|  |
| --- |
|  |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  «Московский технологический университет» |

Институт комплексной безопасности и специального приборостроения

Специальность (направление): 09.03.02

Кафедра: КБ-4

Дисциплина: Глобальные и локальные сети

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 7

Студент: Коваленко В.А.

Группа: БСБО-01-15

№зачетной книжки: 15Б0155

Преподаватель: Скворцова Т.И.

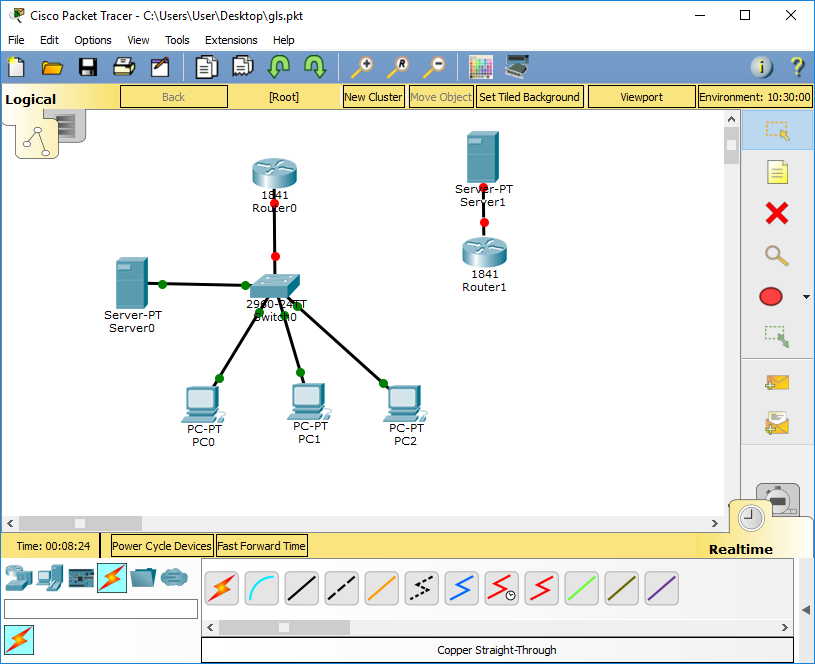
Дата проверки\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Москва, 2018

*Рассмотрим работу с перегруженным NAT*

Открываем Cisco Packet Tracer. Перенесем на рабочую область из панели оборудования 3 пользовательских ПК, коммутатор 2960-24TT, два маршрутизатора 1841, два сервера.

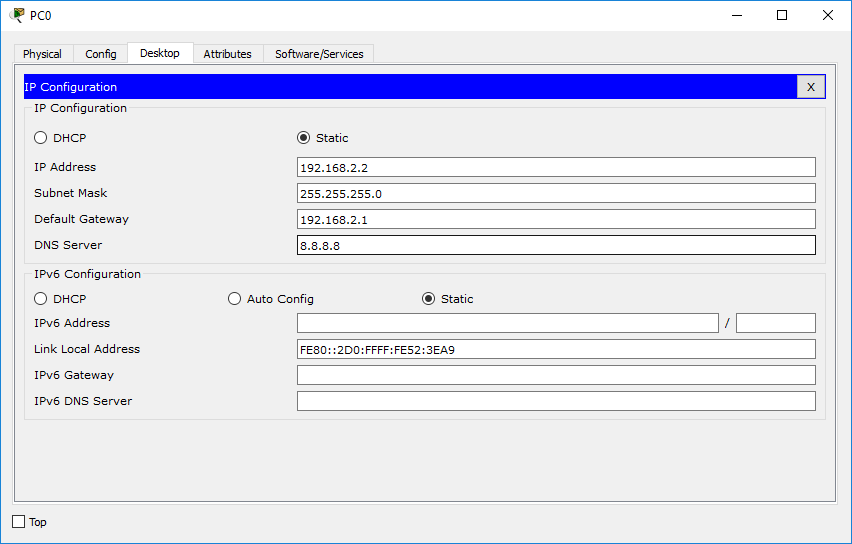
Переносить сразу несколько элементов можно, зажав клавишу Ctrl.

