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

Таблица 12.1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | 22 | | | |
| Сеть | 192.168.2.1/24 | 192.168.3.1/24 | 192.168.4.1/24 | 192.168.5.1/24 |
| Сеть | 210.210.0.1/30 | 210.210.2.1/24 |  |  |

# Настройка списков доступа.

Собираем следующую схему, которая содержит 4 вилана, требующие различного уровня защиты:

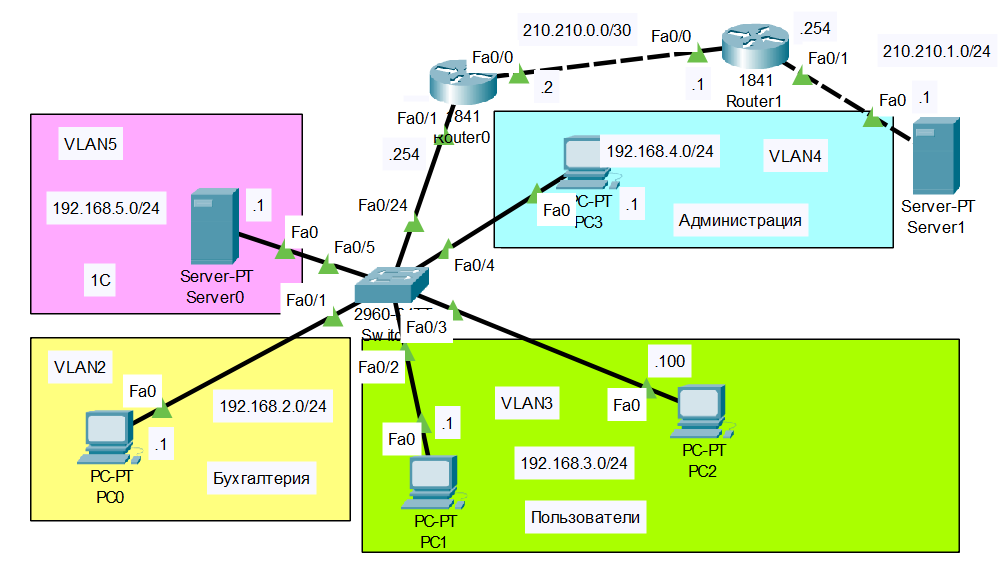
**

Рис. 1

На маршрутизаторе разводим подинтерфейсы, на коммутаторе настраиваем порты в нужные виланы и проверяем доступность оконечных хостов с маршрутизатора. На маршрутизаторе настроен интерфейс с белым ip-адресом (210.210.0.2), направленный в сторону провайдера. Интернет у нас будет симулировать маршрутизатор Router1 и сервер Server1. Проверяем доступность хостов с маршрутизатора.

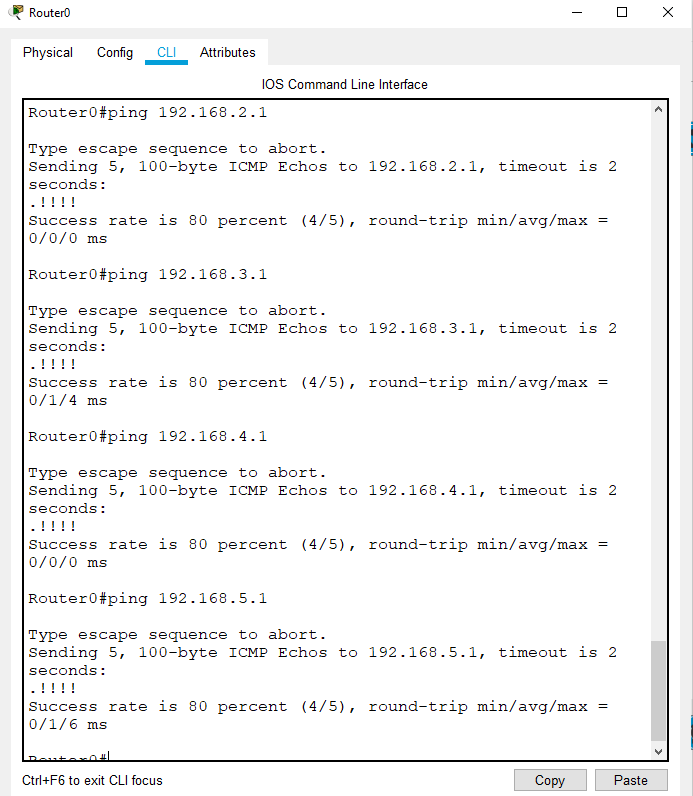


Рис. 2

Теперь нам нужно настроить НАТ для доступа пользователей из внутренней локальной сети в интернет.

Определяем внешние и внутренние интерфейсы как outside и inside в соответствии со схемой (не забывайте, что внутренние интерфейсы прописываются на подинтерфейсах).

Создаем access-list с именем FOR-NAT, в котором разрешаем или запрещаем прохождение пакетов через интерфейс. Аccess-list бывают двух видов: стандартные или расширенные. Для начала воспользуемся стандартным access-list.

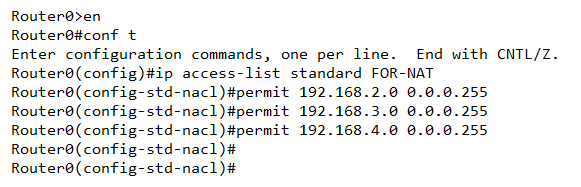


Рис. 3.

Здесь используется команда permit, которая разрешает прохождение трафика, а команда deny – запрещает. Далее идут два параметра: первый – адрес сети в которую разрешаем (запрещаем) трафик, а второй – инверсная маска (маска, у которой заменены 0 на 1 и наоборот). На рис. 3 мы разрешили трафик сетей для виланов 2, 3, 4, а 5 вилан не указали, потому, чтобы исключить доступ сервера 1С к сети интернет. Делается это из соображения безопасности. В конце неявно добавляется еще одно правило, запрещающее весь оставшийся трафик. Следующая команда вешает access-list на интерфейс, который смотрит в сторону интернета.

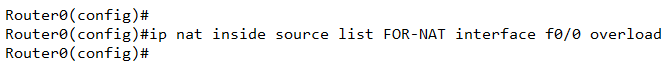


Рис. 4.

Вот настройки оборудования перед началом настройки

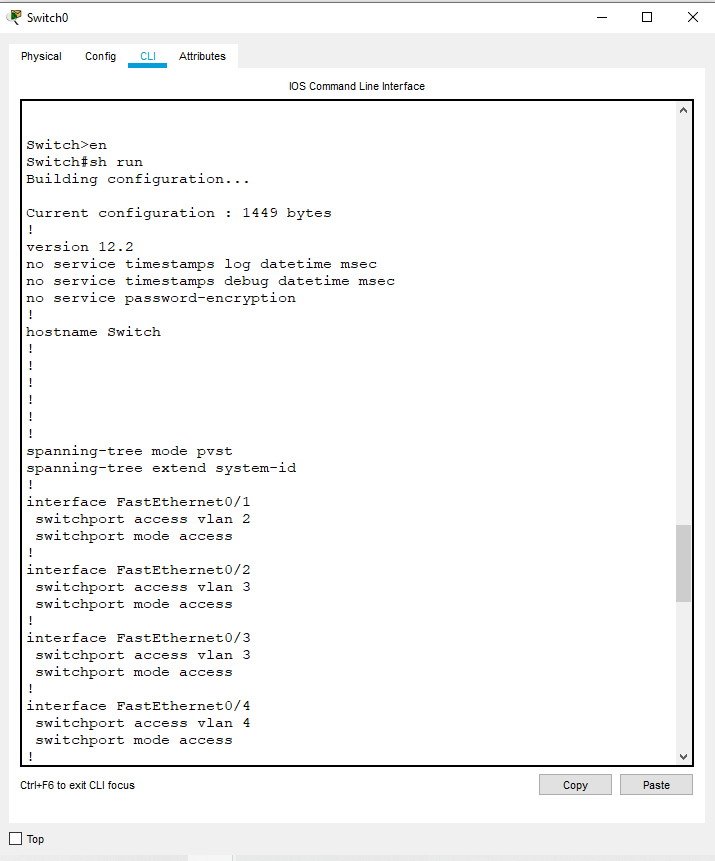


Рис. 5.

