**Курс:\_\_\_3\_\_\_\_\_\_\_, группа(ы)\_\_\_\_ПКС\_179\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Дисциплина (МДК) МДК 02.01.«Инфокоммуникационные системы и сети»\_\_\_\_\_\_\_\_**

**ФИО преподавателя\_\_\_Бусиль К.В.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Программу для работы можно получить по ссылке <https://yadi.sk/d/jcqhS38RV2ar4g>  
Программа запуска Cisco Packet Tracer 5.3.2\bin\PacketTracer5.exe

Результаты с **save.pkt** высылать на почту [miron.sulejman@yandex.ru](mailto:miron.sulejman@yandex.ru) к 01.04.2020

**Тема: Коммутация каналов, пакетов, сообщений.**

**Списки доступа ACL. Настройка статического и динамического NAT**

Списки доступа (access-lists) используются в целом ряде случаев и являются механизмом задания условий, которые роутер проверяет перед выполнением каких-либо действий. *Маршрутизатор* проверяет каждый пакет и на основании вышеперечисленных критериев, указанных в *ACL* определяет, что нужно сделать с пакетом, пропустить или отбросить. Типичными критериями являются адреса отправителя и получателя пакета, тип протокола. Каждый критерий в списке доступа записывается отдельной строкой. *Список* доступа в целом представляет собой набор строк с критериями, имеющих один и тот же номер (или имя). Порядок задания критериев в списке существенен. Проверка пакета на соответствие списку производится последовательным применением критериев из данного списка (в том порядке, в котором они были введены). Пакет, который не соответствует ни одному из введенных критериев будет отвергнут. Для каждого протокола на *интерфейс* может быть назначен только один *список* доступа. Как пример ниже приведена *таблица* списка управления доступом по умолчанию:

|  |  |  |  |
| --- | --- | --- | --- |
| **№ правила** | **Подсеть** | **Конечная точка** | **Разрешить или запретить** |
| 100 | 0.0.0.0/0 | 3389 | Разрешить |

**Без ACL** - по умолчанию при создании конечной точки ей все разрешено.

**Разрешить** - при добавлении одного или нескольких диапазонов "разрешения" все остальные диапазоны по умолчанию запрещаются. Только пакеты из разрешенного диапазона *IP*-адресов смогут достичь конечной точки виртуальной машины.

**Запретить** - при добавлении одного или нескольких диапазонов "запретить" все другие диапазоны трафика по умолчанию разрешаются.

**Сочетание разрешения и запрета** - можно использовать сочетание правил "разрешить" и "запретить", чтобы указать вложенный разрешенный или запрещенный *диапазон* *IP*-адресов.

Рассмотрим два примера стандартных списков:

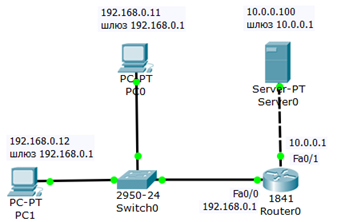
**# access-list 1 permithost 10.0.0.10** - разрешаем прохождение трафика от узла 10.0.0.10.

**# access-list 2 deny 10.0.1.0 0.0.0.255** - запрещаем прохождение пакетов из подсети 10.0.1.0/24.

### Практическая работа 9-1. Создание стандартного списка доступа

Списки доступа бывают нескольких видов: стандартные, расширенные, динамические и другие. В стандартных *ACL* есть возможность задать только *IP* *адрес* источника пакетов для их запретов или разрешений.

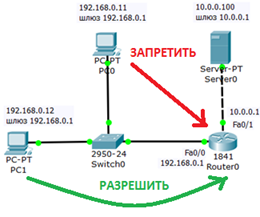
На [рис. 9.1](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=1#image.9.1) показаны две подсети: 192.168.0.0 и 10.0.0.0.



**Рис. 9.1.** Схема сети

#### Постановка задачи

Требуется разрешить доступ на сервер PC1 с адресом 192.168.0.12, а PC0 c адресом 192.168.0.11 – запретить ( [рис. 9.2](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=1#image.9.2)).



**Рис. 9.2.** Постановка задачи

Соберем данную схему и настроим ее. Настройку PC0 и PC1 выполните самостоятельно.