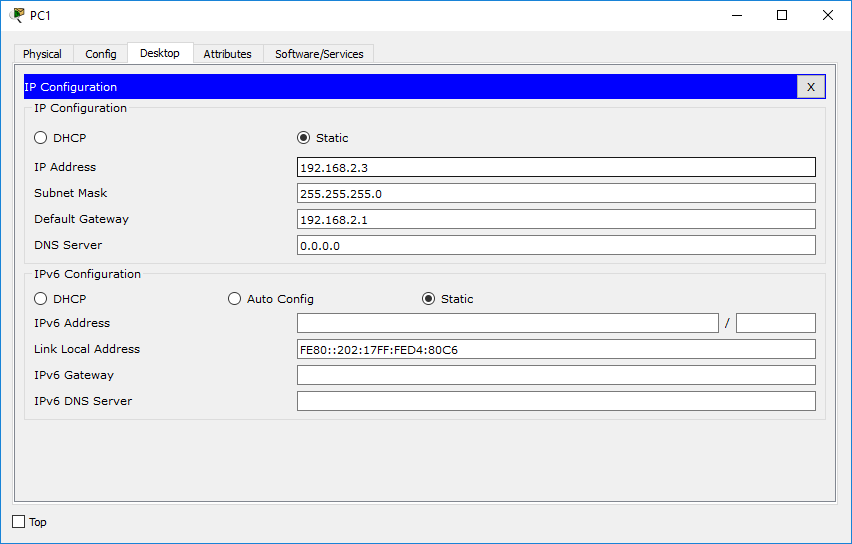


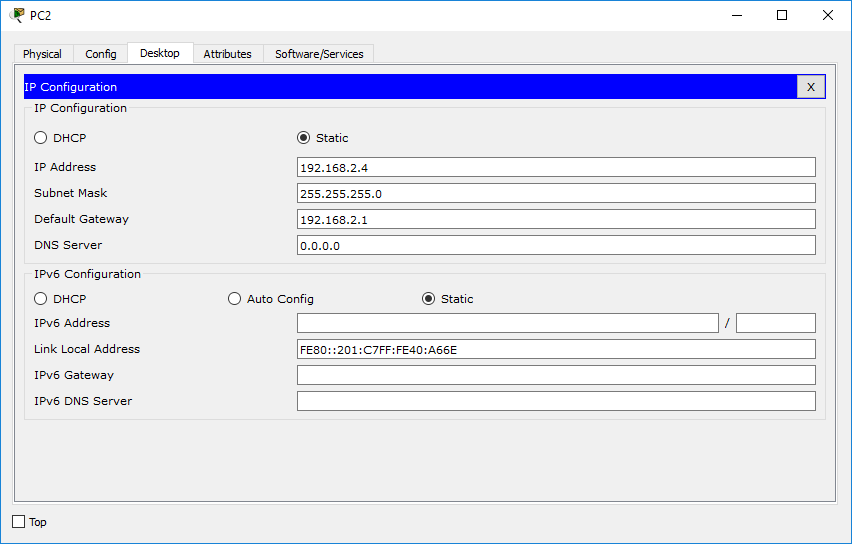
**Рисунок 10. Создание схемы сети**

Настроим ПК пользователей в подсети 192.168.2.0. Присвоим им IP-адреса соответственно 192.168.2.2 – 4, маска 255.255.255.0, основным шлюзом укажем наш роутер0, который настроим чуть позже – 192.168.2.1

