МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Институт математики и информационных систем
Факультет автоматики и вычислительной техники
Кафедра «Систем автоматизации управления»

Лабораторная работа №8.

Cisco Packet Tracer.

Настройка NAT.

Отчёт по дисциплине

«Глобальные сети»

Выполнил студент гр. ИТб-51 _____/ Поздеев Д.Э./

(подпись)

Руководитель доцент _____/ Стариков А.И. /

(подпись)

Киров 2019

1. Настроим на компьютерах и локальном сервере IP-адреса.

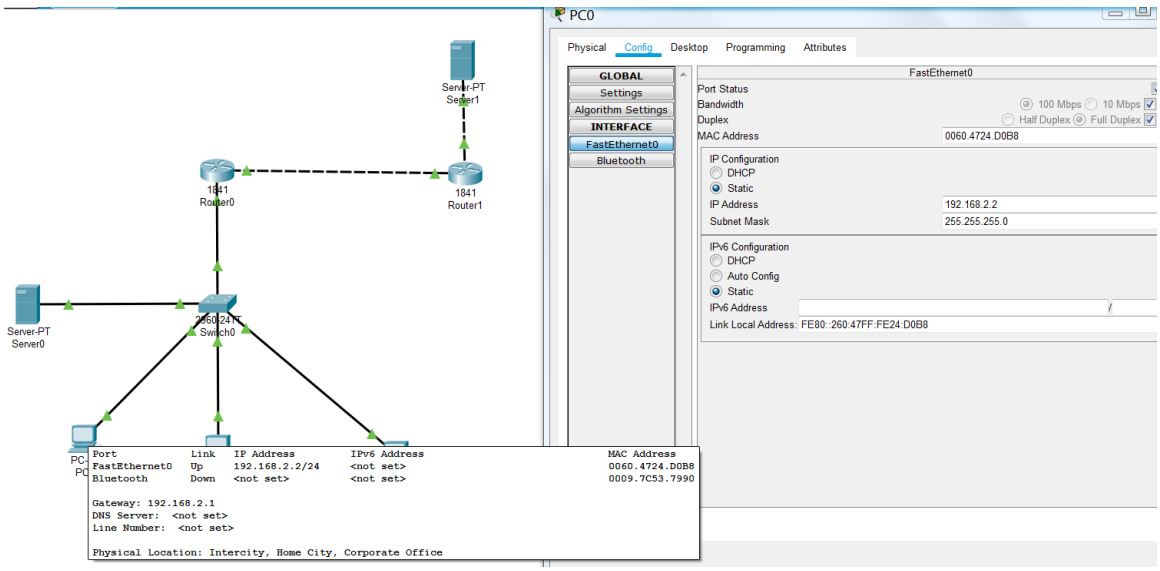


Рис. 1 Настройка IP адресов на локальных PC

Выделяем локальный сервер в отдельный сегмент:

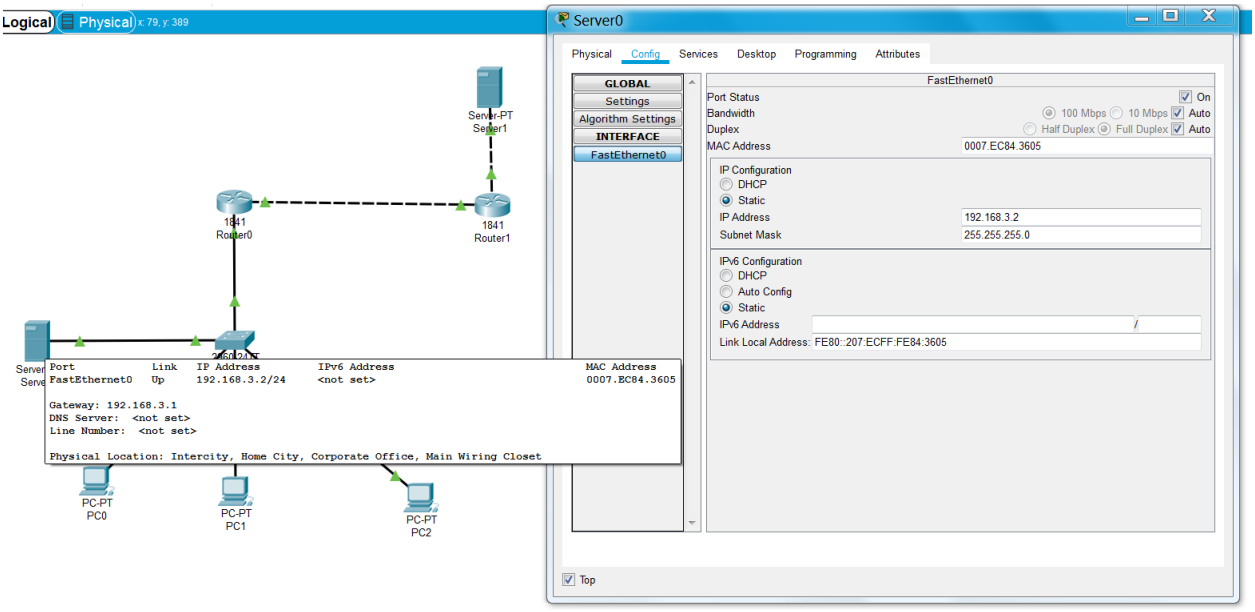


Рис. 2 Настройка IP адреса локального сервера

2. Создадим сегменты локальной сети посредством vlan на коммутаторе:

Vlan 2 – для пользовательских машин, vlan 3 для сервера.

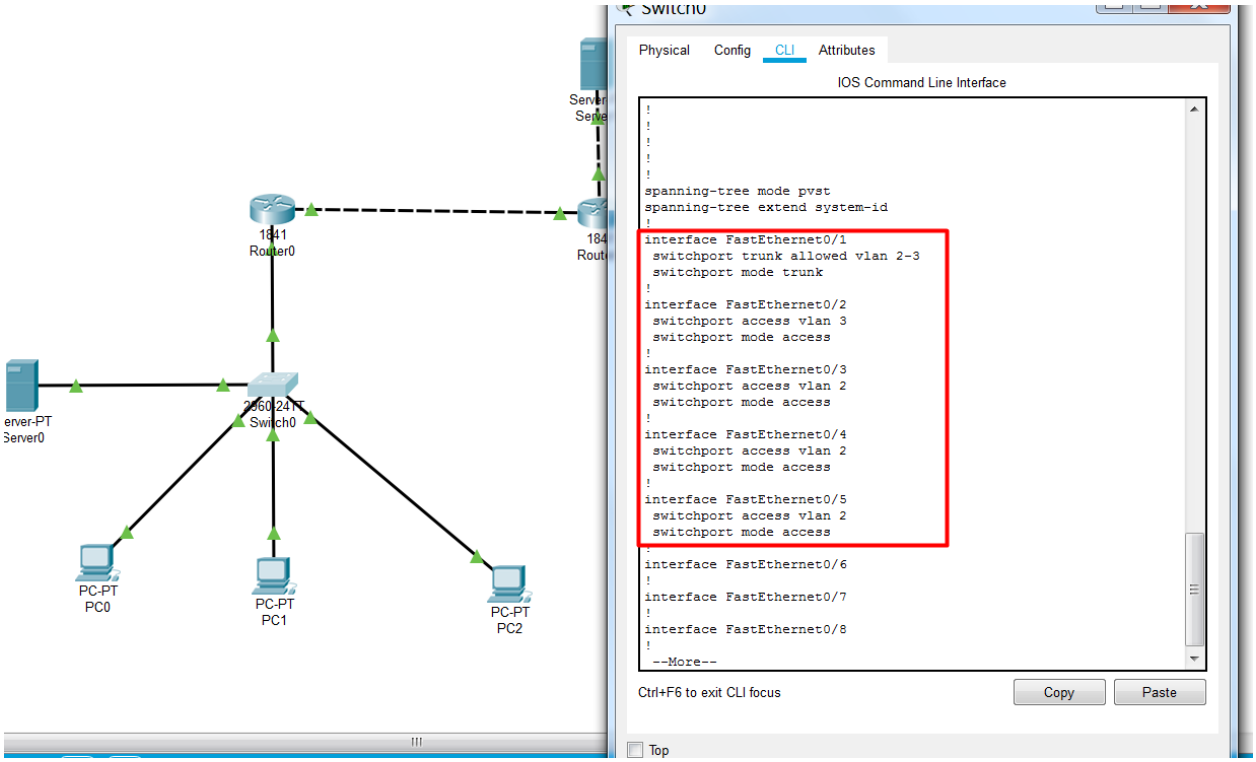


Рис.3 Создание сегментов

Теперь создадим соответствующие sub-интерфейсы для соответствующих vlan’ов на роутере.

