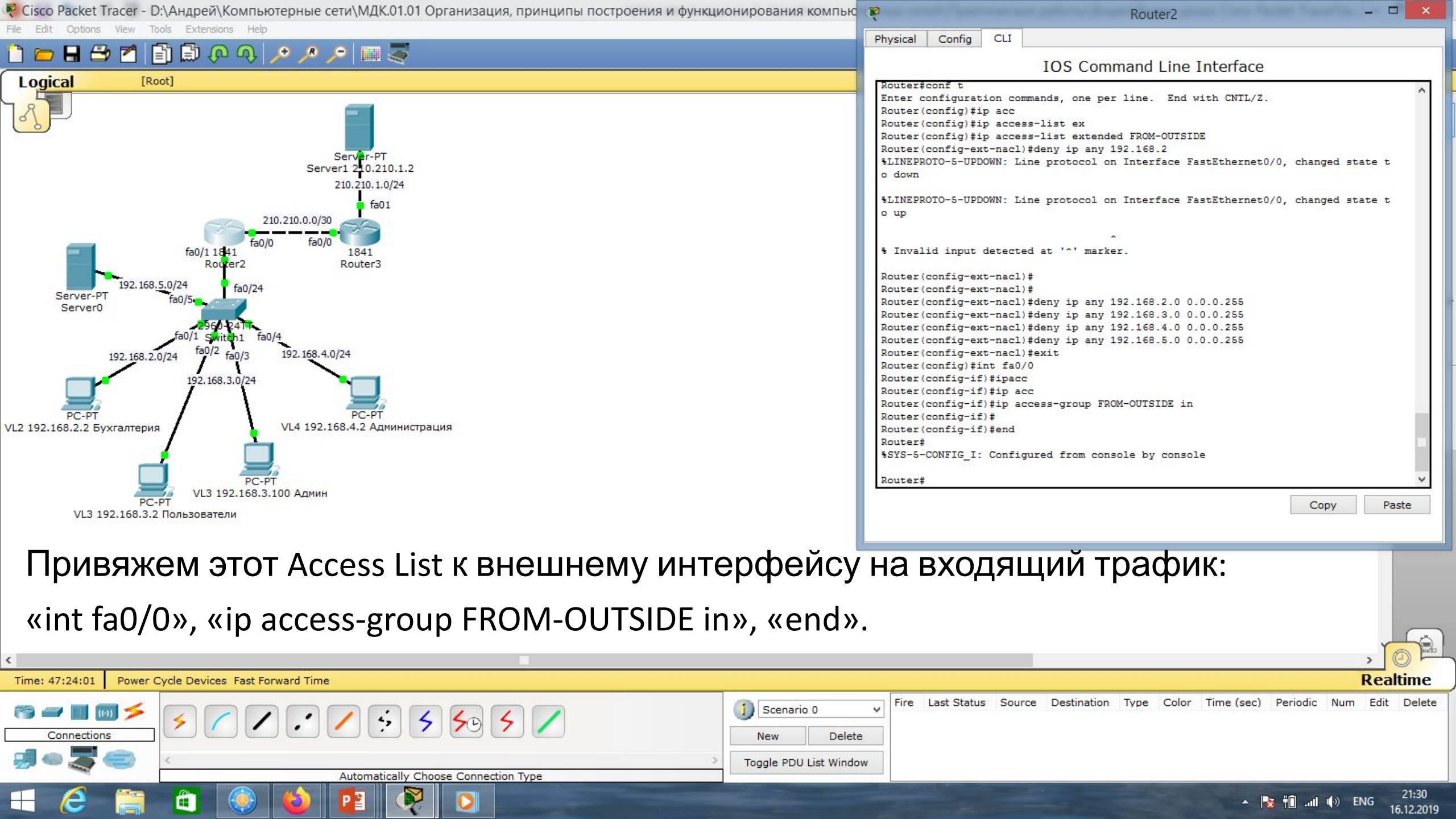
Ограничим доступ на входе в наш маршрутизатор (Router 2).

Будем использовать расширенные Access List-ы.



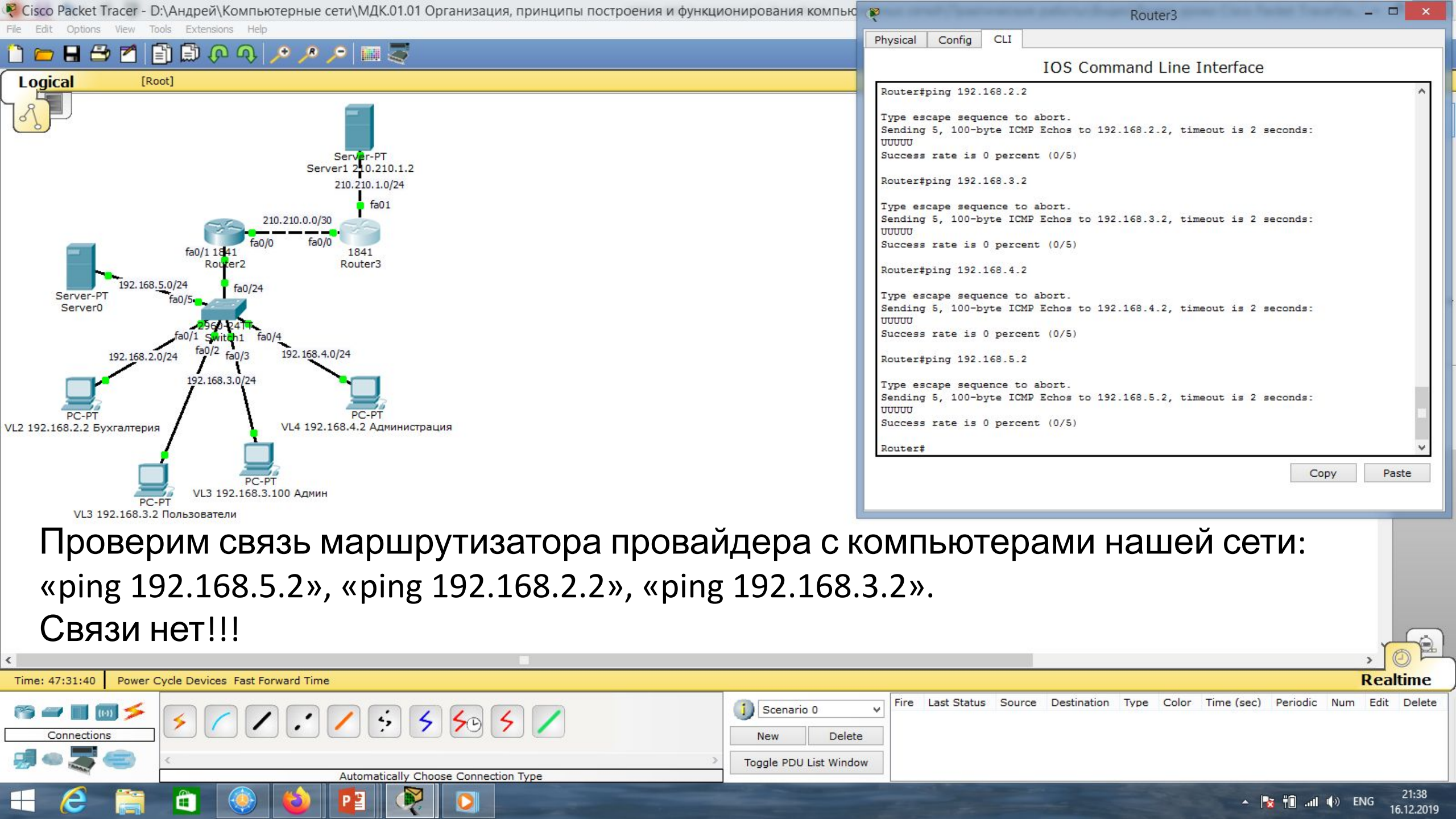


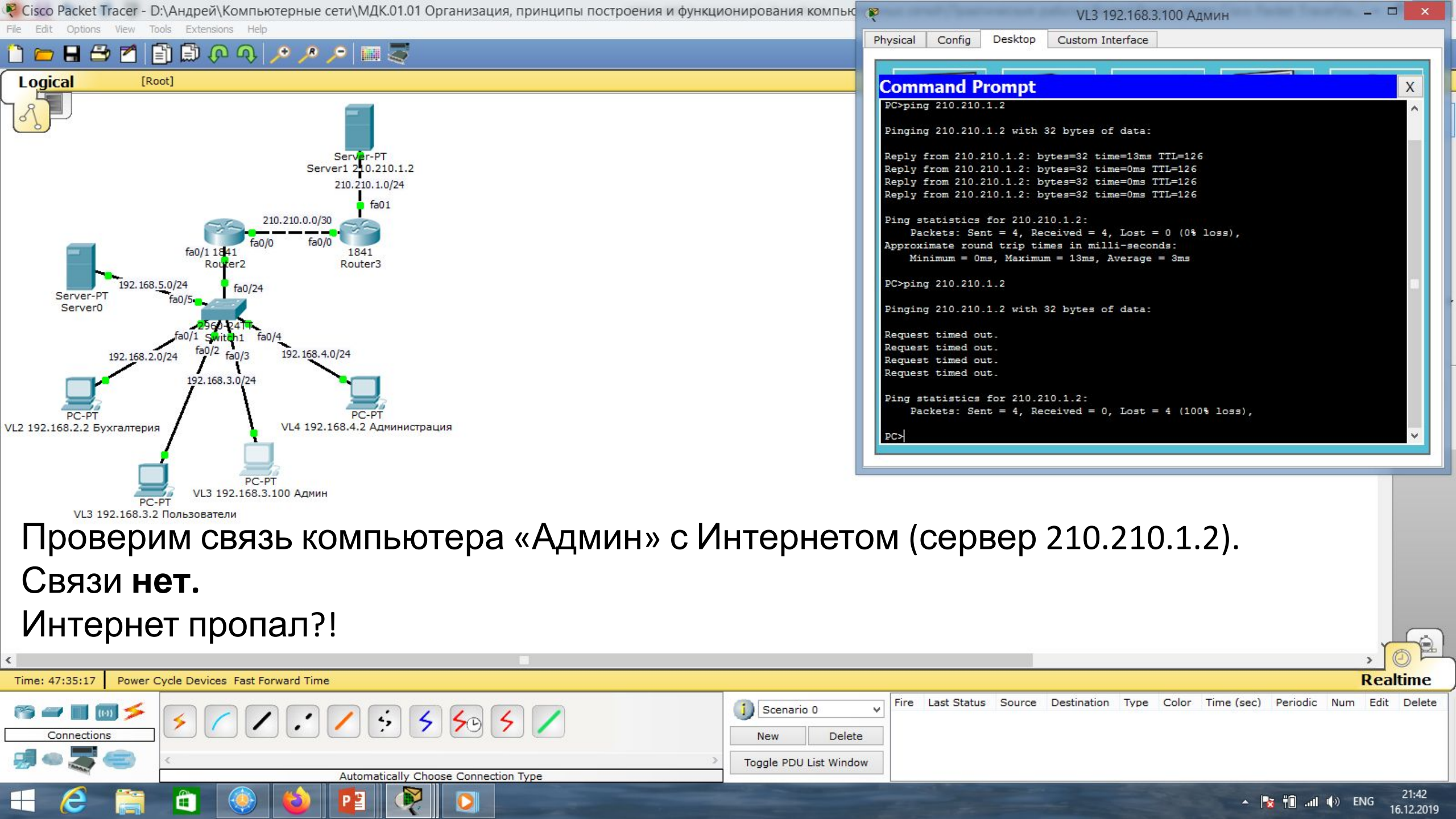
Создадим расширенный Access List с именем FROM-OUTSIDE и запретим трафик в наши сети: «conf t», «ip access-list extended FROM-OUTSIDE», «deny ip any 192.168.2.0 0.0.0.255», «deny ip any 192.168.3.0 0.0.0.255», «deny ip any 192.168.4.0 0.0.0.255» «deny ip any 192.168.5.0 0.0.0.255», «exit».

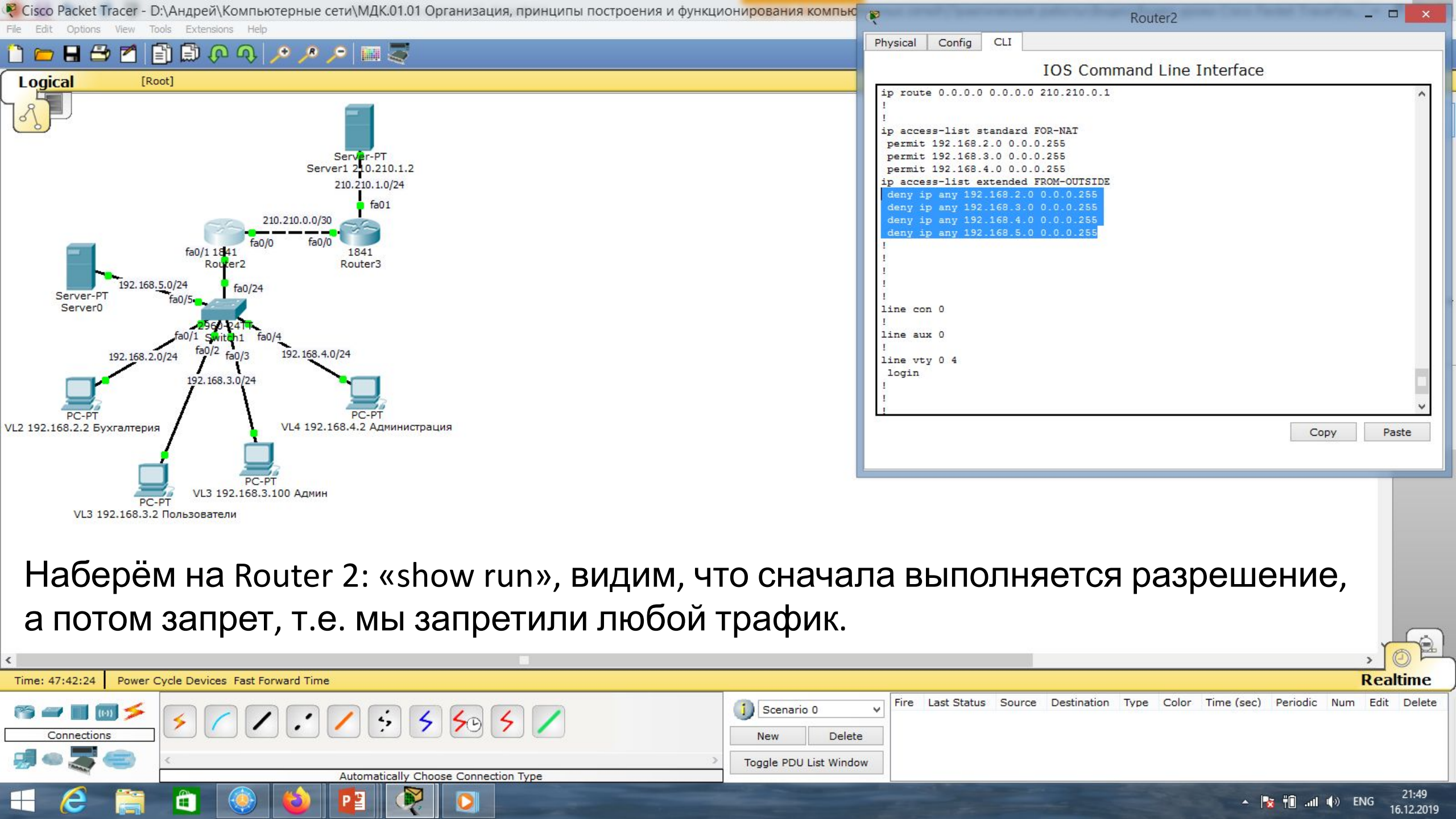


Привяжем этот Access List к внешнему интерфейсу на входящий трафик:

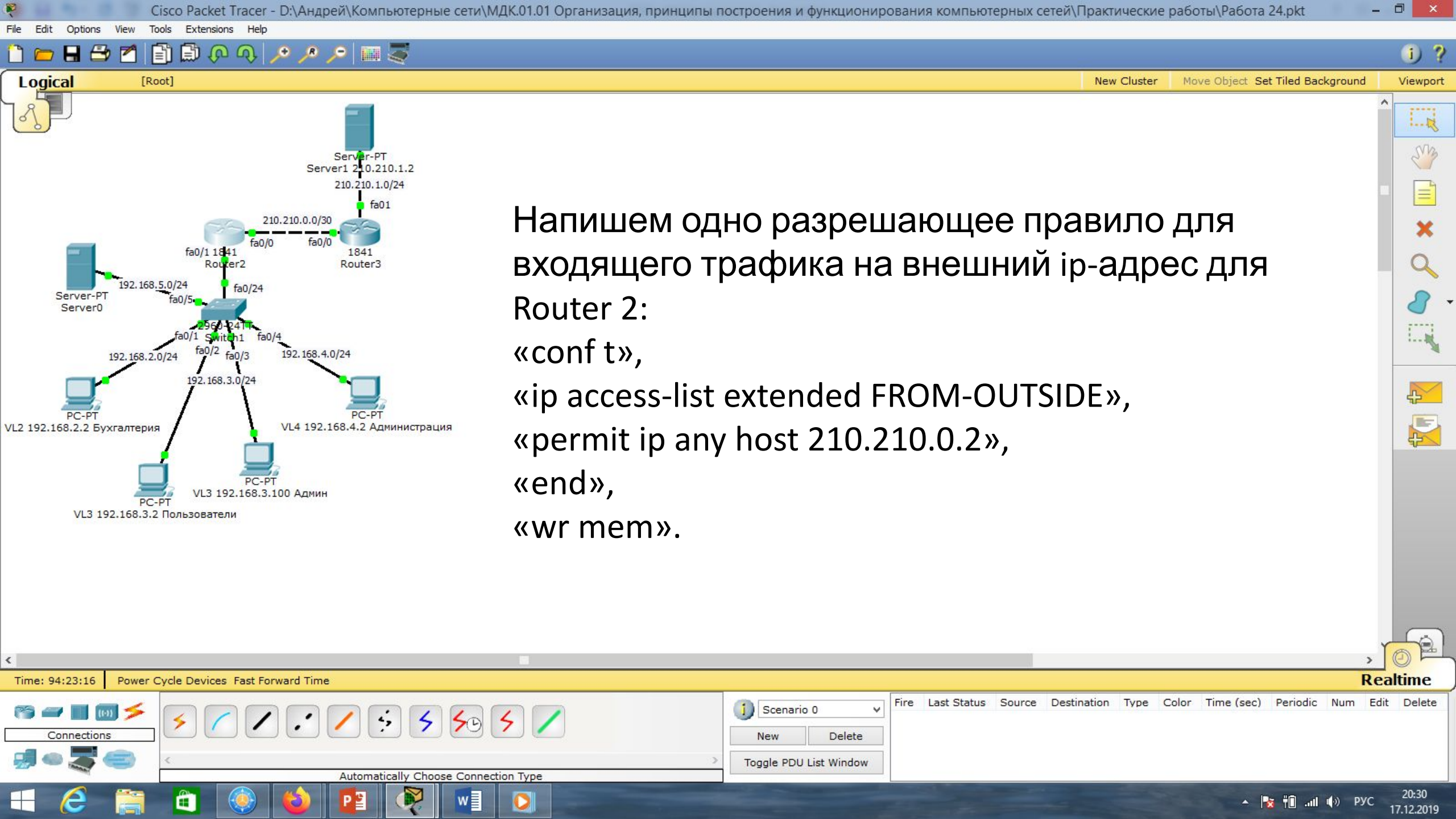
«int fa0/0», «ip access-group FROM-OUTSIDE in», «end».

