САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Практическая работа №6. Трансляция адресов (NAT) в Cisco Packet Tracer.

Выполнил: Титов Г.К. (409687)

Проверил: Харитонов А.Ю.

Санкт-Петербург

2025 год.

Содержание

Цель работы

Закрепить понимание принципов работы NAT, а также сформировать начальные навыки в конфигурировании NAT и Firewall в Cisco Packet Tracer.

Выполнение работы

1. **Добавление эмуляции сервера в сети Интернет в существующей сети.**

Воспользуемся схемой сети из лабораторной работы №3. Заменим коммутатор 3 уровня на маршрутизатор, который будет маршрутизировать трафик из существующей сети наружу, и настроим на нем сабинтерфейсы.

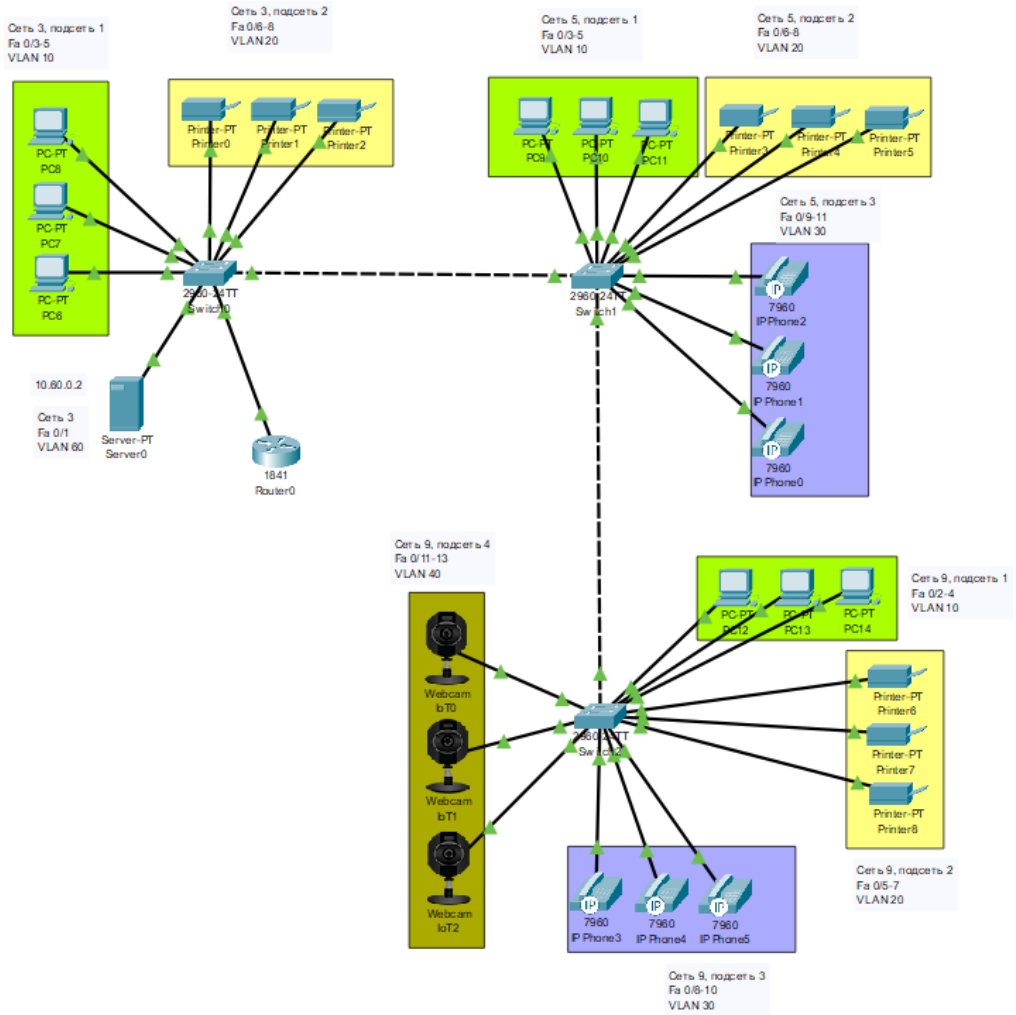

Рисунок 1 - Схема сети после добавления маршрутизатора

Также добавим еще один маршрутизатор, который будет эмулировать провайдера. И сервер, который будет эмулировать сервер в сети интернет.

