**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,**

**СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**

**(СПбГУТ)**

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Дисциплина Принципы организации глобальных вычислительных сетей

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6**

NAT

*(тема отчета)*

Направление/специальность подготовки

11.03.02 Инфокоммуникационные технологии и системы связи

*(код и наименование направления/специальности)*

Студенты группы ИКТЗ-83:

Громов А. А

*(Ф.И.О., № группы) (подпись)*

Миколаени М. С,

*(Ф.И.О., № группы) (подпись)*

Проверил:

Ушаков И. А., ст. преп.

Оглавление

[6.4.5 – Настройка статического преобразования (NAT) 3](#_Toc98866500)

[6.5.6 – Настройка динамического NAT 6](#_Toc98866501)

[6.6.7 – Настройка PAT 9](#_Toc98866502)

[6.8.1 – Настройка NAT для IPv4 14](#_Toc98866503)

# 6.4.5 – Настройка статического преобразования (NAT)

Задачи

Часть 1. Проверка доступа без использования NAT

Часть 2. Настройка статического NAT

Часть 3. Проверка доступа с использованием NAT

Сценарий

В сетях, настроенных по протоколу IPv4, для клиентов и серверов используется частная адресация. Перед выходом из сети в Интернет пакеты с частной адресацией должны быть преобразованы в пакеты с публичной адресацией. Серверам, доступным извне сети компании, обычно назначают как публичный, так и частный статические IP-адреса. В рамках задания необходимо настроить статический NAT таким образом, чтобы внешние устройства могли получать доступ к внутреннему серверу по публичному адресу.

Инструкция

Часть 1: Тестирование доступа без NAT

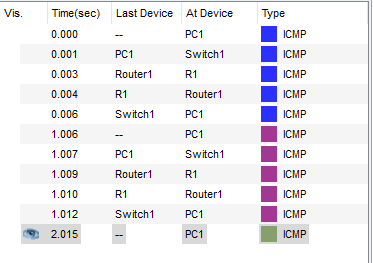
Шаг 1: Попытка подключения к Server1 с помощью режима моделирования.

a.     Перейдите в режим Simulation (Моделирование).

б.     С PC1 или L1 используйте веб-браузер, чтобы попытаться подключиться к веб-странице Server1 по адресу 172.16.16.1. Продолжайте нажимать кнопку Capture Forward, обратите внимание, что пакеты никогда не покидают интернет-облако. Попытки должны завершиться неудачей.

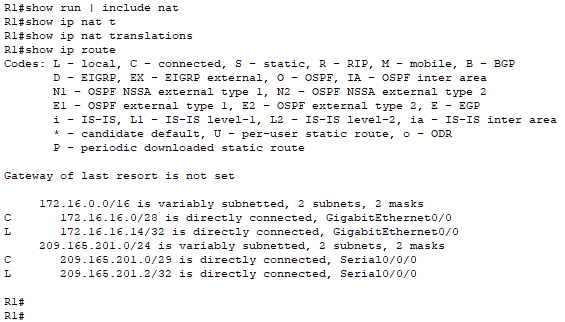
в.     Перейдите в режим моделирования.

г.     С PC1 выполните эхо-запрос интерфейса R1 S0/0/0 (209.165.201.2). Выполнение команды ping должно быть успешным.



Шаг 2. Просмотрите таблицу маршрутизации и конфигурацию running-config маршрутизатора R1.

a.     Просмотрите текущую конфигурацию маршрутизатора R1. Обратите внимание на отсутствие команд, относящихся к NAT. Простой способ подтвердить это - выполнить следующую команду:



б.     Убедитесь, что таблица маршрутизации не содержит записей, относящихся к сетевым IP-адресам для PC1 и L1.

в.     Убедитесь, что NAT не используется маршрутизатором R1.

R1# show ip nat translations

Часть 2. Настройка статического NAT

Шаг 1: Настройка инструкций статического NAT.

См. топологию. Создайте статическое преобразование NAT для сопоставления внутреннего адреса Server1 его внешнему адресу.