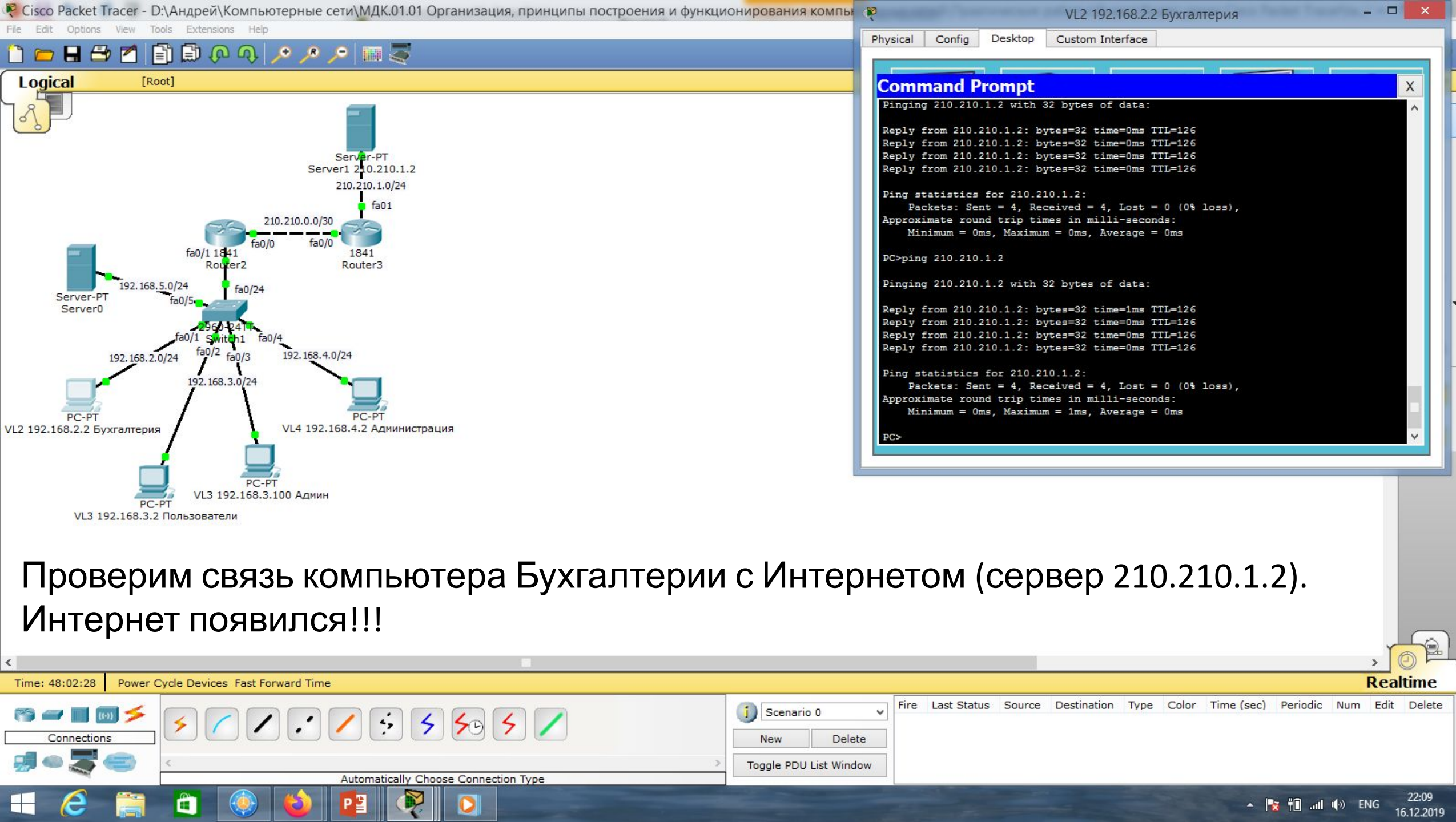

Cisco Packet Tracer - D:\Андрей\Компьютерные сети\МДК.01.01 Организация, принципы построения и функционирования компью
File Edit Options View Tools Extensions Help
Logical [Root]
Server-PT
Server1 210.210.1.2
210.210.1.0/24
fa01
210.210.0.0/30
fa0/1 1841
Router2
fa0/0
fa0/0
1841
Router3
Server-PT
Server0
192.168.5.0/24
fa0/5
fa0/24
2960-24TT
Switch1
fa0/1
fa0/2
fa0/3
fa0/4
192.168.2.0/24
192.168.3.0/24
192.168.4.0/24
PC-PT
VL2 192.168.2.2 Бухгалтерия
PC-PT
VL4 192.168.4.2 Администрация
PC-PT
VL3 192.168.3.100 Админ
PC-PT
VL3 192.168.3.2 Пользователи
Router3
Physical
Config
CLI
IOS Command Line Interface
Router#ping 192.168.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
Router#ping 192.168.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
Router#ping 192.168.4.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
Router#ping 192.168.5.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.2, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
Router#
Copy
Paste
Проверим связь маршрутизатора провайдера с компьютерами нашей сети:
«ping 192.168.5.2», «ping 192.168.2.2», «ping 192.168.3.2».
Связи нет!!!
Time: 47:31:40
Power Cycle Devices Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
Periodic
Num
Edit
Delete
ENG
21:38
16.12.2019


Cisco Packet Tracer - D:\Андрей\Компьютерные сети\МДК.01.01 Организация, принципы построения и функционирования компью
File Edit Options View Tools Extensions Help
Logical [Root]
Server-PT
Server1 210.210.1.2
210.210.1.0/24
fa01
210.210.0.0/30
fa0/0
fa0/0
fa0/1 1841
Router2
1841
Router3
Server-PT
Server0
192.168.5.0/24
fa0/5
fa0/24
2960-24TT
Switch1
fa0/1
fa0/2
fa0/3
fa0/4
192.168.2.0/24
192.168.3.0/24
192.168.4.0/24
PC-PT
VL2 192.168.2.2 Бухгалтерия
PC-PT
VL4 192.168.4.2 Администрация
PC-PT
VL3 192.168.3.100 Админ
PC-PT
VL3 192.168.3.2 Пользователи
VL3 192.168.3.100 Админ
Physical Config Desktop Custom Interface
Command Prompt
X
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=13ms TTL=126
Reply from 210.210.1.2: bytes=32 time=0ms TTL=126
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 = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 13ms, Average = 3ms
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>
Проверим связь компьютера «Админ» с Интернетом (сервер 210.210.1.2).
Связи нет.
Интернет пропал?!
Time: 47:35:17
Power Cycle Devices Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time (sec) Periodic Num Edit Delete
ENG
21:42
16.12.2019



Наберём на Router 2: «show run», видим, что сначала выполняется разрешение, а потом запрет, т.е. мы запретили любой трафик.


Cisco Packet Tracer - D:\Андрей\Компьютерные сети\МДК.01.01 Организация, принципы построения и функционирования компьютерных сетей\Практические работы\Работа 24.pkt
File Edit Options View Tools Extensions Help
Logical [Root]
New Cluster Move Object Set Tiled Background Viewport
Server-PT
Server1 210.210.1.2
210.210.1.0/24
fa01
210.210.0.0/30
fa0/1 1841
Router2
fa0/0
fa0/0
1841
Router3
Server-PT
Server0
192.168.5.0/24
fa0/5
fa0/24
2960-24TT
Switch1
fa0/1
fa0/2
fa0/3
fa0/4
192.168.2.0/24
192.168.3.0/24
192.168.4.0/24
PC-PT
VL2 192.168.2.2 Бухгалтерия
PC-PT
VL4 192.168.4.2 Администрация
PC-PT
VL3 192.168.3.100 Админ
PC-PT
VL3 192.168.3.2 Пользователи
Напишем одно разрешающее правило для входящего трафика на внешний ip-адрес для Router 2:
«conf t»,
«ip access-list extended FROM-OUTSIDE»,
«permit ip any host 210.210.0.2»,
«end»,
«wr mem».
Time: 94:23:16 Power Cycle Devices Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time (sec) Periodic Num Edit Delete
РУС
20:30
17.12.2019

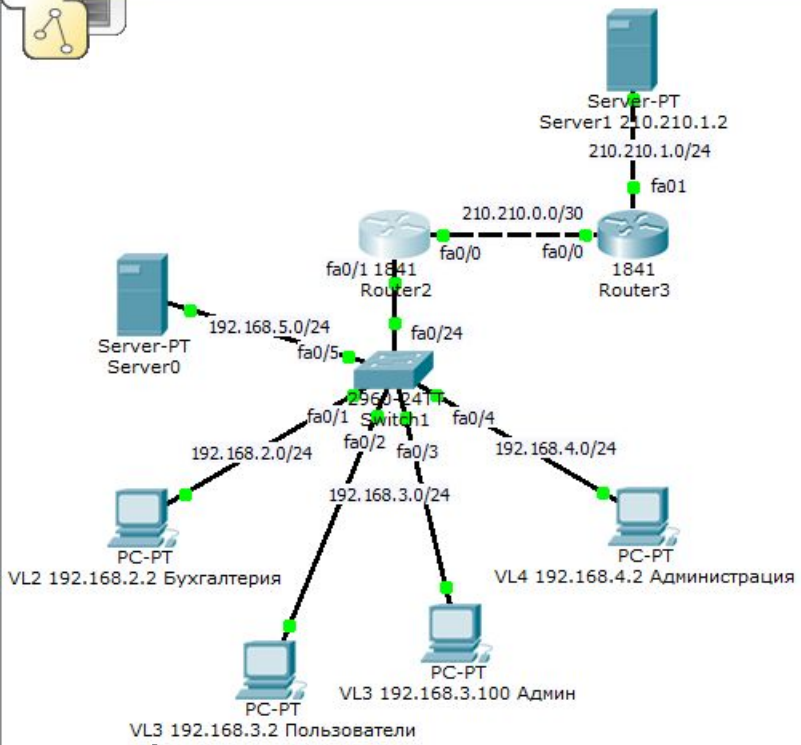


Проверим связь компьютера Бухгалтерии с Интернетом (сервер 210.210.1.2). Интернет появился!!!

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

File Edit Options View Tools Extensions Help

Logical [Root]



Router2

Physical Config CLI

IOS Command Line Interface

```
!
ip nat inside source list FOR-NAT interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 210.210.0.1
!
!
ip access-list standard FOR-NAT
 permit 192.168.2.0 0.0.0.255
 permit 192.168.3.0 0.0.0.255
 permit 192.168.4.0 0.0.0.255
ip access-list extended FROM-OUTSIDE
 deny ip any 192.168.2.0 0.0.0.255
 deny ip any 192.168.3.0 0.0.0.255
 deny ip any 192.168.4.0 0.0.0.255
 deny ip any 192.168.5.0 0.0.0.255
 permit ip any host 210.210.0.2
!
!
!
!
!
line con 0
!
line aux 0
!
 --More--
```

Copy Paste

Наберём на Router 2:

«show run», видим, что появилась разрешающая команда.

Time: 48:04:28 Power Cycle Devices Fast Forward Time

Realtime

Connections

Automatically Choose Connection Type

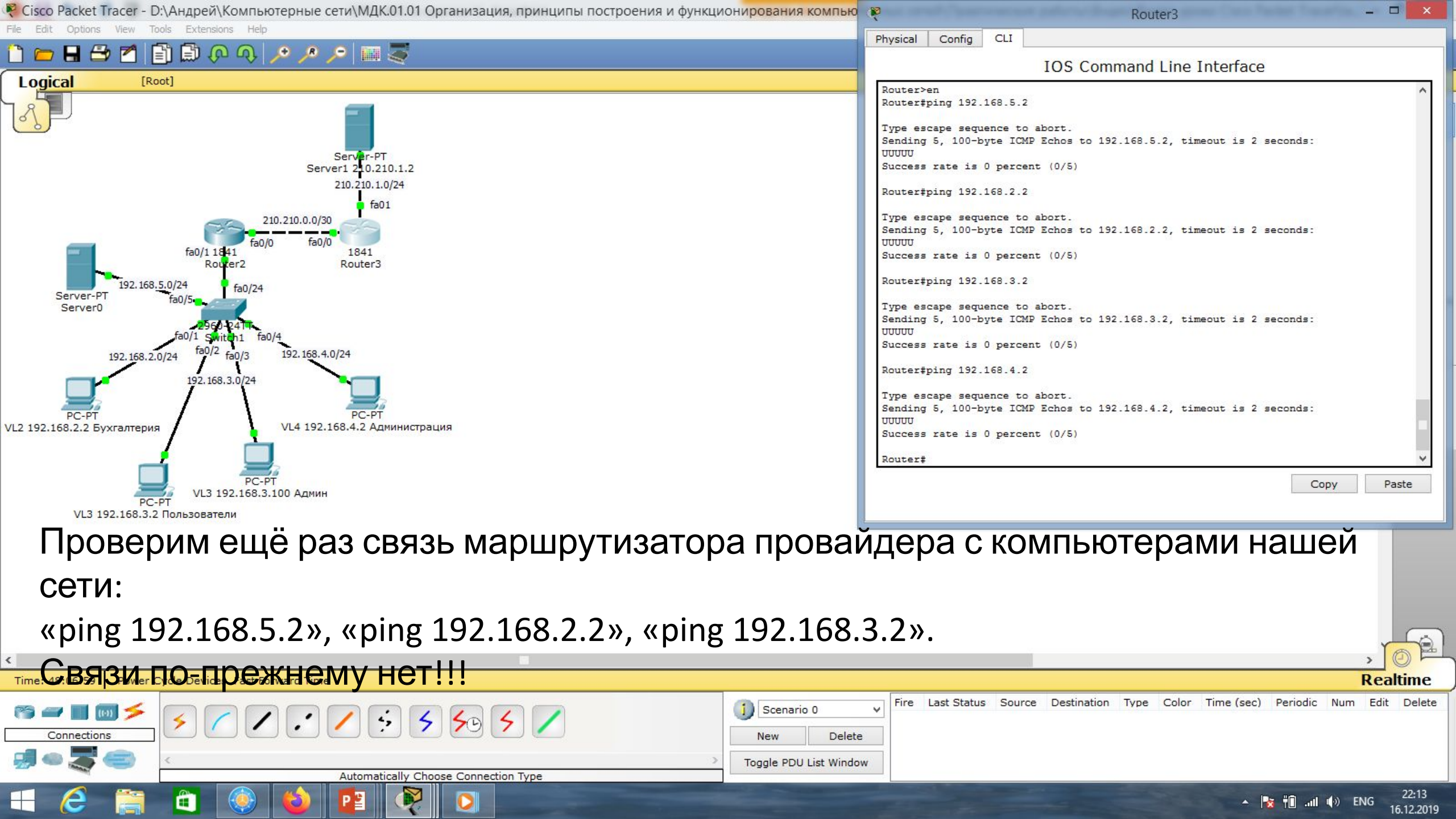
Scenario 0

New Delete

Toggle PDU List Window

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

РУС 22:11 16.12.2019



Проверим ещё раз связь маршрутизатора провайдера с компьютерами нашей сети:

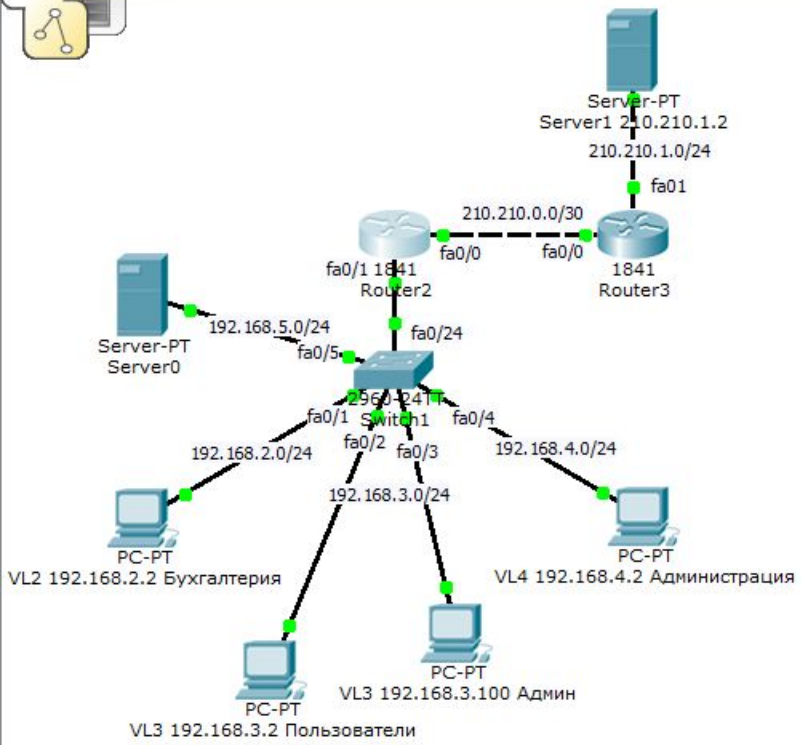
«ping 192.168.5.2», «ping 192.168.2.2», «ping 192.168.3.2».

Связи по-прежнему нет!!!

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

File Edit Options View Tools Extensions Help

Logical [Root]



Router2

Physical Config CLI

IOS Command Line Interface

```
ip nat inside source list FOR-NAT interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 210.210.0.1
!
!
ip access-list standard FOR-NAT
 permit 192.168.2.0 0.0.0.255
 permit 192.168.3.0 0.0.0.255
 permit 192.168.4.0 0.0.0.255
ip access-list extended FROM-OUTSIDE
 deny ip any 192.168.2.0 0.0.0.255
 deny ip any 192.168.3.0 0.0.0.255
 deny ip any 192.168.4.0 0.0.0.255
 deny ip any 192.168.5.0 0.0.0.255
 permit ip any host 210.210.0.2
!
!
!
!
!
line con 0
!
line aux 0
!
 --More--
```

Copy Paste

Если зайти на наш маршрутизатор (Router 2) и набрать: «show run»,
то увидим, что наши Access List-ы не оптимально сконфигурированы. Нужно было разрешить один Access List, а все остальные были бы запрещены по умолчанию.