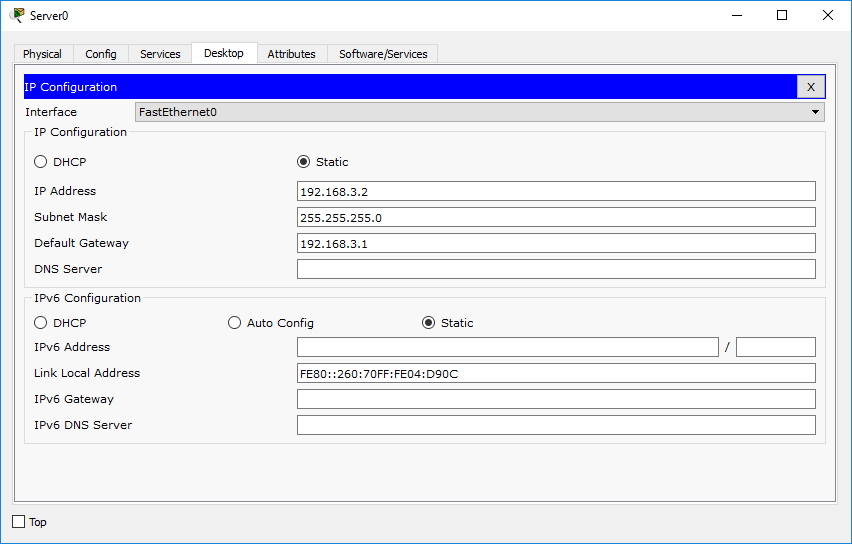
Сервер настроим в другой подсети.





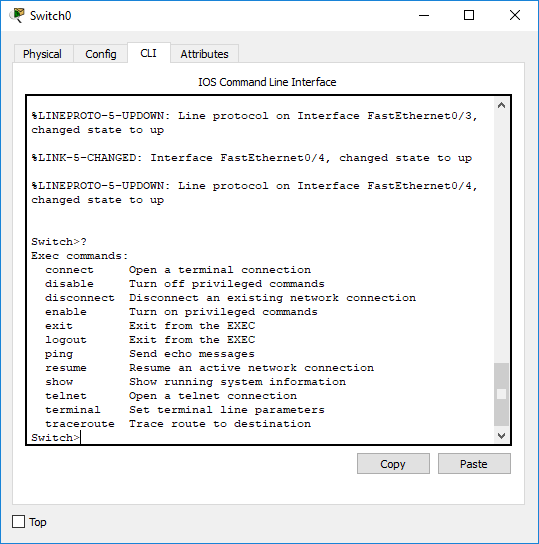


**Рисунок 10-12. Настройка ПК пользователей**



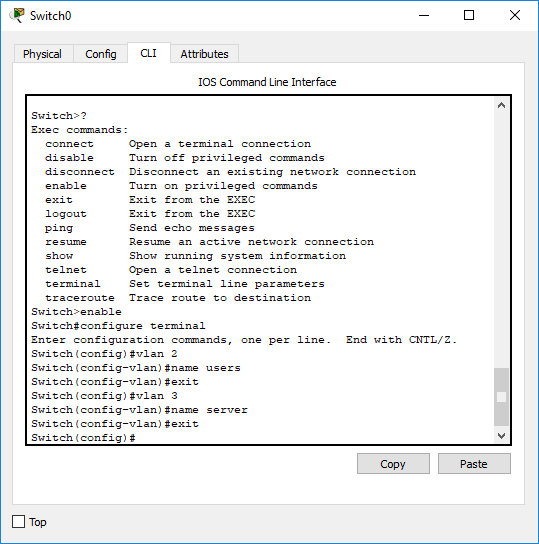
**Рисунок 11. Конфигурация сервера Server0**

Далее выделим сегменты, настроив VLAN. Двойным щелчком на коммутаторе открываем окно настроек и переходим во вкладку CLI (Command Line Interface). Изучить команды можно в документации или ввести «?» в командную строку.



**Рисунок 12. Ознакомление с другими командами в режиме пользователя.**

Введём команду enable для входа в привилегированный режим (появится знак «#»). Далее configure terminal для входа в режим глобального конфигурирования. Создадим VLAN и дадим им названия. Команды можно писать сокращенно, консоль их поймет (например, вместо enable – en, вместо configure terminal – conf t), или нажимать Tab, чтобы консоль сама дописала команду.



**Рисунок 13. Создание VLAN**

Таким образом, созданы VLANы для пользователей и серверов. Теперь нужно настроить интерфейсы и определить порты Access и Trunk. Чтобы узнать, какие порты нам нужны, наводим на канал связи (рис. 14). Определим порты FastEthernet 0/1, 0/2, 0/3 в сегмент Users (vlan 2), fa 0/4 в Server (vlan 3), а порт, соединяющий коммутатор и роутер, fa 0/5 сделаем Trunk.

