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

Таблица 13.1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | 22 | | | |
| Сеть 1 | 192.168.1.1/24 | 210.210.0.1/30 | 210.210.1.1/24 |  |

# Cisco ASA

В связи с тем, что скачать образ cisco ASA скачать не удается, придется лабораторную работу делать в приложении Cisco Packet Tracer.

Межсетевой экран ASA 5506 выглядит так:

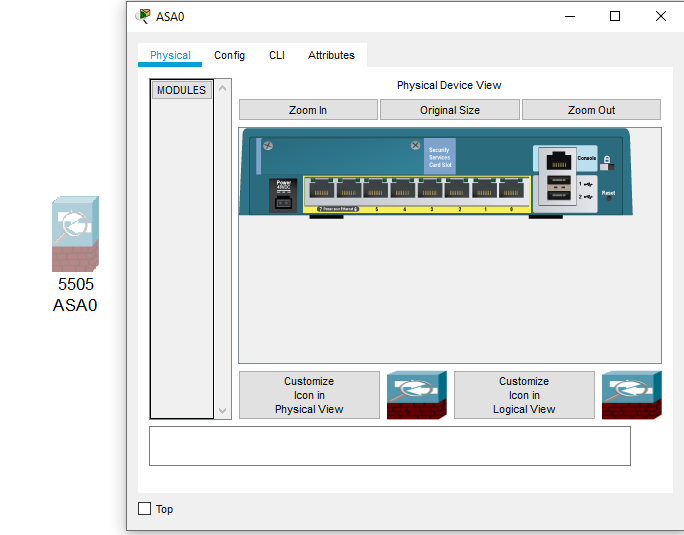


Рис. 1

Необходимо собрать следующую схему

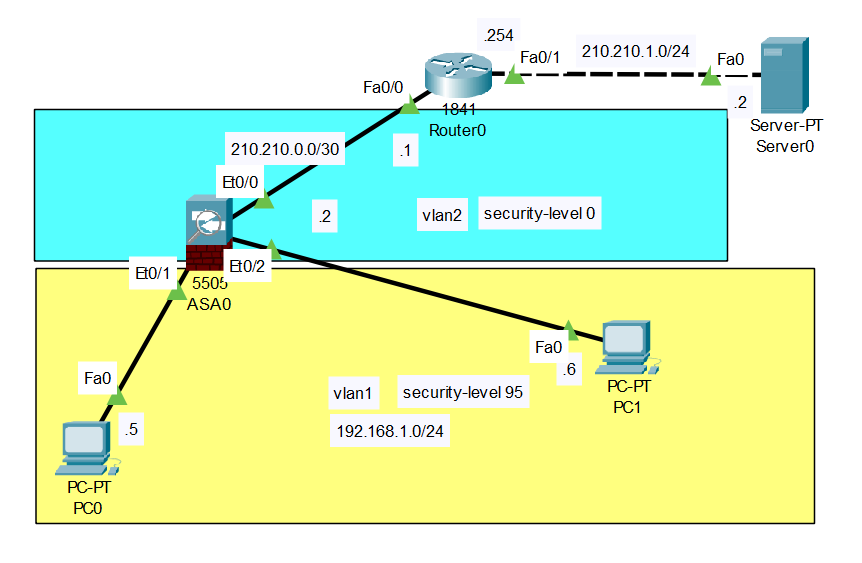


Рис. 2

Входим в привилегированный режим cisco ASA, используя вместо пароля просто ENTER. С помощью команды sh ver проверяем версию прошивки и видим имя файла прошивки.

