В самом начале отчета в лабораторной работе необходимо привести таблицу вашего варианта задания, например:

Таблица 11.1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | 22 | | | |
| Сеть 1 | 192.168.2.1/24 | 192.168.3.1/24 | 213.234.10.1/30 | 213.234.20.1/24 |

# Типовой пример для небольшого офиса

Собираем следующую схему:

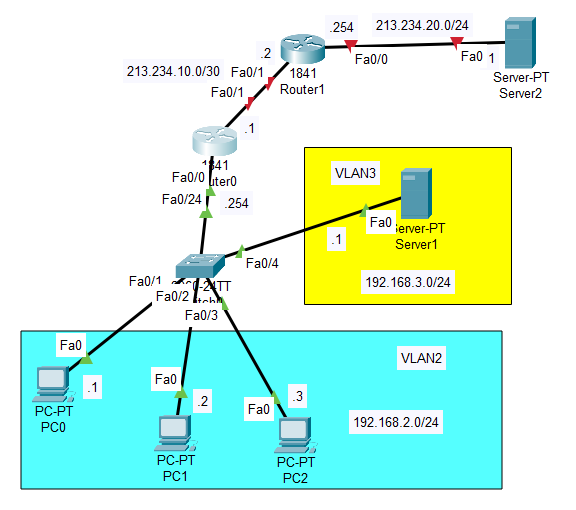
**

Рис. 1

В нашем офисе имеется несколько компьютеров, объединенных в один сегмент и локальный сервер, для которого создан также отдельный сегмент согласно правилам хорошего тона. На коммутаторе создаем сегменты используя виланы. Все виланы приземлим на маршрутизаторе и сделаем проверку.