R1(config)# ip nat inside source static 172.16.16.1 64.100.50.1

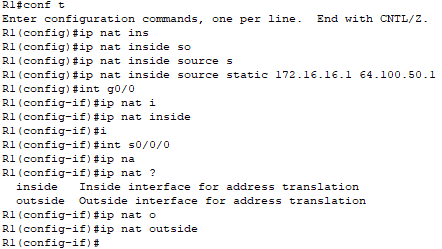
Шаг 2. Настройте интерфейсы.

a.     Настройте интерфейс G0/0 в качестве внутреннего интерфейса.

R1(config)# interface g0/0

R1(config-if)# ip nat inside

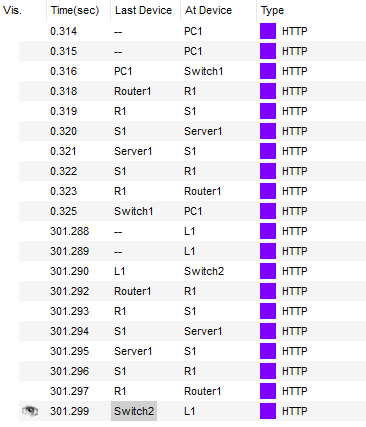
б.     Настройте интерфейс s0/0/0 в качестве внешнего интерфейса.

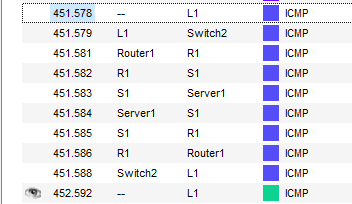


Часть 3: Тестовый доступ с NAT.

Шаг 1: Проверьте подключение к веб-странице Server1.

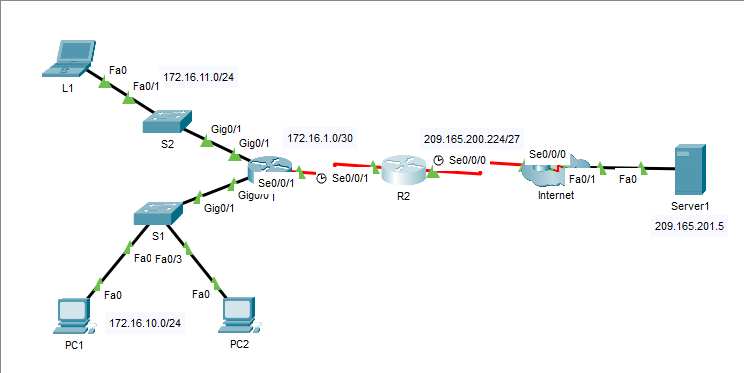
a.     Откройте командную строку на PC1 или L1, попытайтесь отправить эхо-запрос, используя публичный адрес сервера Server1. Эхо-запросы должны быть успешными.

б.     Убедитесь, что со стороны и PC1, и L1 есть доступ к веб-странице сервера Server1 . 



# 6.5.6 – Настройка динамического NAT

Топология



Задачи

Часть 1. Настройка динамического преобразования NAT

Часть 2. Проверка реализации NAT

Инструкция

Часть 1: Настройка динамического NAT

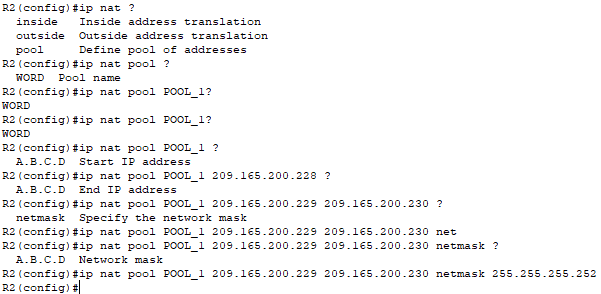
Шаг 1: Настройка разрешенного трафика.

На маршрутизаторе R2 настройте одно правило для ACL-списка 1, разрешающее любой адрес, принадлежащий подсети 172.16.0.0/16.



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

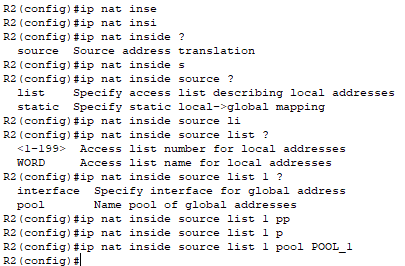
Настройте R2, определяя пул NAT, использующий два адреса из адресного пространства 209.165.200.228/30

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? – Последнее из них не сможет получить доступ.