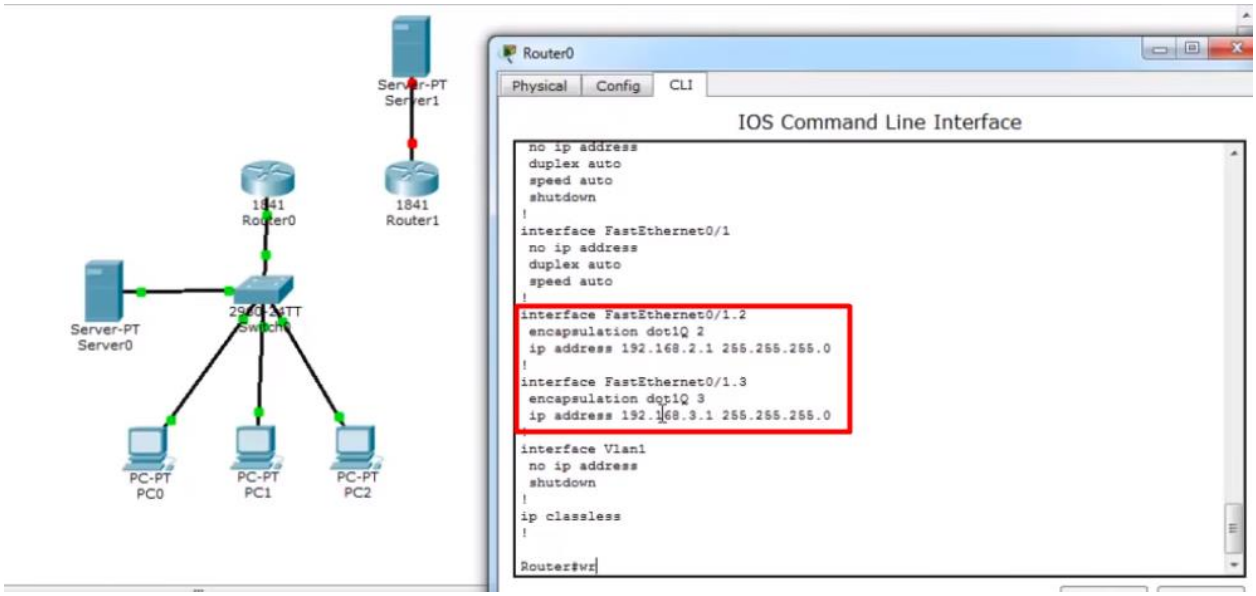


Рис. 4 Создание sub-интерфейсов.

Пропингуем сервер и другой PC, чтобы убедиться, что локальная сеть настроена правильно:

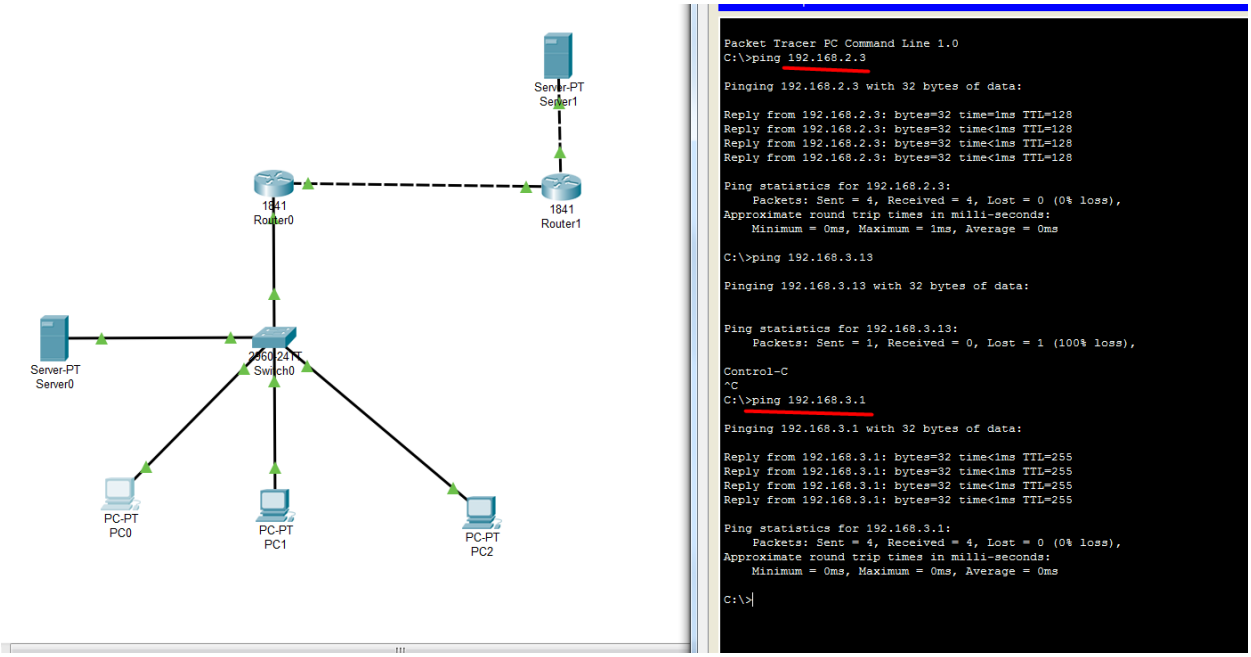


Рис. 5. Пинги в локальной сети

3. Теперь мы захотели подключить нашу локальную сеть к сети Интернет, симулировав провайдера посредством роутера и сервера, приняв, что провайдер нам выделил статический IP-адрес. Также настроим сервер.

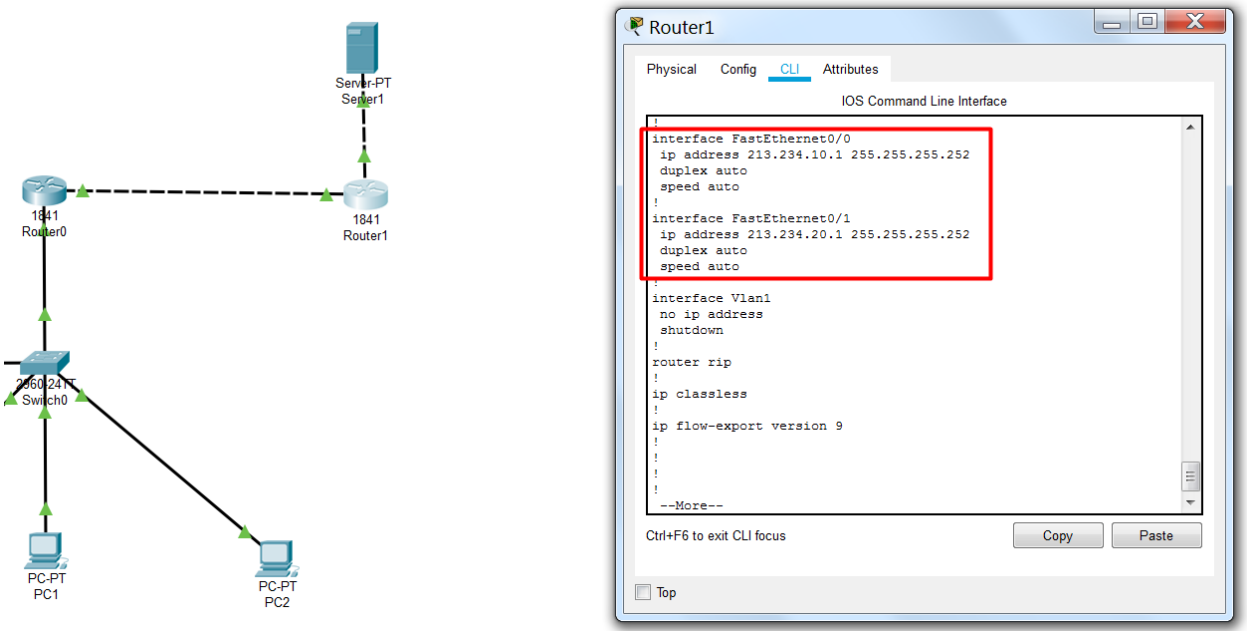


Рис. 6 Настройка роутера провайдера.

Получаем, что на роутере провайдера мы имеем: один белый IP-адрес который смотрит в сторону роутера нашей локальной сети, другой в сторону публичного сервера.

Пропишем на нашем роутере IP-адрес интернета, который нам выделил провайдер 213.234.10.2 и установим адрес шлюза провайдера.