Time: 48:13:25 Power Cycle Devices Fast Forward Time

Realtime

Connections

Automatically Choose Connection Type

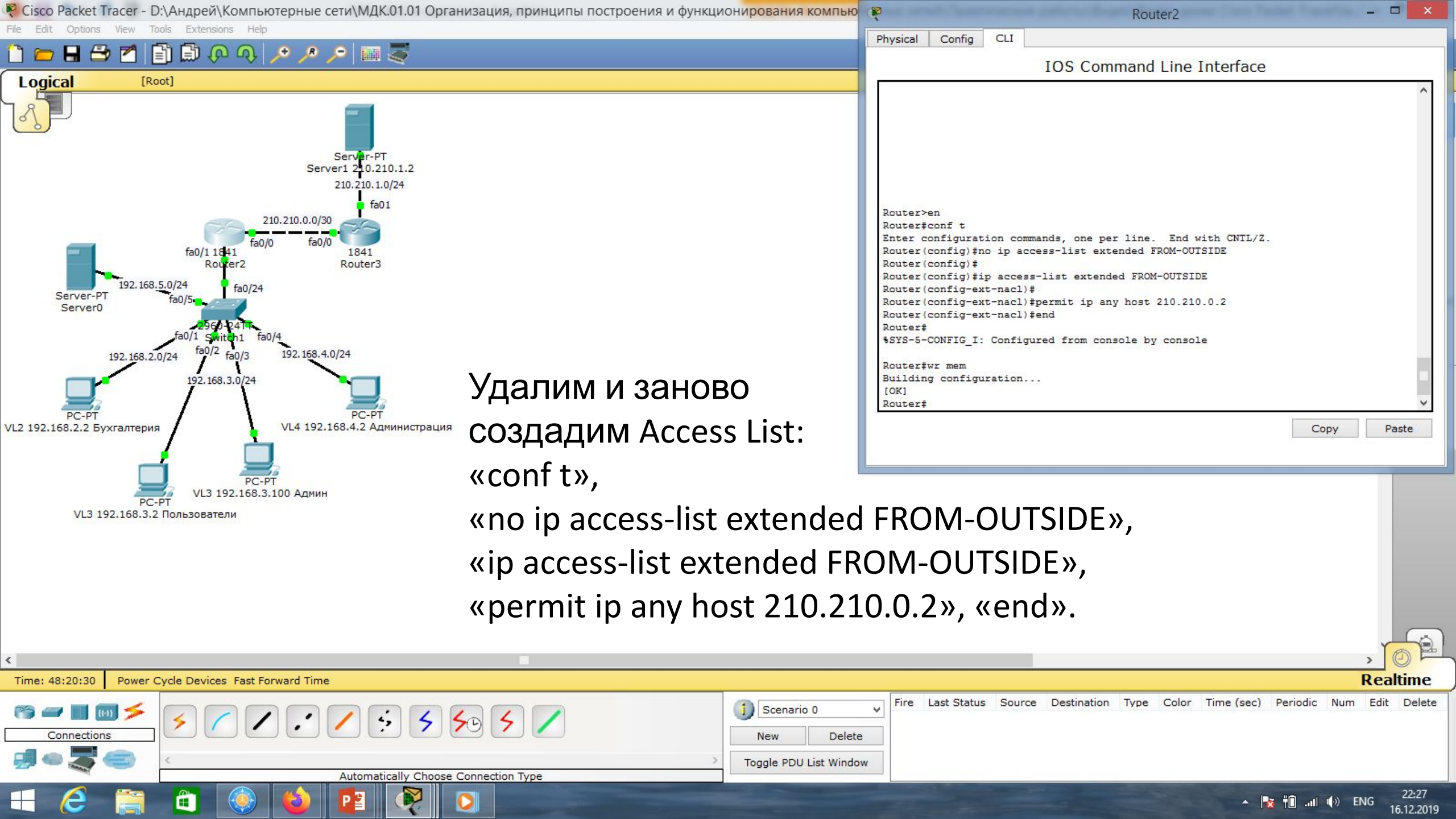
Scenario 0

New Delete

Toggle PDU List Window

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

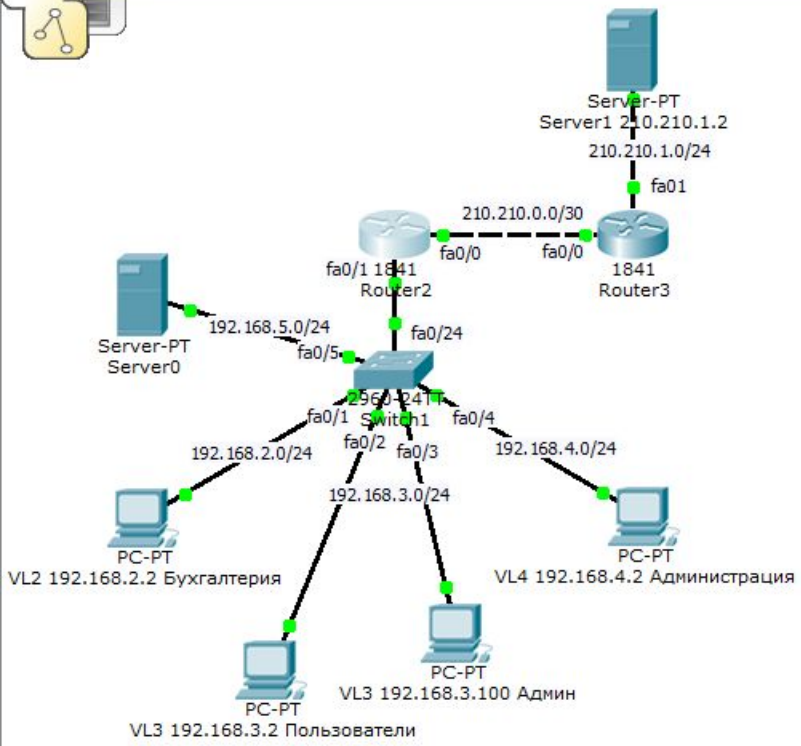
РУС 22:20 16.12.2019


Cisco Packet Tracer - D:\Андрей\Компьютерные сети\МДК.01.01 Организация, принципы построения и функционирования компью
File Edit Options View Tools Extensions Help
Logical [Root]
Server-PT
Server1 210.210.1.2
210.210.1.0/24
fa01
210.210.0.0/30
fa0/1 1841
Router2
fa0/0
fa0/0
1841
Router3
Server-PT
Server0
192.168.5.0/24
fa0/5
fa0/24
2960-24TT
Switch1
fa0/1
fa0/2
fa0/3
fa0/4
192.168.2.0/24
192.168.3.0/24
192.168.4.0/24
PC-PT
VL2 192.168.2.2 Бухгалтерия
PC-PT
VL4 192.168.4.2 Администрация
PC-PT
VL3 192.168.3.100 Админ
PC-PT
VL3 192.168.3.2 Пользователи
Router2
Physical
Config
CLI
IOS Command Line Interface
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip access-list extended FROM-OUTSIDE
Router(config)#
Router(config)#ip access-list extended FROM-OUTSIDE
Router(config-ext-nacl)#
Router(config-ext-nacl)#permit ip any host 210.210.0.2
Router(config-ext-nacl)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#wr mem
Building configuration...
[OK]
Router#
Copy
Paste
Удалим и заново создадим Access List:
«conf t»,
«no ip access-list extended FROM-OUTSIDE»,
«ip access-list extended FROM-OUTSIDE»,
«permit ip any host 210.210.0.2», «end».
Time: 48:20:30
Power Cycle Devices Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
Periodic
Num
Edit
Delete
ENG
22:27
16.12.2019

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

File Edit Options View Tools Extensions Help

Logical [Root]



Router2

Physical Config CLI

IOS Command Line Interface

```
!
ip nat inside source list FOR-NAT interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 210.210.0.1
!
!
ip access-list standard FOR-NAT
 permit 192.168.2.0 0.0.0.255
 permit 192.168.3.0 0.0.0.255
 permit 192.168.4.0 0.0.0.255
ip access-list extended FROM-OUTSIDE
 permit ip any host 210.210.0.2
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
 --More--
```

Copy Paste

Если зайти на наш маршрутизатор (Router 2) и набрать: «show run»,
то увидим, что наш Access List сконфигурирован оптимально.

Time: 48:29:03 Power Cycle Devices Fast Forward Time

Realtime

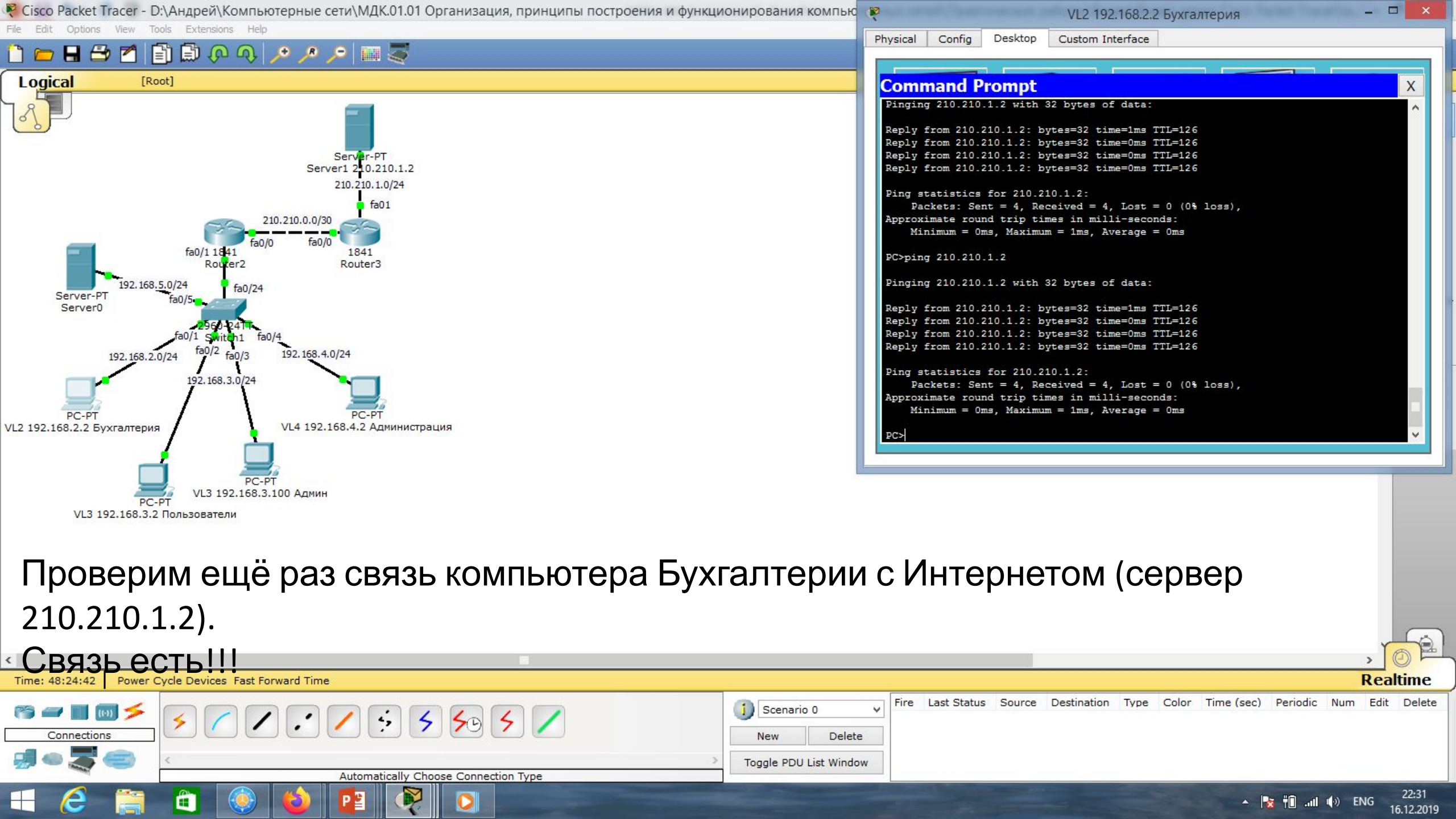
Connections

Automatically Choose Connection Type

Scenario 0 New Delete Toggle PDU List Window

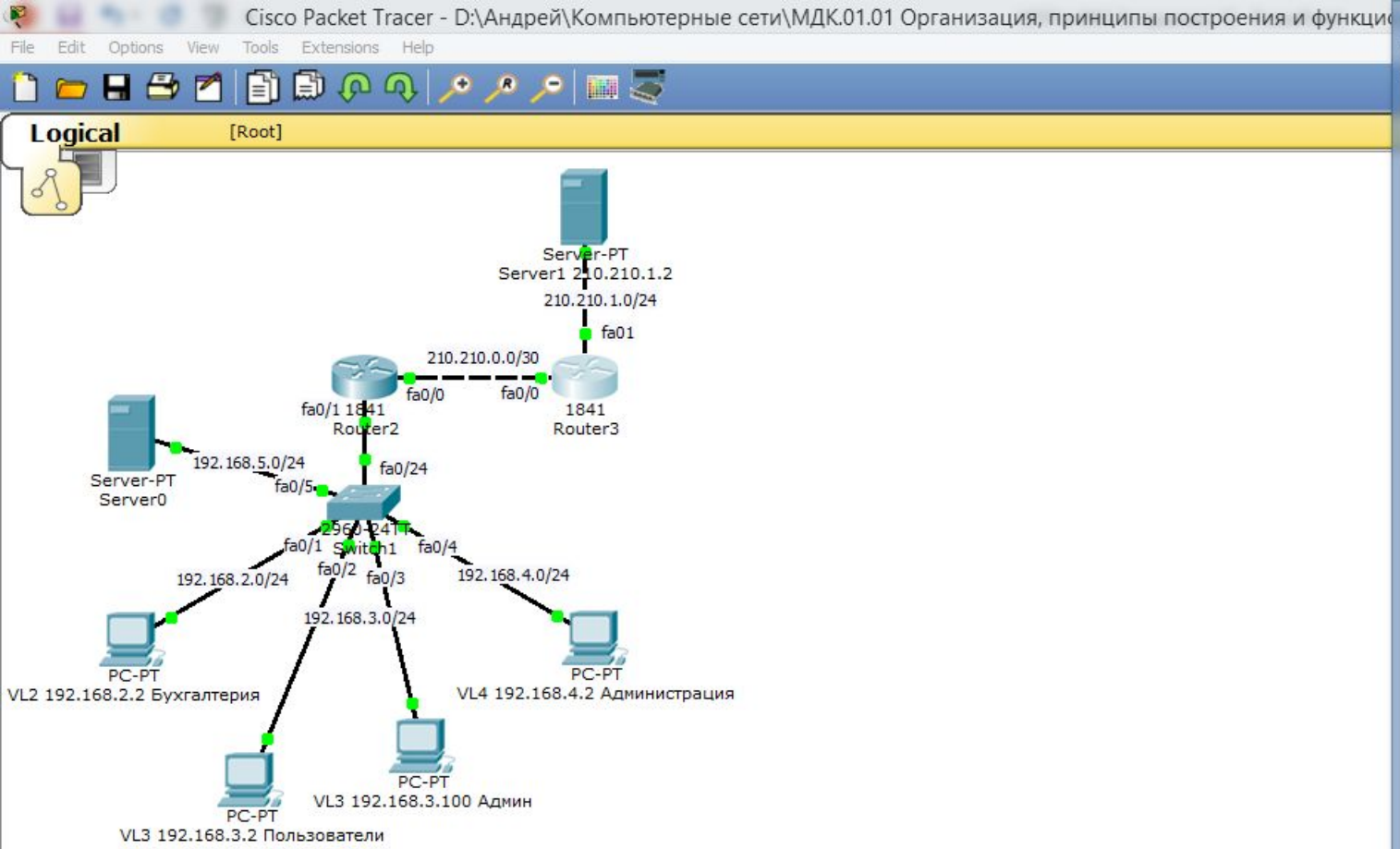
Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete

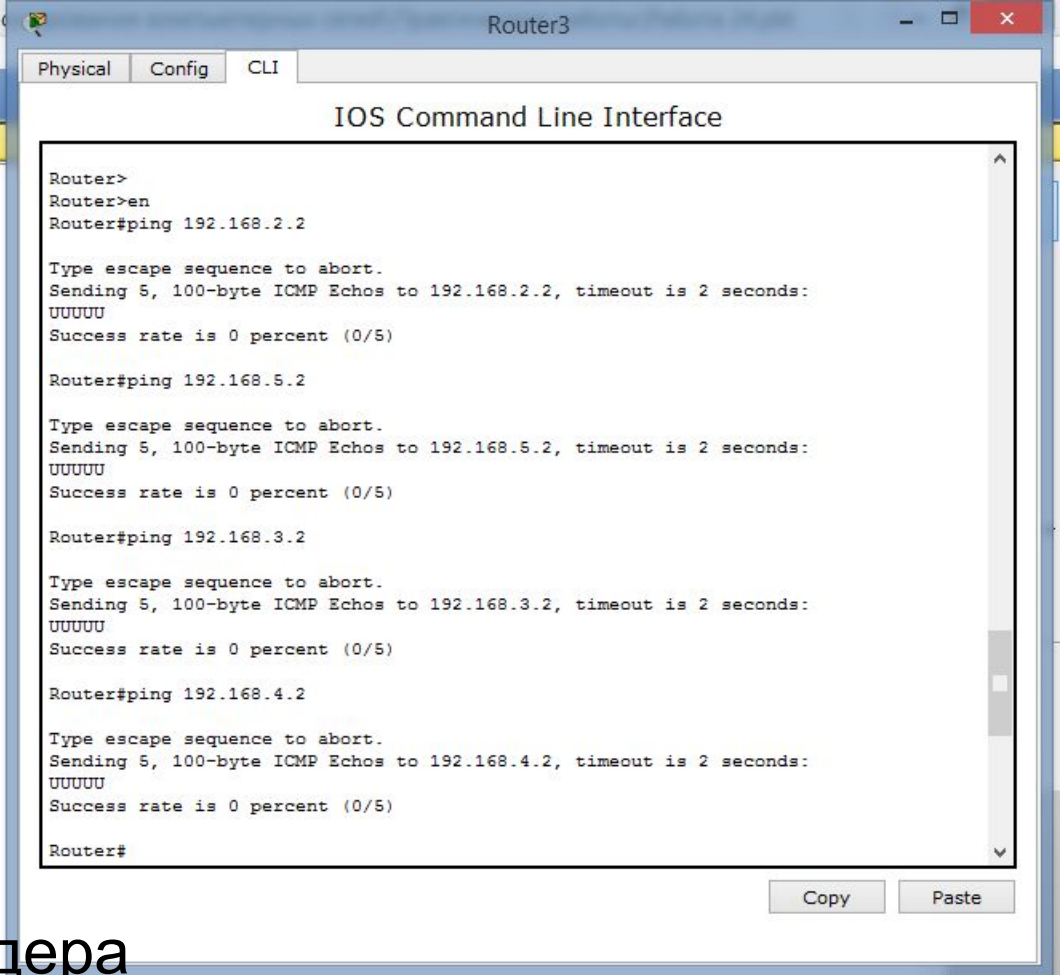
ENG 22:36 16.12.2019



Проверим ещё раз связь компьютера Бухгалтерии с Интернетом (сервер 210.210.1.2).