Самостоятельно определите интерфейсы fa 0/2 и fa 0/3 в VLAN 2 и fa 0/5 Trunk, чтобы он передавал VLAN 2 и 3 (команда switchport trunk allowed vlan 2, 3).

**Switch(config)#int fa 0/4**

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 3

Switch(config-if)#exit

**Switch(config)#int fa 0/1**

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 2

Switch(config-if)#exit

**Switch(config)#int fa 0/2**

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 2

Switch(config-if)#exit

**Switch(config)#int fa 0/3**

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 2

Switch(config-if)#exit

**Switch(config)#int fa 0/5**

Switch(config-if)#switchport mode access

Switch(config-if)#switchport trunk allowed vlan 2,3

Switch(config-if)# switchport mode trunk

Switch(config)#

Проверьте результат командой show running-config и сохраните настройки командой write memory.

!

**interface FastEthernet0/1**

switchport access vlan 2

switchport mode access

!

**interface FastEthernet0/2**

switchport access vlan 2

switchport mode access

!

**interface FastEthernet0/3**

switchport access vlan 2

switchport mode access

!

**interface FastEthernet0/4**

switchport access vlan 3

switchport mode access

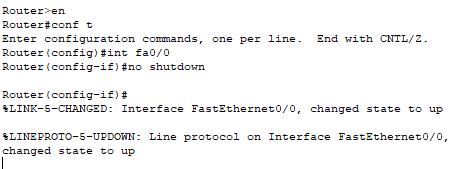
!

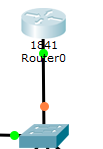
**interface FastEthernet0/5**

switchport trunk allowed vlan 2-3

switchport mode trunk

Далее приступим к настройке Router0. По умолчанию порты на маршрутизаторах в Cisco Packet Tracer закрыты, о чём свидетельствуют красные индикаторы на схеме в канале связи. Откроем нужный нам порт командой no shutdown, после чего цвет индикатора должен измениться на зелёный.





**Рисунок 16. Открытие порта fa0/0**

Создадим виртуальный интерфейс или иначе его называют подинтерфейс или ещё сабинтерфейс (sub-interface). 

Router(config-if)# int fa0/0.2

  
 Логика тут простая. Сначала указываем обычным образом физический интерфейс, к которому подключена нужная сеть, а после точки ставим некий уникальный идентификатор этого виртуального интерфейса. Для удобства, обычно номер сабинтерфейса делают аналогичным влану, который он терминирует.

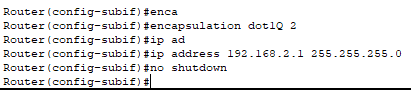
Теперь вспомним о стандарте 802.1q, который описывает тегирование кадра меткой влана. Следующей командой вы обозначаете, что кадры, исходящие из этого виртуального интерфейса, будут помечены тегом 2-го влана. А кадры, входящие на физический интерфейс FastEthernet0/0 с тегом этого влана будут приняты виртуальным интерфейсом FastEthernet0/0.2.

Router(config-if)#encapsulation dot1Q 2

И определим IP-адрес. Этот адрес будет шлюзом по умолчанию (default gateway) для всех устройств в этом влане и откроем его.

Router(config-if)# ip address 192.168.2.1 255.255.255.0

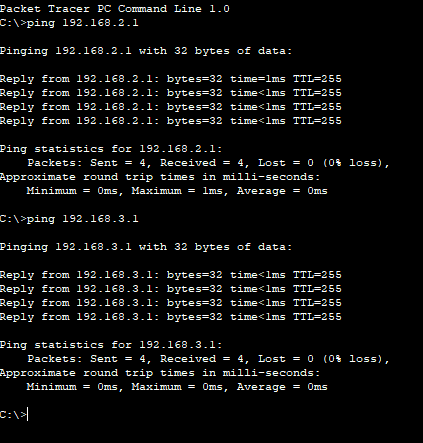
Router(config-if)# no shutdown



Аналогичным образом настройте для vlan 3 и проверьте настройки.