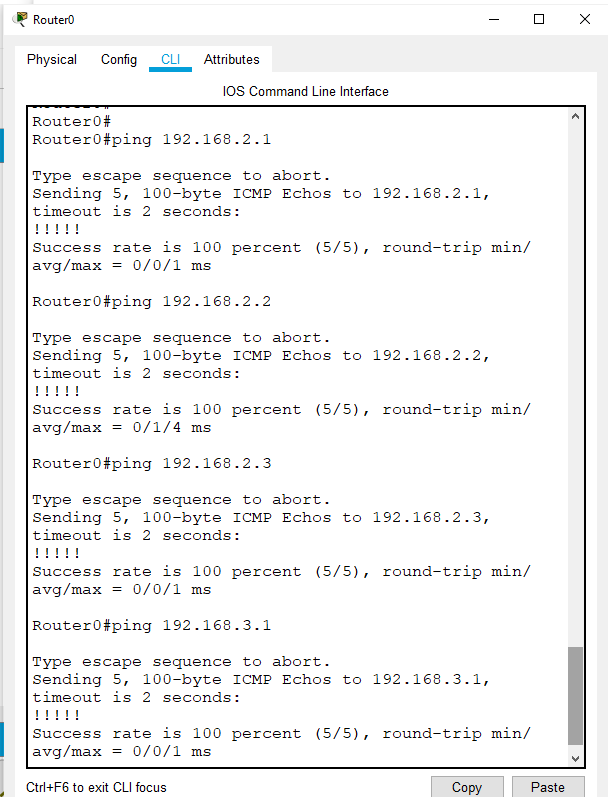


Рис. 2

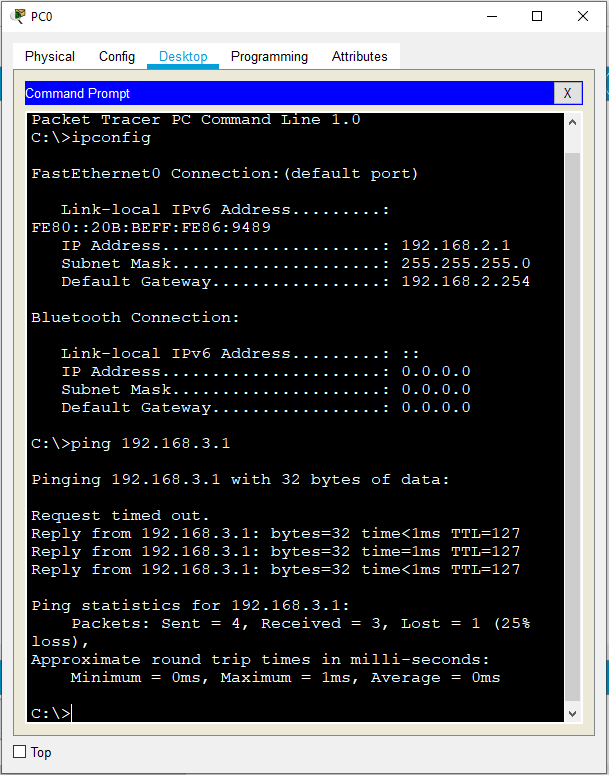


Рис. 3.

После настройки локальной сети мы обратились к провайдеру для того, чтобы подключить интернет. Провайдер прокинул линк и выделил нам белый ip-адрес 213.234.10.1. В Packet Tracer мы не можем подключить интернет, поэтому симулируем его, используя маршрутизатор провайдера и его сервер, у которых будут публичные белые ip-адреса. На маршрутизаторе провайдера настройки следующие:

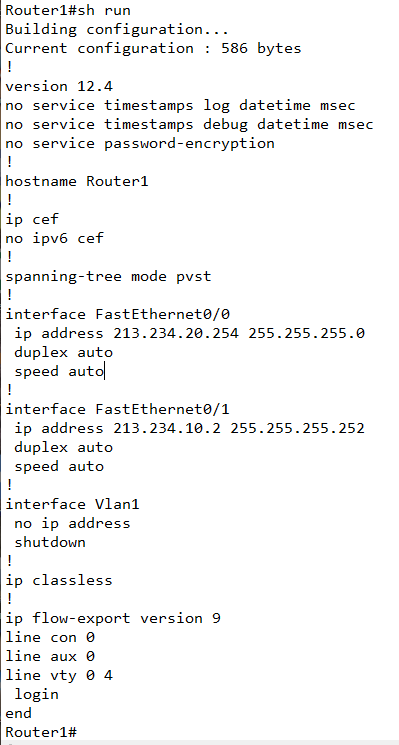


Рис. 4.

На граничном маршрутизаторе нужно прописать в качестве шлюза по умолчанию адрес роутера провайдера. Проверяем связь с роутером провайдера.

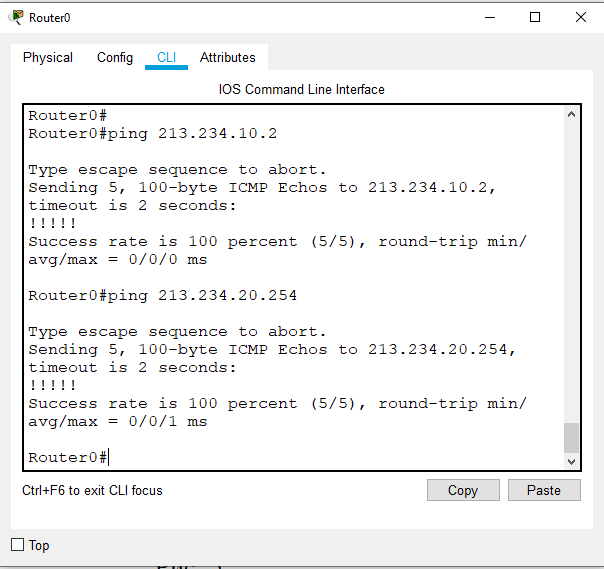


Рис. 5.

Если мы попытаемся достучаться до сети провайдера:

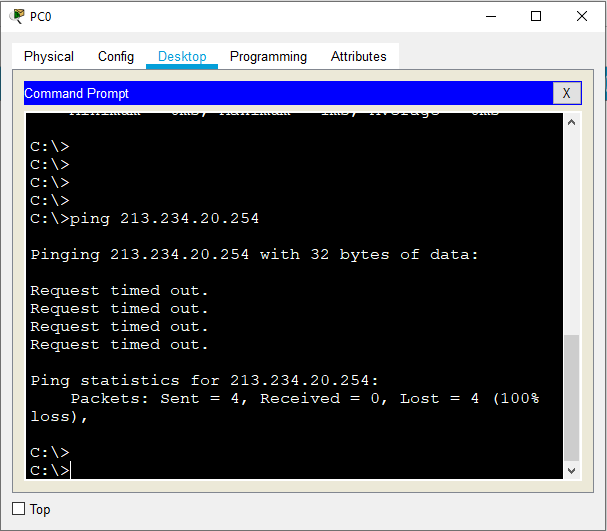


Рис. 6.