#### Настройка R0

Интерфейс 0/0 маршрутизатора1841 настроим на адрес 192.168.0.1 и включим следующими командами:

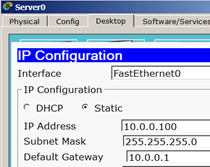
Router>enRouter#conf tRouter (config)#int fa0/0Router (config-if)#ip addr 192.168.0.1 255.255.255.0Router (config-if)#no shutRouter (config-if)#exit

Второй интерфейс маршрутизатора (порт 0/1) настроим на адресом 10.0.0.1 и так же включим:

Router (config)#intfa0/1Router (config-if)#ip addr 10.0.0.1 255.255.255.0Router (config-if)#no shut

#### Настройка сервера

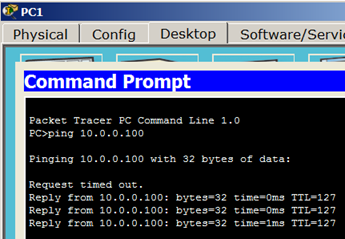
Настройки сервера приведены на [рис. 9.3](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=1#image.9.3).



**Рис. 9.3.** Конфигурирование S0

#### Диагностика сети

Проверяем связь ПК из разных сетей ( [рис. 9.4](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=1#image.9.4)).



**Рис. 9.4.** ПК из разных сетей могут общаться

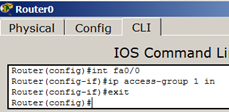
#### Приступаем к решению задачи

Правило запрета и разрешения доступа будем составлять с использованием стандартных списков доступа (ACL). Пока не задан список доступа на интерфейсе всё разрешено (**permit**). Но, стоит создать список, сразу действует механизм "Всё, что не разрешено, то запрещено". Поэтому нет необходимости что-то запрещать (**deny**) – указываем что разрешено, а "остальным – запретить" подразумевается автоматически. По условиям задачи нам нужно на R0 пропустить пакеты с узла 192.168.0.12 на сервер ( [рис. 9.5](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=1#image.9.5)).



**Рис. 9.5.** Создаем на R0 разрешающий ACL

Применяется данное правило на интерфейс в зависимости от направления (PC1 расположен со стороны порта Fa0/0) – [рис. 9.6](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=1#image.9.6). Эта настройка означает, что список доступа (правило с номером 1) будет действовать на интерфейсе fa0/0 на входящем (in) от PC1 направлении.

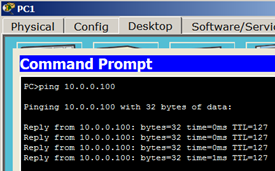


**Рис. 9.6.** Применяем правило к порту Fa0/0

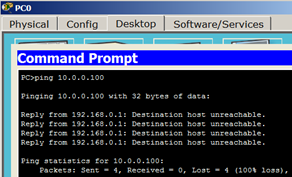
**Примечание**

Входящий трафик (in) — этот тот, который приходит на интерфейс извне. Исходящий (out) — тот, который отправляется с интерфейса вовне. Список доступа вы можете применить либо на входящий трафик, тогда неугодные пакеты не будут даже попадать на маршрутизатор и соответственно, дальше в сеть, либо на исходящий, тогда пакеты приходят на маршрутизатор, обрабатываются им, доходят до целевого интерфейса и только на нём обрабатываются. Как правило, списки применяют на входящий трафик (in).

Проверяем связь ПК с сервером ( [рис. 9.7](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=1#image.9.7) и [рис. 9.8](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=1#image.9.8)).

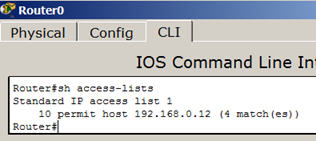


**Рис. 9.7.** Для PC1 сервер доступен



**Рис. 9.8.** Для PC0 сервер не доступен

Давайте посмотрим ACL ( [рис. 9.9](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=1#image.9.9)).



**Рис. 9.9.** Узел 192.168.0.12 разрешен

**Примечание**

Теперь, предположим, нужно добавить новый узел, например, PC2 с адресом 192.168.0.13 в раздел "разрешённых". Пишем команду **Router (config)#access-list 1 permit host 192.168.0.13**. Теперь адреса 192.168.0.12 и 192.168.0.13 могут общаться с сервером, в 192.168.0.11 – нет. А для отмены какого-либо правила – повторяем его с приставкой "no". Тогда это правило исключается из конфигурации. Например, если выполнить команду **Router (config-if)#no ip access-group 1 in**, то ACL будет отменен и снова все ПК могут пинговать сервер.