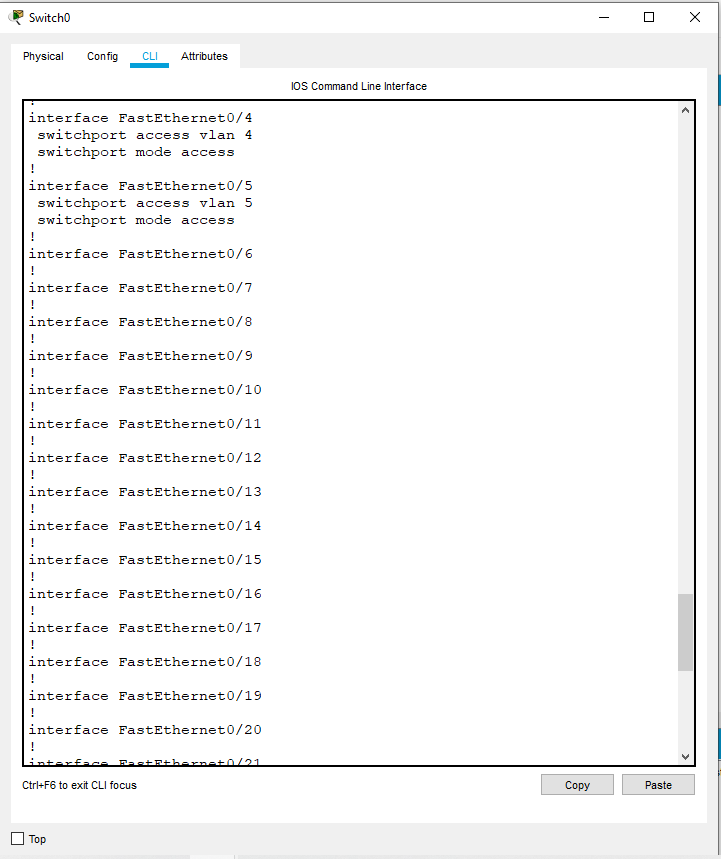


Рис. 6.

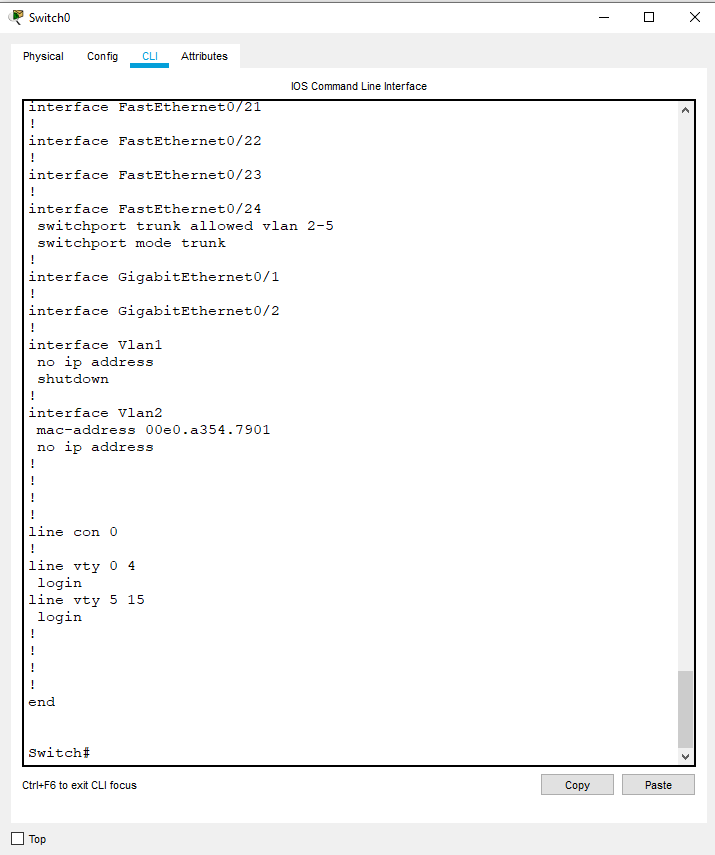


Рис. 7.

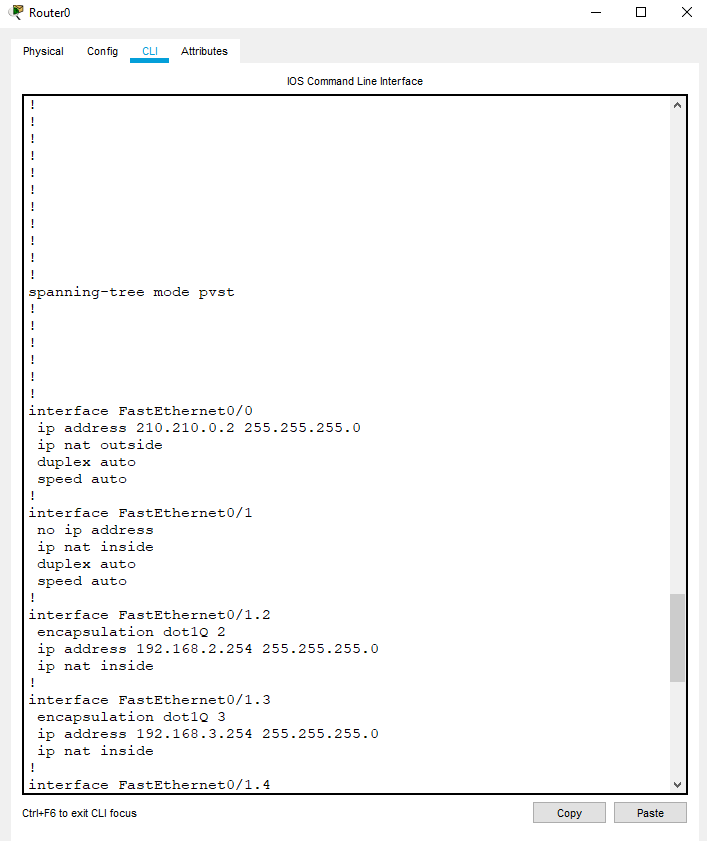


Рис. 8.

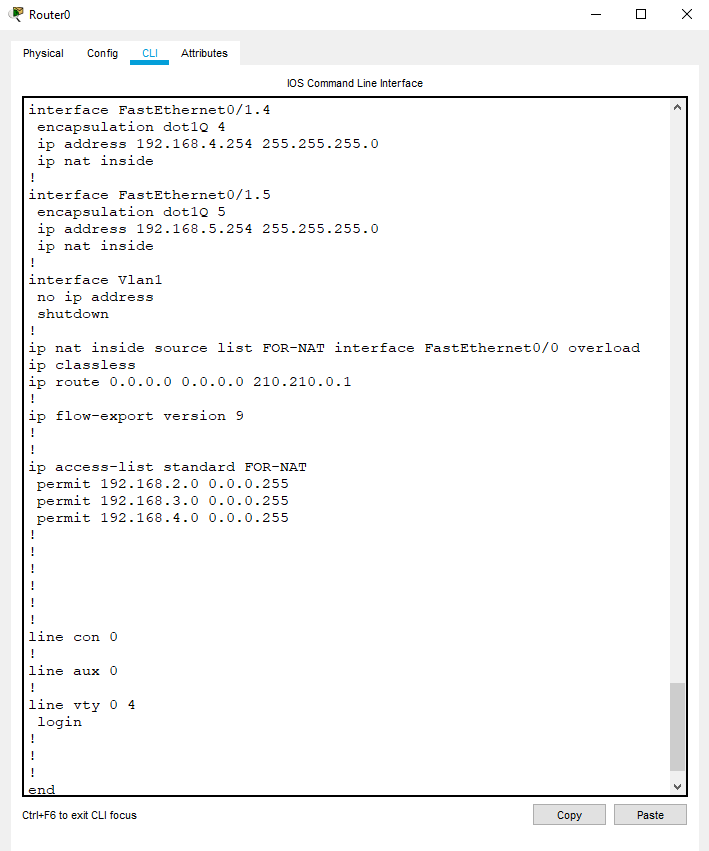


Рис. 9.