То увидим, что пинг не проходит несмотря на то, что прописан статический роутинг. Дело в том, что в нашей локальной сети серые адреса и роутер провайдера их не видит. Для решения данной задачи используем технологию NAT. Настраиваем NAT на нашем граничном маршрутизаторе.

Для начала нужно определить какой интерфейс маршрутизатора будет внешним, а какой – внутренним.

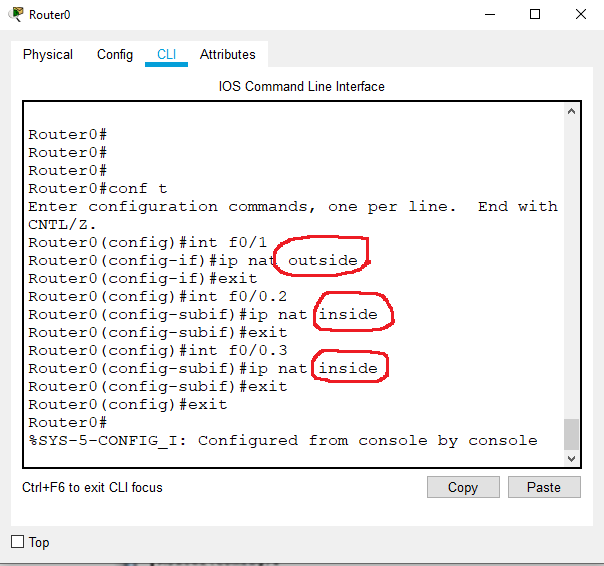


Рис. 7.

Здесь интерфейс outside является внешним, inside – внутренним. Теперь необходимо создать access-list (ACL) для того, чтобы указать какой именно трафик натить и подключаем его к нужному интерфейсу. Что такое ACL мы более подробно изучим позднее.

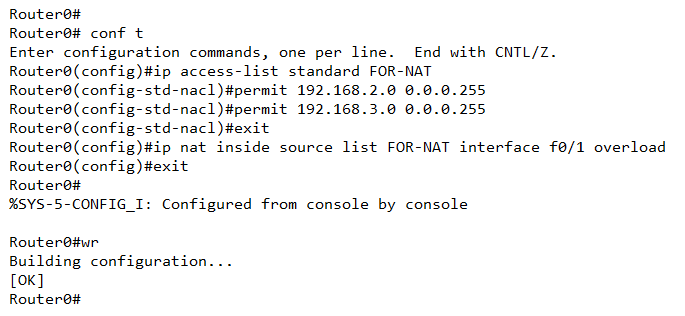


Рис. 8.

Теперь посмотрим пинг с хоста пользователя.

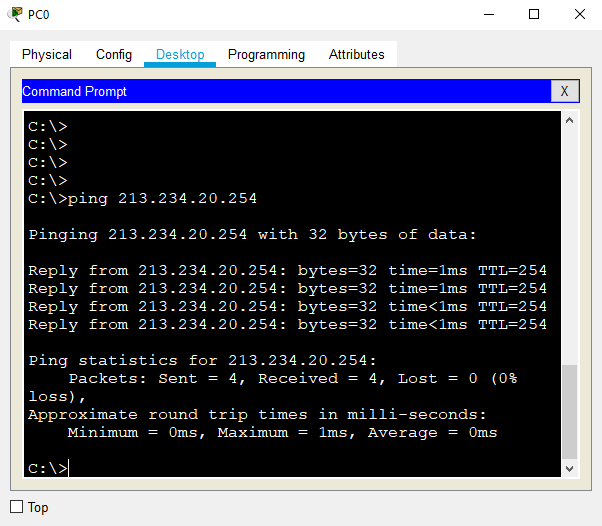


Рис.9.