Проверим работу локальной сети, выбрав любой ПК, открыв Command Prompt и пропинговав основной шлюз и сервер.

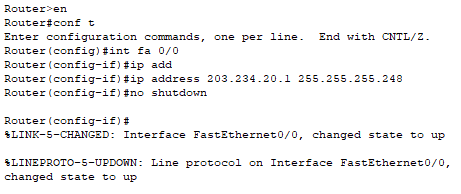
Видим из рис. 17, что всё работает корректно.

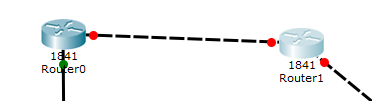


**Рисунок 17. Проверка работоспособности локальной сети**

Далее необходимо подключить ЛВС к Сети Интернет. Допустим, что мы обратились к провайдеру, и тот выделил статический белый IP-адрес. В Cisco Packet Tracer мы симулируем сеть Интернет посредством роутера1 и сервера1.

Допустим провайдер выделил нам адрес 203.234.10.1 с маской 255.255.255.248





**Рисунок 18. Выделение белого IP-адреса**

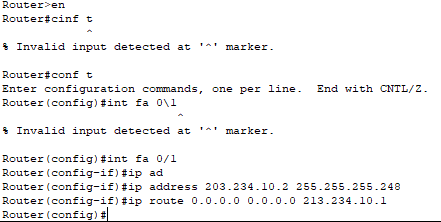
А серверу выделил адрес 203.234.20.1 с маской 255.255.255.248. Сохраним настройки.

Настроим сервер, присвоив IP-адрес – 203.234.20.2, маску 255.255.255.248 и шлюз 203.234.20.1

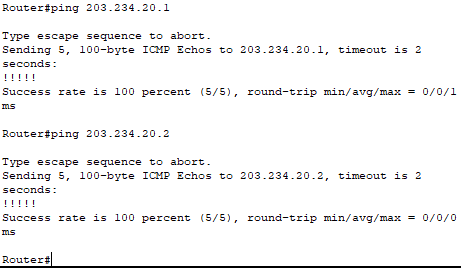


На роутере0 на интерфейсе fa0/1 пропишем адрес, который выделил на провайдер: адрес 203.234.10.2 с маской 255.255.255.248. И создаем шлюз по умолчанию:

Router(config-if)# ip route 0.0.0.0 0.0.0.0 213.234.10.1

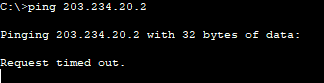


Проверим связь с Интернет-провайдером и вторым сервером.

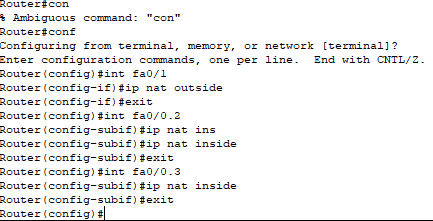


**Рисунок 19. Проверка связи**

Если выполнить пинг сервера1 с локального компьютера, то пинг не пойдёт, так как мы используем серые IP-адреса, и роутер1 не знает о них. С помощью технологии NAT мы обеспечим нашим компьютерам доступ в сеть Интернет.



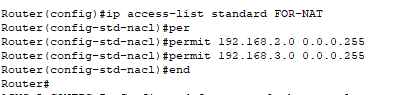
Для начала нужно определить какой интерфейс для NAT будет внешним, а какой внутренним.



**Рисунок 20. Определение NAT интерфейса для ПК пользователей**

Самостоятельно определите интерфейс аналогичным образом для сервера0.

Теперь необходимо создать Access lists, которые будут характеризовать, какой именно трафик мы будем передавать через NAT.



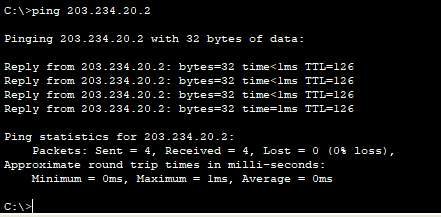
**Рисунок 21. Создание Access List**

0.0.0.255 – это обратная маска (WildCard bits) от маски 255.255.255.0

Вводим последнюю команду, указывающую по какому интерфейсу надо производить «NAT», указав также тип NAT и Access List.