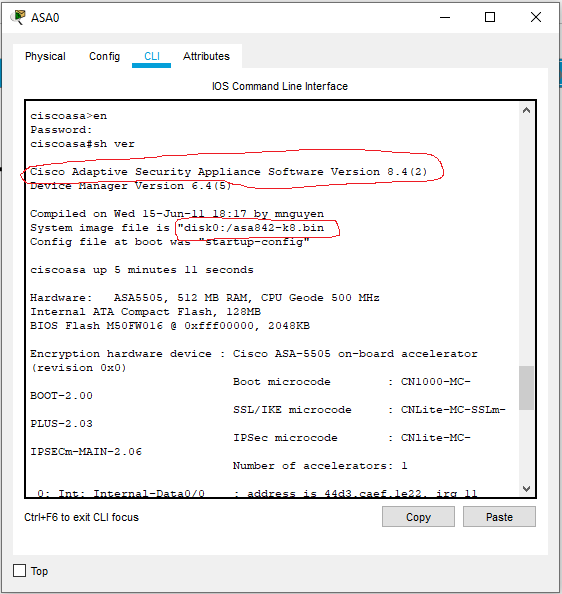


Рис. 3

Здесь установлено:

1 базовая лицензия

2 максимальное количество vlan-ов всего 3

3 нет возможности использовать транковые порты

Поэтому моделировать здесь не очень хорошо, но некоторые начальные сведения получить все же можно.

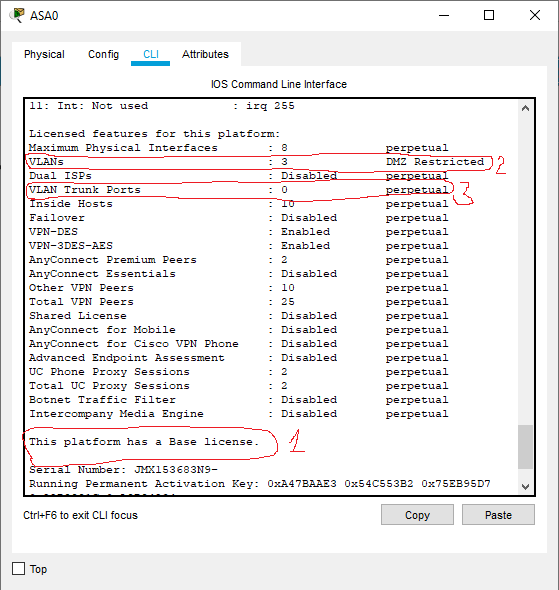


Рис. 4

ASA 5505 – это L3-коммутатор с функциями межсетевого экрана

5510, 5520, 5540 – это маршрутизатор с функциями межсетевого экрана

Посмотрим, что предустановлено на ASA 5505:

1 порт e0/0, к которому подключен провайдер уже подключен в vlan2.

Остальные порты настроены в vlan1 по умолчанию. Эти виланы преднастроены, т.е. на них настроены виртуальные интерфейсы. На ASA 5505 настроены наименования интерфейсов. Обратите внимание, что настроен security-level. На вилане 2 настроен dhcp-клиент, который будет ждать адреса от провайдера. Во внутреннюю сеть настроен dhcp-сервер, который будет раздавать адреса в нее.

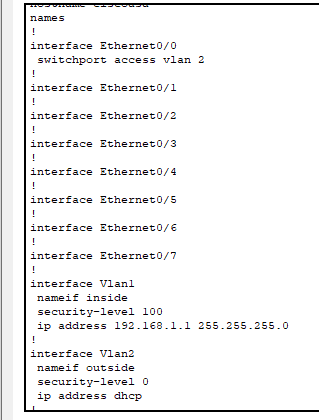


Рис. 5

Посмотрим, получили ли адреса компьютеры:

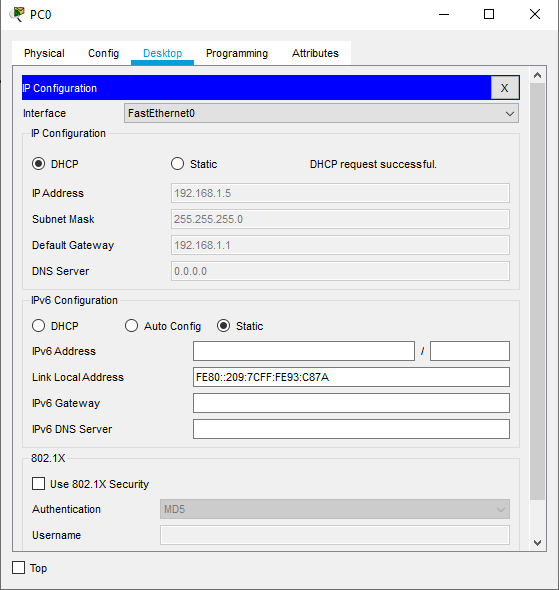


Рис. 6

Адрес действительно получен. Предположим, что на РС0 находится администратор. Выполним на cisco ASA следующие команды:

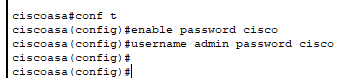


Рис. 7

Просмотрите настройки

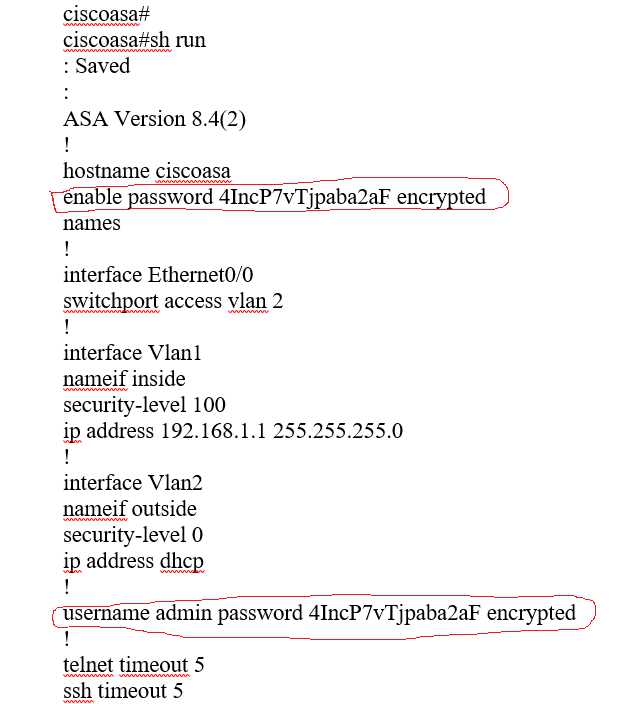


Рис. 8

Пароль по умолчанию на enable и на пользователя зашифрован. Это одна из включенных функций безопасности. На маршрутизаторах и коммутаторах их необходимо включать явно. Настраиваем протокол SSH. А далее задаем параметры аутентификации пользователя, в которой указываем, чтобы использовать локальную базу.

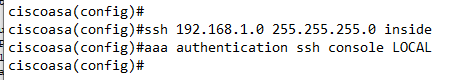


Рис. 9

Пробуем доступ от пользователя.