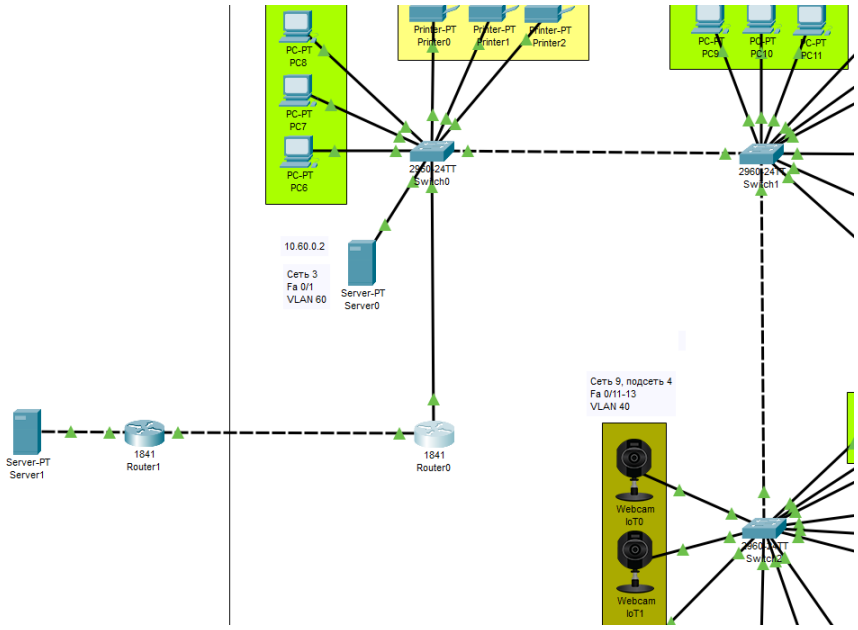

Рисунок 2 - Финальная схема сети

Также назначим на устройствах белые IP-адреса.

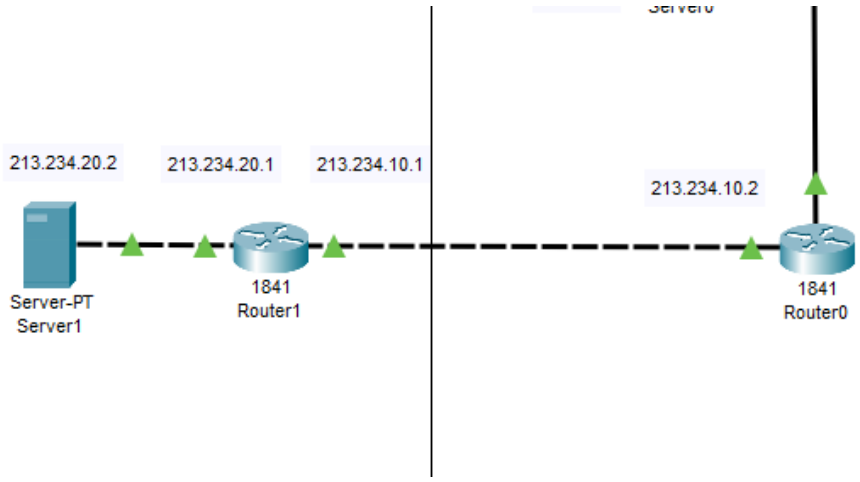

Рисунок 3 - Белые IP-адреса

Если, мы попробуем пропинговать с маршрутизатора в локальной сети маршрутизатор провайдера, то пинг пройдет. Если же тоже самое попробуем сделать с компьютера в нашей локальной сети, то пинг не пройдет. Дело в том что мы используем в нашей локальной сети серые IP-адреса, да и маршрутизатор провайдера не знает об устройствах в нашей локальной сети.

2. Настройка PAT

Сначала нужно определиться, какой интерфейс маршрутизатора провайдера будет являться внешним, а какой внутренним. К внешнему интерфейсу нужно применить команду ip nat outside, а к внутреннему ip nat inside. Необходимо учесть, что внутренних интерфейсов несколько, по количеству VLAN, но доступ в Интернет нужен только компьютерам, ноутбукам и серверу.