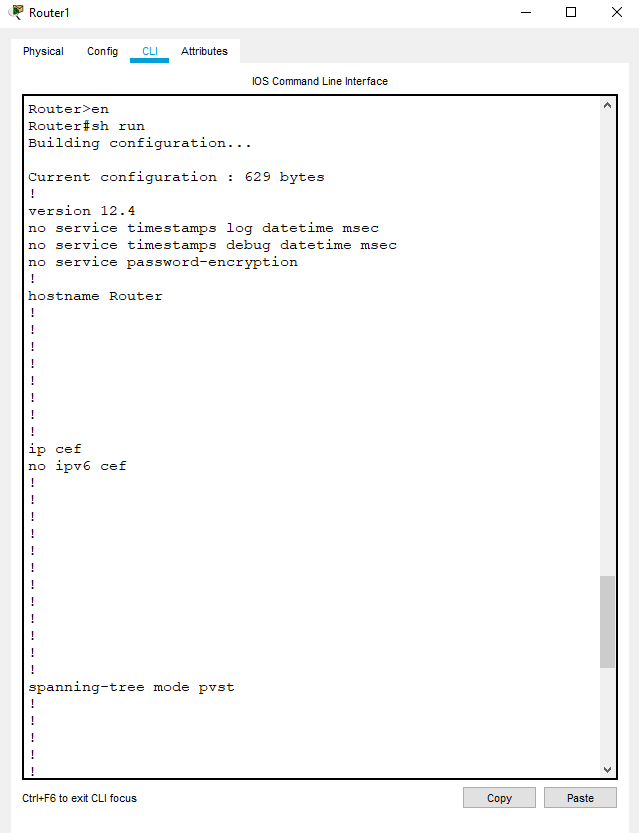


Рис. 10.

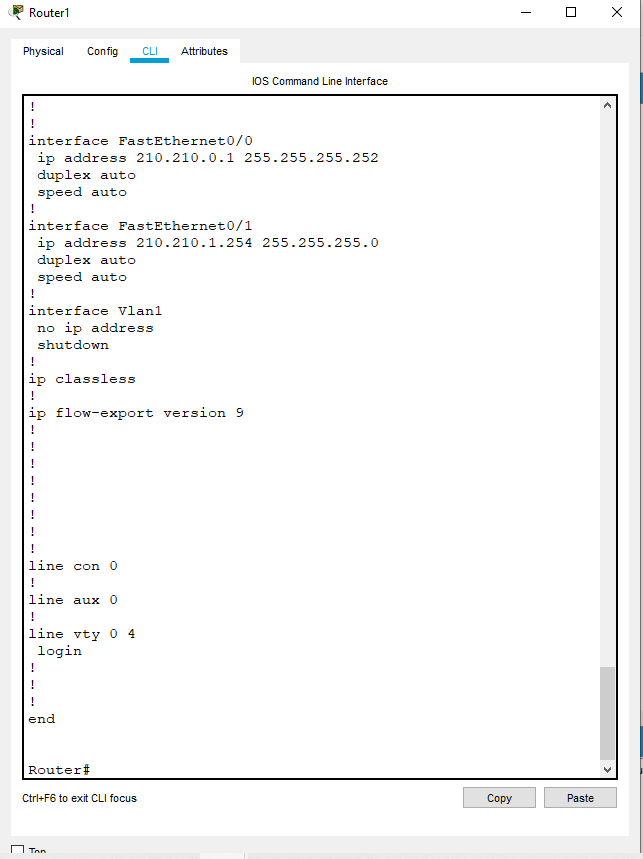


Рис. 11.

Проверяем доступность сервера провайдера.

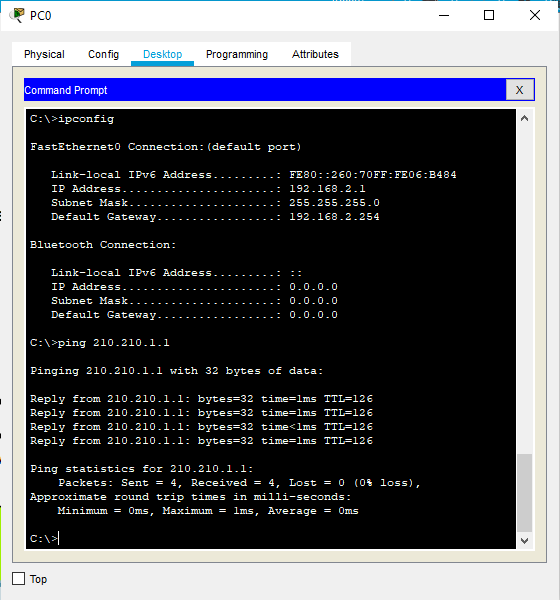


Рис. 12. Сервер провайдера доступен.

# Доступ к сети интернет с сервера 1С

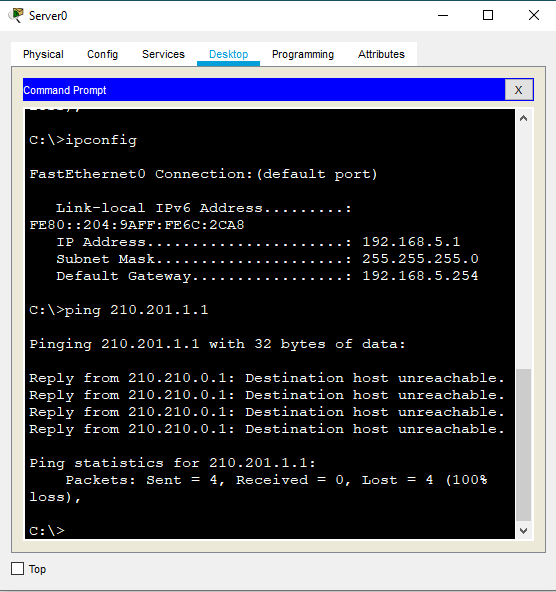


Рис. 13.

Как видим доступа нет, поскольку мы не включили его в access-list. Это первый пример использования access-list для ограничения доступа к сети интернет средствами НАТ.

В локальной сети мы имеем серые ip-адреса, которые не светятся в сети интернет. На рис. 12 мы видели доступ из локальной сети от РС0 до сервера провайдера, а теперь попробуем обратный пинг от сервера провайдера до локальной машины РС0:

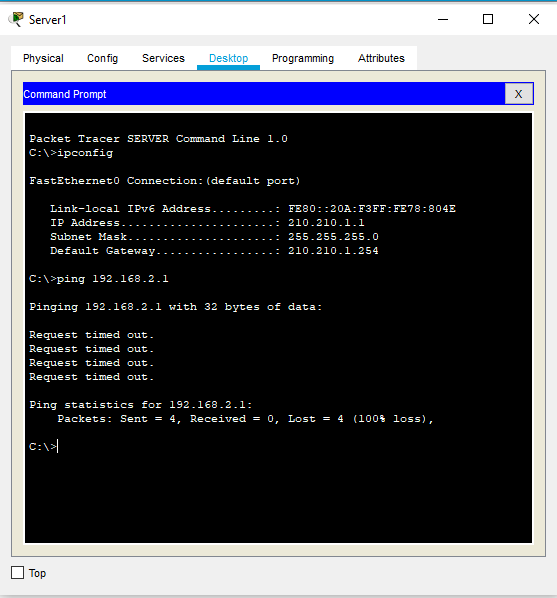


Рис. 14.