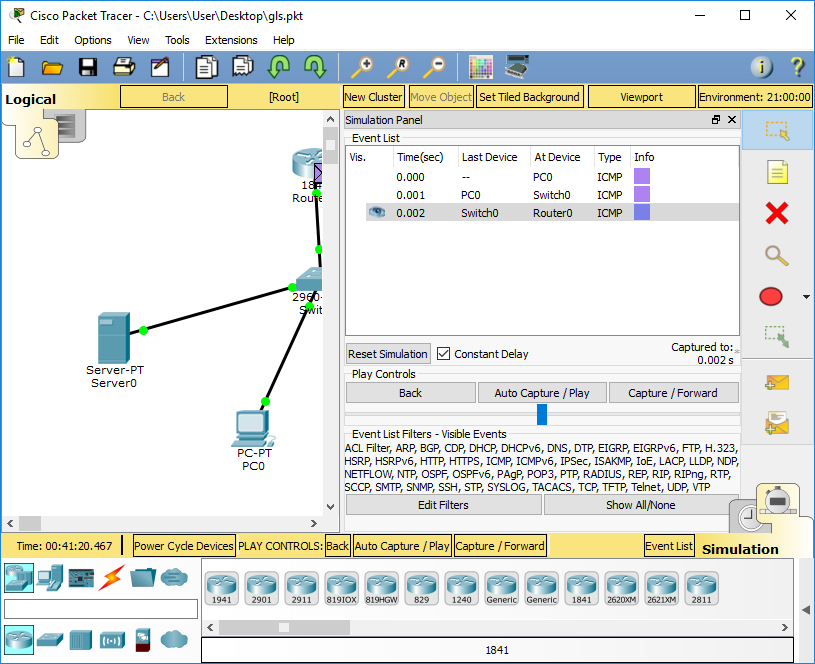
Router (config-if)# ip nat inside source list FOR-NAT interface fastEthernet 0/1 overload

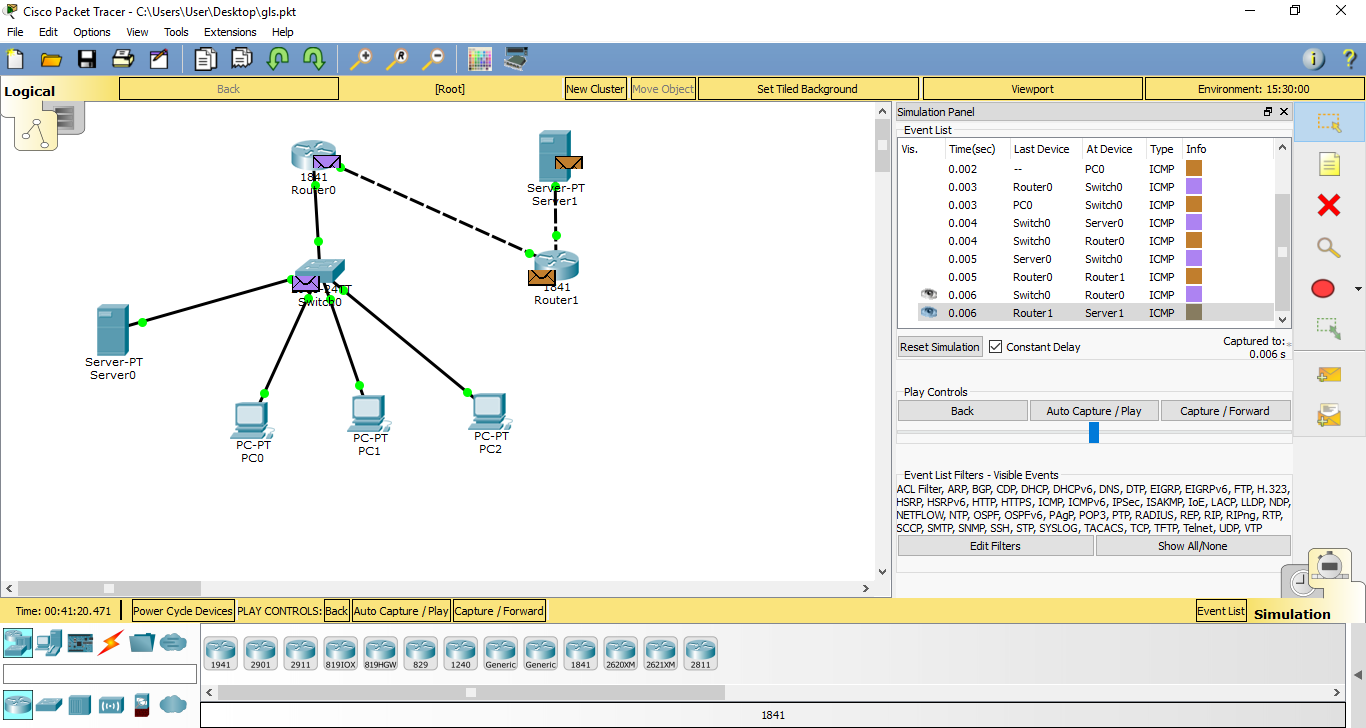
Снова выполнить пинг сервера1 с локального компьютера. Пинг проходит.