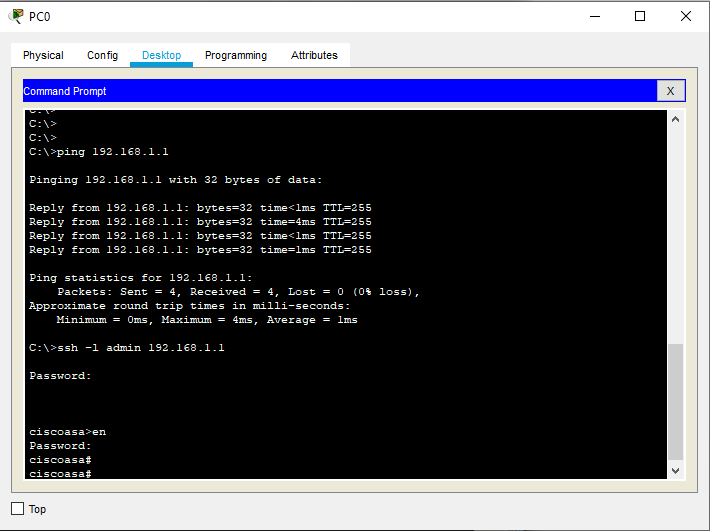


Рис. 10

Теперь настройка security-level. А именно: security-level – это уровень доверия к интерфейсу и чем выше этот номер, тем выше уровень доверия. Самый доверенный интерфейс – это внутренний, т.е. наша локальная сеть и самый не доверенный, самый опасный для нашей сети – это внешний интерфейс (интерфейс провайдера). Поэтому на внешнем интерфейсе должен быть самый маленький security-level. В cisco ASA по умолчанию разрешен трафик с интерфейса с большим уровнем доверия на интерфейс с меньшим уровнем доверия. Если представить уровни доверия в виде ступенек, а трафик – в виде воды, то вода при естественных условиях может течь только сверху вниз, а наоборот – никак, так и трафик – ***может проходить только с интерфейса с большим уровнем доверия на интерфейс с меньшим уровнем доверия.***

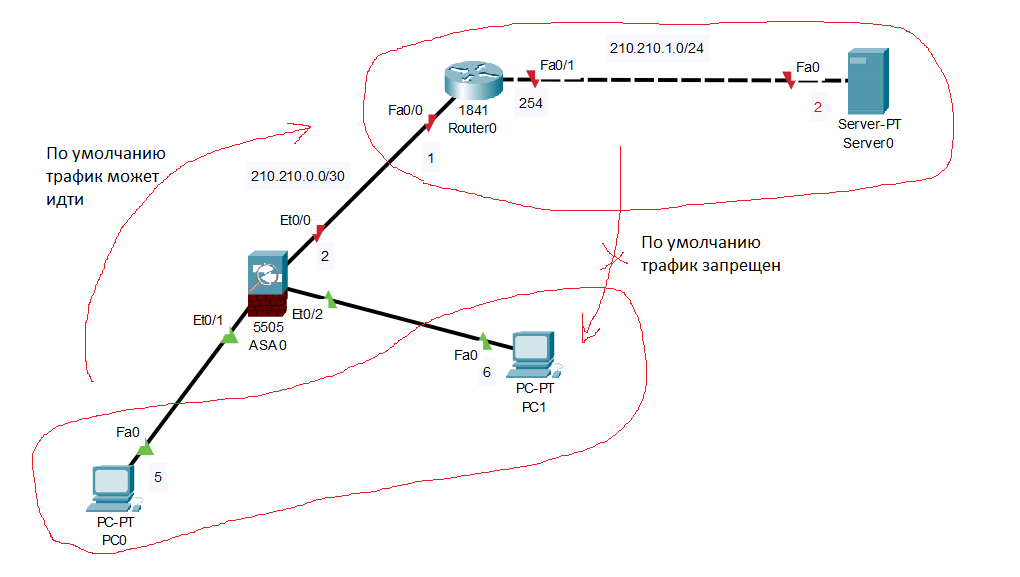


Рис. 11

security-level легко изменить.

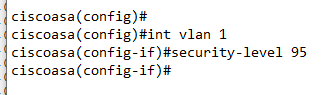


Рис. 12

Донастроим интерфейс провайдера. Будем считать, что нам дали адрес 210.210.0.2/30.

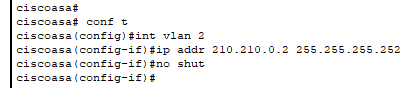


Рис. 13

Прописываем адреса на маршрутизаторе в соответствии со схемой на рис.2. Проверим с cisco ASA доступ до провайдера. Прописываем маршрут по умолчанию на cisco ASA.

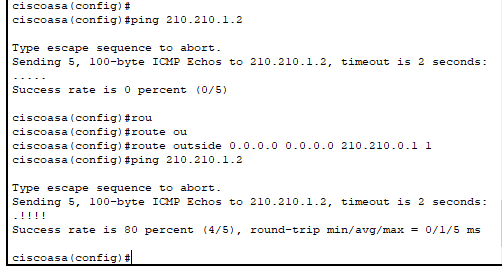


Рис. 14

На роутере прописать шлюз по умолчанию. Проверить доступность провайдера с хоста внутренней сети.