Необходимо создать access list'ы, чтобы определить, какой трафик должны пропускать через NAT, с помощью команды ip accesslist standard <ИМЯ_ЛИСТА>, permit (IP адрес VLAN сети 1, wildcard маска VLAN сети 1), permit (IP адрес VLAN сети 2, wildcard маска VLAN сети 2) и т.д.

Настраиваем NAT с помощью команды ip nat inside source list <ИМЯ_ЛИСТА> interface <ИМЯ_ИНТЕРФЕЙСА_OUTSIDE> overload;

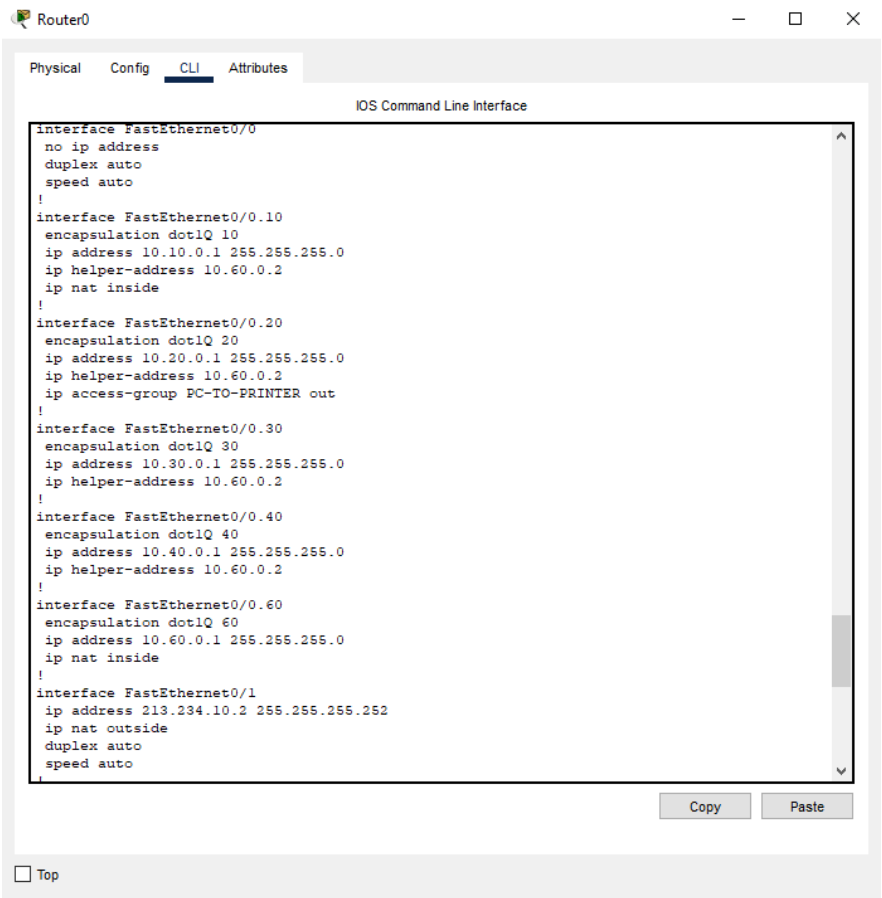