### Расширенные списки доступа ACL

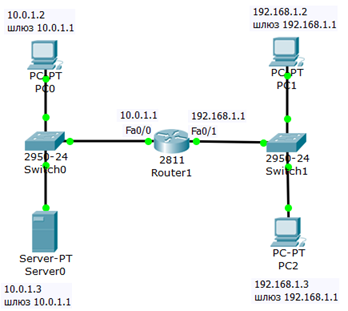
Стандартные *права* не так гибки, как хотелось бы. В отличие от стандартных списков, расширенные списки фильтруют трафик более "тонко". При создании расширенных списков в правилах доступа можно включать фильтрацию трафика по протоколам и портам. Для указания портов в правиле доступа указываются следующие обозначения ():

Таблица 9.1. Обозначение портов в ACL

|  |  |
| --- | --- |
| **обозначение** | **действие** |
| lt n | Все номера портов, меньшие n. |
| gt n | Все номера портов, большие n. |
| eq n | Порт n |
| neq n | Все порты, за исключением n. |
| range n m | Все порты от n до m включительно. |

### Практическая работа 9-2-1. Расширенные списки доступа ACL

Соберите схему сети, показанную на [рис. 9.10](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=2#image.9.10).

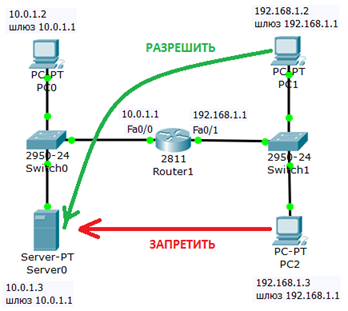


**Рис. 9.10.** Схема сети

Задача: разрешить *доступ* к *FTP* серверу 10.0.1.3 для узла 192.168.1.2 и запретить для узла 192.168.1.3.

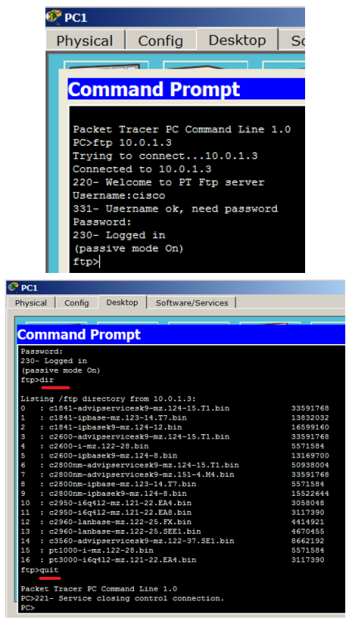
#### Создаем расширенные списки доступа и запрещаем FTP трафик

Постановка задачи графически изображена на [рис. 9.11](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=2#image.9.11).



**Рис. 9.11.** Стрелками показана цель нашей работы

Изначально на сервере 10.0.1.3 FTP сервис поднят по умолчанию со значениями имя пользователя Cisco, пароль Cisco. Убедимся, что узел S0 доступен и FTP работает, для этого заходим на PC1 и связываемся с сервером ( [рис. 9.12](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=2#image.9.12)). Выполняем какие-либо команды, например, DIR – чтение директории.

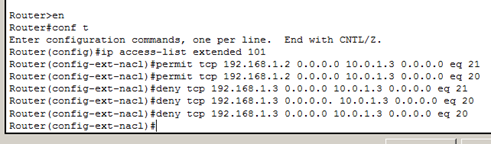


**Рис. 9.12.** FTPсервер доступен

**Примечание**

При наборе пароля на экране ничего не отображается.

Теперь создадим список правил с номером 101 в котором укажем 2 разрешающих и по 2 запрещающих правила для портов сервера 21 и 20 (Эти порты служат для FTP - передачи команд и данных) – [рис. 9.13](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=2#image.9.13).

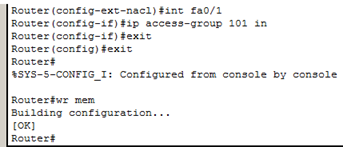


**Рис. 9.13.** Составляем расширенные списки доступа

**Совет**

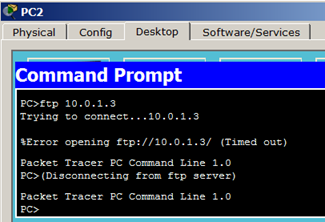
Набирайте команды аккуратно и внимательно: даже один лишний пробел может привести к ошибке при выполнении команды.

А теперь применяем наш список с номером 101 на вход (in) Fa0/1 потому, что трафик входит на этот порт роутера со стороны сети 192.168.1.0 ( [рис. 9.14](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=2#image.9.14)).