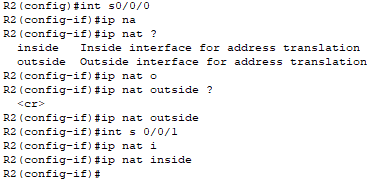
Шаг 3. Свяжите список контроля доступа ACL1 с пулом NAT.

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



Шаг 4.Настройте интерфейсы NAT.

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

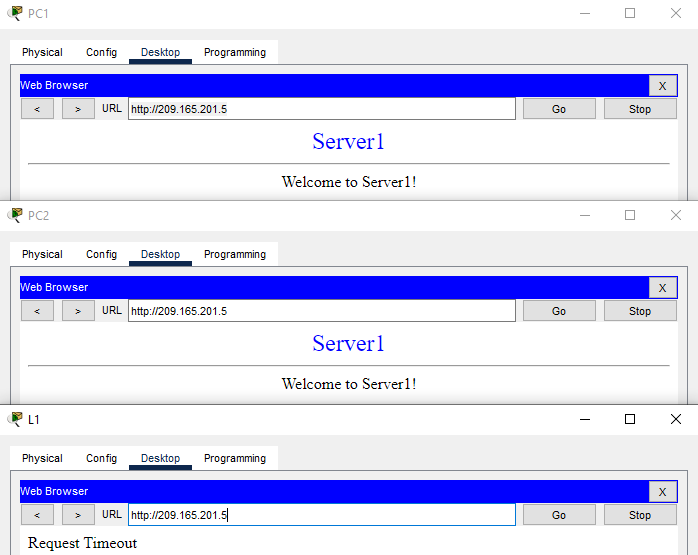


*Закройте окно настройки.*

Часть 2. Проверка выполнения NAT

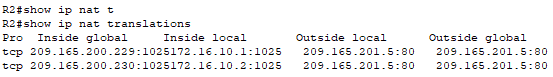
Шаг 1: Доступ к службам через Интернет.

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



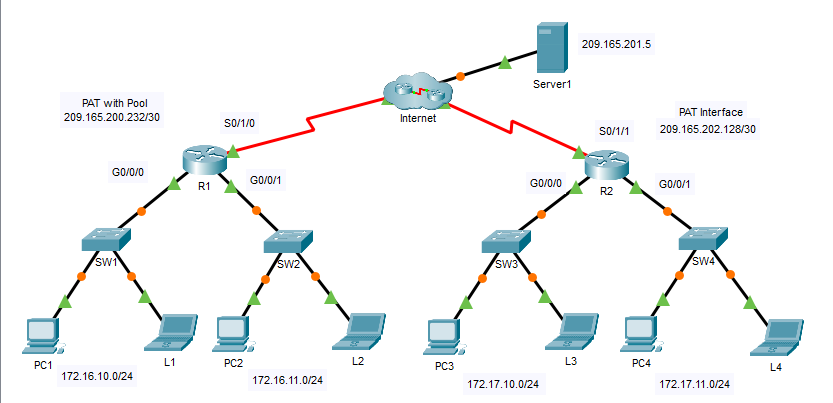
Шаг 2. Просмотрите преобразования NAT.

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



# 6.6.7 – Настройка PAT

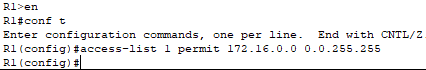
Топология



Часть 1. Настройка динамического NAT с перегрузкой

Шаг 1: Настройка разрешенного трафика.

На маршрутизаторе **R1** настройте одно правило для ACL-списка 1, разрешающее любой адрес, принадлежащий подсети 172.16.0.0/16.



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

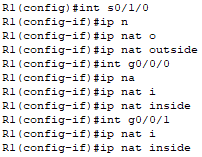
Настройте **R1** с пулом NAT, который использует два используемых адреса в адресном пространстве 209.165.200.232/30.

Шаг 3. Свяжите ACL 1 с пулом NAT и разрешите повторно использовать адреса.



Шаг 4.Настройте интерфейсы NAT.

Настройте интерфейсы маршрутизатора **R1** с помощью соответствующих внутренних и внешних команд NAT.



