

## Практическая работа 24 – Перегруженный NAT

### Теоретическая часть:

Перегруженный NAT (Port Address Translation, PAT) — это технология, которая позволяет использовать один публичный IP-адрес для множества устройств в частной сети. В отличие от статического NAT, где каждому частному IP-адресу соответствует уникальный публичный IP-адрес, PAT использует один публичный IP-адрес и различает соединения по номерам портов.

Пример: Дома у вас есть роутер, и вы можете подключиться к нему из разных устройств, чтобы выйти в интернет. У вас на роутере один публичный IP-адрес, например, 203.0.113.5. Каждому устройству в вашей домашней сети назначается уникальный частный IP-адрес и номер порта для выхода в интернет.

### Компьютер:

Частный IP-адрес: 192.168.1.2

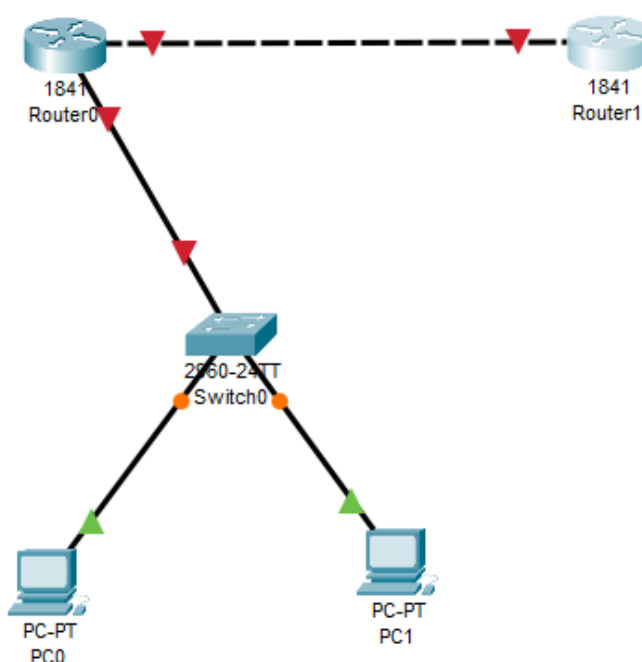
Компьютер отправляет запрос на веб-сайт, например, example.com.

Роутер получает этот запрос и записывает, что запрос от 192.168.1.2 будет отправлен с публичного IP-адреса 203.0.113.5 и порта, например, 1025.

Запрос, отправляемый в интернет, будет выглядеть как 203.0.113.5:1025.

### Практическая часть:

#### 1. Построение сети:



Настраиваем адреса, fa0/0, fa0/1 и шлюз по умолчанию у наших устройств, как в предыдущих практических работах.

## 2. Начинаем конфигурацию роутера0. Переходим в терминал:

```
Router(config-if)#exit
Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255
Router(config)#ip nat inside source list 1 int fa0/1 overload
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#int fa0/1
Router(config-if)#ip nat outside
```

- ip nat inside source list 1 int fa0/1 overload

Эта команда настраивает перегруженный NAT (PAT) для внутренних (inside) источников.

list 1 указывает, что NAT будет применяться к трафику, соответствующему списку управления доступом с номером 1.

int fa0/1 указывает интерфейс, через который будет проходить трафик.

overload указывает, что будет использоваться перегруженный NAT, где один публичный IP-адрес будет использоваться для множества частных IP-адресов с помощью различных номеров портов.

Используем команду ping, чтобы достучаться до внешнего адреса в сети 100.10.10.2.

Pro	Inside global	Inside local	Outside local	Outside global
icmp	100.10.10.1:10	192.168.0.2:10	100.10.10.2:10	100.10.10.2:10
icmp	100.10.10.1:11	192.168.0.2:11	100.10.10.2:11	100.10.10.2:11
icmp	100.10.10.1:12	192.168.0.2:12	100.10.10.2:12	100.10.10.2:12
icmp	100.10.10.1:1	192.168.0.1:1	100.10.10.2:1	100.10.10.2:1
icmp	100.10.10.1:2	192.168.0.1:2	100.10.10.2:2	100.10.10.2:2
icmp	100.10.10.1:3	192.168.0.1:3	100.10.10.2:3	100.10.10.2:3
icmp	100.10.10.1:4	192.168.0.1:4	100.10.10.2:4	100.10.10.2:4
icmp	100.10.10.1:9	192.168.0.2:9	100.10.10.2:9	100.10.10.2:9

Можем увидеть, что для каждого пакета добавляется порт. То есть, один публичный адрес используется для взаимодействия с глобальной сетью, через множество устройств из локальной сети.