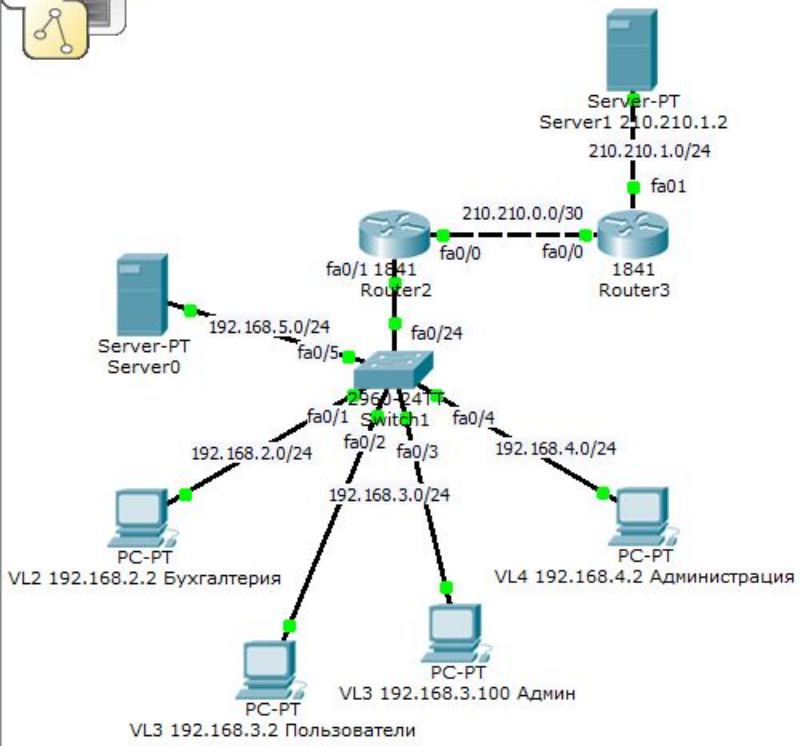
Связь есть!!!





Проверим ещё раз связь маршрутизатора провайдера с компьютерами нашей сети: «ping 192.168.5.2», «ping 192.168.2.2», «ping 192.168.3.2».

Связи по-прежнему нет!!! **Мы защитили нашу сеть от внешнего проникновения!!!**

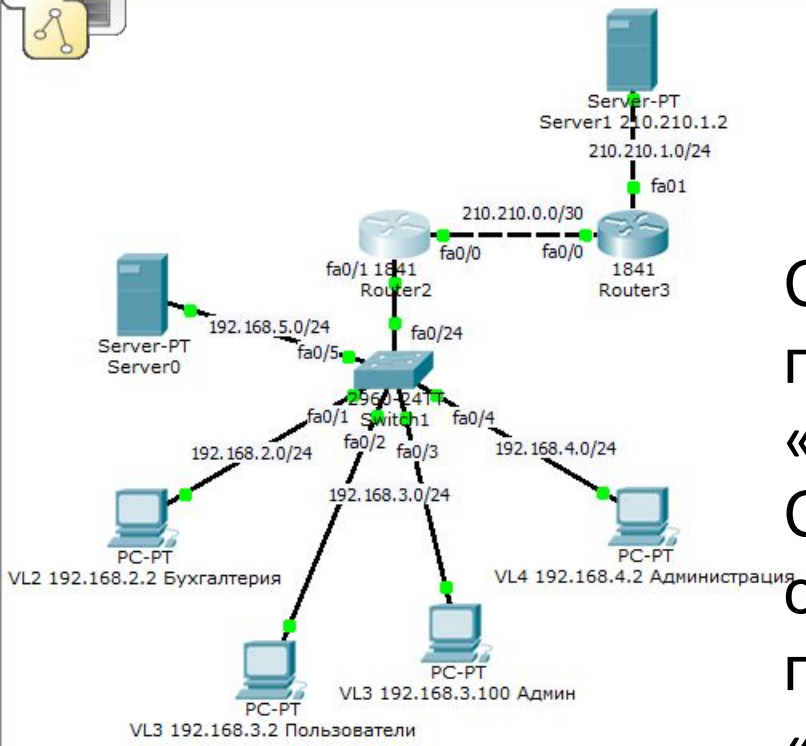


Предположим, что у нас есть удалённый доступ по telnet.
Такой доступ требует пароль.
Даже если злоумышленник не знает пароль, он может его подобрать.
Поэтому администратор решает его запретить доступ из внешней сети.

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

File Edit Options View Tools Extensions Help

Logical [Root]



Router2

Physical Config CLI

IOS Command Line Interface

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#us
Router(config)#username ?
  WORD  User name
Router(config)#username admin ?
  password   Specify the password for the user
  privilege  Set user privilege level
  secret     Specify the secret for the user
  <cr>
Router(config)#username admin
Router(config)#username admin pri
Router(config)#username admin privilege ?
  <0-15>  User privilege level
Router(config)#username admin privilege 15 ?
  password  Specify the password for the user
  secret    Specify the secret for the user
  <cr>
Router(config)#username admin privilege 15 pass
Router(config)#username admin privilege 15 password cisco
Router(config)#
```

Copy Paste

Сконфигурируем доступ по telnet на Router 2:
«conf t».
Создадим пользователя с именем **admin** и паролем **cisco**:
«username admin privilege 15 password cisco»
Пользуемся знаками «?» чтобы узнать возможные варианты продолжения записи команды.

Time: 94:47:00 Power Cycle Devices Fast Forward Time

Realtime

Connections

Automatically Choose Connection Type

Scenario 0 New Delete Toggle PDU List Window

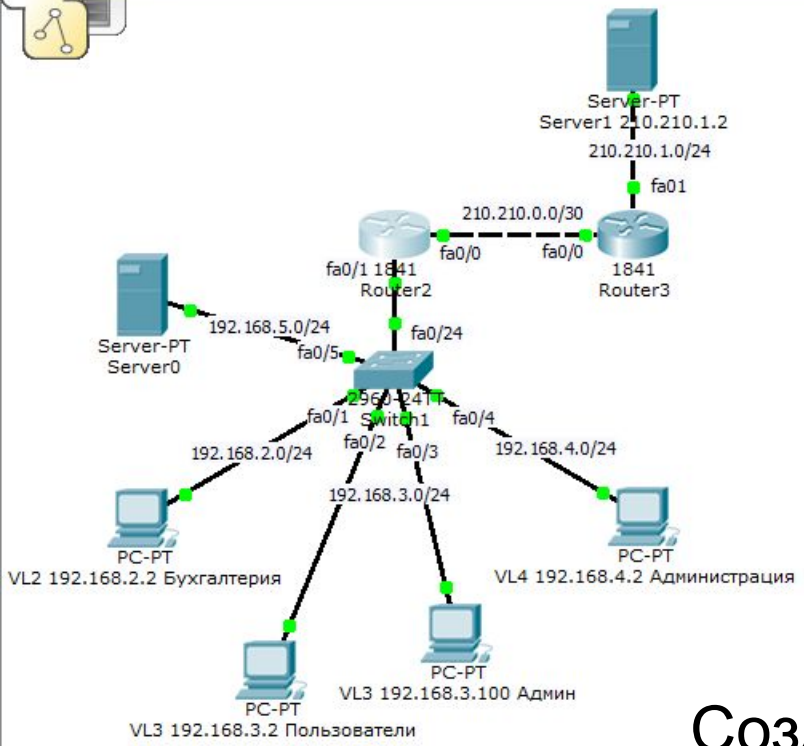
Fire | Last Status | Source | Destination | Type | Color | Time (sec) | Periodic | Num | Edit | Delete

ENG 20:54 17.12.2019

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

File Edit Options View Tools Extensions Help

Logical [Root]



Router2

Physical Config CLI

IOS Command Line Interface

```
Router(config)#username admin ?
  password   Specify the password for the user
  privilege  Set user privilege level
  secret     Specify the secret for the user
  <cr>
Router(config)#username admin
Router(config)#username admin pri
Router(config)#username admin privilege ?
  <0-15>  User privilege level
Router(config)#username admin privilege 15 ?
  password  Specify the password for the user
  secret    Specify the secret for the user
  <cr>
Router(config)#username admin privilege 15 pass
Router(config)#username admin privilege 15 password cisco
Router(config)#
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#en
Router(config)#ena
Router(config)#enable pass
Router(config)#enable password cisco
Router(config)#
```

Copy Paste

Создадим пароль на **enable**.
Пусть будет тоже **cisco**:
«enable password cisco».

Time: 94:55:46 Power Cycle Devices Fast Forward Time

Realtime

Connections

Automatically Choose Connection Type

Scenario 0 New Delete Toggle PDU List Window

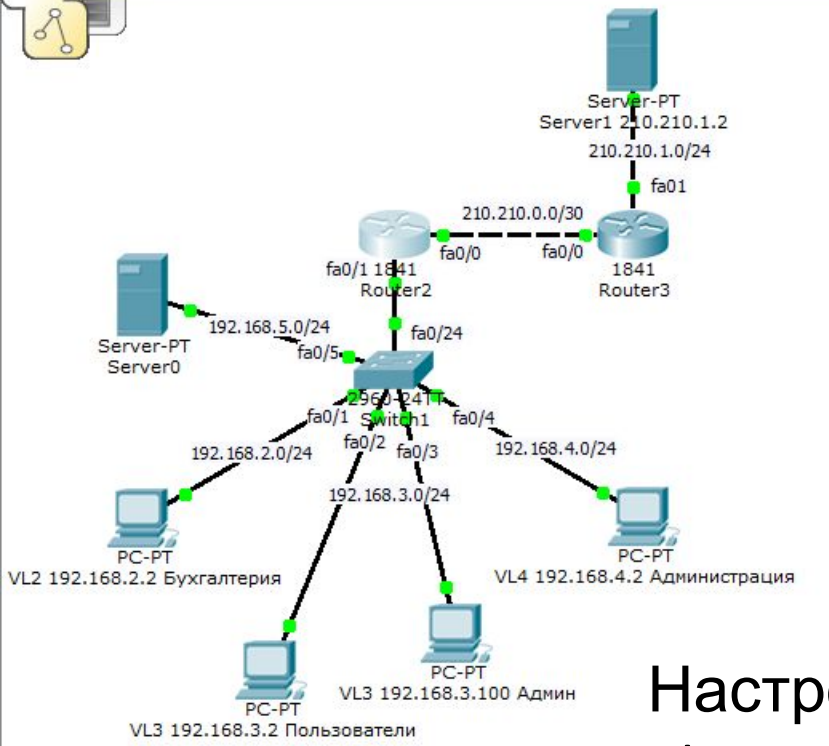
Fire | Last Status | Source | Destination | Type | Color | Time (sec) | Periodic | Num | Edit | Delete

ENG 21:03 17.12.2019

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

File Edit Options View Tools Extensions Help

Logical [Root]



Router2

Physical Config CLI

IOS Command Line Interface

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#en
Router(config)#ena
Router(config)#enable pass
Router(config)#enable password cisco
Router(config)#line ?
  <2-499>  First Line number
  aux      Auxiliary line
  console  Primary terminal line
  tty      Terminal controller
  vty      Virtual terminal
  x/y/z    Slot/Subslot/Port for Modems
Router(config)#line vty ?
  <0-15>  First Line number
Router(config)#line vty 0 ?
  <1-15>  Last Line number
  <cr>
Router(config)#line vty 0 4
Router(config-line)#login LOCAL
Router(config-line)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Copy Paste

Настроим удалённый доступ:
«line vty 0 4»,
«login LOCAL»,
«end».

Time: 95:05:30 Power Cycle Devices Fast Forward Time

Realtime

Connections

Automatically Choose Connection Type

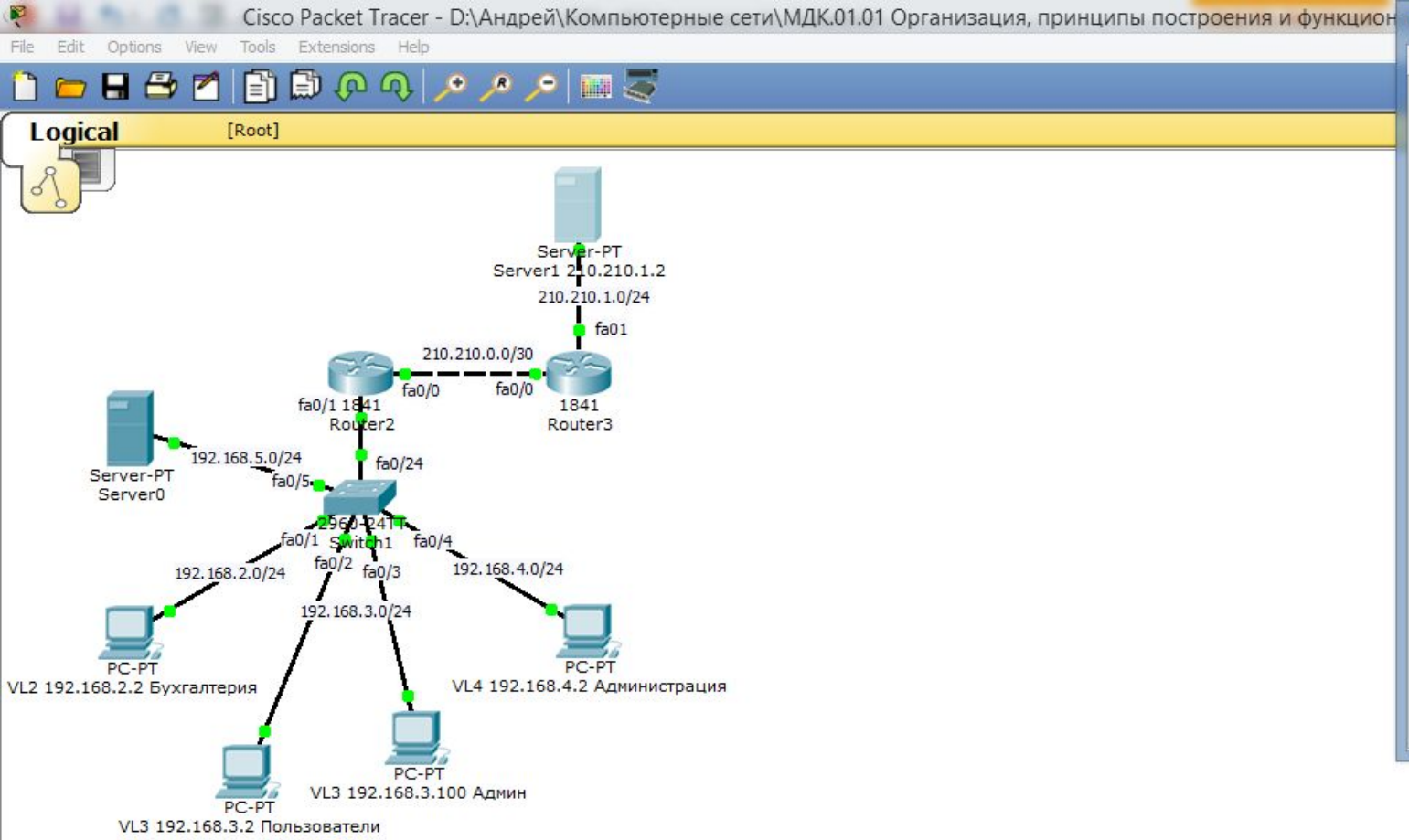
Scenario 0

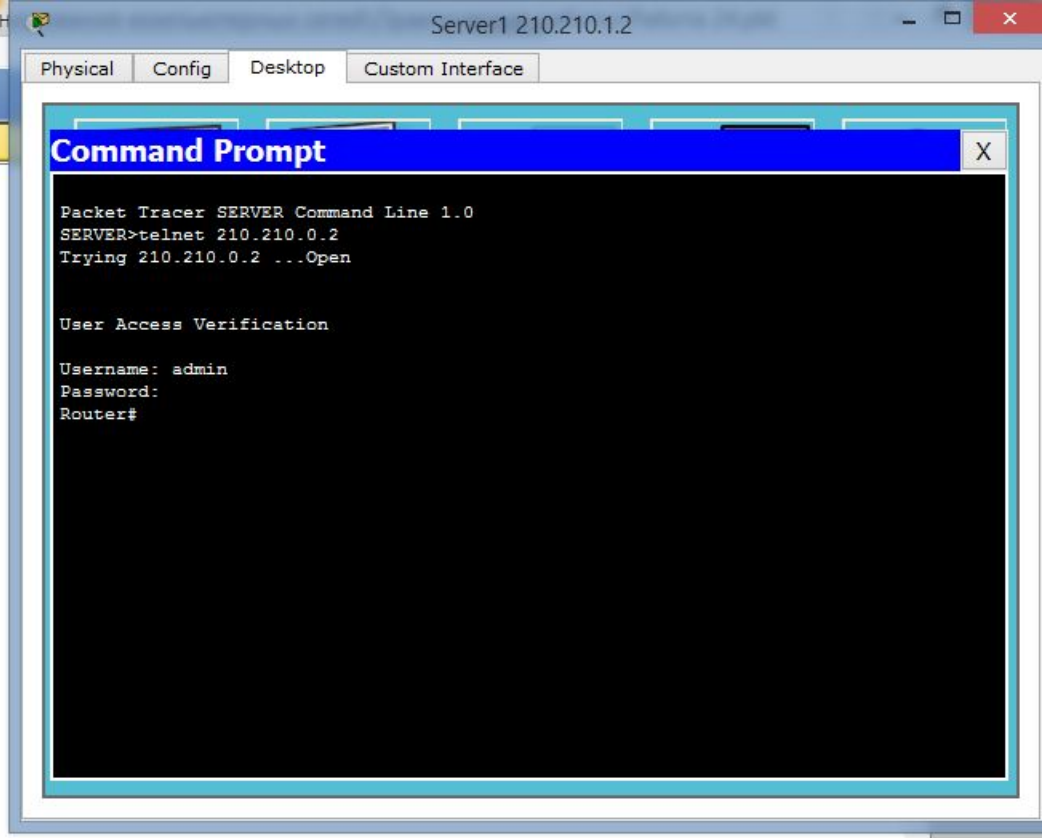
New Delete

Toggle PDU List Window

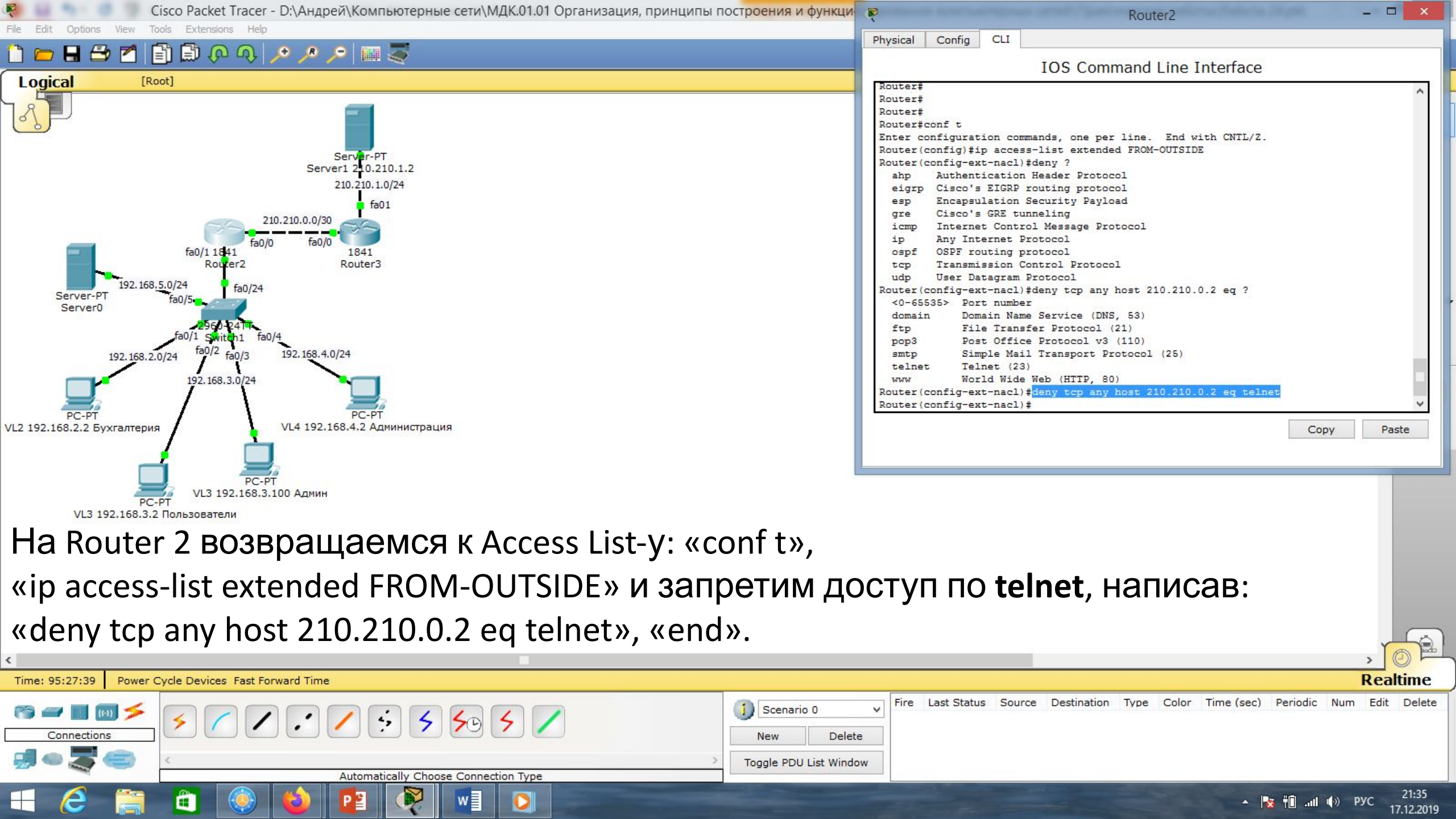
Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete

ENG 21:12 17.12.2019





Опробуем доступ с публичного сервера на наш роутер: «telnet 210.210.0.2», «Username: admin», «Password: cisco». Связь есть. Это плохо. Попробуем запретить доступ по **telnet** из внешней сети.

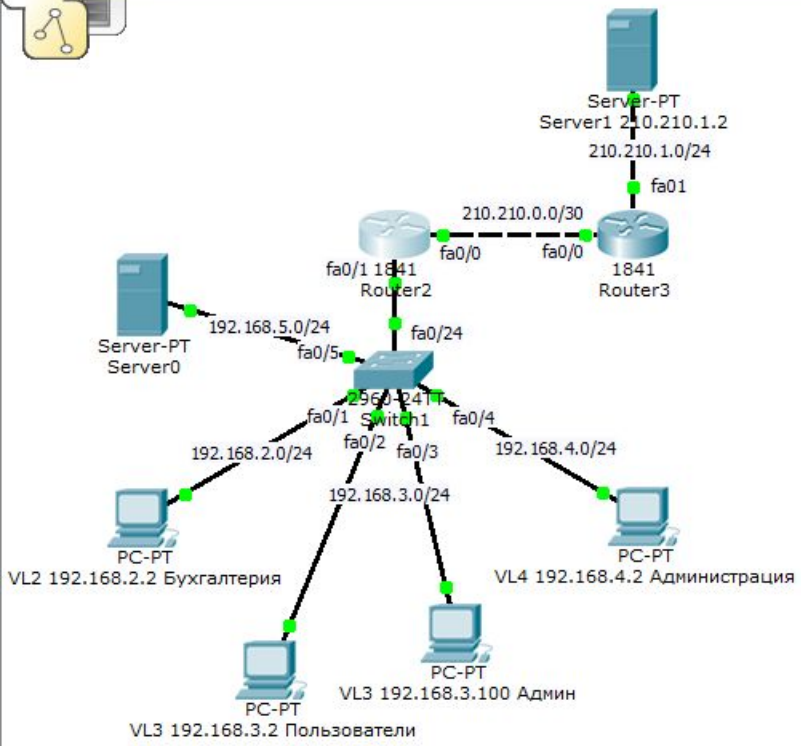


На Router 2 возвращаемся к Access List-у: «conf t»,
«ip access-list extended FROM-OUTSIDE» и запретим доступ по **telnet**, написав:
«deny tcp any host 210.210.0.2 eq telnet», «end».

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

File Edit Options View Tools Extensions Help

Logical [Root]



Router2

Physical Config CLI

IOS Command Line Interface