Из интернета локальная сеть не видна. Но если злоумышленник взломал роутер провайдера или смог вклиниться между нашим роутером и роутером провайдера, то он может прописать маршруты во внутренние сети. Внутренние сети он даже может не знать, но достаточно выбрать какие-нибудь популярные сети, например, 192.168.0.0/16, которые есть практически в любой организации. Таким образом получить доступ во внутреннюю сеть. Предположим взломан маршрутизатор провайдера и на нем выполнено:

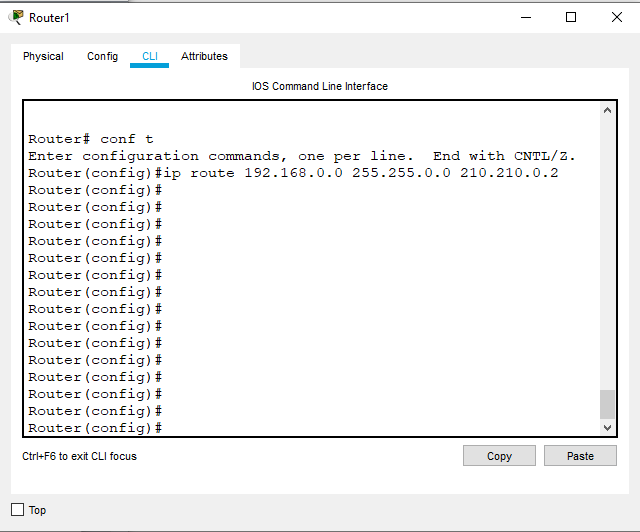


Рис. 15.

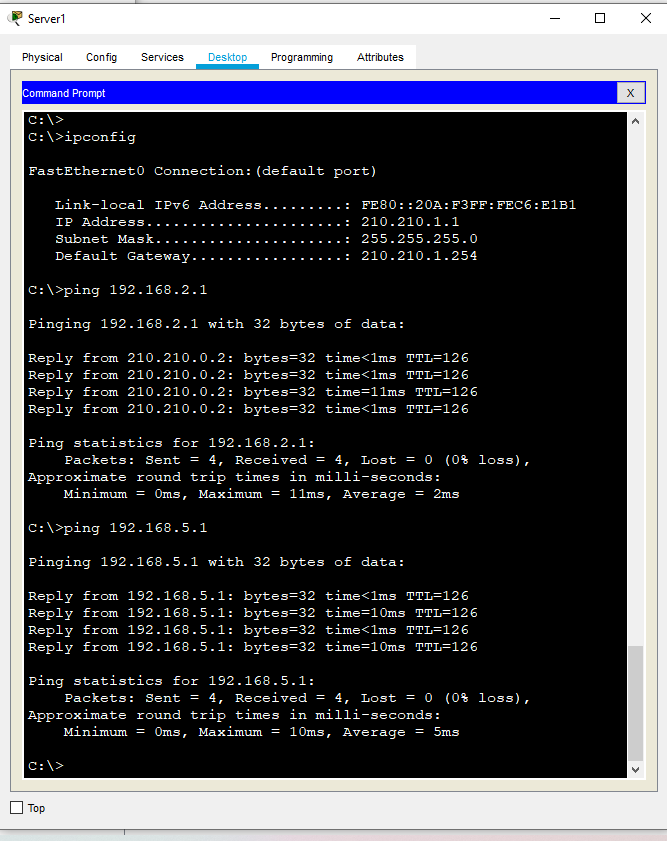


Рис. 16.

И так, злоумышленник получил доступ ко всей нашей сети, даже к серверу 1С! Теперь будем ограничивать доступ к внутренней сети. Можем ограничить на входе в граничный маршрутизатор или на его выходе. Будем ограничивать на входе, чтобы трафик не входил в маршрутизатор. Для этого будем использовать расширенные access-list применяя их на входящий трафик потому, что инициация сессий будет идти с внешней сети и в качестве отправителя может выступать любой адрес, а в качестве получателя будут выступать сегменты локальной сети.

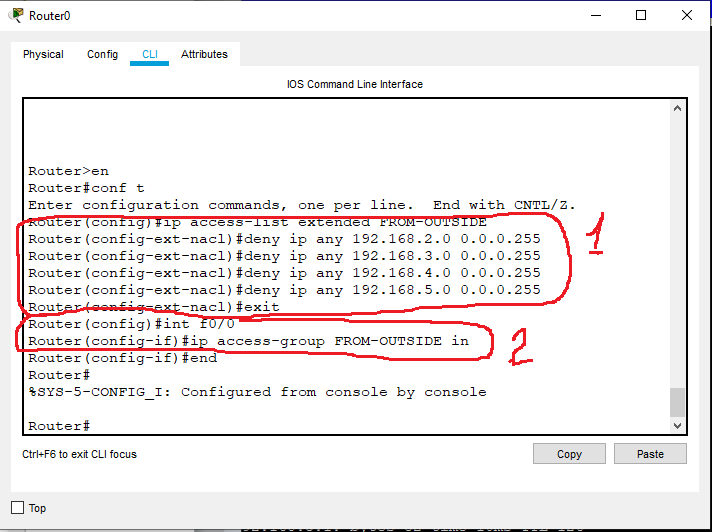


Рис.17.

Создаем access-list (1) и применяем его на входном интерфейсе (2). Проверяем доступность компьютеров.

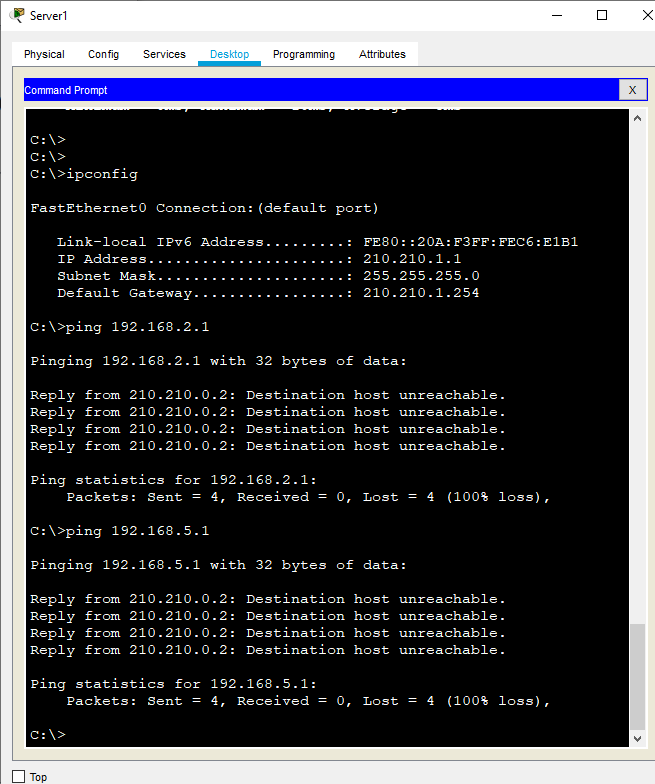


Рис. 18.

Видим, что пинг уже не проходит, однако проверим доступ в интернет.

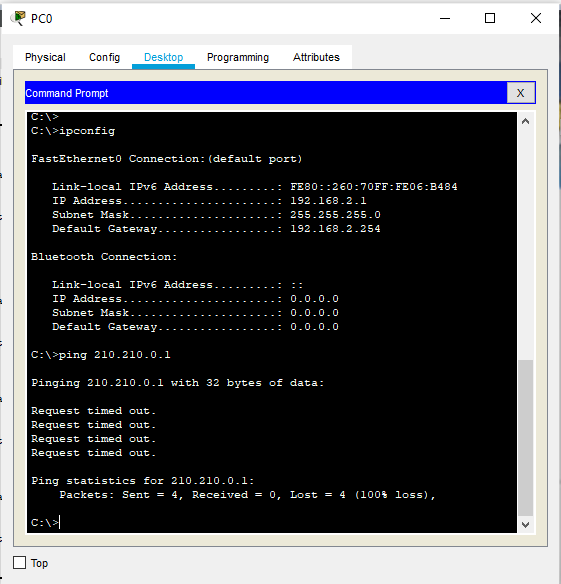


Рис. 19.

