

# Packet Tracer - Настройка динамического NAT

## Задачи

Часть 1. Настройка динамического преобразования NAT

Часть 2. Проверка реализации NAT

## Инструкция

### Часть 1: Настройка динамического NAT

#### Шаг 1: Настройка разрешенного трафика.

На маршрутизаторе **R2** настройте одно правило для ACL-списка 1, разрешающее любой адрес, принадлежащий подсети 172.16.0/16.

```
R2>enable
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip access-list standard 1
R2(config-std-nacl)#permit ip 172.16.0.0 0.0.255.255 ?
% Unrecognized command
R2(config-std-nacl)#permit ip ?
% Unrecognized command
R2(config-std-nacl)#?
<1-2147483647> Sequence Number
default      Set a command to its defaults
deny         Specify packets to reject
exit         Exit from access-list configuration mode
no           Negate a command or set its defaults
permit       Specify packets to forward
remark       Access list entry comment
R2(config-std-nacl)#permit ?
A.B.C.D      Address to match
any          Any source host
host         A single host address
R2(config-std-nacl)#permit 172.16.0.0 0.0.255.255 ?
<cr>
R2(config-std-nacl)#permit 172.16.0.0 0.0.255.255
R2(config-std-nacl)#
```

#### Шаг 2. Настройте пул адресов для преобразования (NAT).

Настройте **R2**, определяя пул NAT, использующий два адреса из адресного пространства 209.165.200.228/30

Обратите внимание, что в топологии имеется 3 сетевых адреса, которые должны преобразовываться согласно созданному ACL-списку.

Что произойдёт, если более 2 устройств попытаются осуществить доступ к Интернету? Какому то из устройств не удастся выйти в интернет

```
R2(config)#ip nat pool p1 200.165.200.229 200.165.200.230 netmask 255.255.255.252
```

#### Шаг 3. Свяжите список контроля доступа ACL1 с пулом NAT.

Введите команду, связывающую ACL 1 с только что созданным пулом NAT.

```
R2(config)#ip nat inside source list 1 pool p1 overload
```

#### Шаг 4. Настройте интерфейсы NAT.

Настройте интерфейсы маршрутизатора **R2** с помощью соответствующих внутренних и внешних команд NAT.

```
R2(config)#int s0/0/1
R2(config-if)#ip nat ?
    inside    Inside interface for address translation
    outside   Outside interface for address translation
R2(config-if)#ip nat inside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat outside
R2(config-if)#
```

## Часть 2. Проверка выполнения NAT

### Шаг 1: Доступ к службам через Интернет.

Из веб-браузера **L1**, **PC1** или **PC2** перейдите на веб-страницу на **Server1**.

### Шаг 2. Просмотрите преобразования NAT.

Просмотрите преобразования NAT на маршрутизаторе **R2**. Определите внутренний адрес источника ПК и переведенный адрес из пула NAT в выходных данных команды.

```
R2# show ip nat translations
```

```
R2#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
tcp  200.165.200.229:1024  172.16.10.2:1025  209.165.201.5:80   209.165.201.5:80
tcp  200.165.200.229:1025  172.16.10.1:1025  209.165.201.5:80   209.165.201.5:80
tcp  200.165.200.229:1026  172.16.10.1:1026  209.165.201.5:80   209.165.201.5:80
tcp  200.165.200.229:1027  172.16.11.1:1025  201.165.201.5:80   201.165.201.5:80
```