```
!
interface Vlan1
 no ip address
 shutdown
!
ip nat inside source list FOR-NAT interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 210.210.0.1
!
!
ip access-list standard FOR-NAT
 permit 192.168.2.0 0.0.0.255
 permit 192.168.3.0 0.0.0.255
 permit 192.168.4.0 0.0.0.255
ip access-list extended FROM-OUTSIDE
 permit ip any host 210.210.0.2
 deny tcp any host 210.210.0.2 eq telnet
!
!
!
!
!
line con 0
!
line aux 0
 --More--
```

Copy Paste

Взглянем на Access List-ы:

«show run», видим, что запрещающий Access List мы прописали.

Time: 95:30:57 Power Cycle Devices Fast Forward Time

Realtime

Connections

Automatically Choose Connection Type

Scenario 0

New Delete

Toggle PDU List Window

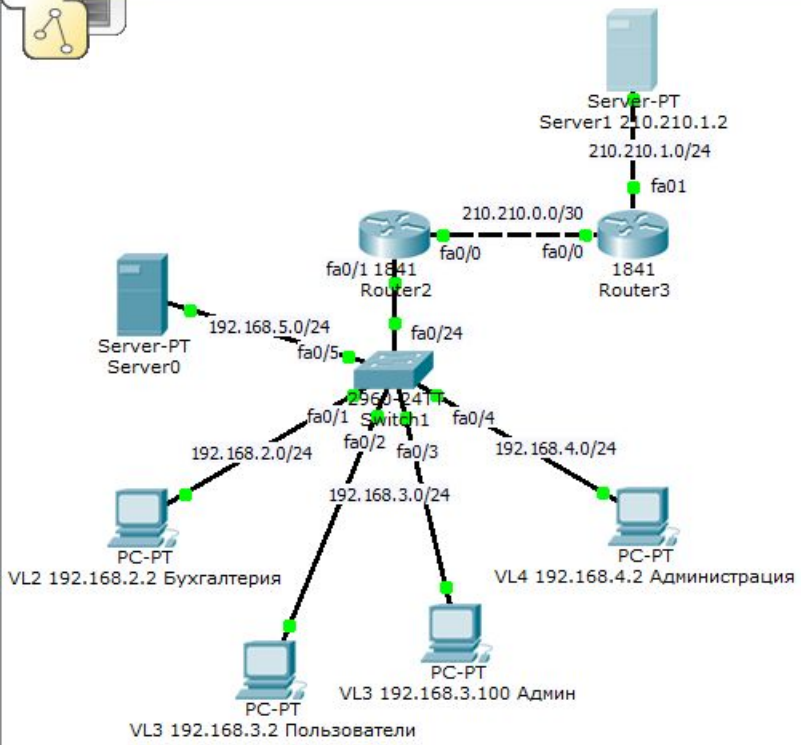
Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete

ENG 21:38 17.12.2019

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

File Edit Options View Tools Extensions Help

Logical [Root]



Server1 210.210.1.2

Physical Config Desktop Custom Interface

Command Prompt

```
Packet Tracer SERVER Command Line 1.0
SERVER>telnet 210.210.0.2
Trying 210.210.0.2 ...Open


User Access Verification

Username: admin
Password:
Router#

[Connection to 210.210.0.2 closed by foreign host]
SERVER>
SERVER>
SERVER>telnet 210.210.0.2
Trying 210.210.0.2 ...Open


User Access Verification

Username: admin
Password:
Router#
```

Ещё раз проверим доступ по **telnet** с публичного сервера на наш роутер: «telnet 210.210.0.2», «Username: admin», «Password: cisco». Доступ по-прежнему есть. **Почему???**

Time: 95:35:11 | Power Cycle Devices Fast Forward Time | Realtime

Connections

Automatically Choose Connection Type

Scenario 0 | New | Delete | Toggle PDU List Window

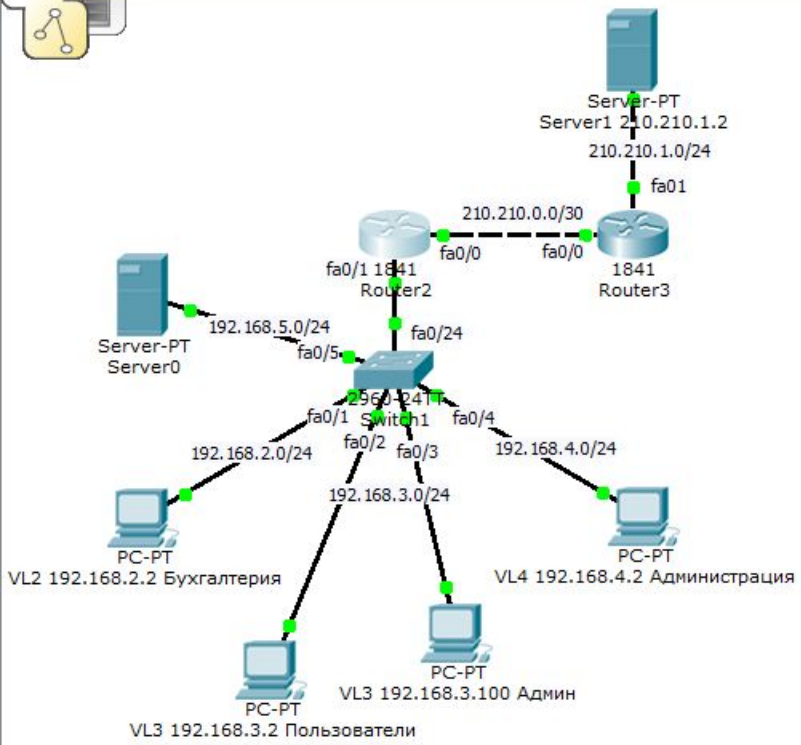
Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete

ENG 21:42 17.12.2019

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

File Edit Options View Tools Extensions Help

Logical [Root]



Router2

Physical Config CLI

IOS Command Line Interface

```
!
interface Vlan1
 no ip address
 shutdown
!
ip nat inside source list FOR-NAT interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 210.210.0.1
!
!
ip access-list standard FOR-NAT
 permit 192.168.2.0 0.0.0.255
 permit 192.168.3.0 0.0.0.255
 permit 192.168.4.0 0.0.0.255
ip access-list extended FROM-OUTSIDE
 permit ip any host 210.210.0.2
 deny tcp any host 210.210.0.2 eq telnet
!
!
!
!
!
line con 0
!
line aux 0
 --More--
```

Copy Paste

Если внимательно посмотрим на Access List-ы:
«show run», то увидим, что запрещающее правило находится под разрешающим, которое разрешает весь трафик. Более специфические правила должны быть выше.

Power Cycle Devices Fast Forward Time

Realtime

Connections

Automatically Choose Connection Type

Scenario 0 New Delete Toggle PDU List Window

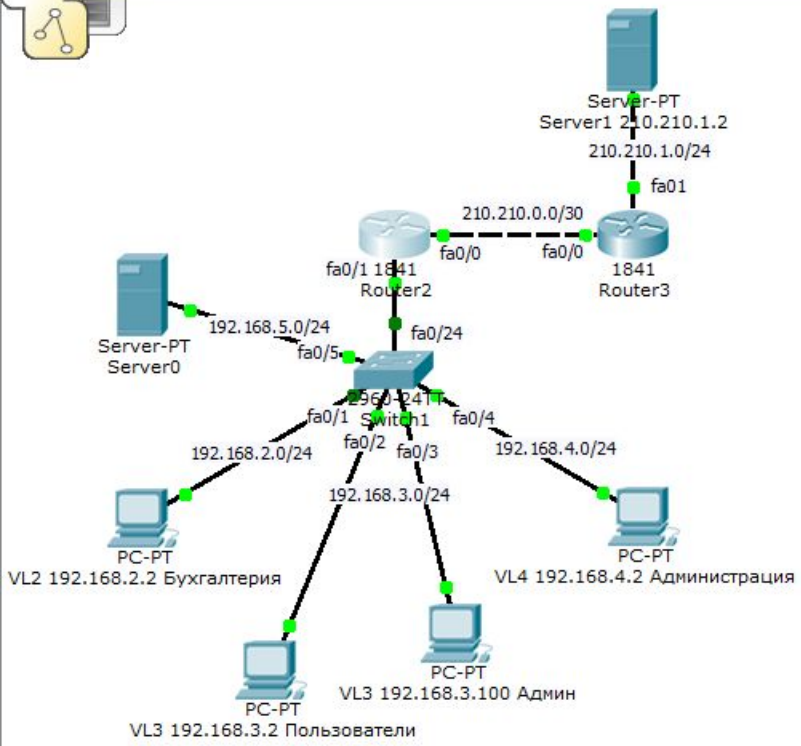
Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete

ENG 21:38 17.12.2019

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

File Edit Options View Tools Extensions Help

Logical [Root]



Router2

Physical Config CLI

IOS Command Line Interface

```
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#no ip access-list extended FROM-OUTSIDE
Router(config)#
Router(config)#ip access-list extended FROM-OUTSIDE
Router(config-ext-nacl)#deny tcp any host 210.210.0.2 eq telnet
Router(config-ext-nacl)#permit ip any host 210.210.0.2
Router(config-ext-nacl)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

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

Copy Paste

Чтобы это сделать, удалим Access List, создадим его снова и поменять правила местами: «conf t», «no ip access-list extended FROM-OUTSIDE», «ip access-list extended FROM-OUTSIDE», «deny tcp any host 210.210.0.2 eq telnet», «permit ip any host 210.210.0.2», «end», «wr mem».