Доступа тоже нет. Если посмотреть на access-list, то видим:

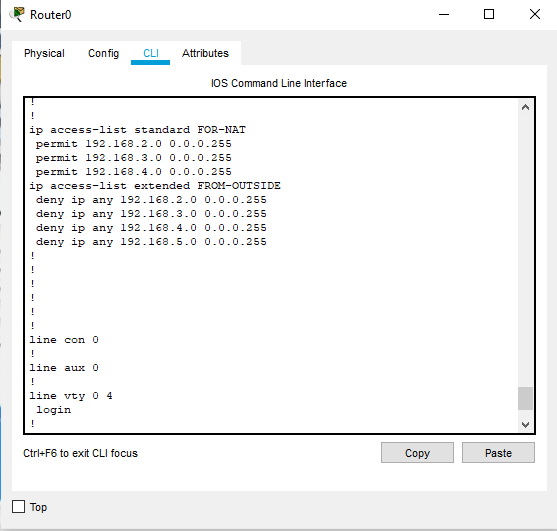


Рис. 20.

На access-list FROM-OUTSIDE запрещающие правила, а в конце существует еще одно запрещающее правило, которое запрещает все остальное. Поэтому интернет не работает. В конце списка доступа нужно разрешающее правило, которое разрешит ответы из интернета.

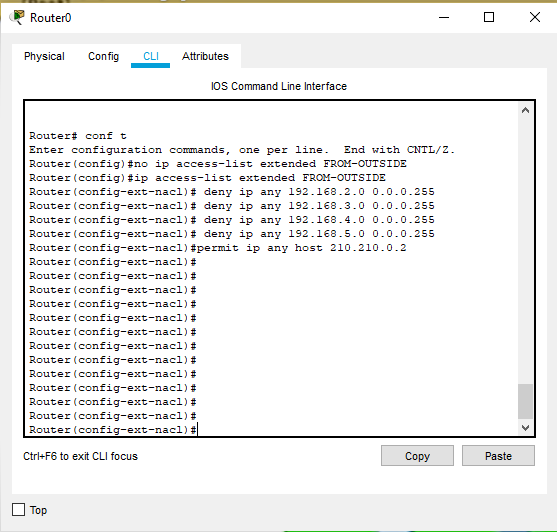


Рис. 21.

Проверяем доступность компьютеров.

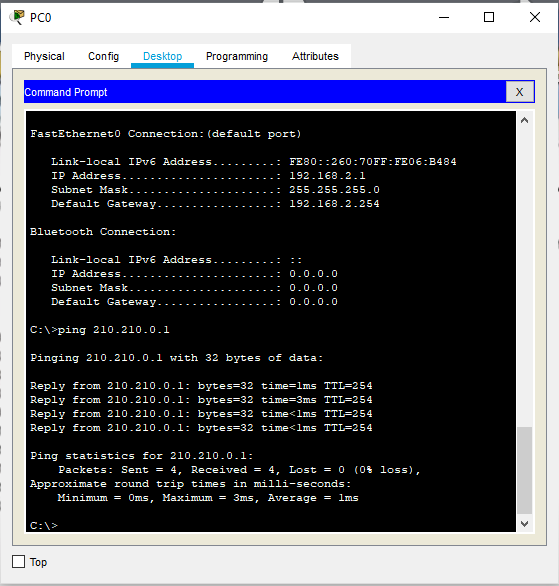


Рис. 22.

Теперь трафик проходит, посмотрим а как из интернета.

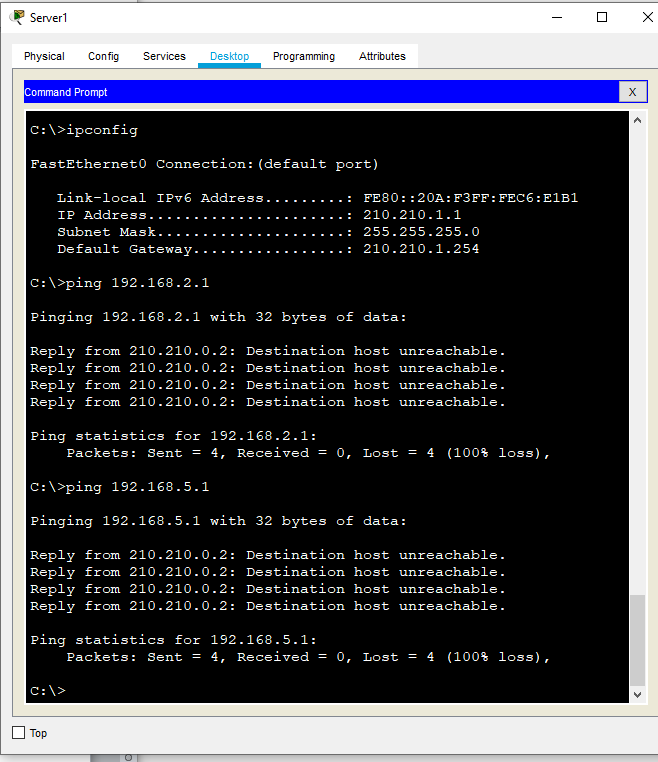


Рис. 23.

По-прежнему ничего не проходит. Трафик из интернета не прохоит. Но можно все это же сделать гораздо проще:

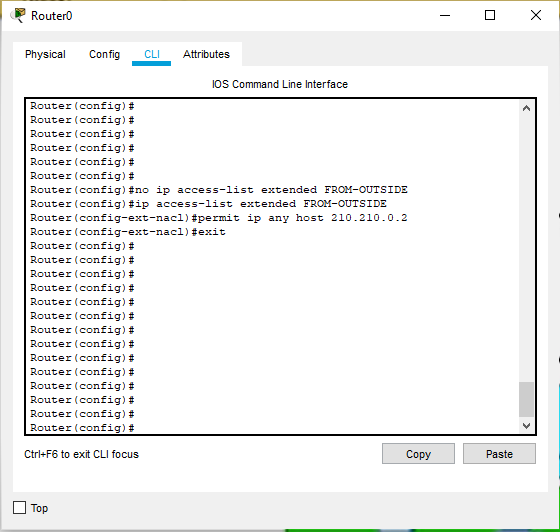


Рис. 24.

Со стороны локальной сети все работает:

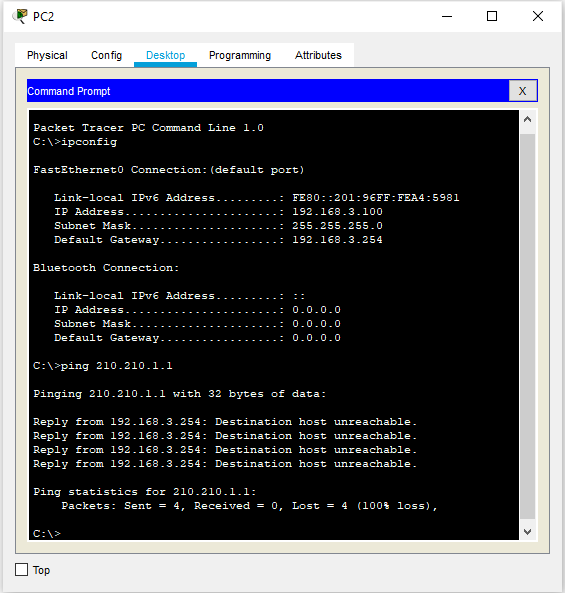


Рис. 25.