Часть 2. Проверка динамического NAT с реализацией перегрузки

Шаг 1: Доступ к службам через Интернет.

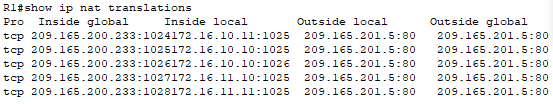
Из веб-браузера каждого компьютера, использующего **R1 в** качестве шлюза (**PC1**, **L1**, **PC2** и **L2**), откройте веб-страницу **Server1**.



Все ли соединения были успешными? - Да

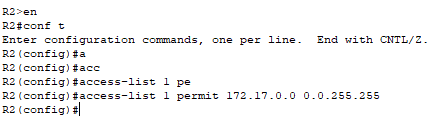
Шаг 2. Просмотрите преобразования NAT.

Просмотрите преобразования NAT на маршрутизаторе **R1**.



Часть 3. Настройка PAT с помощью интерфейса

Шаг 1: Настройка трафика, который будет разрешен.



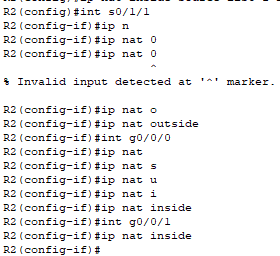
Шаг 2. Свяжите ACL 2 с интерфейсом NAT и разрешить повторное использование адресов.

Введите инструкцию **R2** NAT, чтобы использовать интерфейс, подключенный к Интернету, и предоставить переводы для всех внутренних устройств.



Шаг 3.Настройте интерфейсы NAT.

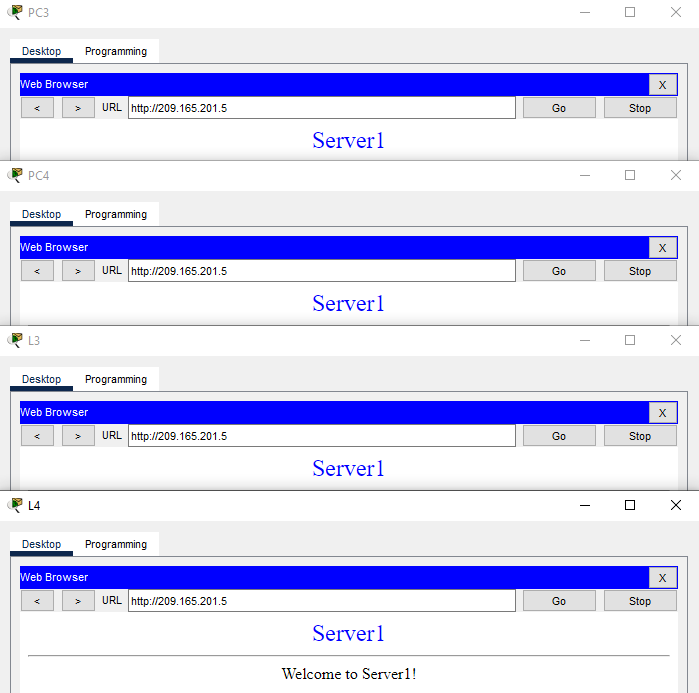
Настройте интерфейсы маршрутизатора **R2** с помощью соответствующих внутренних и внешних команд NAT.



Часть 4: Проверка реализации интерфейса PAT

Шаг 1: Доступ к службам через Интернет.

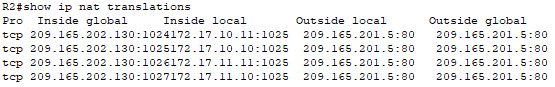
Из веб-браузера каждого компьютера, использующего **R2 в** качестве шлюза (**PC3**, **L3**, **PC4** и **L4**), откройте веб-страницу **Server1**.