Time: 95:48:58 Power Cycle Devices Fast Forward Time

Realtime

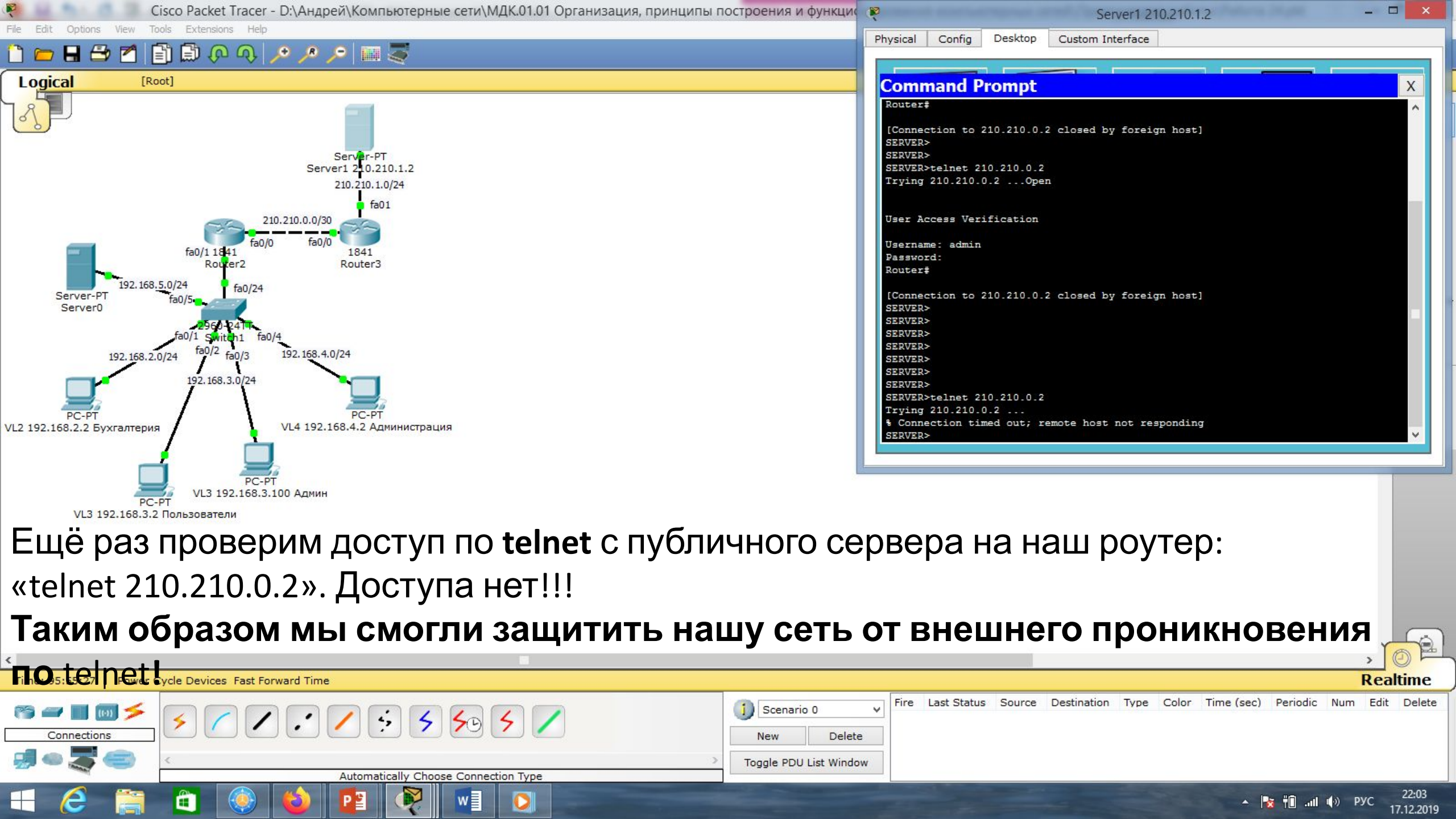
Connections

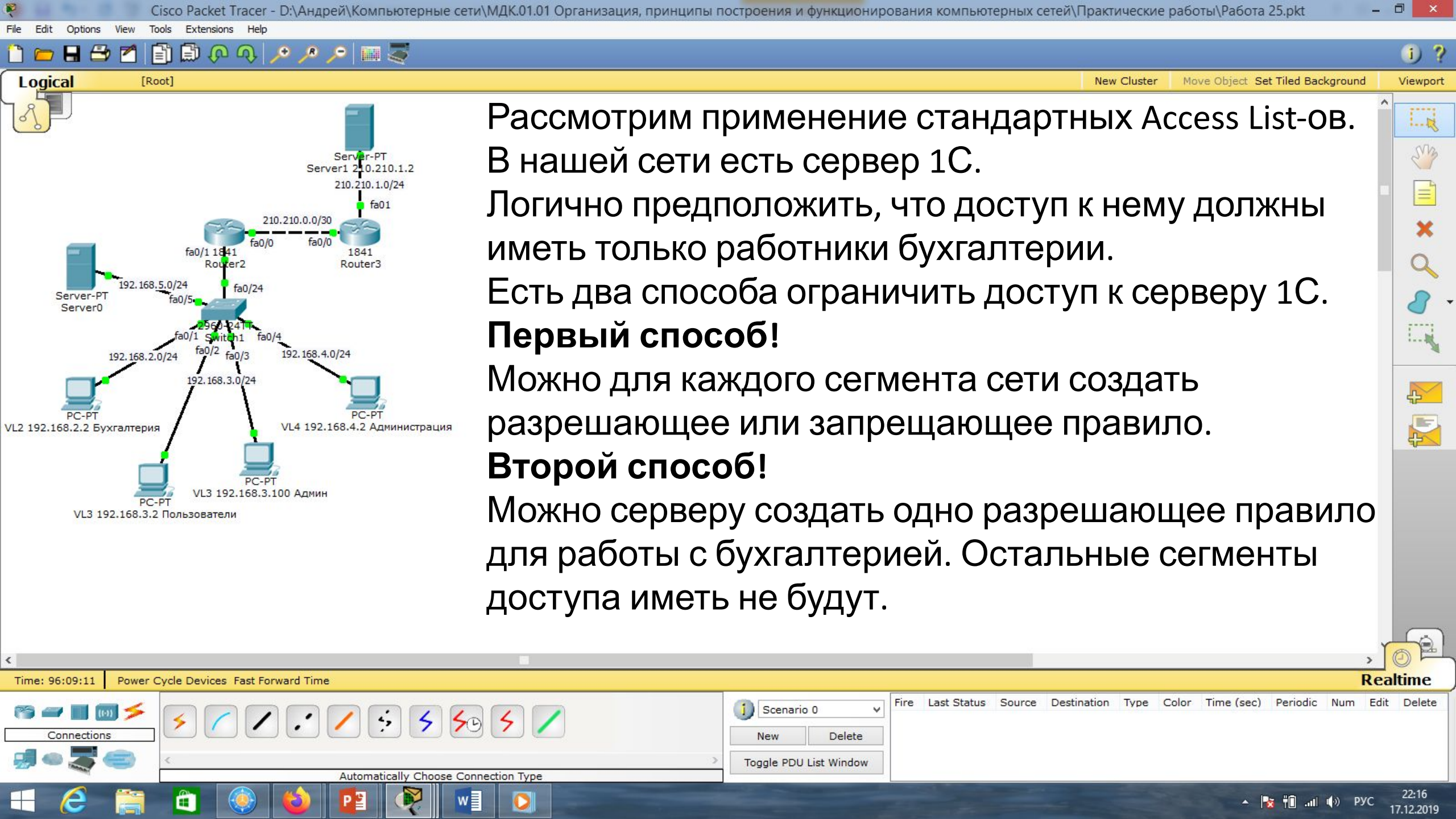
Automatically Choose Connection Type

Scenario 0 New Delete Toggle PDU List Window

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

ENG 21:56 17.12.2019

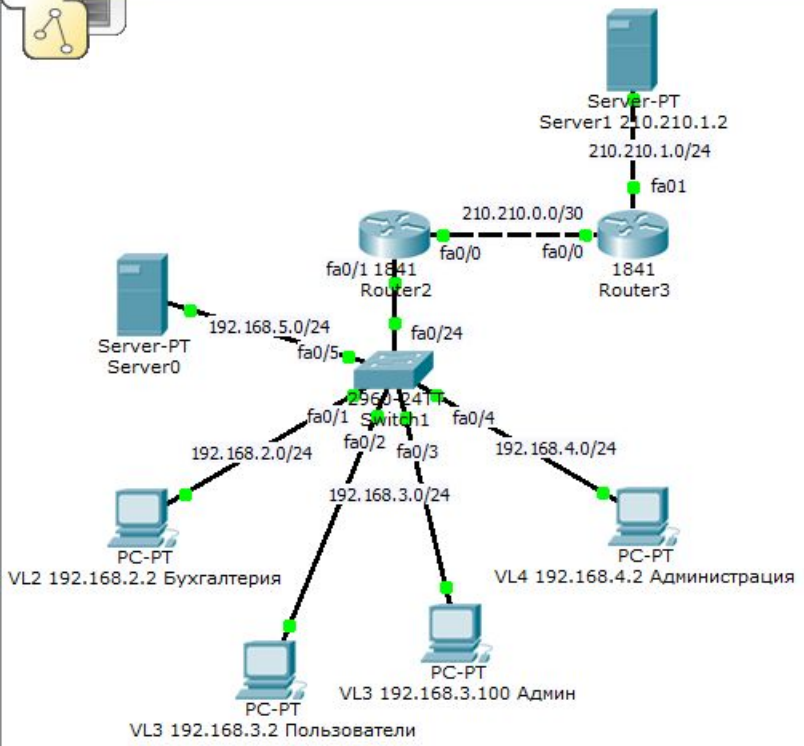

Cisco Packet Tracer - D:\Андрей\Компьютерные сети\МДК.01.01 Организация, принципы построения и функцио
File Edit Options View Tools Extensions Help
Logical [Root]
Server-PT
Server1 210.210.1.2
210.210.1.0/24
fa01
210.210.0.0/30
fa0/1 1841
Router2
fa0/0
fa0/0
1841
Router3
Server-PT
Server0
192.168.5.0/24
fa0/5
fa0/24
2960-24TT
Switch1
fa0/1
fa0/2
fa0/3
fa0/4
192.168.2.0/24
192.168.3.0/24
192.168.4.0/24
PC-PT
VL2 192.168.2.2 Бухгалтерия
PC-PT
VL4 192.168.4.2 Администрация
PC-PT
VL3 192.168.3.100 Админ
PC-PT
VL3 192.168.3.2 Пользователи
Server1 210.210.1.2
Physical Config Desktop Custom Interface
Command Prompt
X
Router#
[Connection to 210.210.0.2 closed by foreign host]
SERVER>
SERVER>
SERVER>telnet 210.210.0.2
Trying 210.210.0.2 ...Open
User Access Verification
Username: admin
Password:
Router#
[Connection to 210.210.0.2 closed by foreign host]
SERVER>
SERVER>
SERVER>
SERVER>
SERVER>
SERVER>
SERVER>
SERVER>telnet 210.210.0.2
Trying 210.210.0.2 ...
% Connection timed out; remote host not responding
SERVER>
Ещё раз проверим доступ по telnet с публичного сервера на наш роутер: «telnet 210.210.0.2». Доступа нет!!!
Таким образом мы смогли защитить нашу сеть от внешнего проникновения по telnet!
Power Cycle Devices Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time (sec) Periodic Num Edit Delete
РУС
22:03
17.12.2019


Cisco Packet Tracer - D:\Андрей\Компьютерные сети\МДК.01.01 Организация, принципы построения и функционирования компьютерных сетей\Практические работы\Работа 25.pkt
File Edit Options View Tools Extensions Help
Logical [Root]
New Cluster Move Object Set Tiled Background Viewport
Server-PT Server1 210.210.1.2
210.210.1.0/24
fa01
210.210.0.0/30
fa0/1 1841 Router2
fa0/0
fa0/0
1841 Router3
Server-PT Server0
192.168.5.0/24
fa0/5
fa0/24
2960-24TT Switch1
fa0/1
fa0/2
fa0/3
fa0/4
192.168.2.0/24
192.168.3.0/24
192.168.4.0/24
PC-PT VL2 192.168.2.2 Бухгалтерия
PC-PT VL4 192.168.4.2 Администрация
PC-PT VL3 192.168.3.100 Админ
PC-PT VL3 192.168.3.2 Пользователи
Рассмотрим применение стандартных Access List-ов.
В нашей сети есть сервер 1С.
Логично предположить, что доступ к нему должны иметь только работники бухгалтерии.
Есть два способа ограничить доступ к серверу 1С.
Первый способ!
Можно для каждого сегмента сети создать разрешающее или запрещающее правило.
Второй способ!
Можно серверу создать одно разрешающее правило для работы с бухгалтерией. Остальные сегменты доступа иметь не будут.
Time: 96:09:11 Power Cycle Devices Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time (sec) Periodic Num Edit Delete
РУС
22:16
17.12.2019

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

File Edit Options View Tools Extensions Help

Logical [Root]



Router2

Physical Config CLI

IOS Command Line Interface

```
Press RETURN to get started.



Router>en
Password:
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip acc
Router(config)#ip access-list st
Router(config)#ip access-list standard TO-1C
Router(config-std-nacl)#per
Router(config-std-nacl)#permit 192.168.2.0 0.0.0.255
Router(config-std-nacl)#exit
Router(config)#
Router(config)#
```

Copy Paste

Настроим Router 2:
«conf t»,
создадим Access List
с именем TO-1C:
«ip access-list standard TO-1C»,
Создаём разрешающий трафик из бухгалтерии:
«permit 192.168.2.0 0.0.0.255», «exit».
Остальные сегменты сети будут запрещены.

Time: 96:17:03 Power Cycle Devices Fast Forward Time

Realtime

Connections

Automatically Choose Connection Type

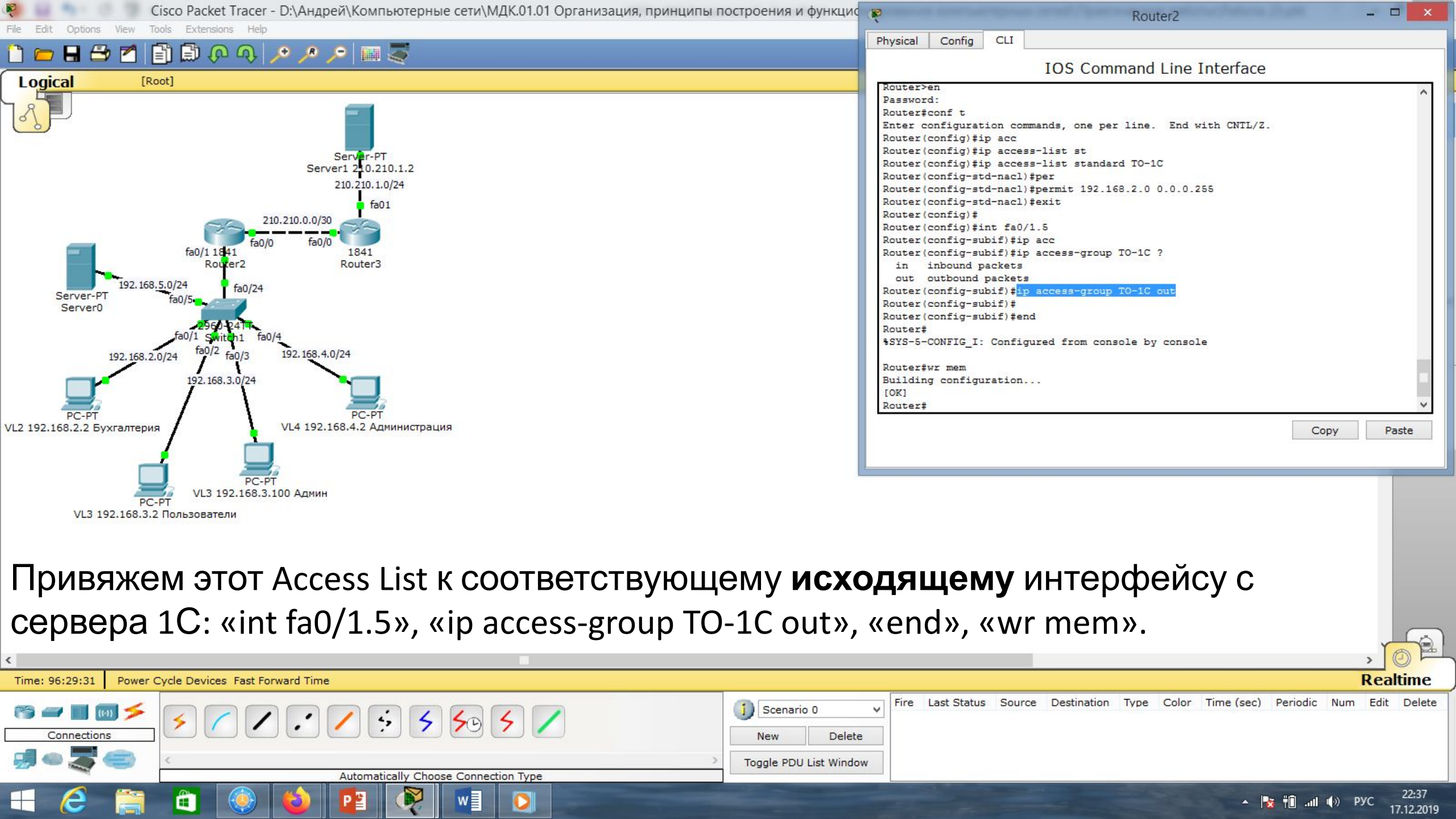
Scenario 0

New Delete

Toggle PDU List Window

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

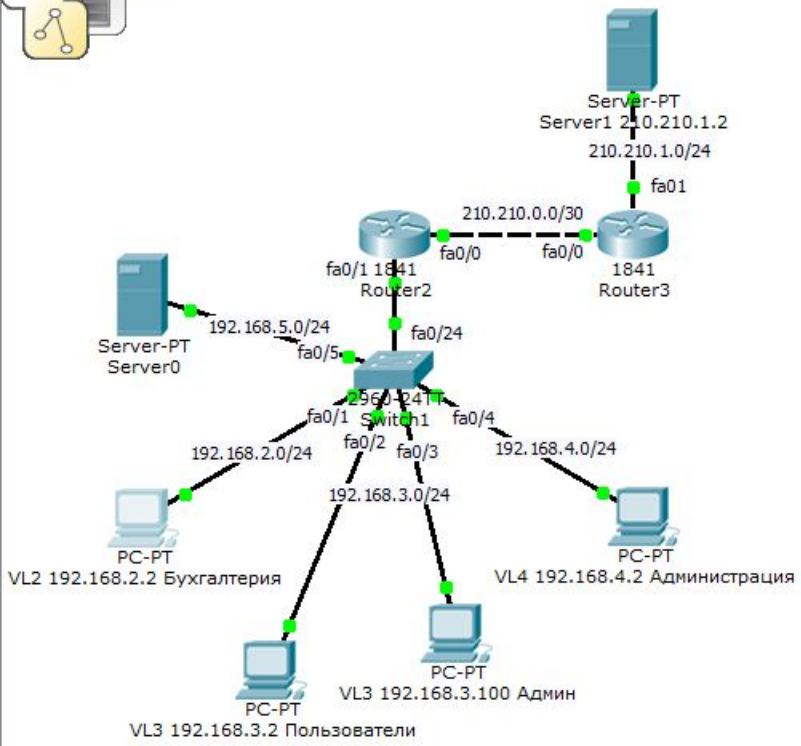
ENG 22:24 17.12.2019


Cisco Packet Tracer - D:\Андрей\Компьютерные сети\МДК.01.01 Организация, принципы построения и функцио
File Edit Options View Tools Extensions Help
Logical [Root]
Server-PT
Server1 210.210.1.2
210.210.1.0/24
fa01
210.210.0.0/30
fa0/1 1841
Router2
fa0/0
fa0/0
1841
Router3
Server-PT
Server0
192.168.5.0/24
fa0/5
fa0/24
2960-24TT
Switch1
fa0/1
fa0/2
fa0/3
fa0/4
192.168.2.0/24
192.168.3.0/24
192.168.4.0/24
PC-PT
VL2 192.168.2.2 Бухгалтерия
PC-PT
VL4 192.168.4.2 Администрация
PC-PT
VL3 192.168.3.100 Админ
PC-PT
VL3 192.168.3.2 Пользователи
Router2
Physical
Config
CLI
IOS Command Line Interface
Router>en
Password:
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip acc
Router(config)#ip access-list st
Router(config)#ip access-list standard TO-1C
Router(config-std-nacl)#per
Router(config-std-nacl)#permit 192.168.2.0 0.0.0.255
Router(config-std-nacl)#exit
Router(config)#
Router(config)#int fa0/1.5
Router(config-subif)#ip acc
Router(config-subif)#ip access-group TO-1C ?
in inbound packets
out outbound packets
Router(config-subif)#ip access-group TO-1C out
Router(config-subif)#
Router(config-subif)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#wr mem
Building configuration...
[OK]
Router#
Copy
Paste
Привяжем этот Access List к соответствующему исходящему интерфейсу с сервера 1С: «int fa0/1.5», «ip access-group TO-1C out», «end», «wr mem».
Time: 96:29:31
Power Cycle Devices Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
Periodic
Num
Edit
Delete
РУС
22:37
17.12.2019

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

File Edit Options View Tools Extensions Help

Logical [Root]