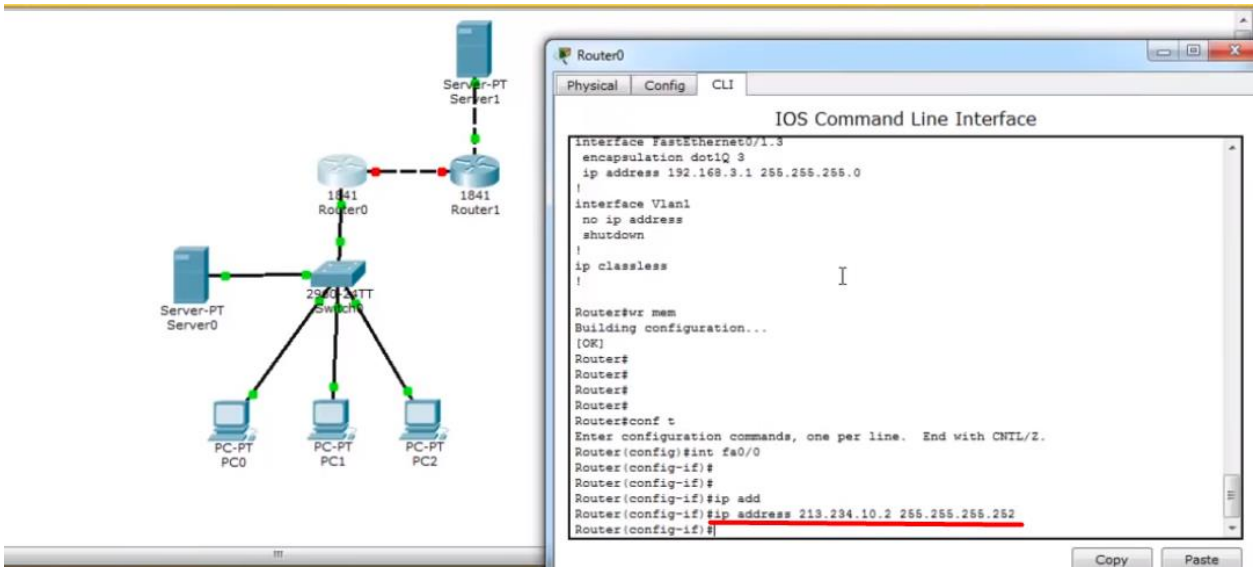


Рис. 7 Настройка IP-адреса интернета на локальном роутере

Убедимся, что наш роутер установил связь с интернет-провайдером и соответственно с публичным сервером, пропинговав их.