Как видим ping теперь проходит. Если посмотреть трансляцию НАТА, то увидим:

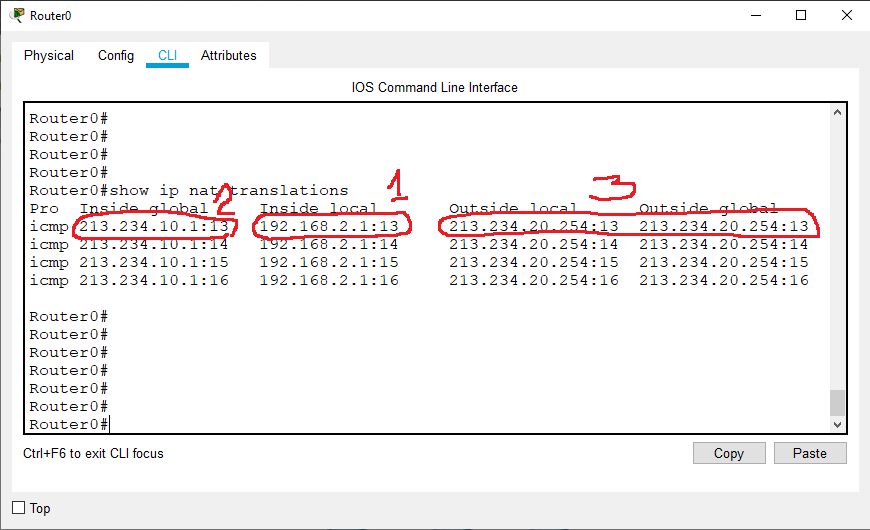


Рис. 10.

Здесь видно, что локальный адрес 192.168.2.1 (1) заменяется внешним белым адресом 213.234.10.1 (2) и далее уже идет к провайдеру (3). Попробуем обмен данными, используя режим симуляции. Первоначально от хоста РС0 отправляется пакет, который достигает маршрутизатора. На входе маршрутизатора пакет имеет адрес отправителя 192.168.2.1 (1), а на выходе – 213.234.10.1 (2). Как видим в пакете произошла подмена адресов. Это и есть НАТ.

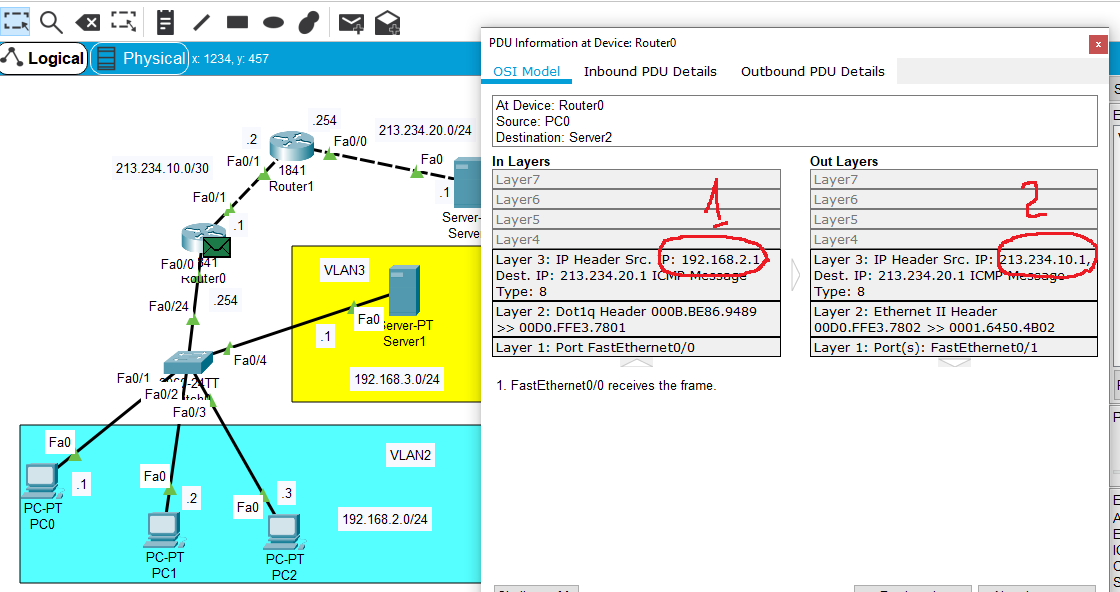


Рис. 11.