А со стороны интернета все закрыто:

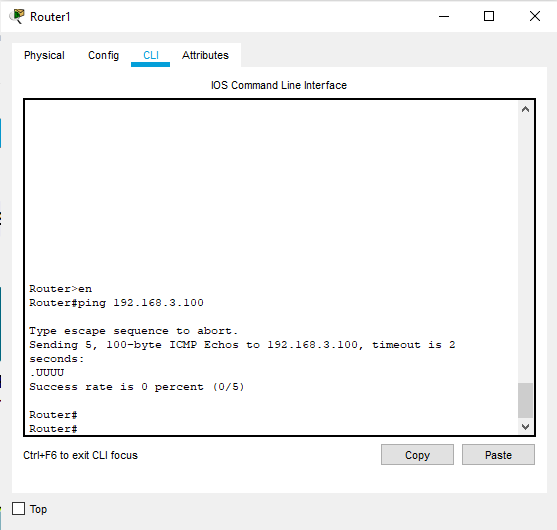


Рис. 26.

Таким образом одним access-list мы обезопасили внутреннюю сеть от внешнего воздействия и проникновения.

**Доступ по телнету.**

На граничном маршрутизаторе создаем пользователя, задаем пароль для enble и предоставим удаленный доступ используя локальную базу пользователя.

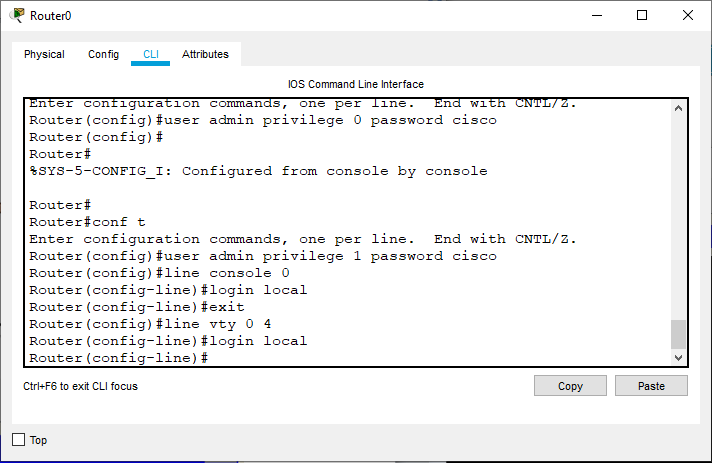


Рис. 27.

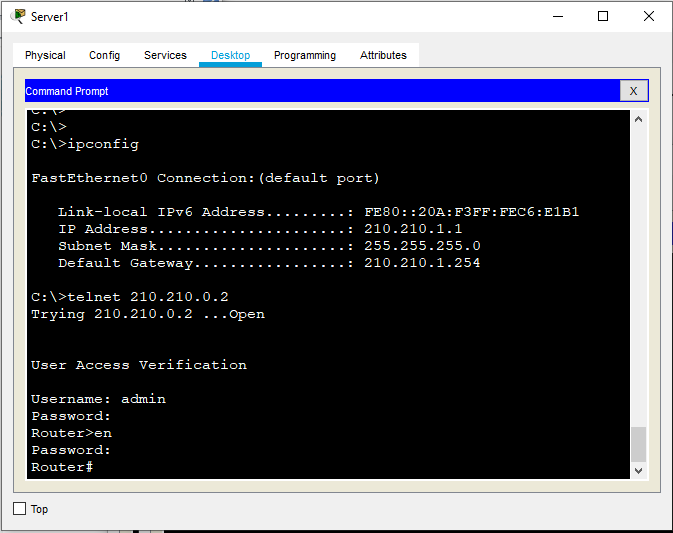


Рис. 28.

Доступ к роутеру есть, но это не совсем хорошо, поскольку даже если злоумышленник не знает пароля, он может его подобрать. Поэтому администратор решает запретить доступ по телнету из внешней сети.

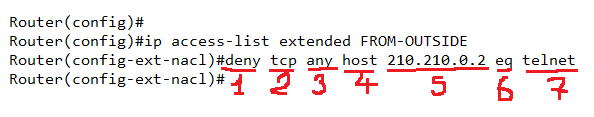


Рис. 29.

Здесь создается запрещающее правило (1), которое работает по протоколу tcp (2) для всех источников (3) на один приемник (4) в виде хоста с адресом 210.210.0.2 (5) только по одному порту (6), предназначенному для работы с телнетом. После его применения доступ по телнету сохранился.

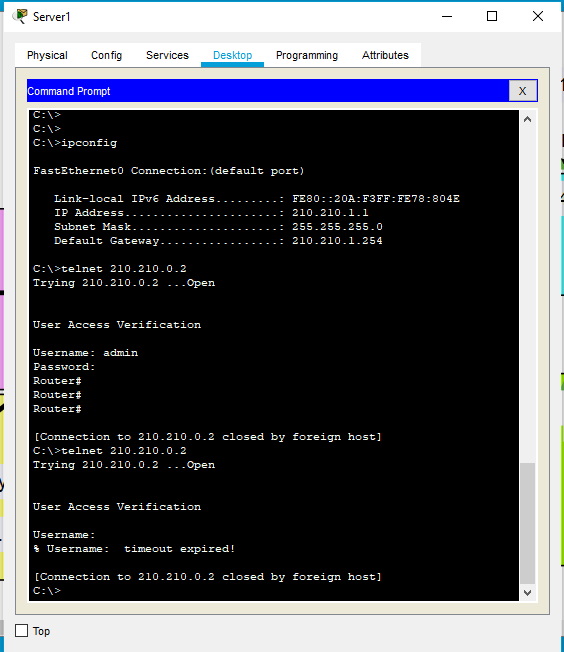


Рис. 30.

Если внимательно посмотреть на список доступа, то можно заметить:

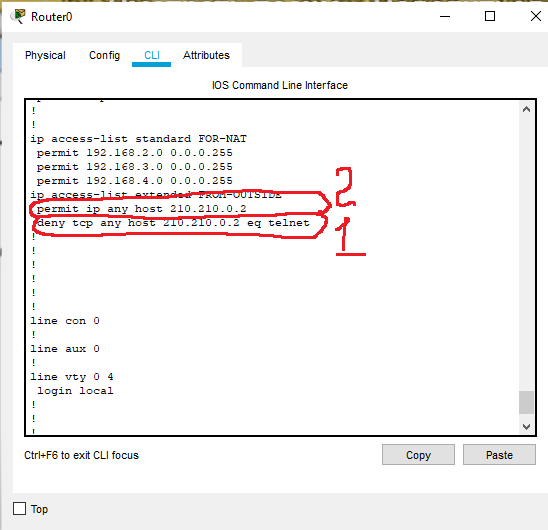


Рис. 31.

Запрещющее правило (1) расположено после разрешающего (2). Практически везде списки доступа работают сверху вниз: т.е. трафик, попав на маршрутизатор проверяется сначала первым правилом, которое разрешает весь трафик, а до второго правила очередь так и не дошла. Поэтому более детальное правило должно быть раньше. Наиболее специфичные правила с указанием портов всегда должны быть расположены раньше. Исправим список доступа:

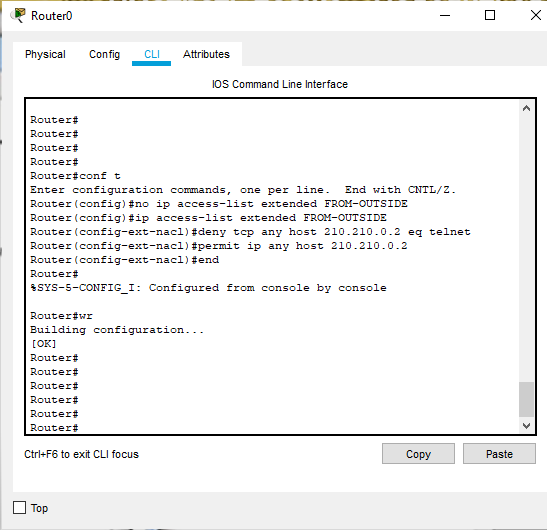


Рис. 32.

Попробуем подключиться снова.