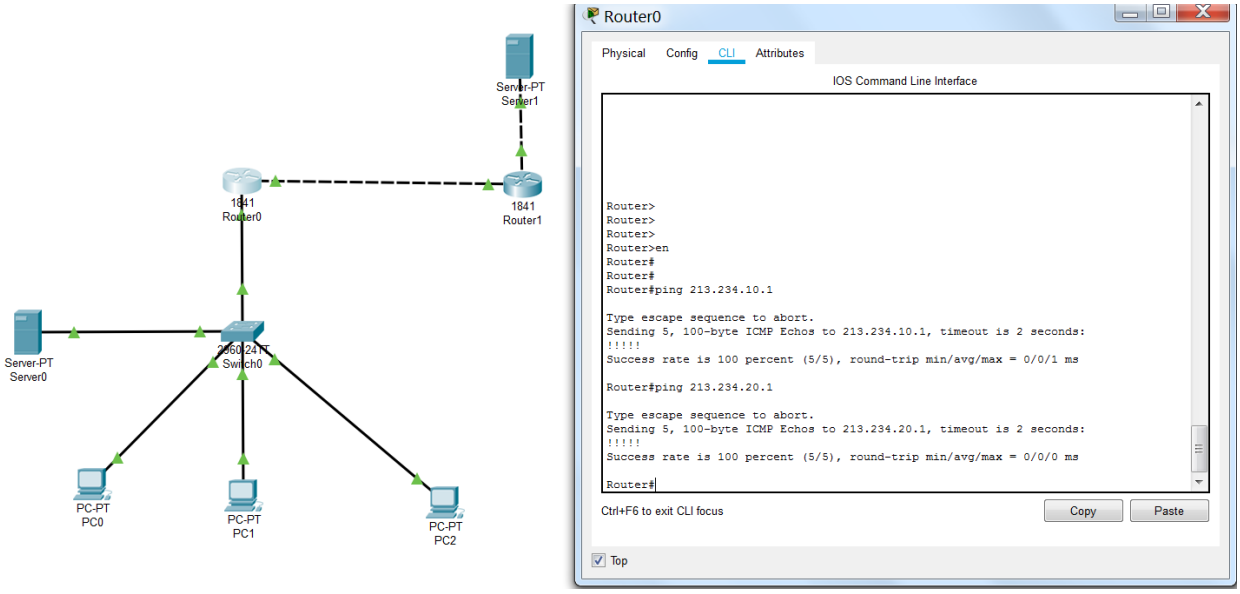


Рис.8 Пинги роутра к провайдеру и публичному серверу

Теперь попробуем связаться с публичным сервером с локального PC, пинг не пройдёт, потому что мы используем серые IP-адреса и наш роутер не знает про эту сеть.

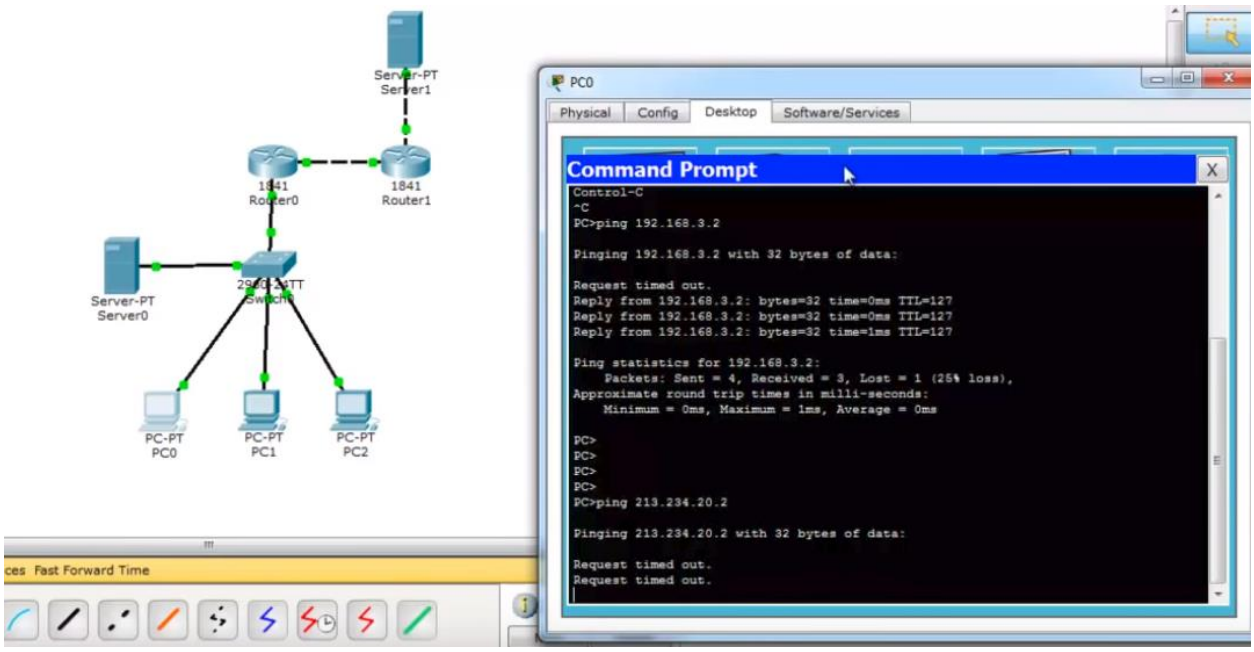
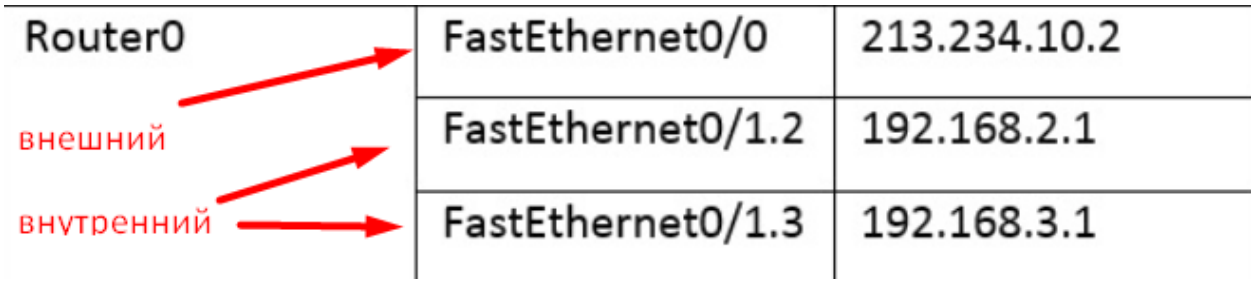