VL2 192.168.2.2 Бухгалтерия

Physical Config Desktop Custom Interface

Command Prompt

```
Pinging 192.168.5.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.5.2: bytes=32 time=0ms TTL=127
Reply from 192.168.5.2: bytes=32 time=0ms TTL=127
Reply from 192.168.5.2: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Reply from 192.168.5.2: bytes=32 time=0ms TTL=127
Reply from 192.168.5.2: bytes=32 time=0ms TTL=127
Reply from 192.168.5.2: bytes=32 time=0ms TTL=127
Reply from 192.168.5.2: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

Проверим связи компьютеров с сервером.
С сегментом бухгалтерии связь есть.

Time: 96:33:40 | Power Cycle Devices Fast Forward Time

Realtime

Connections

Automatically Choose Connection Type

Scenario 0 | New | Delete | Toggle PDU List Window

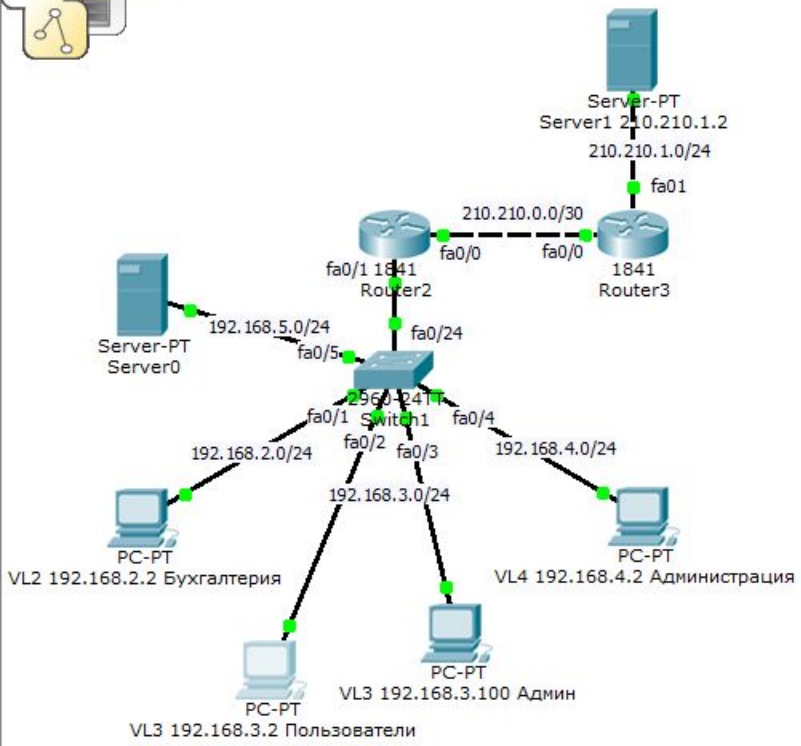
Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete

РУС 22:41 17.12.2019

Cisco Packet Tracer - D:\Андрей\Компьютерные сети\

File Edit Options View Tools Extensions Help

Logical [Root]



VL3 192.168.3.2 Пользователи

Physical Config Desktop Custom Interface

Command Prompt

```
PC>
PC>
PC>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

VL4 192.168.4.2 Администрация

Physical Config Desktop Custom Interface

Command Prompt

```
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=1ms TTL=126
Reply from 210.210.1.2: bytes=32 time=0ms TTL=126
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 = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Остальные сегменты сети связи с сервером 1С не имеют.

Таким образом мы ограничили доступ к 1С серверов всех сегментов сети кроме бухгалтерии!!!

Time: 96:36:29 Power Cycle Devices Fast Forward Time

Realtime

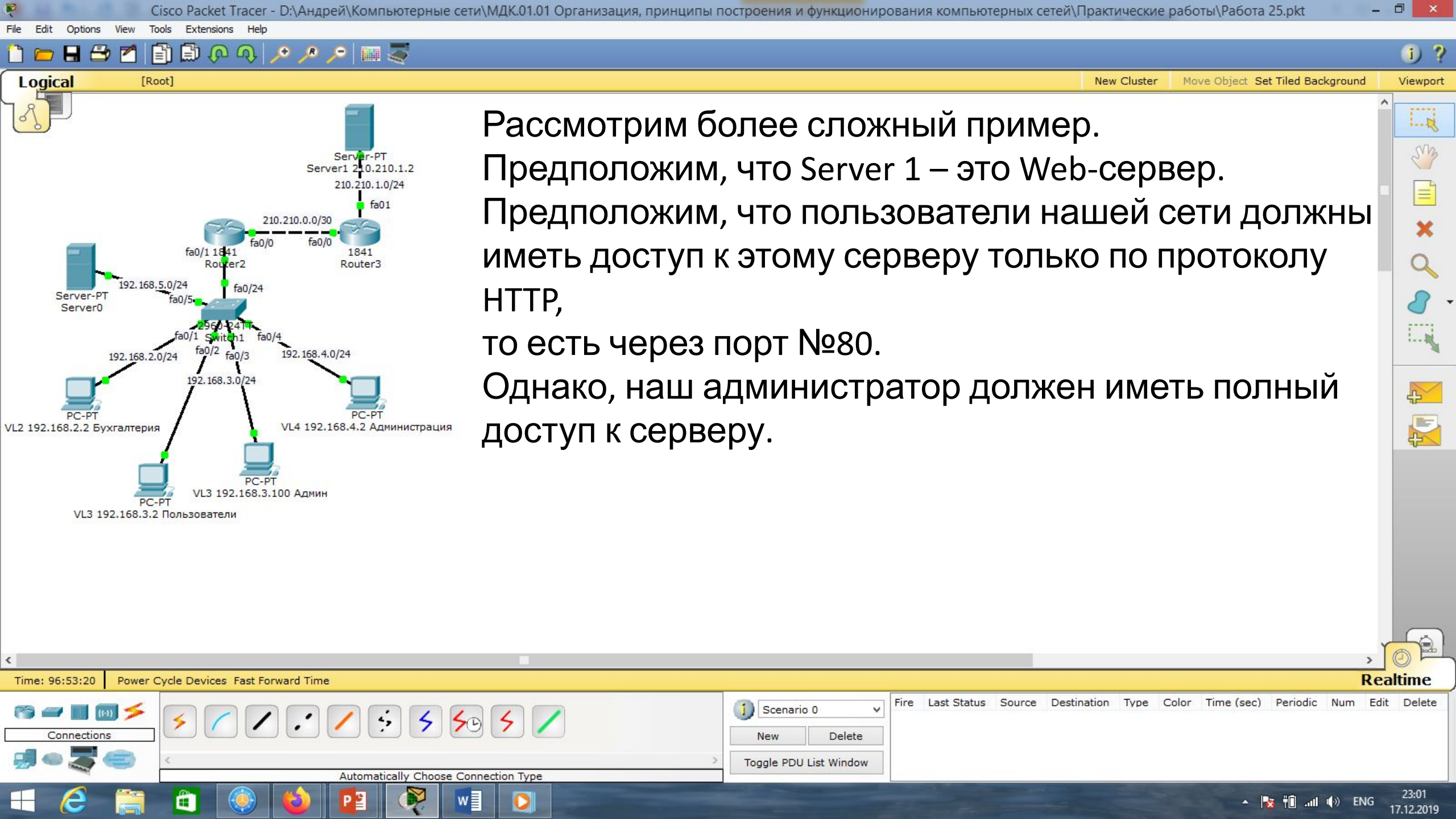
Connections

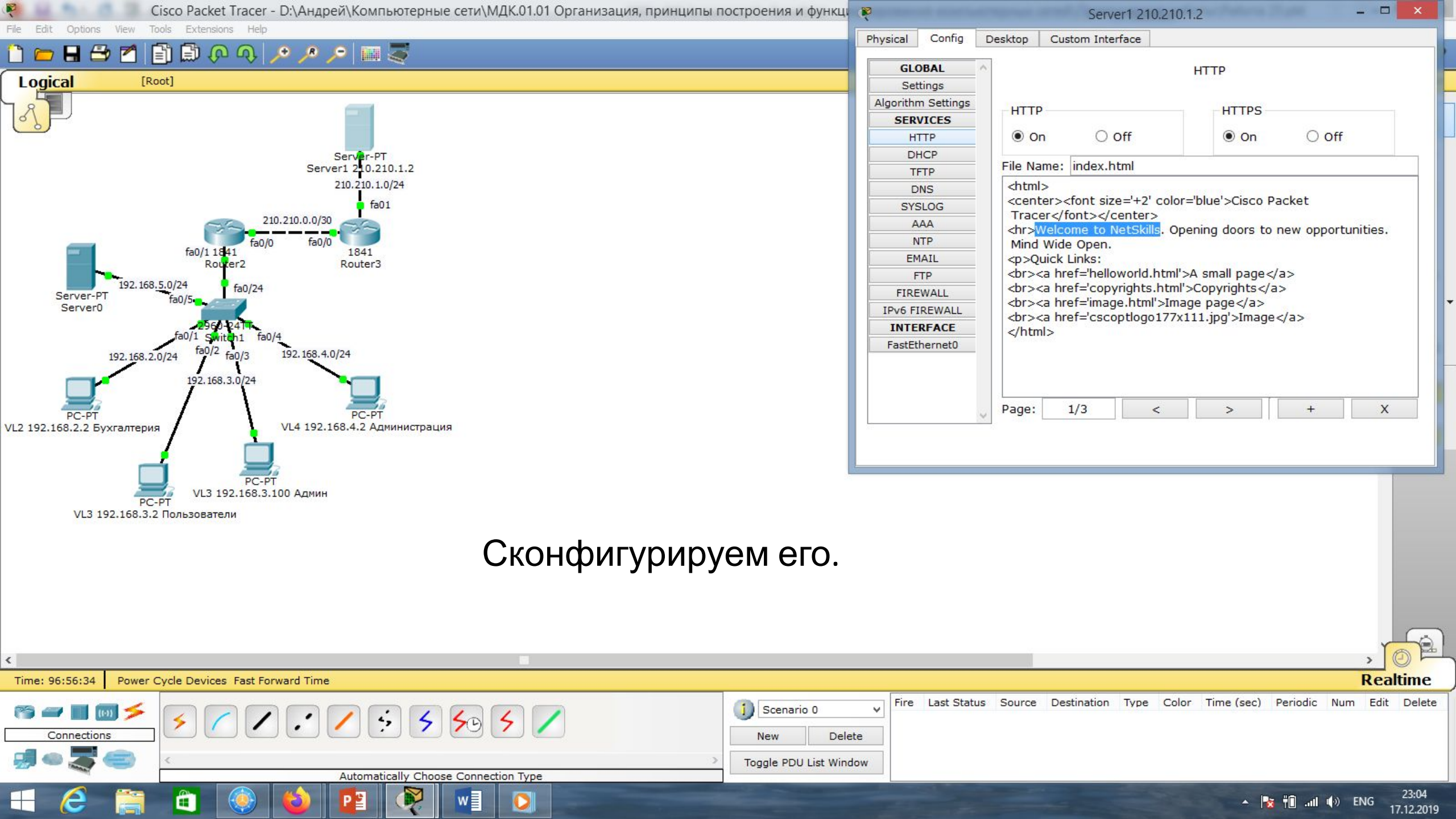
Automatically Choose Connection Type

Scenario 0 New Delete Toggle PDU List Window

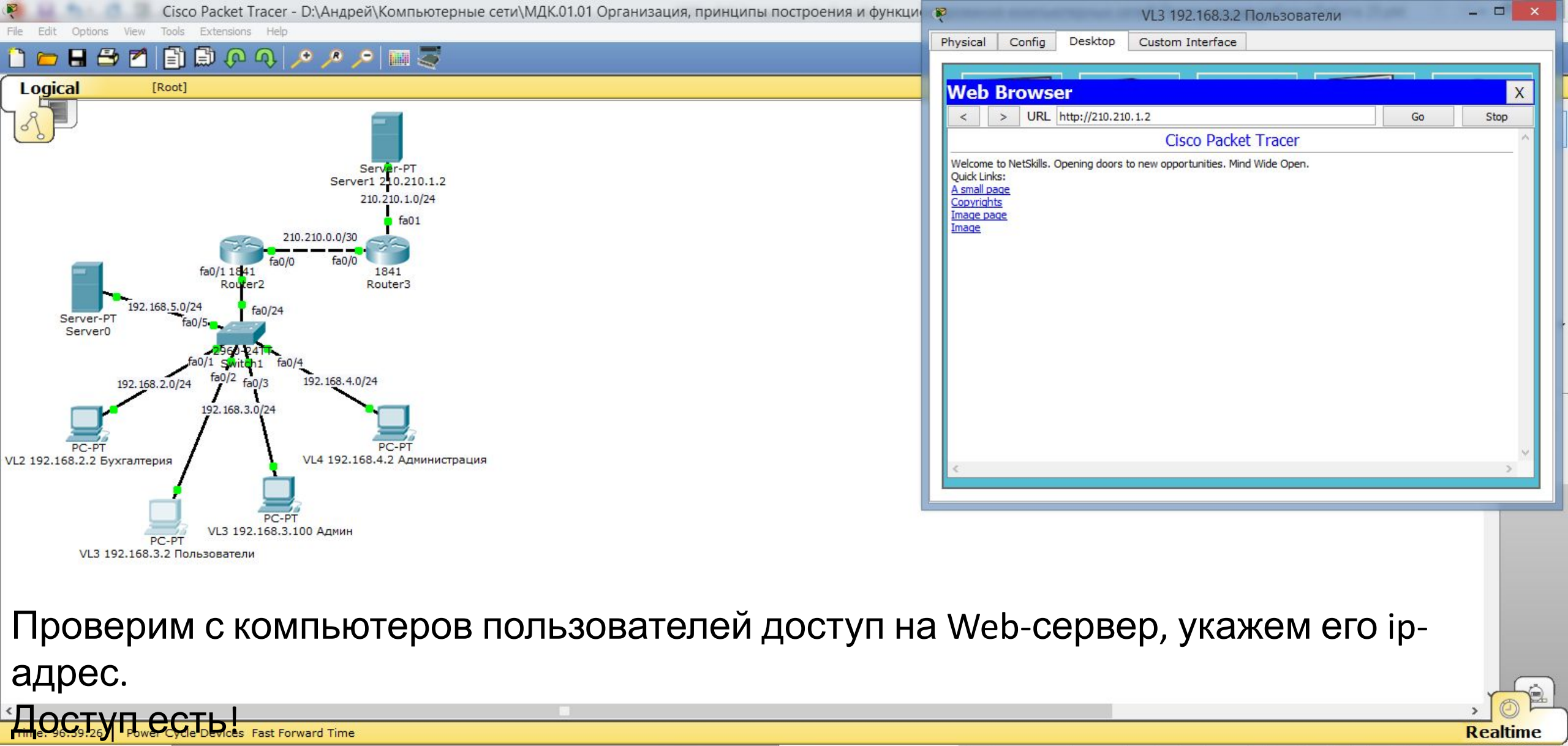
Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete

ENG 22:44 17.12.2019


Cisco Packet Tracer - D:\Андрей\Компьютерные сети\МДК.01.01 Организация, принципы построения и функционирования компьютерных сетей\Практические работы\Работа 25.pkt
File Edit Options View Tools Extensions Help
Logical [Root]
New Cluster Move Object Set Tiled Background Viewport
Server-PT
Server1 210.210.1.2
210.210.1.0/24
fa01
210.210.0.0/30
fa0/1 1841
Router2
fa0/0
fa0/0
1841
Router3
Server-PT
Server0
192.168.5.0/24
fa0/5
fa0/24
2960-24TT
Switch1
fa0/1
fa0/2
fa0/3
fa0/4
192.168.2.0/24
192.168.3.0/24
192.168.4.0/24
PC-PT
VL2 192.168.2.2 Бухгалтерия
PC-PT
VL4 192.168.4.2 Администрация
PC-PT
VL3 192.168.3.100 Админ
PC-PT
VL3 192.168.3.2 Пользователи
Рассмотрим более сложный пример.
Предположим, что Server 1 – это Web-сервер.
Предположим, что пользователи нашей сети должны иметь доступ к этому серверу только по протоколу HTTP,
то есть через порт №80.
Однако, наш администратор должен иметь полный доступ к серверу.
Time: 96:53:20 Power Cycle Devices Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time (sec) Periodic Num Edit Delete
ENG
23:01
17.12.2019



Сконфигурируем его.



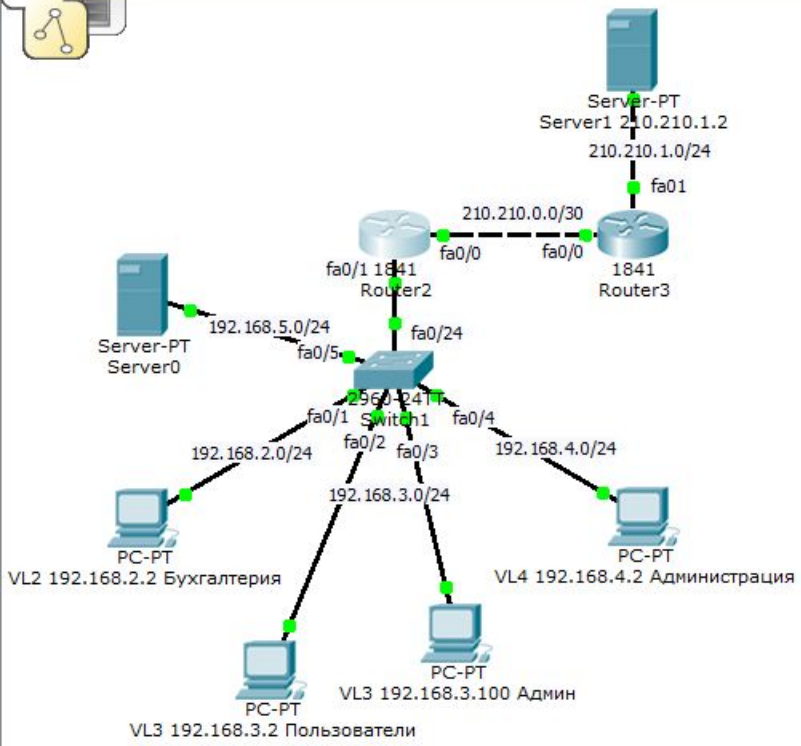
Проверим с компьютеров пользователей доступ на Web-сервер, укажем его ip-адрес.

Доступ есть!

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

File Edit Options View Tools Extensions Help

Logical [Root]



Router2

Physical Config CLI

IOS Command Line Interface

```
Router>en
Password:
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip acc
Router(config)#ip access-list ex
Router(config)#ip access-list extended FROM-USERS
Router(config-ext-nacl)#perm
Router(config-ext-nacl)#permit tcp 192.168.3.0 0.0.0.255 host 210.210.1.2 eq www

Router(config-ext-nacl)#permit ip 192.168.3.100 host 210.210.1.2
                                                              ^
% Invalid input detected at '^' marker.