А на обратном пути ситуация наоборот. Адрес назначения на входе 213.234.10.1 (1), а на выходе 192.168.2.1 поскольку роутер запомнил с какого компьютера была инициализирована данная сессия, то и восстановил адрес, по которому нужно отправить ответ.

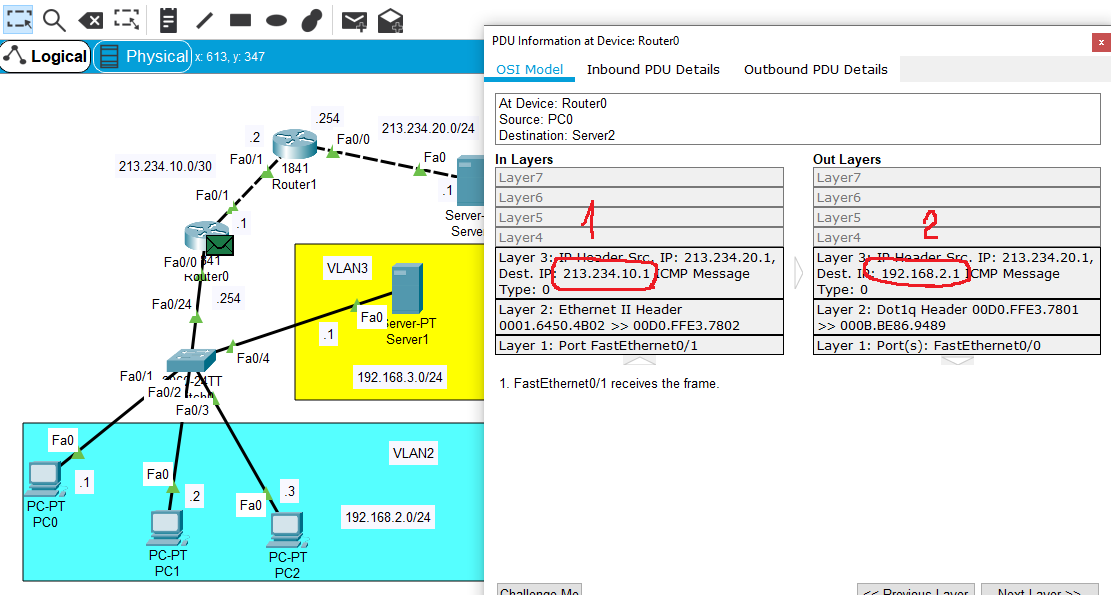


Рис. 12.

Попробуем с сервера доступ в интернет.

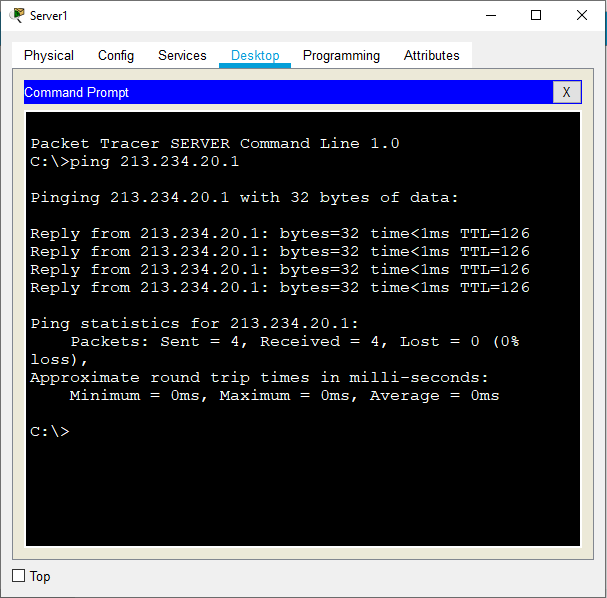


Рис. 13.

Все хорошо проходит. Сейчас настроен, если строго говорить, порт адрес трансляция, т.е. доступ из локальной сети в интернет. А сейчас настроим static NAT. А именно доступ из интернета к локальному серверу. Для начала поднимем HTTP сервер на нашем сервере из локальной сети. Для этого входим на сервер, открываем вкладку Services (1), выбираем закладку HTTP (2), отмечаем файл index.html (3) и нажимаем кнопну edit (4).