Рис. 9 Локальная сеть не видит интернет.

4. С помощью технологии NAT мы обеспечим доступ локальных компьютеров и сервера в сеть Интернет.

Для начала на локальном роутере настроим какой интерфейс будет являться для NAT внешним, а какой внутренним.



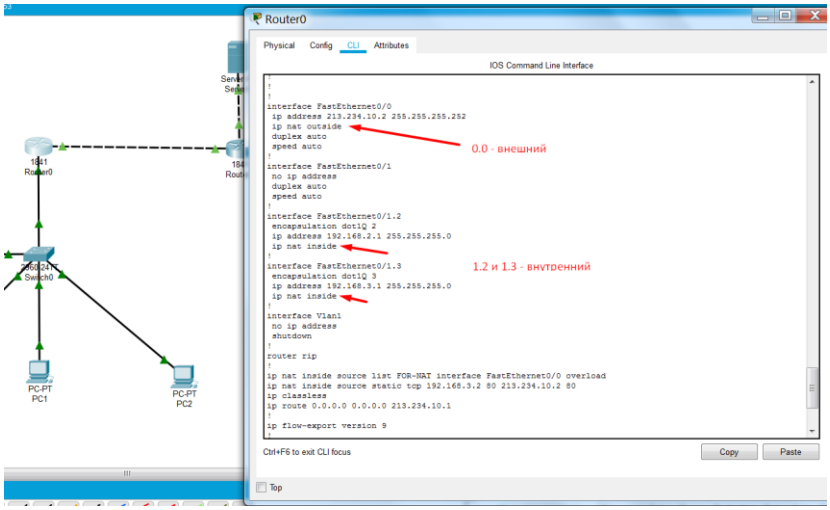


Рис. 10 Настройка NAT локального роутера.

5. Затем мы создаём access-list которые будут характеризовать, какой именно траффик мы будем «натить».