Router(config-ext-nacl)#permit ip host 192.168.3.100 host 210.210.1.2
Router(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 host 210.210.1.2
Router(config-ext-nacl)#
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#
Router(config-ext-nacl)#exit
Router(config)#
```

Copy Paste

Настроим Router 2:
«conf t».
Создадим Access List с именем FROM-USERS:
«ip access-list extended FROM-USERS».

Разрешим трафик всем пользователям до Web-сервера через порт 80 (в cisco – это www):
«permit tcp 192.168.3.0 0.0.0.255 host 210.210.1.2 eq www»

Администратору разрешим весь доступ: «permit ip host 192.168.3.100 host 210.210.1.2», запретим пользователям трафик до Web-сервера кроме порта 80 «deny ip 192.168.3.0 0.0.0.255 host 210.210.1.2» и разрешим весь остальной трафик: «permit ip any any», «exit».

Time: 97:28:20 Power Cycle Devices Fast Forward Time

Realtime

Connections

Automatically Choose Connection Type

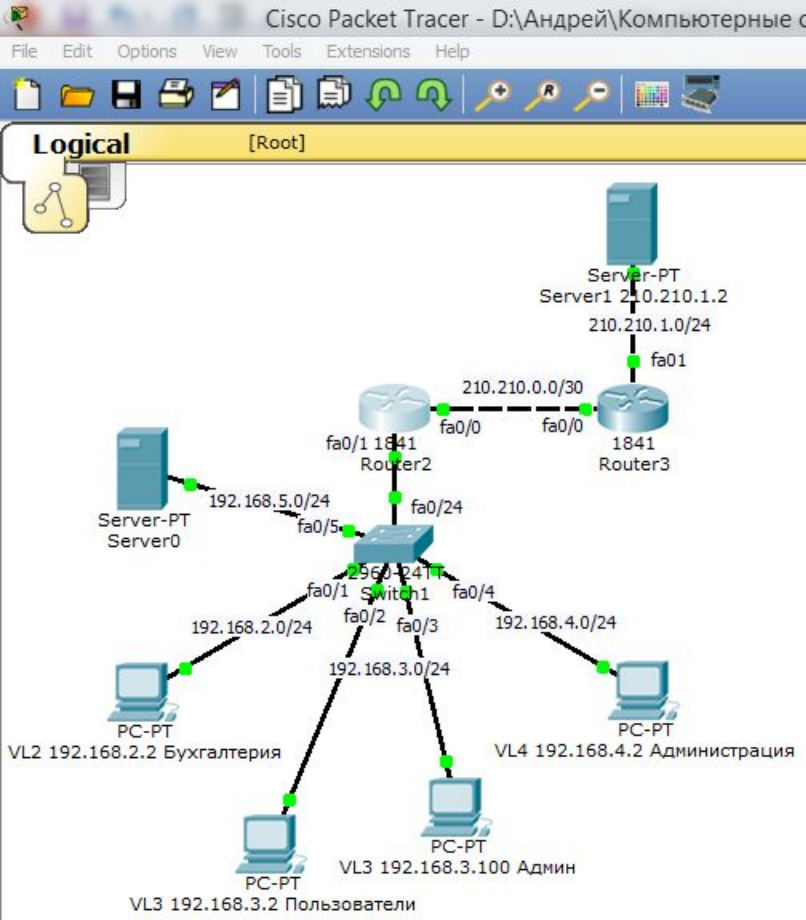
Scenario 0

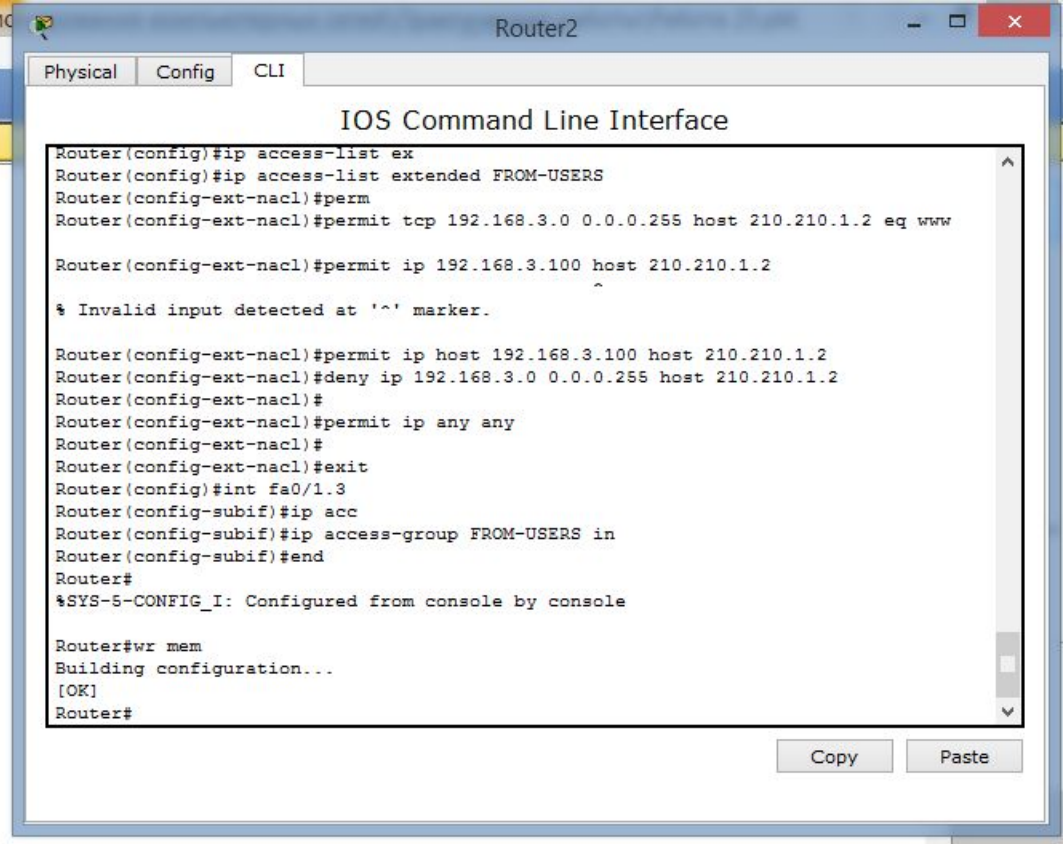
New Delete

Toggle PDU List Window

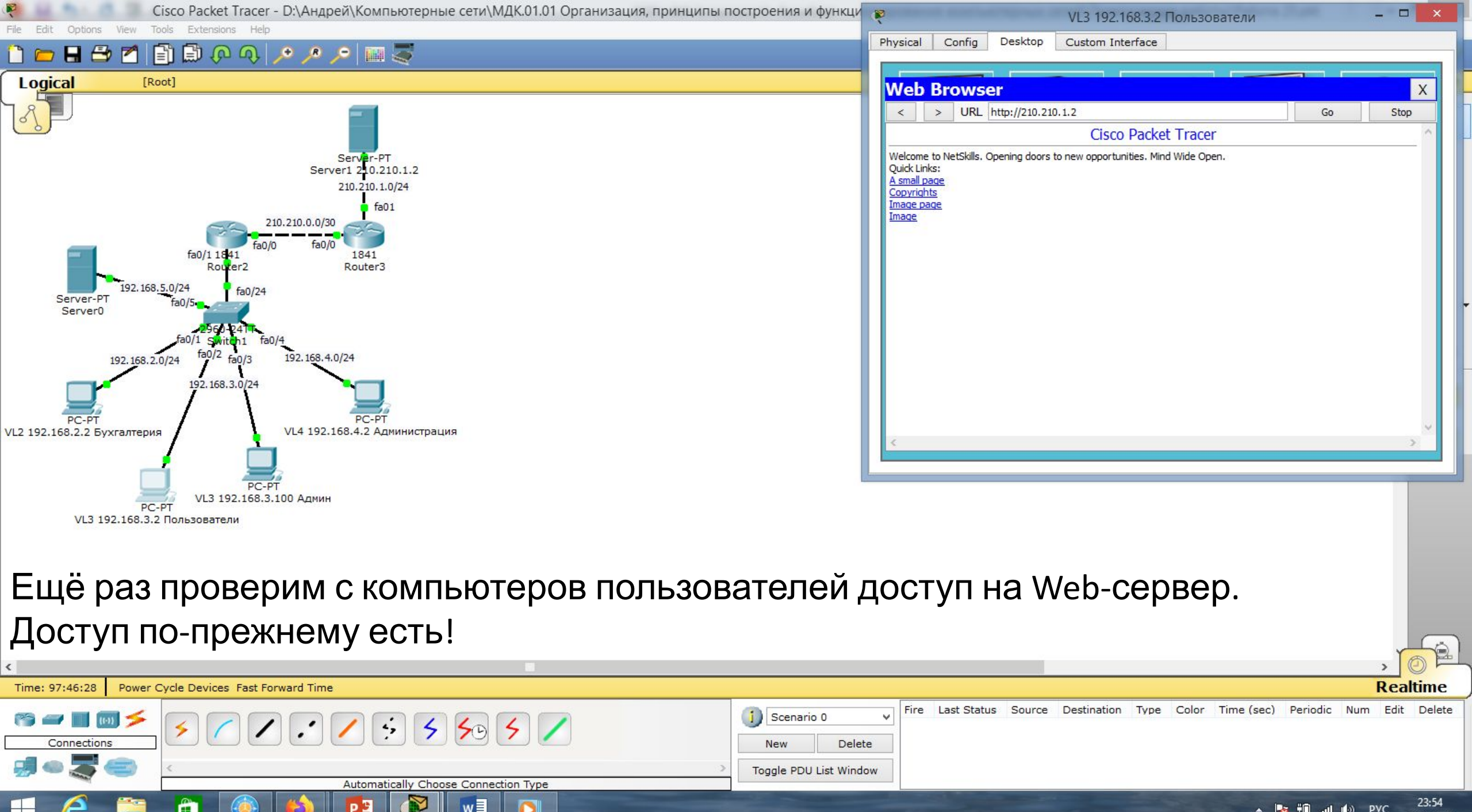
Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete

ENG 23:36 17.12.2019





Теперь нужно этот Access List привязать к интерфейсу:
«int fa0/1.3»,
«ip access-group FROM-USERS in» (на входящий трафик),
«end»,
«wr mem».

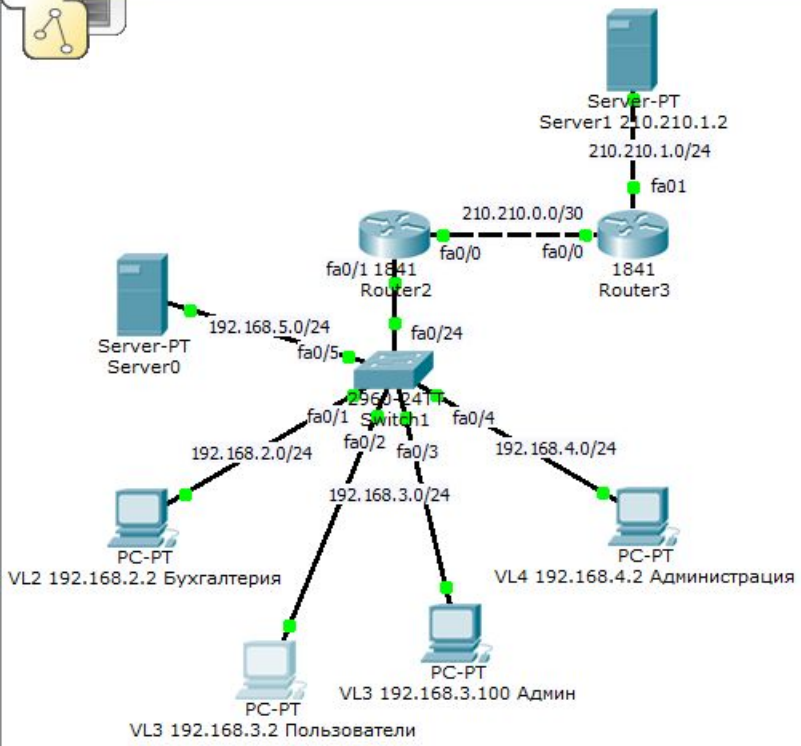


Ещё раз проверим с компьютеров пользователей доступ на Web-сервер.
Доступ по-прежнему есть!

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

File Edit Options View Tools Extensions Help

Logical [Root]



VL3 192.168.3.2 Пользователи

Physical Config Desktop Custom Interface

Command Prompt

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 210.210.1.2

Pinging 210.210.1.2 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

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

PC>
```

Проверим ping с компьютеров пользователей на Web-сервер.

Связи нет, так как мы это запретили!!!

Time: 97:49:57 Power Cycle Devices Fast Forward Time

Realtime

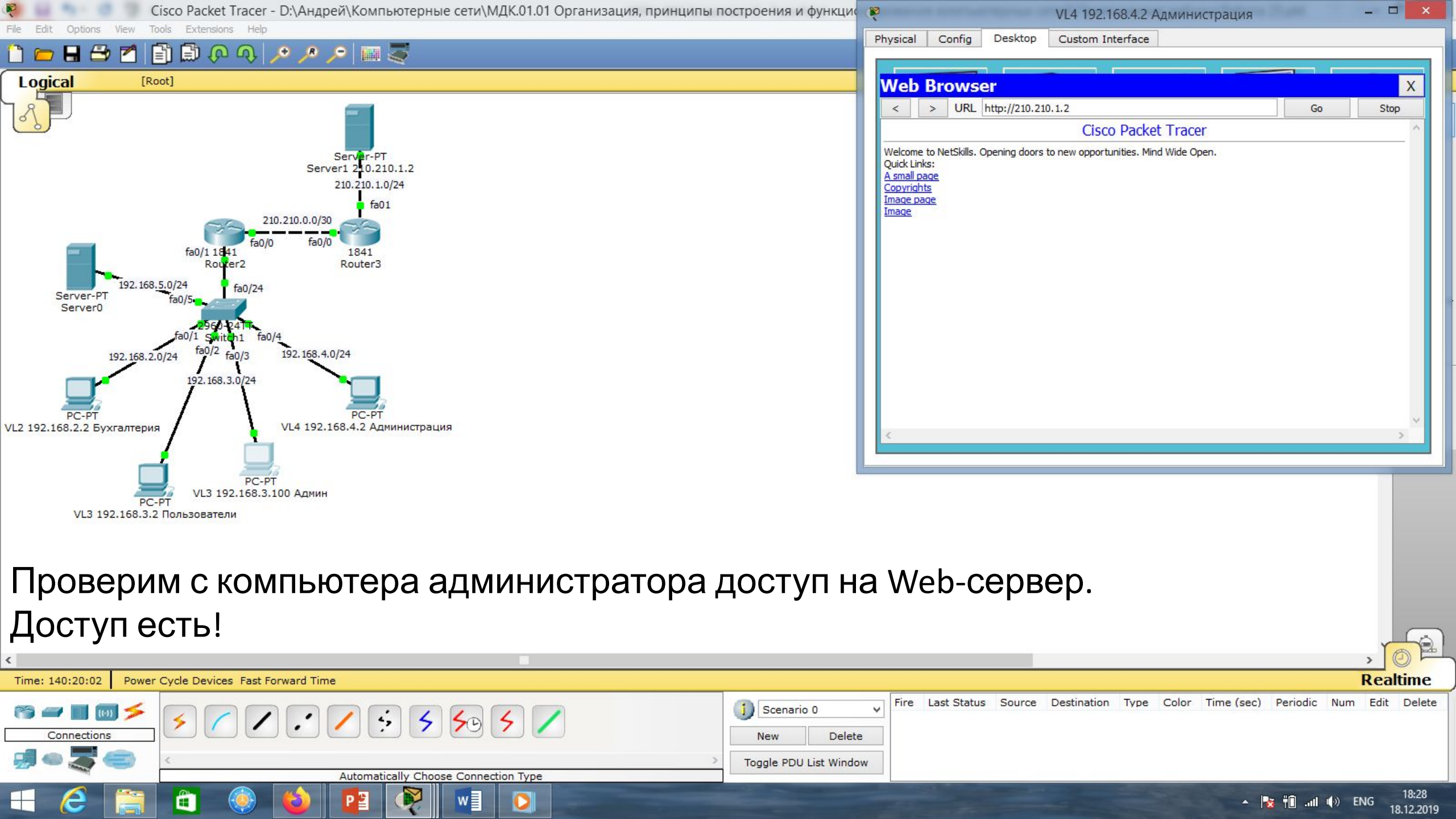
Connections

Automatically Choose Connection Type

Scenario 0 New Delete Toggle PDU List Window

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

РУС 23:58 17.12.2019

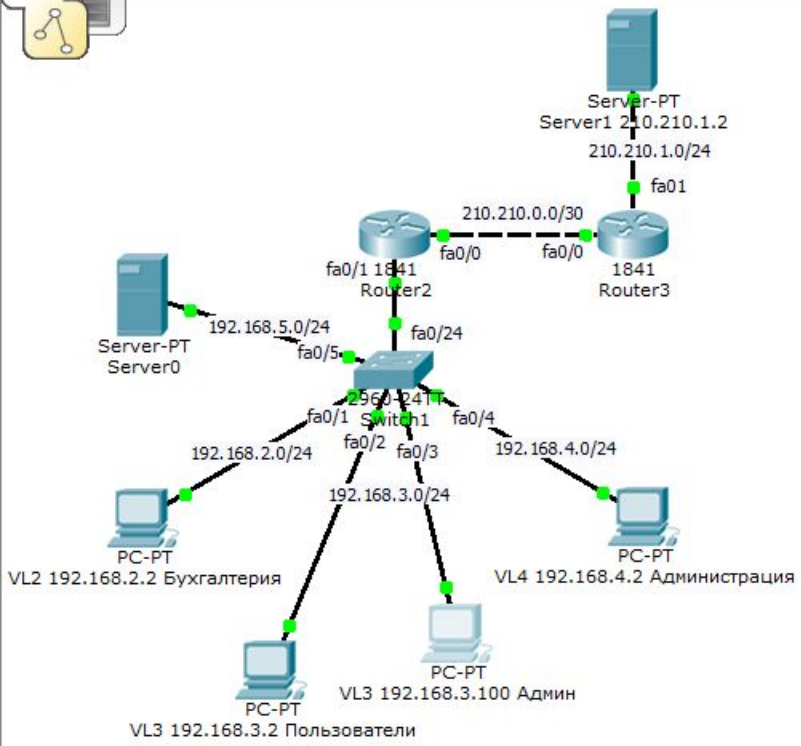


Проверим с компьютера администратора доступ на Web-сервер.
Доступ есть!

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

File Edit Options View Tools Extensions Help

Logical [Root]



VL4 192.168.4.2 Администрация

Physical Config Desktop Custom Interface

Command Prompt

```
Pinging 210.210.1.2 with 32 bytes of data:

Reply from 210.210.1.2: bytes=32 time=1ms TTL=126
Reply from 210.210.1.2: bytes=32 time=0ms TTL=126
Reply from 210.210.1.2: bytes=32 time=0ms 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 = 0ms, Maximum = 1ms, 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=0ms TTL=126
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 = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

PC>
```

Проверим ping с компьютера администратора на Web-сервер.

Связь сохранилась!!! Мы добивались именно этого!

Time: 140:23:36 | Power Cycle Devices Fast Forward Time | Realtime

Connections

Automatically Choose Connection Type

Scenario 0 | New | Delete | Toggle PDU List Window

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

РУС 18:32 18.12.2019

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:

https://studfiles.net/html/2706/610/html_1t7827cn0P.AOQ6/htmlconvd-5FjQl116x1.jpg

https://bigslide.ru/images/51/50961/960/img12.jpg

https://bigslide.ru/images/51/50961/960/img11.jpg

https://1.bp.blogspot.com/-qptz15WfEJE/XDoN736gSvI/AAAAAAAAAU8/ESDrBE1iP-0vt5keIdxrnh_Y6ZpF2_2tQCLcBGAs/s1600/Hybrid-Network.jpg

http://www.klikglodok.com/toko/19948-thickbox_default/jual-harga-allied-telesis-switch-16-port-gigabit-10-100-1000-unmanaged-at-gs900-16.jpg

http://900igr.net/up/datas/221400/029.jpg

Спасибо за внимание!

Преподаватель: Солодухин Андрей Геннадьевич

Электронная почта: asoloduhin@kait20.ru