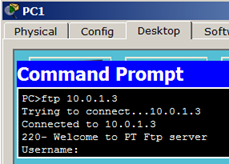
**Рис. 9.14.** Применяем правило с номером 101 к порту 0/1 роутера

Проверяем связь сервера с PC2 ( [рис. 9.15](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=2#image.9.15)).



**Рис. 9.15.** Для PC2 FTP сервер не доступен

Проверяем связь сервера с PC1 ( [рис. 9.16](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=2#image.9.16)).



**Рис. 9.16.** Для PC1 FTP сервер доступен

### Настройка статического NAT

*NAT* (*Network Address* *Translation*) — *трансляция* сетевых адресов, технология, которая позволяет преобразовывать (изменять) *IP* адреса и порты в сетевых пакетах. *NAT* используется чаще всего для осуществления доступа устройств из локальной сети предприятия в *Интернет*, либо наоборот для доступа из *Интернет* на какой-либо *ресурс* внутри сети. *Локальная сеть* предприятия строится на частных *IP* адресах:

* 10.0.0.0 — 10.255.255.255 (10.0.0.0/255.0.0.0 (/8))
* 172.16.0.0 — 172.31.255.255 (172.16.0.0/255.240.0.0 (/12))
* 192.168.0.0 — 192.168.255.255 (192.168.0.0/255.255.0.0 (/16))

Эти адреса не маршрутизируются в Интернете, и провайдеры должны отбрасывать пакеты с такими *IP* адресами отправителей или получателей. Для преобразования частных адресов в Глобальные (маршрутизируемые в Интернете) применяют *NAT*.

**Новый термин**

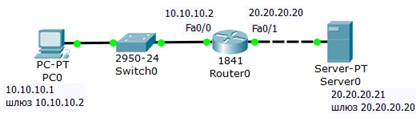
**NAT** — технология трансляции сетевых адресов, т.е. подмены адресов (или портов) в заголовке IP-пакета. Другими словами, пакет, проходя через маршрутизатор, может поменять свой адрес источника и/или назначения. Подобный механизм служит для обеспечения доступа из LAN, где используются частные IP-адреса, в Internet, где используются глобальные IP-адреса.

Существует три вида трансляции Static *NAT*, *Dynamic* *NAT*, Overloading (*PAT*).

* Static NAT (**статический NAT**) осуществляет преобразование IP адреса один к одному, то есть сопоставляется один адрес из внутренней сети с одним адресом из внешней сети. Иными словами, при прохождении через маршрутизатор, адрес(а) меняются на строго заданный адрес, один-к-одному (Например, 10.1.1.5 всегда заменяется на 11.1.1.5 и обратно). Запись о такой трансляции хранится неограниченно долго, пока есть соответствующая строчка в конфигурации роутера.
* Dynamic NAT (**динамический NAT**) производит преобразование внутреннего адреса/ов в один из группы внешних адресов. То есть, перед использованием динамической трансляции, нужно задать nat-пул внешних адресов. В этом случае при прохождении через маршрутизатор, новый адрес выбирается динамически из некоторого диапазона адресов, называемого пулом (pool). Запись о трансляции хранится некоторое время, чтобы ответные пакеты могли быть доставлены адресату. Если в течение некоторого времени трафик по этой трансляции отсутствует, трансляция удаляется и адрес возвращается в пул. Если требуется создать трансляцию, а свободных адресов в пуле нет, то пакет отбрасывается. Иными словами, хорошо бы, чтобы число внутренних адресов было ненамного больше числа адресов в пуле, иначе высока вероятность проблем с выходом в WAN.
* Overloading(или **PAT**) позволяет преобразовывать несколько внутренних адресов в один внешний. Для осуществления такой трансляции используются порты, поэтому такой NAT называют PAT (Port Address Translation). С помощью PAT можно преобразовывать внутренние адреса во внешний адрес, заданный через пул или через адрес на внешнем интерфейсе.

### Практическая работа 9-3-1. Статическая трансляция адресов NAT

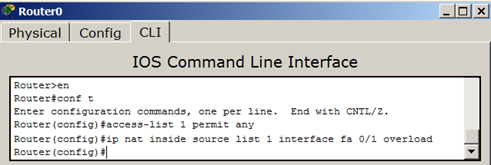
На [рис. 9.17](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=3#image.9.17) имеется внешний *адрес* 20.20.20.20 (внешний *интерфейс* fa0/1) и внутренняя *сеть* 10.10.10.0 (внутренний *интерфейс* fa0/0). Нужно настроить *NAT*. Предполагается, что адреса уже прописаны, и *сеть* поднята (рабочая).



