

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

Отчет по лабораторной работе №6
по курсу «Компьютерные сети»
Тема: Трансляция адресов (NAT) в Cisco Packet Tracer

Выполнил:
Закоурцев Андрей
К3220

Проверил:
Харитонов А.Ю.

Санкт-Петербург
2025 г.

СОДЕРЖАНИЕ

Стр.

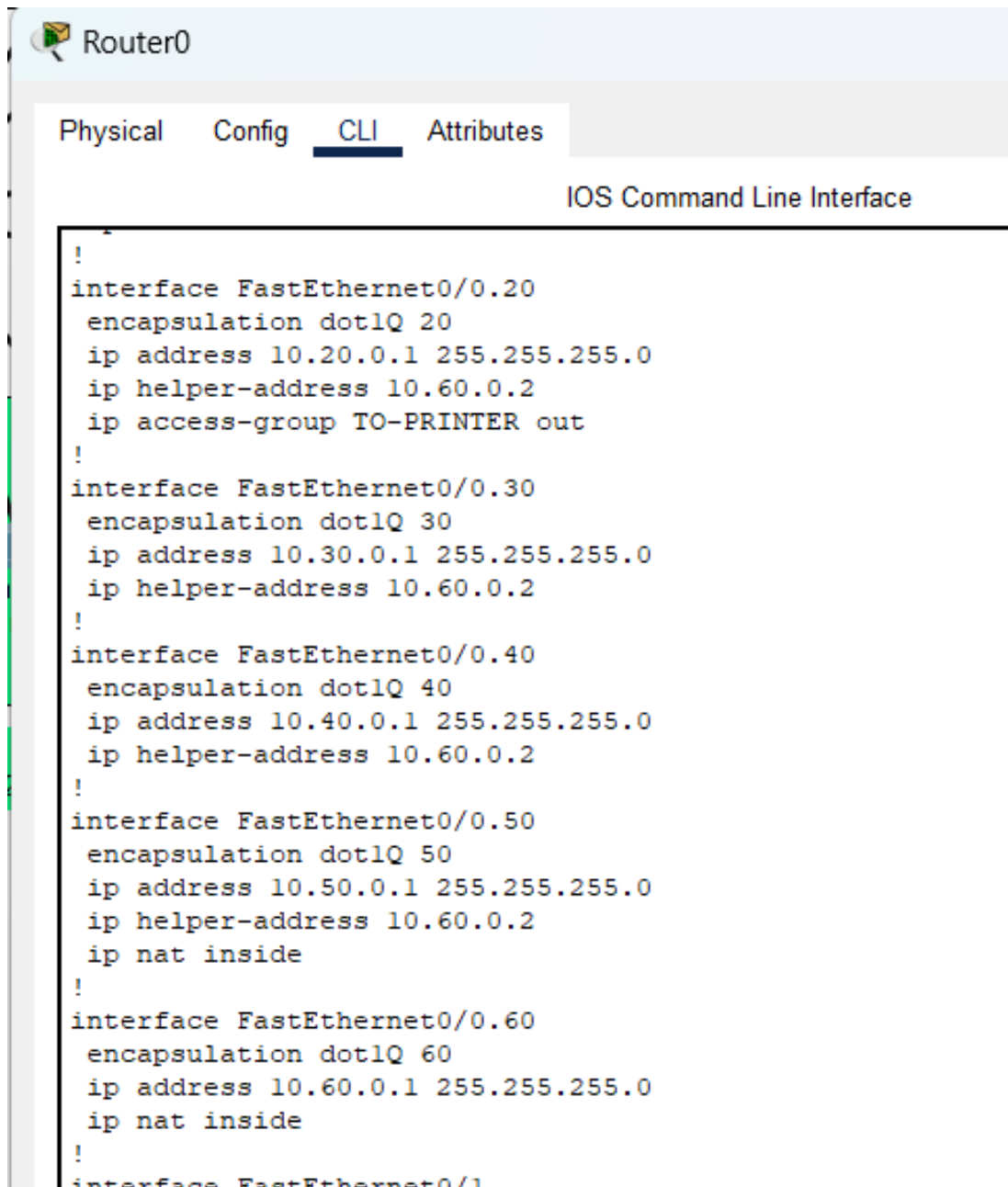
ВВЕДЕНИЕ	3
1 Добавление эмуляции сервера в сети Интернет к существующей сети	4
2 Настройка PAT	6
3 Статический NAT	8
ЗАКЛЮЧЕНИЕ	9