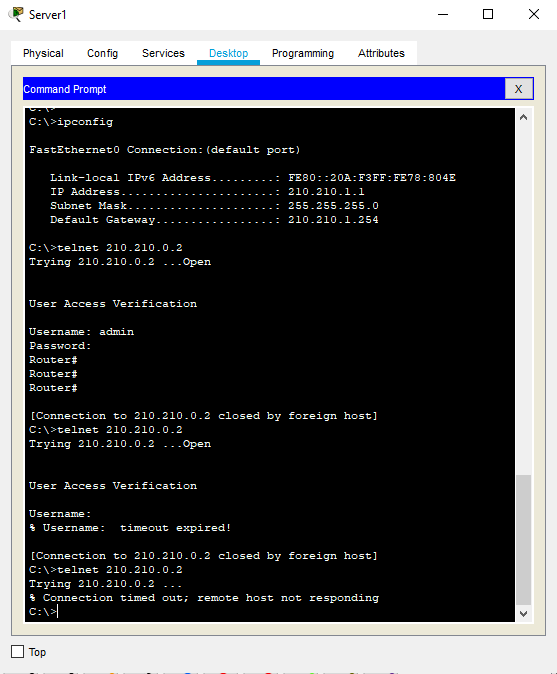


Рис. 33.

А теперь подключиться не удалось. Мы смогли запретить доступ как к локальной сети так и доступ по телнету к маршрутизатору. Все это было установлено на входящий трафик.

# Сервер 1С.

В нашей сети имеется сервер 1С и доступ к нему должны иметь только пользователи из бухгалтерии. Мы можем использовать для этого два способа:

1 Для каждого сегмента создать разрешающее или запрещающее правило и применить эти правила на входящий трафик.

2 Применить одно правило на исходящий трафик с интерфейса сервера, в котором будет разрешена одна сеть бухгалтерии.

Применим второй способ.

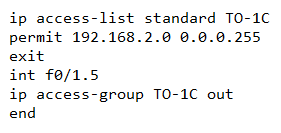


Рис. 34.

Проверим со стороны бухгалтерии:

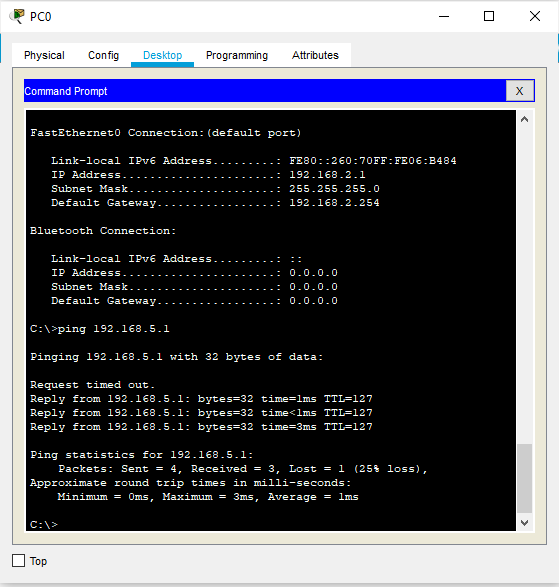


Рис. 35.

Работает, а со стороны других сегментов:

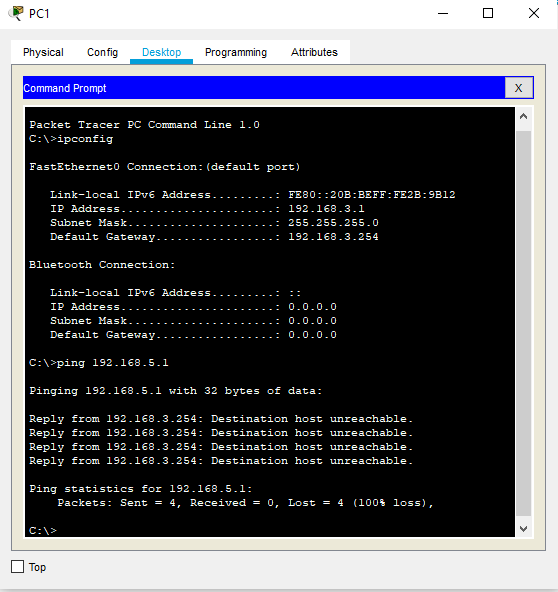


Рис. 36.

Недоступно!

# Веб-сервер.

Теперь предположим, что в интернете есть веб-сервер. Сконфигурируем его.

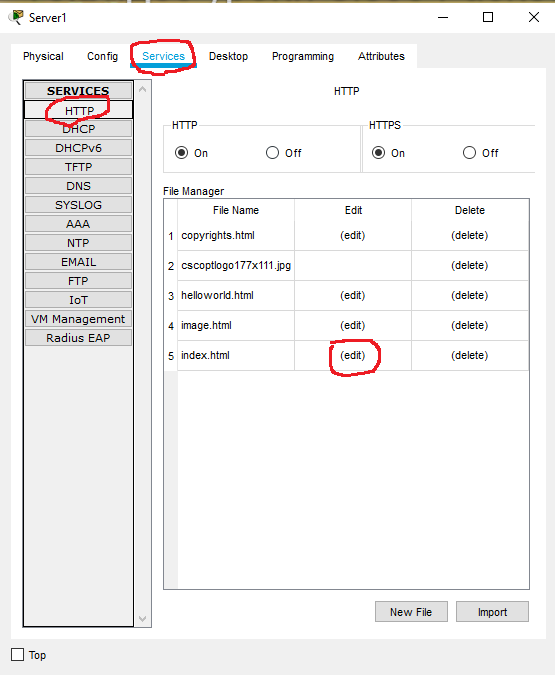


Рис. 37.

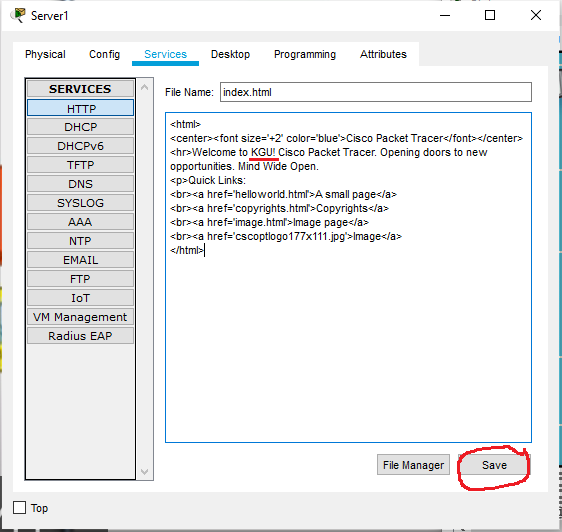


Рис. 38.

Проверим с компьютера пользователя доступ к нему.

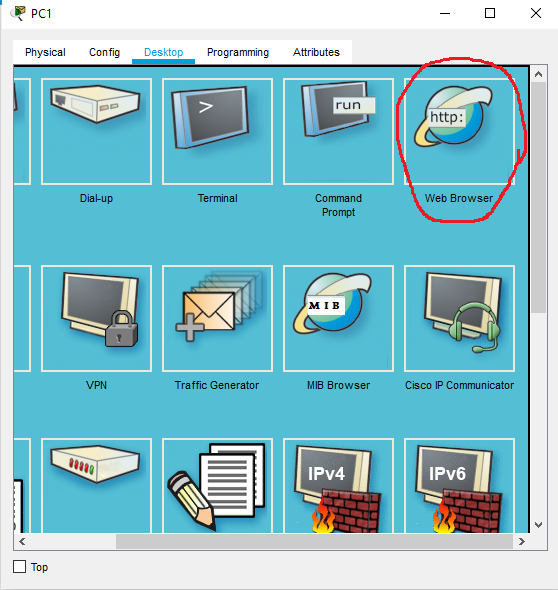


Рис. 39.