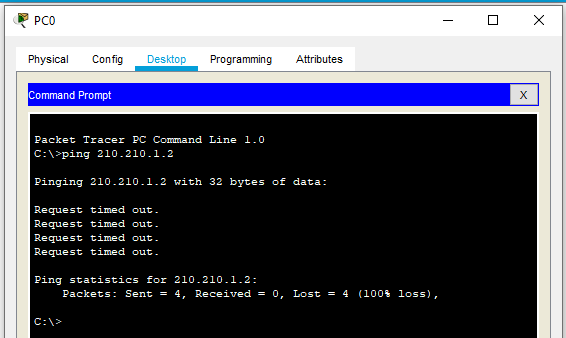


Рис. 15

Как видим доступа нет.

Локальная сеть находится на интерфейсе с security-level = 95, а внешняя сеть находится на интерфейсе с security-level = 0. Уровень доверия локальной сети выше и поэтому трафик по умолчанию разрешен, но ping не проходит, потому, что нужен Stateful packet inspection – это инспекция пакетов с запоминанием состояния. Пусть пользователь инициирует передачу пакетов со своего хоста. Пакет приходит на cisco ASA, она смотрит, что пакет пришел из inside с более высоким security-level, чем внешний интерфейс. Она запоминает эту сессию (т.е. записывает себе в динамическую таблицу) и пропускает дальше пакет. Маршрутизатор отвечает на ping и отсылает встречный пакет. Cisco ASA инспектирует этот пакет: соответствие источника, получателя, портов, номер пакета и если все эти требования удовлетворяют той сессии, которая была запомнена, то пакет пропускается. Пакет проходит только в случае, если сессия была инициирована от интерфейса с более высоким security-level. Если придет «левый» пакет с внешнего интерфейса, то он будет отброшен если нет ранее запомненной для него информации. Это и есть **ИНСПЕКТИРОВАНИЕ ТРАФИКА**! В данном случае инспектирование трафика по умолчанию не настроено.

Настраиваем инспектирование трафика.

1 определяем class-map (тип трафика) и указываем, что мы инспектируем весь трафик, который проходит через cisco ASA;

2 создаем политику (действия над трафиком). В данном случае действия применяются к созданному ранее классу;

3 определяем в каком направлении нужно действовать (входящий, исходящий, глобальный, т.е. во всех направлениях).

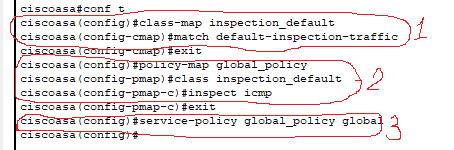


Рис. 16

Пингуем маршрутизатор, затем и сервер провайдера.

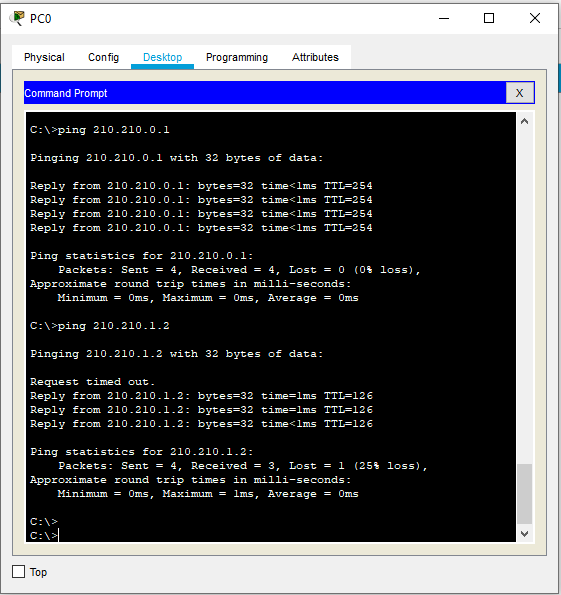


Рис. 17

Все работает. Проверим установлен ли на сервере web-сервис.