**Рис. 9.17.** Схема сети

#### На R0 добавляем access-list, разрешаем всё (any)

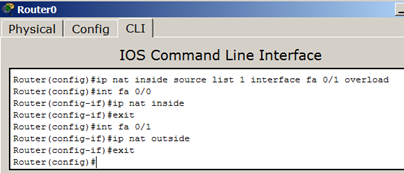
Разрешаем весь трафик, то есть, любой IP адрес ( [рис. 9.18](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=3#image.9.18)).



**Рис. 9.18.** Составляем лист допуска

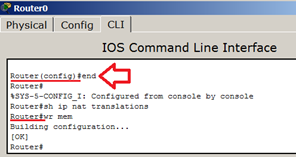
#### Создаём правило трансляции

Теперь настроим трансляцию на интерфейсах (на внутреннем inside, на внешнем – outside), то есть, для R0 указываем внутренний и внешний порты ( [рис. 9.19](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=3#image.9.19)).



**Рис. 9.19.** Для R0 назначаем внутренний и внешний порты

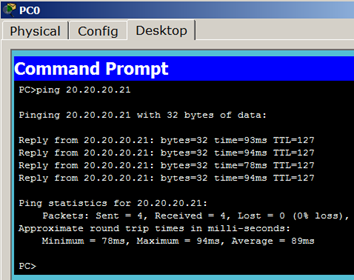
Выходим из режима глобального конфигурирования и записываем настройки роутера в микросхему памяти ( [рис. 9.20](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=3#image.9.20)).



**Рис. 9.20.** Сохраняем настройки в ОЗУ

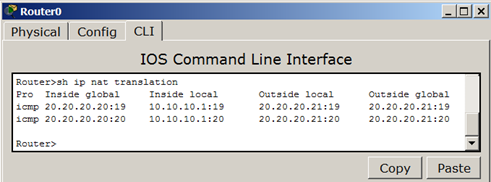
#### Проверяем работу сети (просмотр состояния таблицы NAT)

С PC0 пингуем провайдера и убеждаемся, что PC1 и сервер могут общаться ( [рис. 9.21](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=3#image.9.21)).



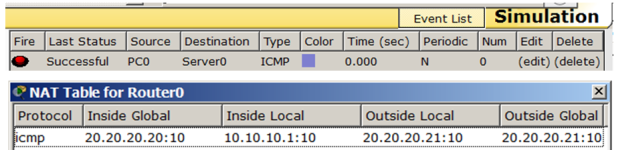
**Рис. 9.21.** Из внутренней сети пингуем внешнюю сеть

Для просмотра состояния таблицы NAT, одновременно с пингом используйте команду **Router#sh ip nat translations** (я запустил пинг с машины 10.10.10.1, т.е., с PC1 на адрес 20.20.20.21, т.е., на S0) – [рис. 9.22](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=3#image.9.22).



**Рис. 9.22.** Вовремя пинга просматриваем состояние таблицы NAT

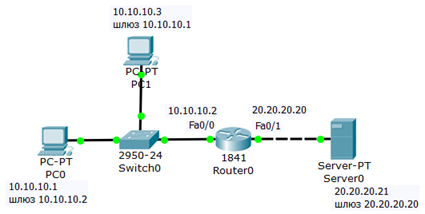
Убеждаемся в успешной маршрутизации в режиме симуляции ( [рис. 9.23](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=3#image.9.23)).



**Рис. 9.23.** Связь PC0 и S0 работает

#### Задание 9.3

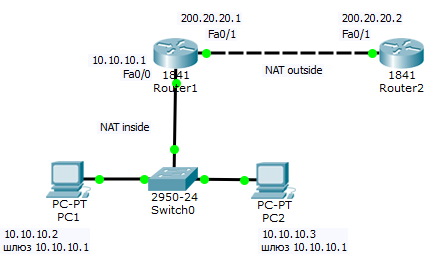
Если в схему добавить PC1 ( [рис. 9.24](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=3#image.9.24)), то будет ли работать статический NAT между ним и S0?



**Рис. 9.24.** Задание для самостоятельной работы

### Практическая работа 9-3-2. Настройка статического NAT

Статический *NAT* - сопоставляет один *NAT* inside (внутренний=частный локальный *ip*-*адрес*) с одним *NAT* outside (глобальным=публичным внешним *ip*-адресом) – [рис. 9.25](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=3#image.9.25). Здесь *ISP* (*Internet* *Service* *Provider*) - поставщик *Интернет*-услуг (*Интернет*-*провайдер*).