ВВЕДЕНИЕ

В данной лабораторной работе рассматриваются основы NAT в Cisco Packet Tracer. NAT позволяет преобразовывать частные IP-адреса во внешние, обеспечивая доступ в интернет и безопасность внутренней сети. Цель работы — закрепить теоретические знания и освоить базовую настройку NAT, PAT и списков контроля доступа (ACL) на сетевом оборудовании Cisco.

1 Добавление эмуляции сервера в сети Интернет к существующей сети

Для начала удалим коммутатор L3 и вместо него добавим маршрутизатор, а также второй маршрутизатор провайдера и сервер провайдера. На первом маршрутизаторе создадим сабинтерфейсы для каждой группы vlan (Рисунок 1.1). Для них пропишем ip адрес, маску и адрес локального сервера.



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.20.0.1 255.255.255.0
 ip helper-address 10.60.0.2
 ip access-group TO-PRINTER out
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.30.0.1 255.255.255.0
 ip helper-address 10.60.0.2
!
interface FastEthernet0/0.40
 encapsulation dot1Q 40
 ip address 10.40.0.1 255.255.255.0
 ip helper-address 10.60.0.2
!
interface FastEthernet0/0.50
 encapsulation dot1Q 50
 ip address 10.50.0.1 255.255.255.0
 ip helper-address 10.60.0.2
 ip nat inside
!
interface FastEthernet0/0.60
 encapsulation dot1Q 60
 ip address 10.60.0.1 255.255.255.0
 ip nat inside
!
interface FastEthernet0/1
```

Рисунок 1.1 — Сабинтерфейсы

После соединяем все линками и настраиваем белые ip адреса, на маршрутизаторе провайдера будут разные ip адреса на разных портах, к нам -

213.234.10.1, к серверу - 213.234.20.1. Ip сервера - 213.234.20.2, из той же подсети, что и адрес порта маршрутизатора. На нашем же роутере мы ставим белый ip, полученный от провайдера - 213.234.10.2

Также на нашем маршрутизаторе не забываем прописать:

```
ip route 0.0.0.0 0.0.0.0 213.234.10.1
```

Это маршрут по умолчанию для нашего роутера.

Для проверки с нашего роутера попробуем пингануть сервера в обе стороны - нам сервер и сервер провайдера. Успешно. (Рисунок 1.2).

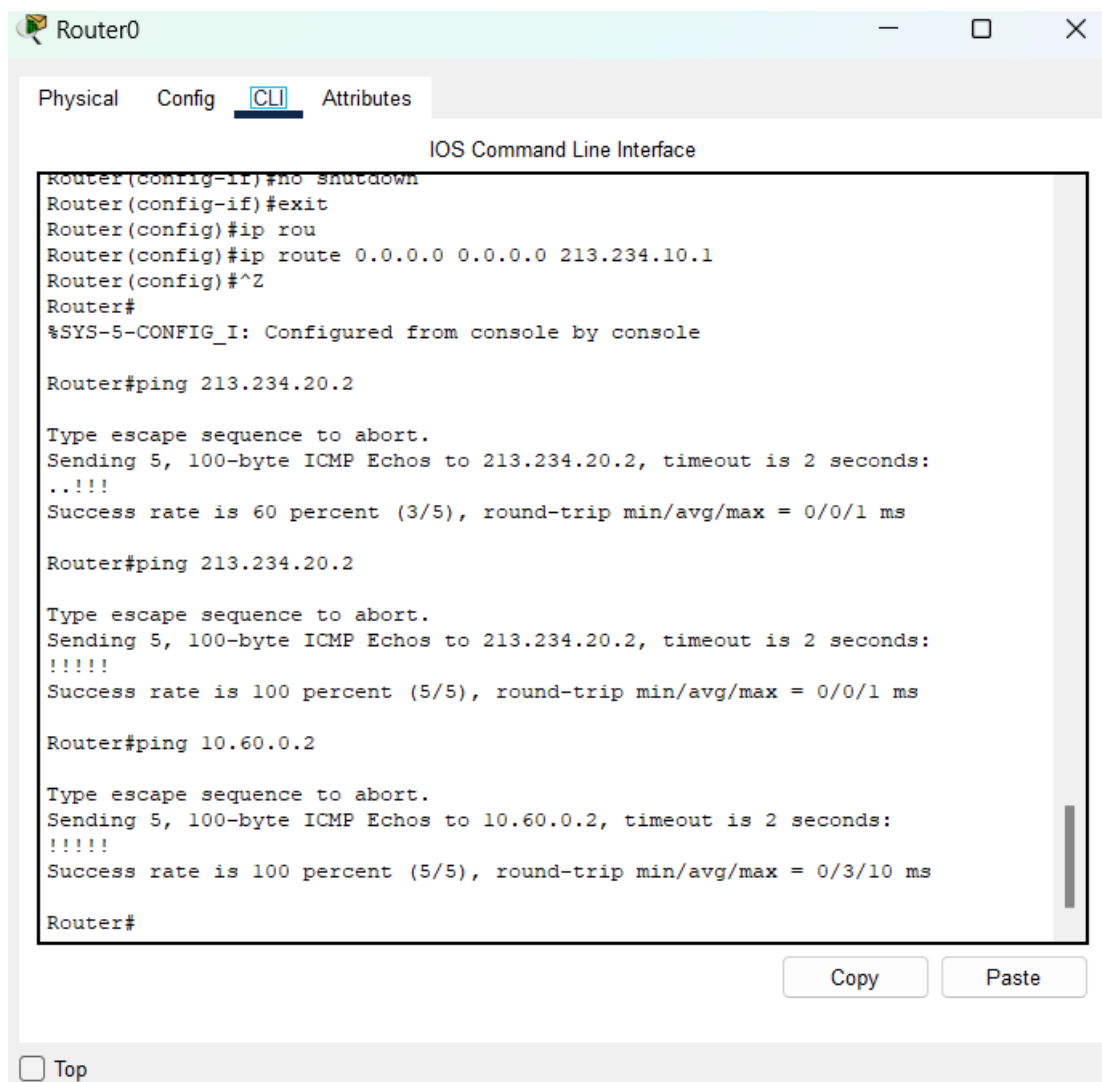


Рисунок 1.2 — Ping серверов

Если же попробуем пинг с устройств нашей локальной сети, то до провайдера не дойдет. Потому что у устройств в локальной сети серые ip адреса.

2 Настройка NAT

Теперь мы должны определить внешние и внутренние интерфейсы для nat. К внешнему интерфейсу нужно применить команду `ip nat outside`, а к внутреннему `ip nat inside`. Внутренние - сабинтерфейсы компьютеров, ноутбуков и сервер. После нужно создать access-list для NAT трафика, в нем мы разрешим трафик для сети сервера, компьютеров и принтеров (Рисунок 2.1).