**Вопрос:**

Все ли соединения были успешными? - Да

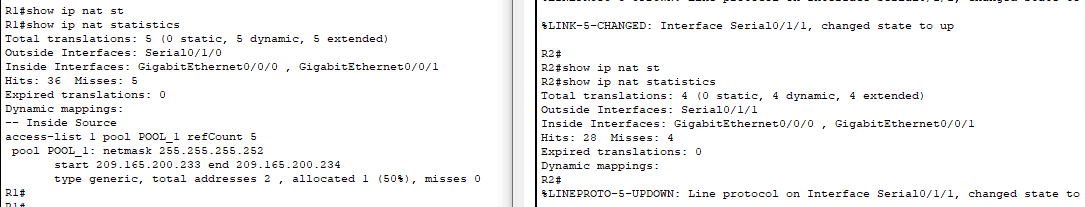
Шаг 2. Просмотрите преобразования NAT.

Просмотрите преобразования NAT на маршрутизаторе **R2**.



Шаг 3. Сравнение статистики NAT на R1 и R2.

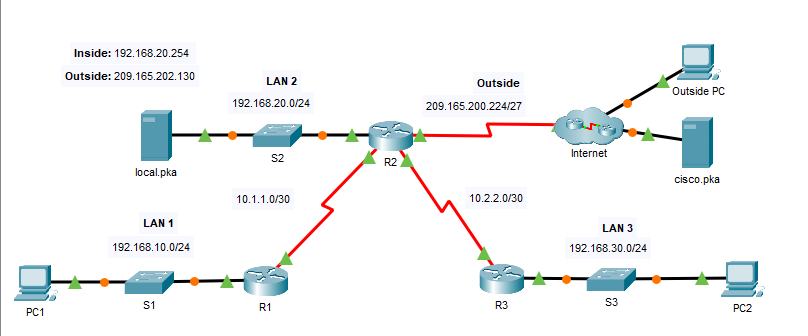
Сравните статистику NAT на двух устройствах.



Почему **R2**не перечисляет никаких динамических сопоставлений? – Так как на R2 настроен только внешний интерфейс для трансляции адресов.

# 6.8.1 – Настройка NAT для IPv4

Топология



Инструкции

В этом задание вы будете настраивать только маршрутизатор R2.*нфигурации*

· Используйте именованный ACL, чтобы разрешить преобразование адресов LAN1, LAN2 и LAN3 . Укажите локальные сети в этом порядке. Используйте имя **R2NAT**. Имя, которое вы используете, должно точно совпадать с этим именем.

· Создание пула NAT с именем **R2POOL**. Пул должен использовать **первый** адрес из адресного пространства **209.165.202.128/30** . Имя пула, которое вы используете, должно точно совпадать с этим именем. Все переведенные адреса должны использовать этот адрес в качестве внешнего адреса.

· Настройте NAT с созданным пулом управления доступом и NAT.

· Настройте статический NAT для сопоставления внутреннего адреса local.pka сервера со **вторым** адресом из адресного пространства **209.165.202.128/30** .

· Настройка интерфейсов, которые будут участвовать в NAT.

SHOW RUN

R2#show run

Building configuration...

Current configuration: 1433 bytes

!

version 12.3

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname R2

!

ip cef

no ipv6 cef

!

ip ssh version 1

!

spanning-tree mode pvst

!

interface FastEthernet0/0

ip address 192.168.20.1 255.255.255.0

ip nat inside

duplex auto

speed auto

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/0/0

ip address 10.1.1.2 255.255.255.252

ip nat inside

!

interface Serial0/0/1

ip address 10.2.2.1 255.255.255.252

ip nat inside

clock rate 64000

!

interface Serial0/1/0

ip address 209.165.200.225 255.255.255.224

ip nat outside

!

interface Serial0/1/1

no ip address

clock rate 2000000

shutdown

!

interface Vlan1

no ip address

shutdown

!

router rip

version 2

passive-interface Serial0/1/0

network 10.0.0.0

default-information originate

no auto-summary

!

ip nat pool R2POOL 209.165.202.129 209.165.202.129 netmask 255.255.255.252

ip nat inside source list R2NAT pool R2POOL overload

ip nat inside source static 192.168.20.254 209.165.202.130

ip classless

ip route 0.0.0.0 0.0.0.0 Serial0/1/0

ip flow-export version 9

!

ip access-list standard R2NAT

permit 192.168.10.0 0.0.0.255

permit 192.168.20.0 0.0.0.255

permit 192.168.30.0 0.0.0.255

!

banner motd ^CAUTHORIZED ACCESS ONLY!^C

line con 0

login

line aux 0

line vty 0 4

login

end