**Рис. 9.25.** Схема сети

#### Алгоритм настройки R1

Ниже приведена последовательность команд конфигурирования маршрутизатора R1 по шагам.

**Шаг 1. Настройка дефолта на R1**

R1(config)# ip route 0.0.0.0 0.0.0.0 200.20.20.2

**Шаг 2. Настройка внутреннего интерфейса в отношение NAT**

R1(config)# interface fastethernet 0/0R1(config-if)# ip nat inside

**Шаг 3. Настройка внешнего интерфейса в отношение NAT**

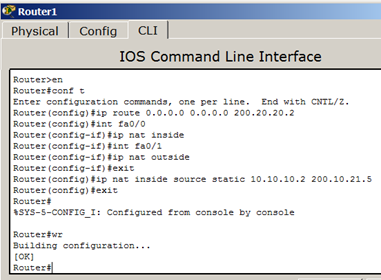
R1(config)# interface fastethernet 0/1 R1(config-if)# ip nat outside

**Шаг 4. Настройка сопоставления ip-адресов.**

R1(config)# ip nat inside source static 10.10.10.2 200.10.21.5

В результате этой команды ip-адресу 200.10.21.5 всегда будет соответствовать внутренний ip-адрес 10.10.10.2, т.е. если мы будем обращаться к адресу 200.10.21.5 то отвечать будет PC1.

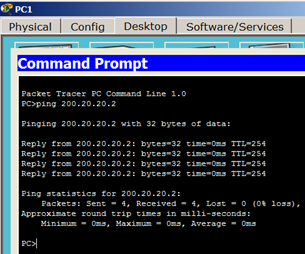
Полный листинг команд приведен на [рис. 9.26](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=3#image.9.26).



**Рис. 9.26.** Полный листинг команд по настройке R1

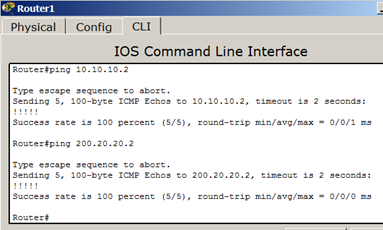
#### Команды для проверки работы NAT

Проверим связь PC1 и R2 ( [рис. 9.27](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=3#image.9.27)).



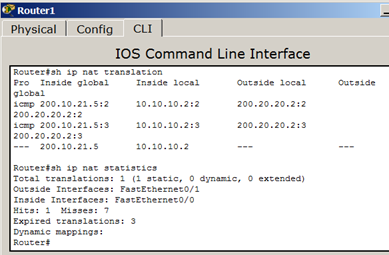
**Рис. 9.27.** PC1 видит R2

Проверим, что R1 видит соседние сети ( [рис. 9.28](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=3#image.9.28)).



**Рис. 9.28.** R1 видит PC1 и R2

Проверим механизм работы статического NAT: команда **show ip nat translations** выводит активные преобразования, а команда **show ip nat statistics** выводит статистику по NAT преобразованиям ( [рис. 9.29](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=3#image.9.29)).

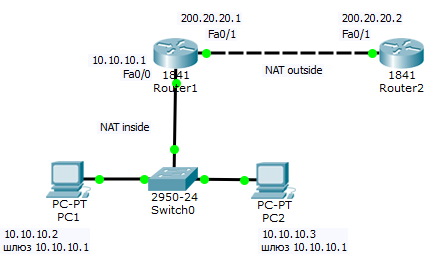


**Рис. 9.29.** Проверка механизма работы статического NAT

Из иллюстрации видим, что глобальному ip-адресу 200.10.21.5 соответствует локальный ip-адрес 10.10.10.2,а также, какой интерфейс является внешним, а какой -внутренним.

### Динамическая трансляция адресов. Настройка динамического NAT

Динамический *NAT* - использует *пул* доступных глобальных (публичных) *ip*-адресов и назначает их внутренним локальным (частным) адресам. Схема для нашей работы приведена на [рис. 9.30](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=4#image.9.30).



**Рис. 9.30.** Схема сети

### Практическая работа 9-4-1. Настройка динамического NAT на маршрутизаторе R1 по шагам.

**Шаг 1. Настройка на R1 списка доступа, соответствующего адресам LAN**

R1 (config)# access-list 1 permit 10.10.10.0 0.0.0.255

Здесь 0.0.0.225 – обратная (инверсная) *маска* для адреса 10.10.10.0.