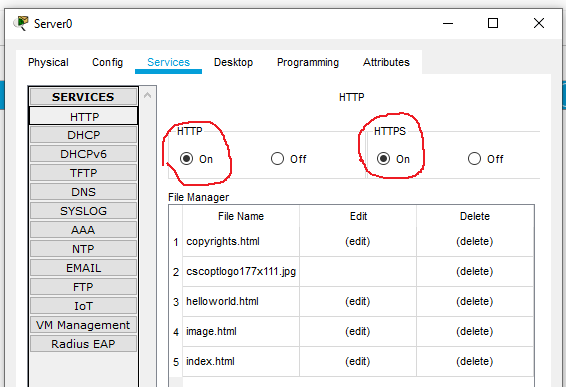


Рис. 18

Проверим доступность сервера с хоста

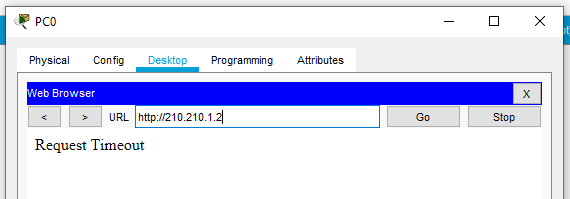


Рис. 19

Видим, что сервер недоступен, в то же время как ping проходит. Это связано с тем, что cisco ASA инспектирует только трафик icmp, а нам нужно, чтобы инспектировал еще и http трафик. Добавим в правило инспектирования следующее:

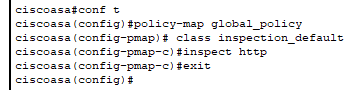


Рис. 20

Проверяем:

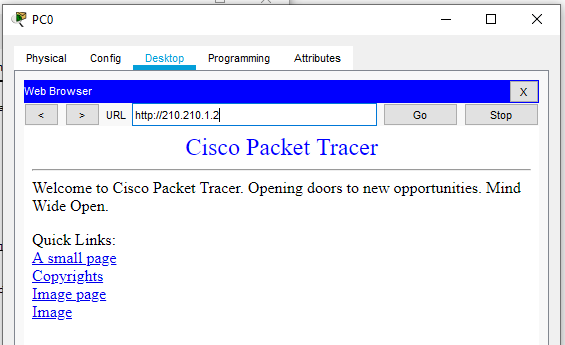


Рис.21

Теперь все работает. Проверяем доступность внутренней сети с сервера.

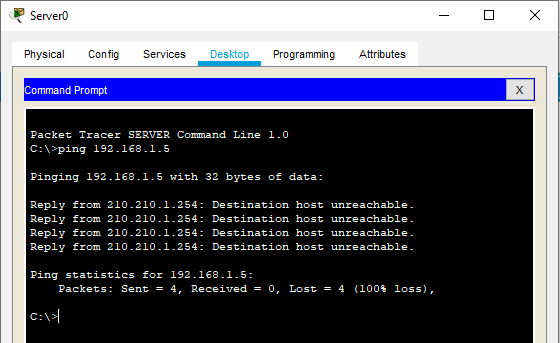


Рис. 22

Как видим внутренняя сеть извне недоступна. Это было сделано по умолчанию, т.к. cisco ASA не разрешает передавать трафик с интерфейса с более низким security-level на интерфейс с высоким security-level. И это было сделано сразу, не прописав ни единого access-list.

А сейчас настроим NAT на cisco ASA, поскольку она существенно отличается от настройки на маршрутизаторах. Во-первых нужно отключить маршрут по умолчанию на маршрутизаторе. Теперь у нас пропал пинг (см. рис.17).

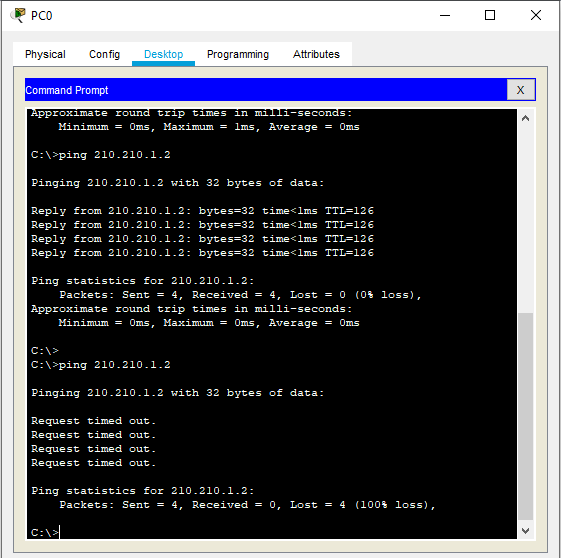


Рис. 23

Настраиваем NAT посредством объектов.