Рисунок 4 - Конфигурация маршрутизатора

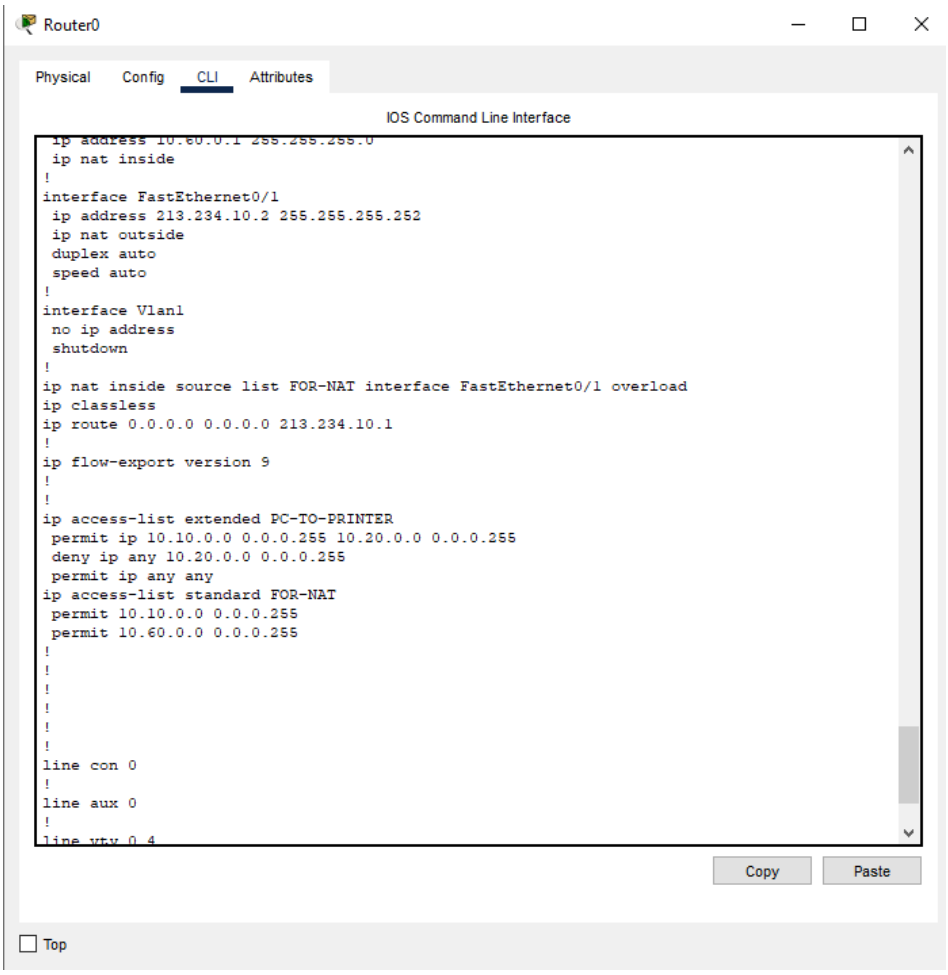

Рисунок 5 - Конфигурация маршрутизатора

Проверим работу NAT с помощью команды show ip nat translations.

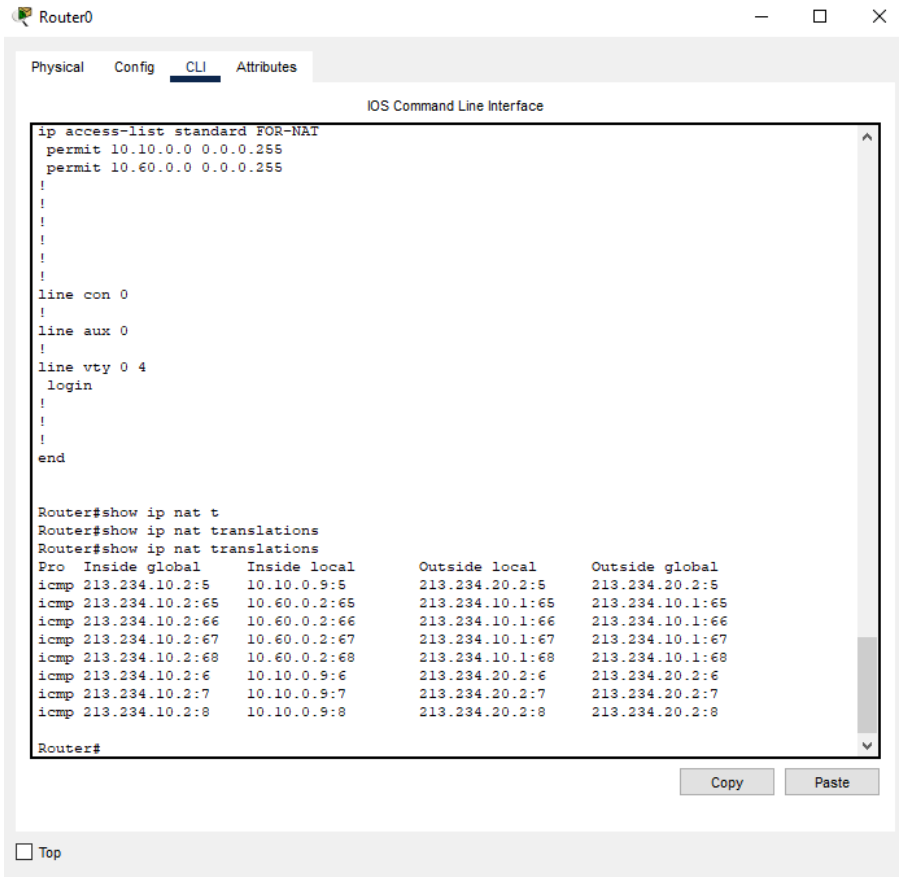

Рисунок 6 - Проверяем работу NAT

3 Статический NAT

Обеспечим доступ из Интернета в наш локальный сервер. Пропишем на маршрутизаторе провайдера следующую команду:

ip ant inside source static tcp 10.60.0.2 80 213.234.10.2 80

Проверим работу static NAT.

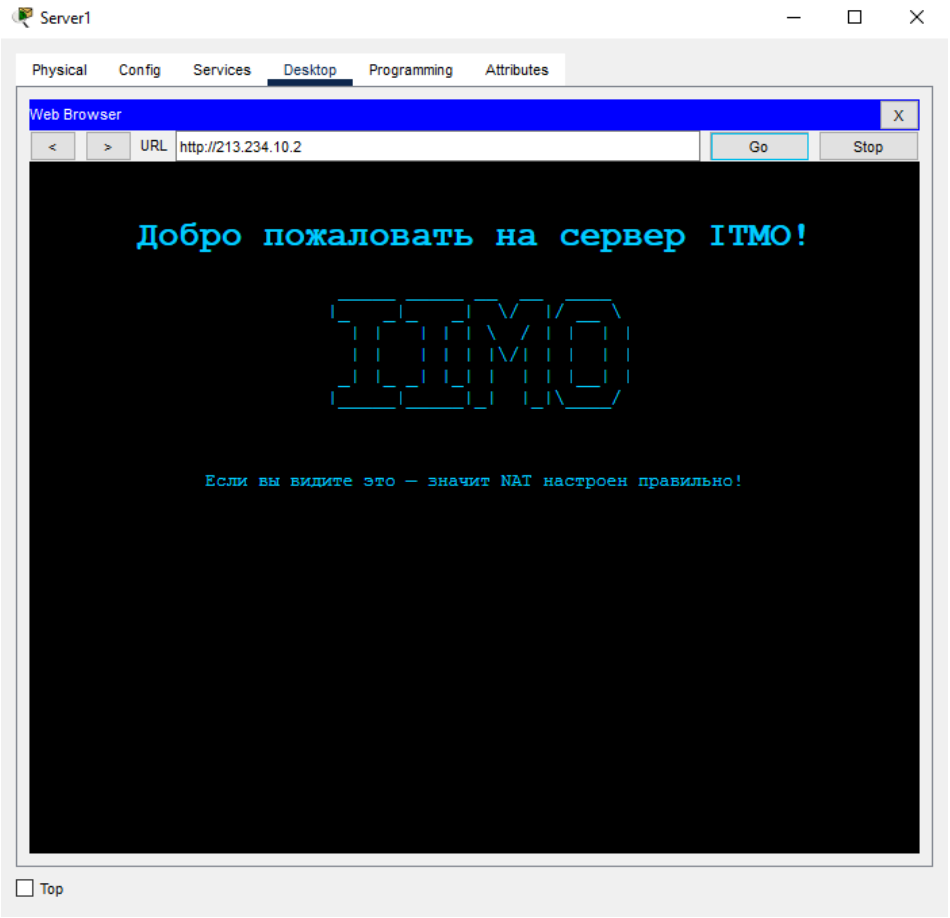

Рисунок 7 - Работа static NAT

Заключение

В ходе выполнения лабораторной работы была смоделирована сеть, в которой реализована трансляция сетевых адресов (NAT) с использованием симулятора Cisco Packet Tracer. Я ознакомился с основными видами NAT: перегруженным (PAT) и статическим, а также выполнил настройку маршрутизатора для трансляции частных IP-адресов внутренней сети в публичный адрес, полученный от провайдера.

Была построена топология, включающая маршрутизатор провайдера, внешний сервер и локальный маршрутизатор, выполняющий функции NAT. С использованием access-list были ограничены VLAN'ы, которым разрешён выход в интернет, что позволило настроить выборочную трансляцию. Также была проведена настройка статического NAT для обеспечения доступа из внешней сети к веб-серверу, размещённому внутри локальной сети.