**Шаг 2. Настройка пула адресов**

R1 (config)# ip nat pool white-address 200.20.20.1 200.20.20.30 netmask 255.255.255.0

**Шаг 3. Настройка трансляции**

R1 (config)# ip nat inside source list 1 pool white-address

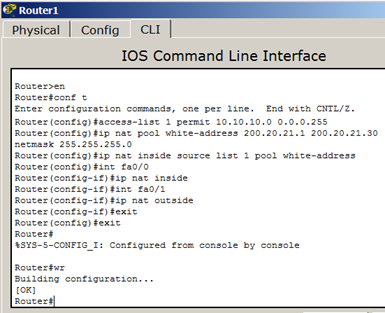
**Шаг 4. Настройка внутреннего интерфейса в отношение NAT**

R1 (config)# interface fastethernet 0/0R1 (config-if)# ip nat inside

**Шаг 5. Настройка внешнего интерфейса в отношение NAT**

R1 (config)# interface fastethernet 0/1R1 (config-if)# ip nat outside

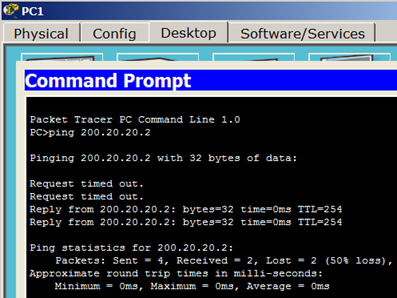
Ниже дан полный листинг команд по настройке R1 ( [рис. 9.31](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=4#image.9.31)).



**Рис. 9.31.** Полный листинг команд по конфигурированию R1

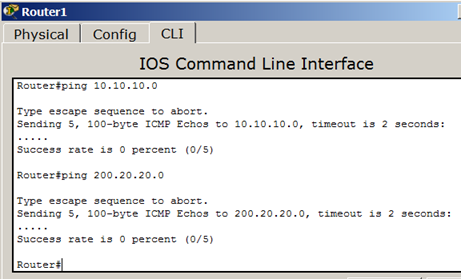
### Команды для проверки работы динамического NAT

Проверим *связь* PC1 и R2 ( [рис. 9.32](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=4#image.9.32)).



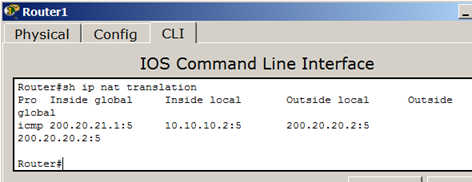
**Рис. 9.32.** PC1 видит R2

Проверим, что R1 видит соседние сети ( [рис. 9.33](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=4#image.9.33)).



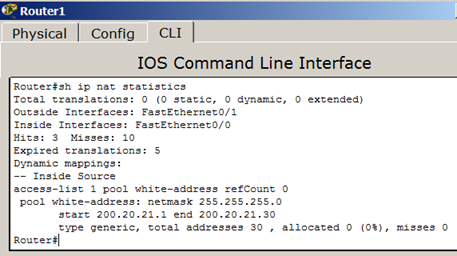
**Рис. 9.33.** R1 видит подсети 10.10.10.0 и 200.20.20.0

Проверим механизм работы динамического *NAT*: для этого выполним одновременно (параллельно) команды **ping** и **show ip nat translations** ( [рис. 9.34](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=4#image.9.34)).



**Рис. 9.34.** Адреса: глобальный, внутренний, внешний

Командой **show ip nat statistics** выведем статистику по *NAT* преобразованиям ( [рис. 9.35](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=4#image.9.35)).

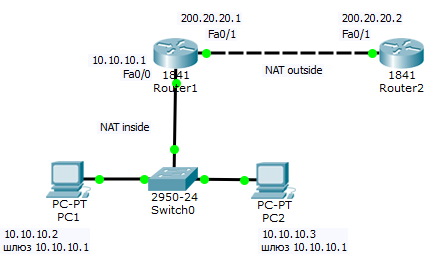


**Рис. 9.35.** Статистика работы динамического NAT

Из иллюстрации видим, что локальным адресам соответствует *пул* внешних адресов от 200.20.20.1 до 20.20.20.30.