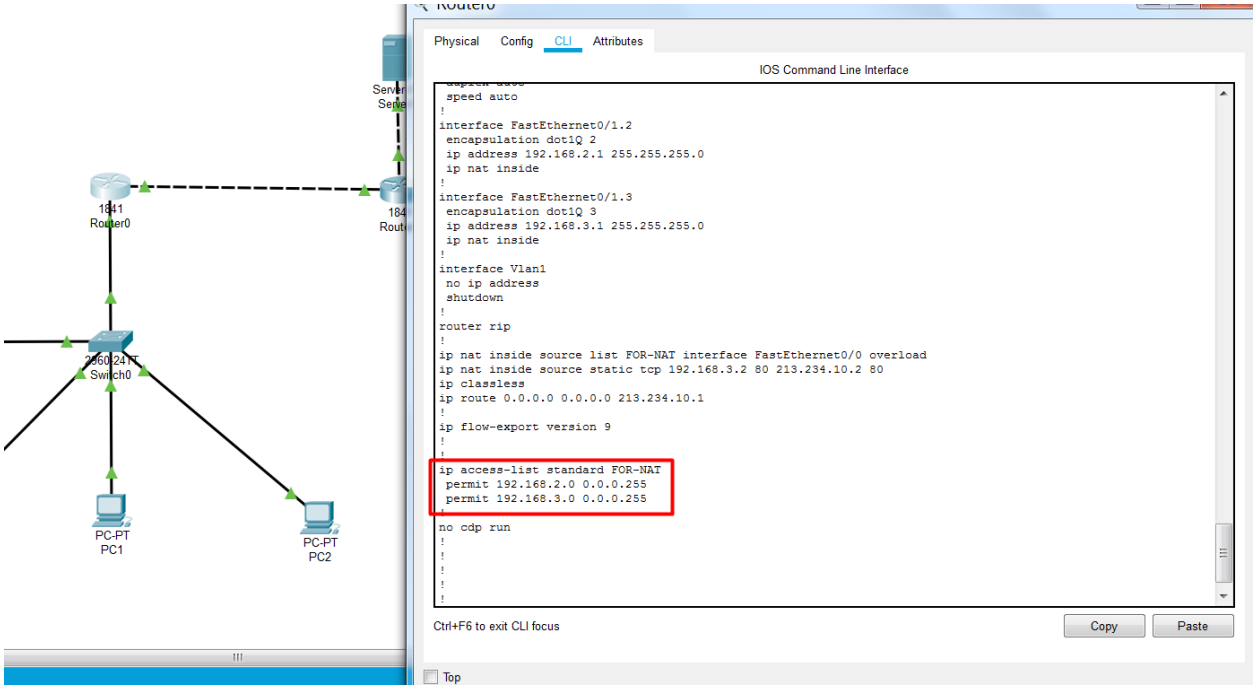
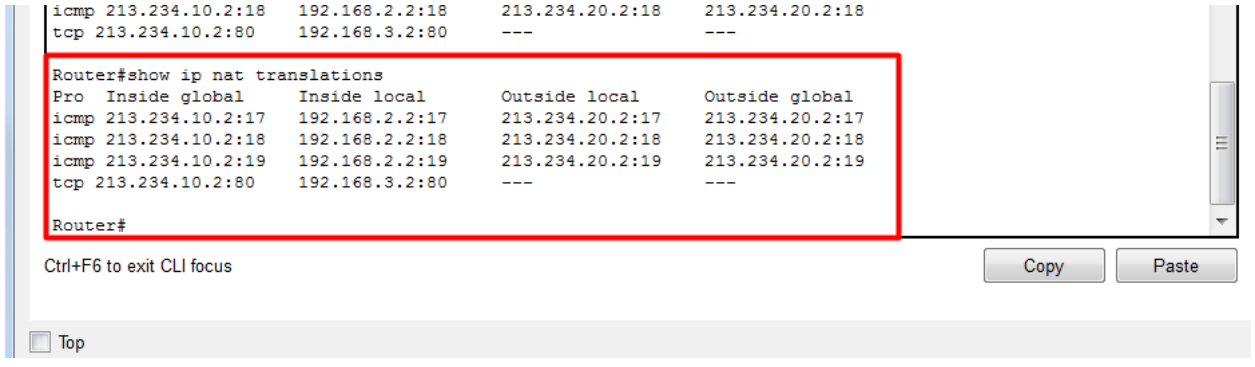


Рис. 11. Создание access-list для NAT

Последней командой ip nat inside source list FOR-NAT interface FastEthernet0/0 overload завершаем настройку роутера.

6. Как работает NAT:

Наш пользователь работает в домашней сети на хосте 192.168.2.2 и запрашивает веб-страницу с веб-сервера (порт 80) с IP-адресом 213.234.20.2. Хост 192.168.2.2 присваивает (произвольно) номер исходного порта 18 и посылает дейтаграмму в локальную сеть. NAT-маршрутизатор получает дейтаграмму, генерирует для нее новый номер исходного порта, в нашем случает такой же 18 порт, заменяет исходный IP-адрес соответствующим IP-адресом, расположенным на стороне ГВС (213.234.10.2) и заменяет старый номер исходного порта 18 новым — 18. При генерировании нового номера исходного порта NAT-маршрутизатор может выбрать любой, которого пока нет в таблице трансляции сетевых адресов. Механизм NAT в маршрутизаторе также добавляет запись в свою таблицу трансляции сетевых адресов.



Веб-сервер, совершенно не представляющий, что прибывшая к нему дейтаграмма с HTTP-запросом уже подверглась обработке на NAT-маршрутизаторе, посылает в ответ дейтаграмму, где адрес получателя — это IP-адрес NAT-маршрутизатора, а порт назначения имеет номер 18. Когда дейтаграмма прибывает на NAT-маршрутизатор, тот делает выборку из таблицы трансляции сетевых адресов. При этом он использует целевой IP-адрес и номер порта назначения, чтобы получить подходящий IP-адрес (192.168.2.2) и номер порта назначения (18) для браузера, работающего в домашней сети. Затем маршрутизатор переписывает адрес назначения дейтаграммы и номер порта назначения и пересылает ее в домашнюю сеть.