**Рисунок 22. Проверка Server1 с PC0**

Запустите анимацию передачи пакета с локального компьютера и Server0 на Server1.





**Задание:** Настройте NAT по данной схеме, продемонстрируйте работоспособность каждого узла и настройки коммутатора и маршрутизаторов командой show running-config.

**Ответьте на вопросы:**

1. Чем отличается белый IP-адрес от серого?

**Публичный или белый IP-адрес** - это тот адрес, под которым устройство видно и работает в единой глобальной сети, которая охватывает весь земной шар.

**Частный или серый IP-адрес** используется во внутренних локальных сетях. С ним компьютер будет доступен с любого другого из этой сети, но из Интернета его видно не будет.

1. Зачем нужен NAT?

Трансляция приватных IP-адресов во внешние. Благодаря этому процессу ваша машина получает доступ в Интернет.

1. Какие бывают базовые концепции NAT?

**Статический NAT** — Отображение незарегистрированного (частного) IP-адреса на зарегистрированный (глобальный) IP-адрес на основании *один к одному*. Особенно полезно, когда устройство должно быть доступным снаружи сети.

**Динамический NAT** — Отображает незарегистрированный IP-адрес на зарегистрированный адрес из *группы зарегистрированных IP-адресов*. Динамический NAT также устанавливает непосредственное отображение между незарегистрированными и зарегистрированными адресами, но *отображение может меняться* в зависимости от зарегистрированного адреса, доступного в пуле адресов, во время коммуникации.

**Перегруженный NAT** (NAPT, NAT Overload, PAT, маскарадинг) — форма динамического NAT, который отображает несколько незарегистрированных адресов в единственный зарегистрированный IP-адрес, используя различные порты. Известен также как *PAT (Port Address Translation)*. При перегрузке каждый компьютер в частной сети транслируется в тот же самый адрес, но с различным номером порта.

1. Чем отличаются trunk и access порты?

*Access port* — порт доступа — к нему подключаются, как правило, конечные узлы. Трафик между этим портом и устройством нетегированный. За каждым access-портом закреплён определённый VLAN, иногда этот параметр называют PVID. Весь трафик, приходящий на этот порт от конечного устройства, получает метку этого влана, а исходящий уходит без метки.  
*Trunk port*. У этого порта два основных применения — линия между двумя коммутаторами или от коммутатора к маршрутизатору. Внутри такой линии, называемой в народе, что логично, транком, передаётся трафик нескольких вланов. Разумеется, тут трафик уже идёт с тегами, чтобы принимающая сторона могла отличить кадр, который идёт в бухгалтерию, от кадра, предназначенного для ИТ-отдела. За транковым портом закрепляется целый диапазон вланов.

1. Открыты ли по умолчанию порты у маршрутизаторов в CPT? Какими командами их открыть/закрыть? Закрыты. No shutdown/ shutdown