```
permit ip any any
ip access-list standard FOR-NAT
permit 10.10.0.0 0.0.0.255
permit 10.50.0.0 0.0.0.255
permit 10.60.0.0 0.0.0.255
!
```

Рисунок 2.1 — NAT access-list

После применяем данный access-list командой "`ip nat inside source list <ИМЯ ЛИСТА> interface <ИМЯ ИНТЕРФЕЙСА OUTSIDE> overload`"

Проверяем, что сервер провайдера пингуется с узлов локальной сети (Рисунок 2.2).

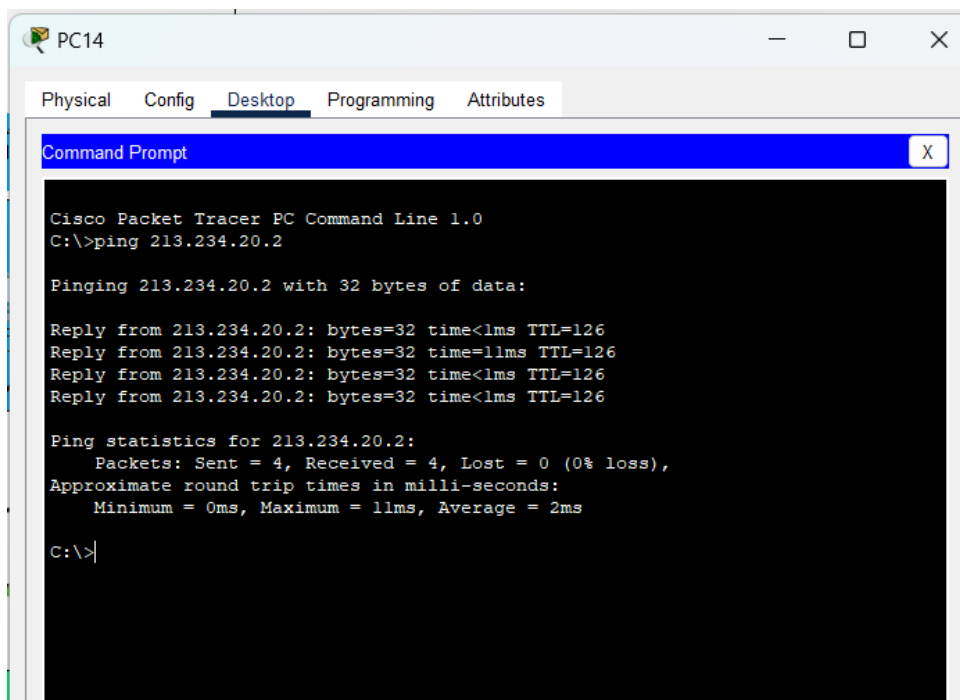


Рисунок 2.2 — Проверка NAT через ping

А также смотрим ip nat translations (Рисунок 2.3).

```
Router#show ip nat translations
Pro  Inside global      Inside local          Outside local          Outside global
icmp 213.234.10.2:1024 10.50.0.5:1          213.234.20.2:1        213.234.20.2:1024
icmp 213.234.10.2:1    10.10.0.3:1          213.234.20.2:1        213.234.20.2:1
icmp 213.234.10.2:5    10.50.0.3:5          213.234.20.2:5        213.234.20.2:5
icmp 213.234.10.2:81   10.60.0.2:81         213.234.20.2:81       213.234.20.2:81
icmp 213.234.10.2:9    10.10.0.2:9          213.234.20.2:9        213.234.20.2:9

Router#
```

Рисунок 2.3 — Ip nat translations

3 Статический NAT

Чтобы мы могли обращаться к из интернета к локальному веб-серверу, необходимо настроить статический NAT. Для этого прописываем на нашем роутере команду:

```
ip nat inside source static tcp 10.60.0.2 80 213.234.10.2 80
```

Также на сервере настроим простую веб-страницу, чтобы отображать информацию о ней.

Теперь при обращении из интернета на адрес нашего ip по протоколу http, мы будем попадать на нашу страницу. При этом локальный сервер не имеет белого ip, а лишь подменяется тем, который выдал нам провайдер. (Рисунок 3.1).

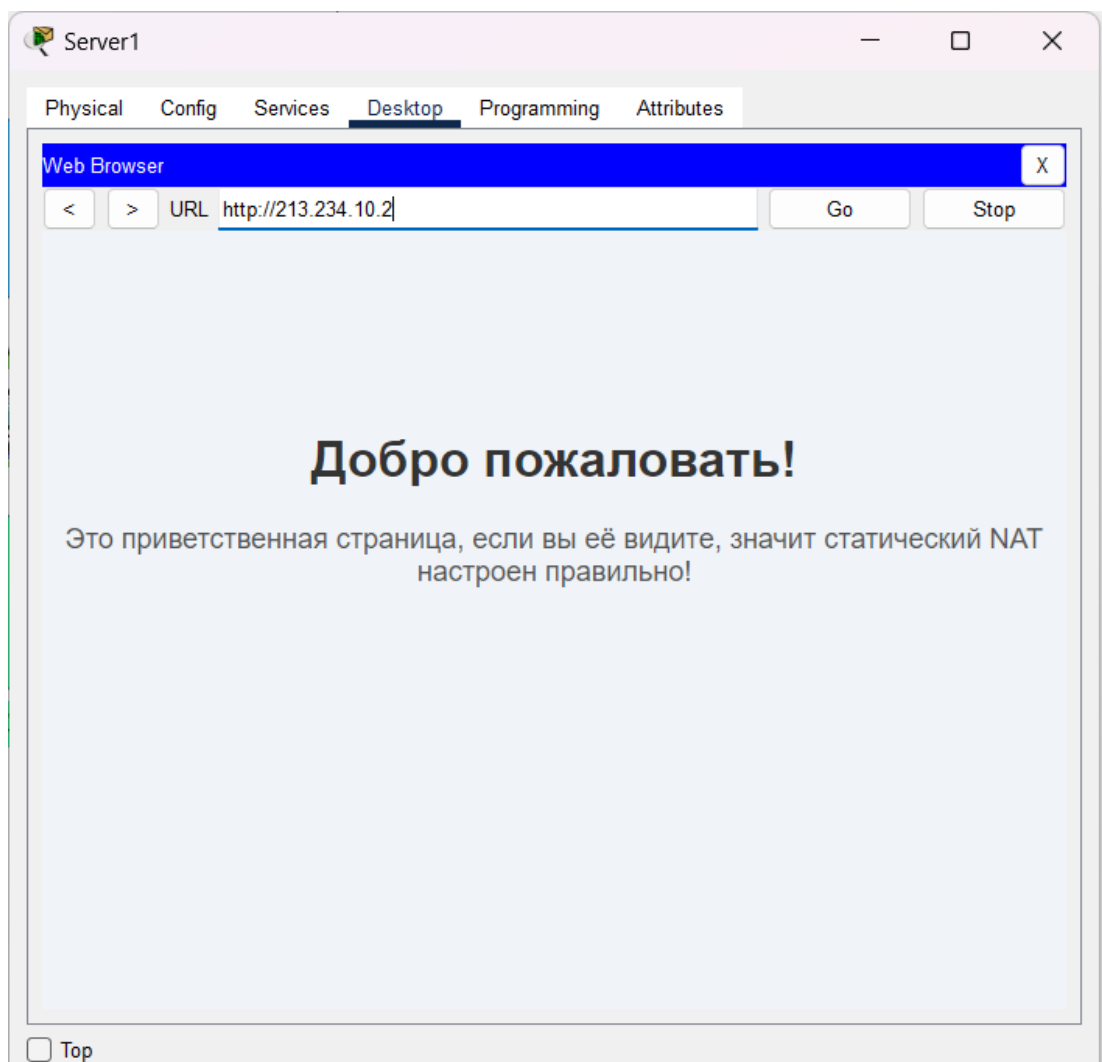


Рисунок 3.1 — Обращение к веб-странице из интернета

ЗАКЛЮЧЕНИЕ

В ходе лабораторной работы была смоделирована сетевая инфраструктура с использованием Cisco Packet Tracer, в которой реализована трансляция сетевых адресов (NAT). Я изучил основные типы NAT — статический и перегруженный (PAT), а также настроил маршрутизатор для преобразования внутренних частных IP-адресов в публичный IP-адрес, предоставленный провайдером.

Была создана сеть с маршрутизатором провайдера, внешним сервером и локальным маршрутизатором, выполняющим функции NAT. С помощью списков контроля доступа (access-list) была организована избирательная трансляция трафика — только определённым VLAN был разрешён доступ в интернет. Кроме того, была выполнена настройка статического NAT, что обеспечило возможность удалённого доступа к веб-серверу, находящемуся внутри локальной сети.