### Практическая работа 9-4-2. Динамический NAT Overload: настройка PAT (маскарадинг)

*PAT* (*Port Address* *Translation*) - отображает несколько локальных (частных) *ip*-адресов в глобальный *ip*-*адрес*, используя различные порты ( [рис. 9.36](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=4#image.9.36)).



**Рис. 9.36.** Схема сети на настройки трансляции адресов PAT

Рассмотрим *алгоритм* нашей работы по шагам.

**Шаг 1. Настройка списка доступа, соответствующего внутренним частным адресам**

R1(config)# access-list 1 permit 10.10.10.0 0.0.0.255

**Шаг 2. Настройка трансляции**

R1(config)# ip nat inside source list 1 interface fastethernet 0/1 overload

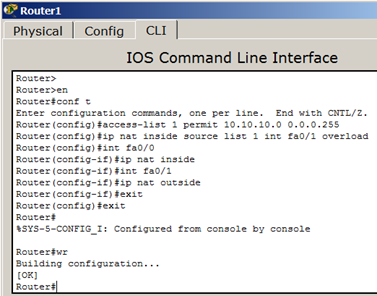
**Шаг 3. Настройка внутреннего интерфейса в отношение NAT**

R1(config)# interface fastethernet 0/0R1(config-if)# ip nat inside

**Шаг 4. Настройка NAT на интерфейсе**

R1(config)# interface fastethernet 0/1R1(config-if)# ip nat outside

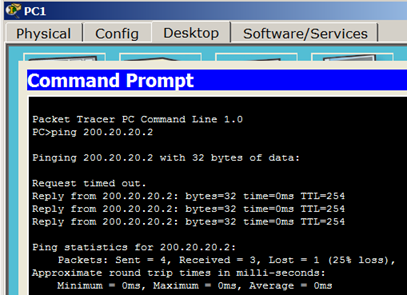
Ниже дан полный листинг команд по конфигурированию R1 ( [рис. 9.37](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=4#image.9.37)).



**Рис. 9.37.** Листинг команд по конфигурированию R1

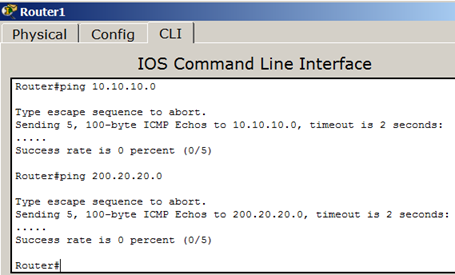
### Команды для проверки работы маскарадинга (PAT)

Проверим *связь* PC1 и R2 ( [рис. 9.38](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=4#image.9.38)).



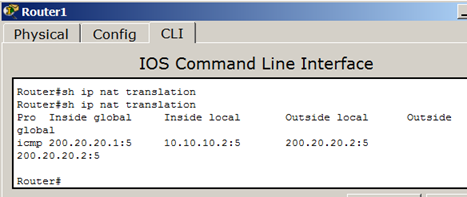
**Рис. 9.38.** PC1 видит R2

Проверим, что R1 видит соседние сети ( [рис. 9.39](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=4#image.9.39)).



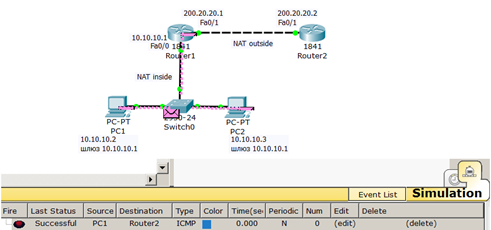
**Рис. 9.39.** R1 видит подсети 10.10.10.0 и 200.20.20.0

Проверим механизм работы динамического *NAT*: для этого выполним одновременно (параллельно) команды **ping и show ip nat translations** ( [рис. 9.40](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=4#image.9.40)).



**Рис. 9.40.** Адреса: глобальный, внутренний, внешний

Проверим работу сети в режиме симуляции ( [рис. 9.41](https://www.intuit.ru/studies/courses/3549/791/lecture/29226?page=4#image.9.41)).



**Рис. 9.41.** PAT работает, PC1 и R2 отправляют и получают пакеты Successful

***Примечание****:*

*Решения сдать в электронном формате* **save.pkt** *до* ***01.04.2020*** *на электронную почту* [miron.sulejman@yandex.ru](mailto:miron.sulejman@yandex.ru)

Программу для работы можно получить по ссылке <https://yadi.sk/d/jcqhS38RV2ar4g>

Программа запуска Cisco Packet Tracer 5.3.2\bin\PacketTracer5.exe