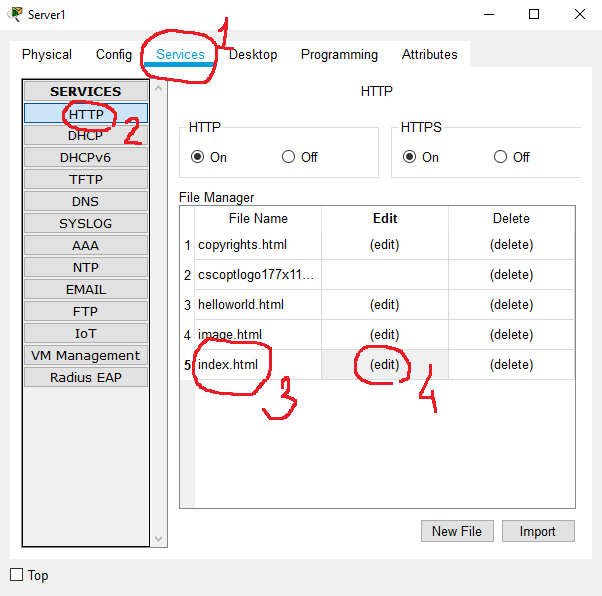


Рис. 14.

В открывшемся окне пишем свой текст

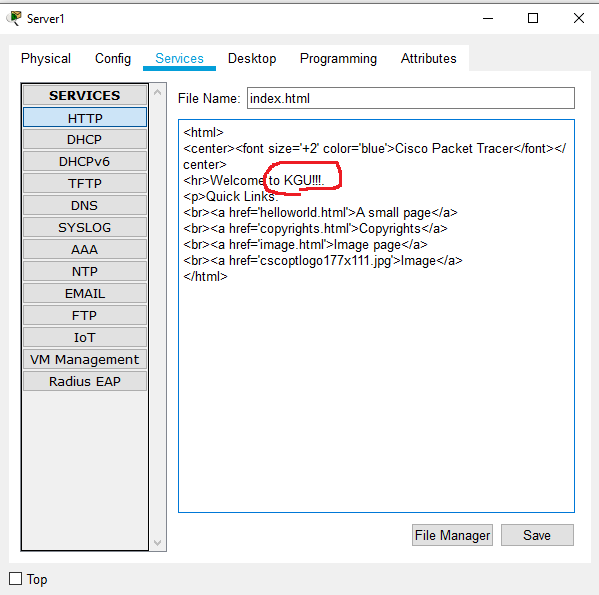


Рис. 15.

На граничном маршрутизаторе необходимо пробросить пакеты на наш сервер (настроить статик НАТ). Указываем адрес куда нужно пробросить и откуда.



Рис. 16.

На сервере провайдера выполняем запрос.

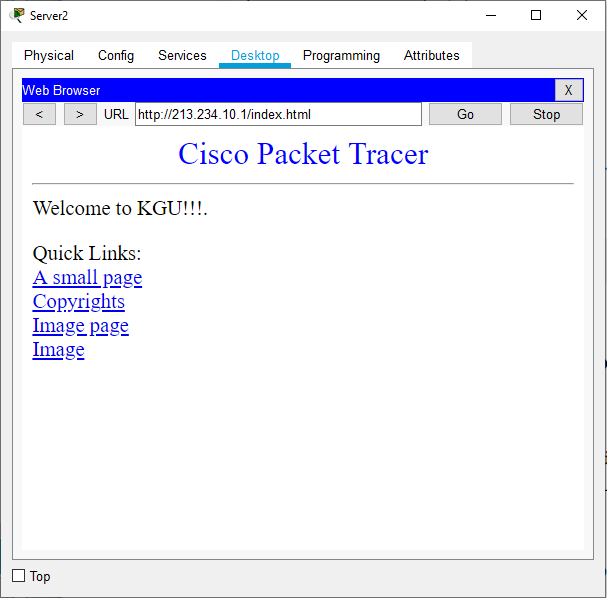


Рис. 17.

Таким образом мы осуществили доступ из интернета к серверу, у которого нет белого адреса.