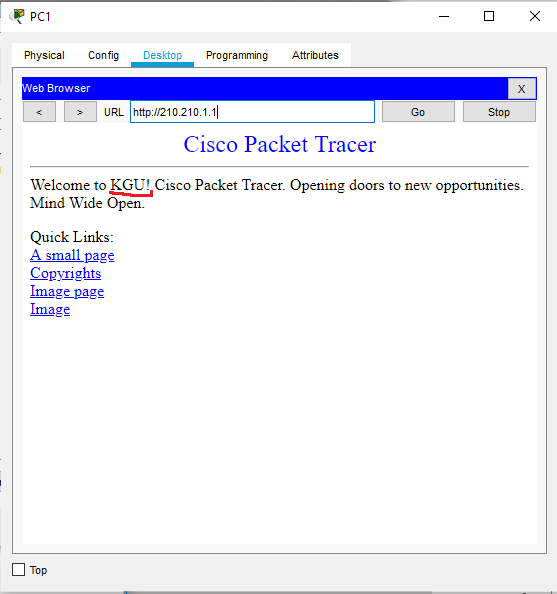


Рис. 40.

А теперь стоит такая задача: до данного сервера пользователи должны иметь доступ только по протоколу http. Но в сегменте «Пользователи» есть администратор с адресом 192.168.3.100 (это ваш компьютер), которому надо дать полный доступ к серверу (зачем же себя ограничивать?). Поэтому для него должны быть разрешены и ping, rdp и т.д. При создании сложных списков доступа лучше сначала их создать в блокноте, а затем применять.

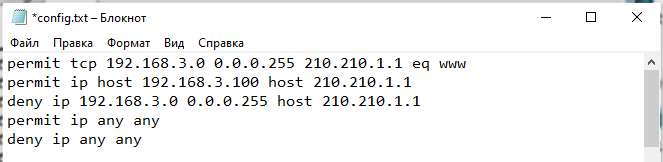


Рис. 41.

Последняя строка добавляется автоматически, а здесь она показана, чтобы помнить, что она есть. Переносим конфигурацию в роутер.

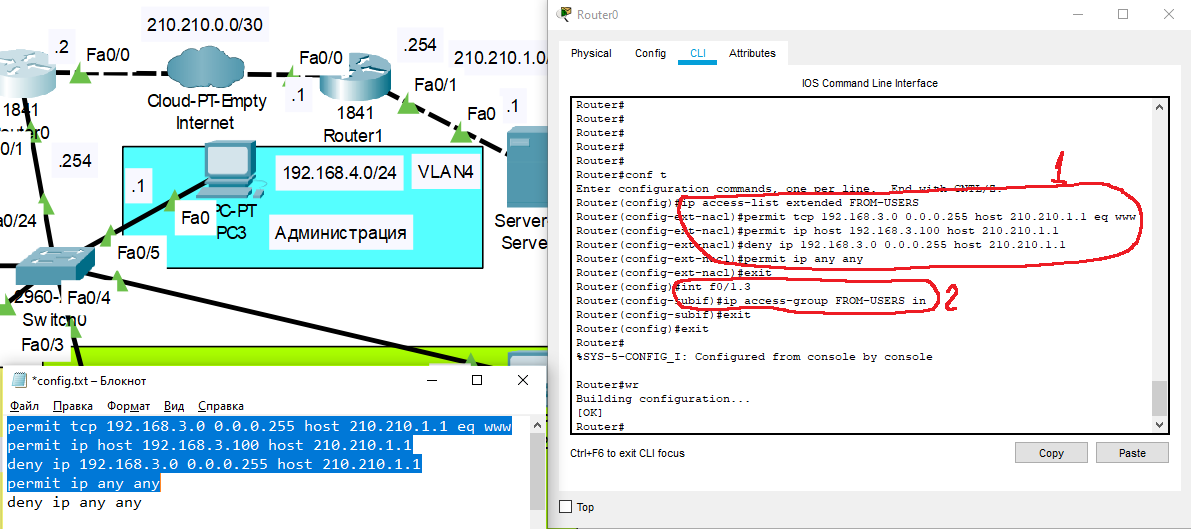


Рис. 42.

Применяем созданный список доступа (1) к подинтерфейсу f0/1.3 на входе (2).

Проверяем доступ пользователей по протоколу http.

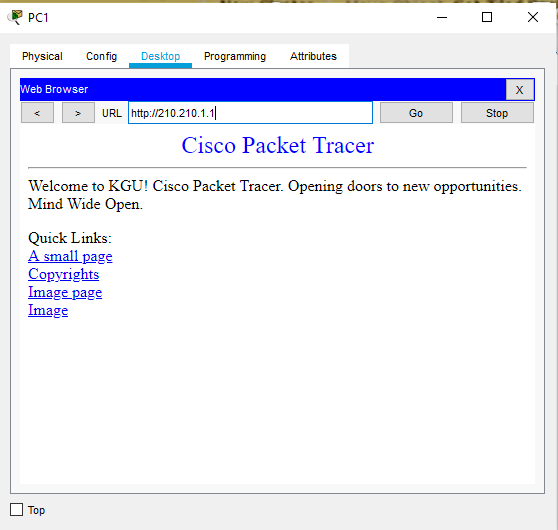


Рис. 43.

А пинги не работают

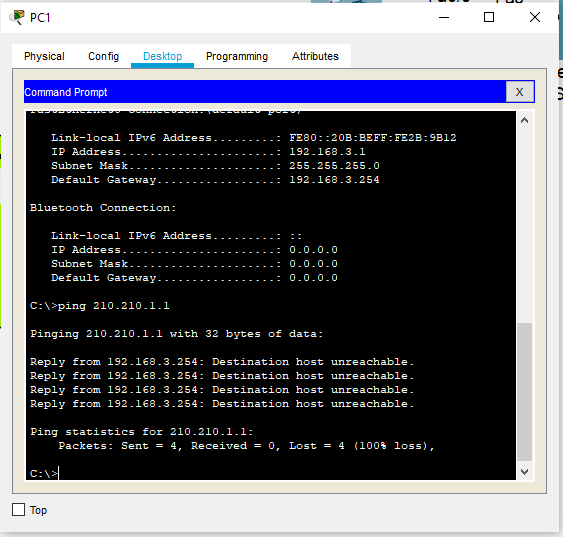


Рис. 44.

Проверим пинг с машины администратора:

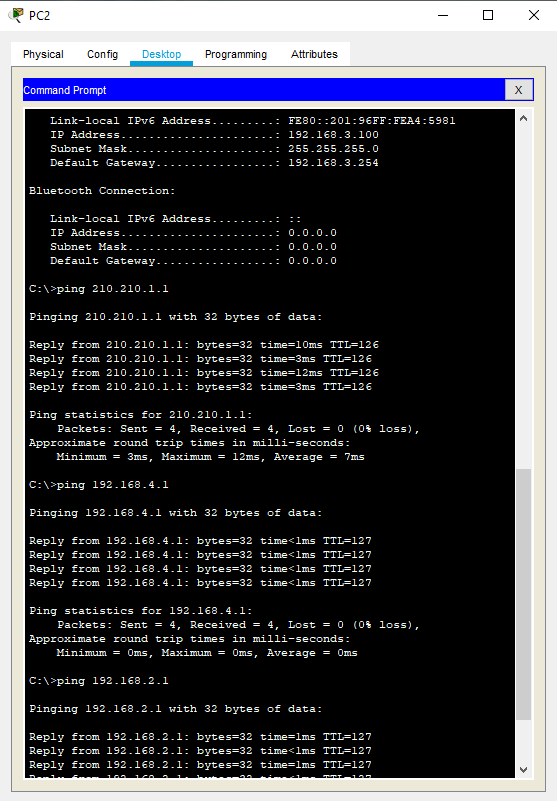


Рис. 45.

Работает!

# Заключение.

Мы ознакомились с расширенными access-list, ограничив доступ как из внешней, так и из внутренней сети, познакомились со стандартным access-list, который мы повесили на исходящий трафик и рассмотрели применение access-list для технологии НАТ