1 создаем объект;

2 в нем определим сеть, которую будем натить;

3 затем переходим к настройкам: указываем внутренний интерфейс, а затем – внешний, указываем, что NAT будет работать динамически, а команда interface говорит, что в качестве адреса, будет использоваться адрес, который висит на внешнем интерфейсе.

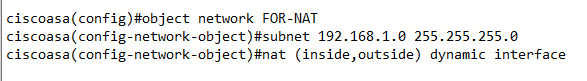


Рис. 24

На этом настройка закончена:

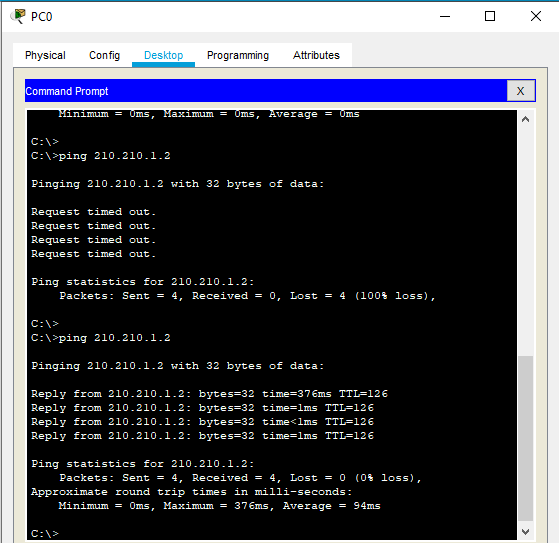


Рис. 25

На cisco ASA можно увидеть следующее:

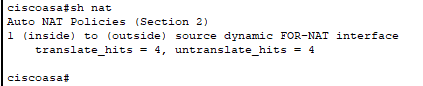


Рис. 26

Видим счетчик пакетов, которые прошли через НАТ.

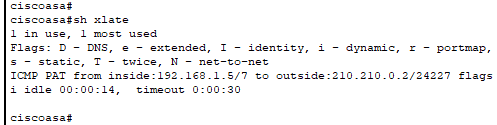


Рис. 27

А здесь мы видим более подробную информацию о работе НАТ.

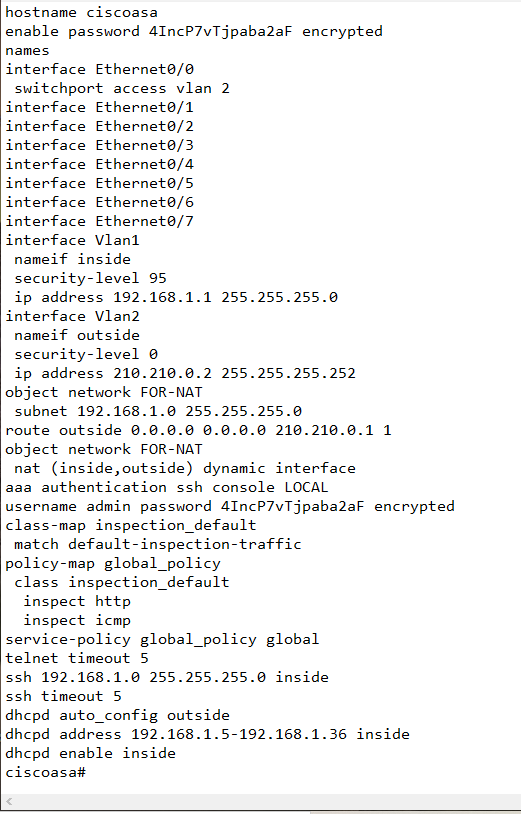


Рис. 28.

Распечатка конфигурации Cisco ASA