**Министерство образования Республики Беларусь**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**Факультет прикладной математики и информатики**

**Технология NANT.**

**Мини-коллоквиум**

Рогозенко дмитрий вадимович

Отчет по лабораторной работе № 12,

вариант 25

(“Компьютерные сети”)

студента 2-го курса 12-ой группы

|  |  |  |
| --- | --- | --- |
|  |  | **Преподаватель** |
|  | **Горячкин В.В.** |
|  | | |
| **2020 г.** | | |

Оглавление

[**Выполнение лабораторной работы** 3](#_Toc39746244)

[**Задание 2** 3](#_Toc39746245)

[**Решение** 3](#_Toc39746246)

[**Задание 3** 4](#_Toc39746247)

[**Решение** 4](#_Toc39746248)

[**Шаг 1. Подсоединение устройств** 4](#_Toc39746249)

[**Шаг 2. Настройка основной конфигурации маршрутизатора 2** 4](#_Toc39746250)

[**Шаг 3. Настройка маршрутизатора, используемого в качестве шлюза.** 5](#_Toc39746251)

[**Шаг 4. Настройка правильного ip-адреса, маски подсети и шлюза по умолчанию.** 6](#_Toc39746252)

[**Шаг 5. Проверка работоспособности сети** 7](#_Toc39746253)

[**Шаг 6. Создание маршрута по умолчанию.** 8](#_Toc39746254)

[**Шаг 7. Создание статического маршрута.** 9](#_Toc39746255)

[**Шаг 8. Создание пула используемых публичных адресов.** 10](#_Toc39746256)

[**Шаг 9. Определение списка доступа, соответствующего внутренним частным IP-адресам.** 10](#_Toc39746257)

[**Шаг 10. Определение NAT из списка внутренних адресов в пул внешних адресов.** 10](#_Toc39746258)

[**Шаг 11. Назначение интерфейсов.** 10](#_Toc39746259)

[**Шаг 12. Генерация трафика с маршрутизатора Gateway к маршрутизатору ISP.** 10](#_Toc39746260)

[**Шаг 13. Проверьте работоспособность NAPT** 12](#_Toc39746261)

[**Реферат на тему «технология NAPT»** 14](#_Toc39746262)

[**Немного о NAT.** 14](#_Toc39746263)

[**Непосредственно NAPT** 15](#_Toc39746264)

[**Теоретический мини-коллоквиум** 17](#_Toc39746265)

# 

**Выполнение лабораторной работы**

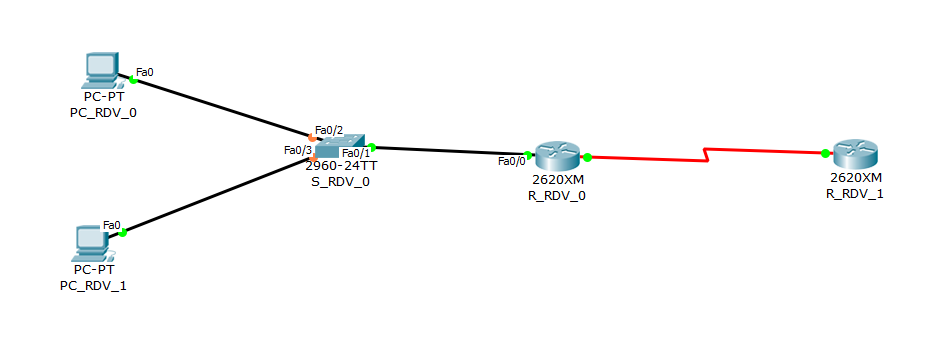
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вариант | Адреса для узлов | Маршрутизатор 1 | Маршрутизатор 2 | IP-адрес  Loopback 1 |
| 25 | 192.168.191.0/24 | 139.224.192.1/30 | 139.224.192.2/30 | 172.16.1.25/32 |

**Задание 2**

*Реализовать схему сети. Присвоить имена маршрутизаторам и хостам по уже принятым правилам.*

## **Решение**

Реализованная схема:



**Задание 3**

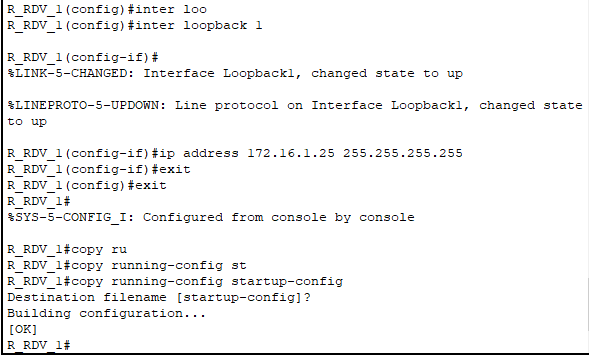
*Выполнить пункты 1-13 методических указаний к лабораторной работе.*

## **Решение**

## **Шаг 1. Подсоединение устройств**

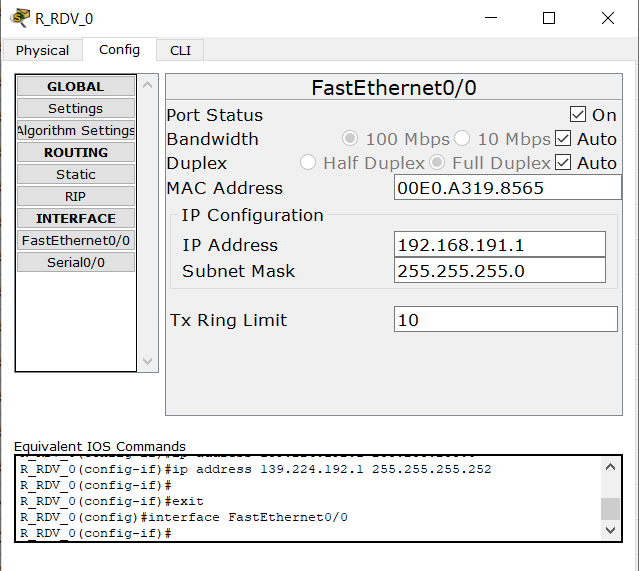
Выполнен в предыдущем задании.

## **Шаг 2. Настройка основной конфигурации маршрутизатора 2**

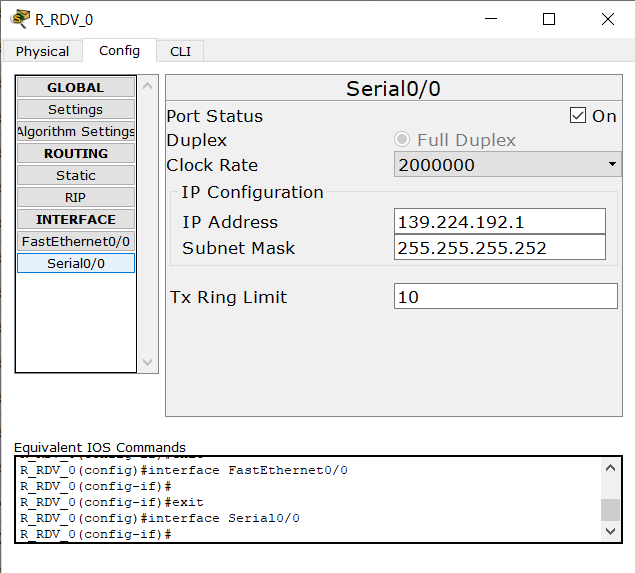


## **Шаг 3. Настройка маршрутизатора, используемого в качестве шлюза.**

Интерфейс FastEthernet 0/0:

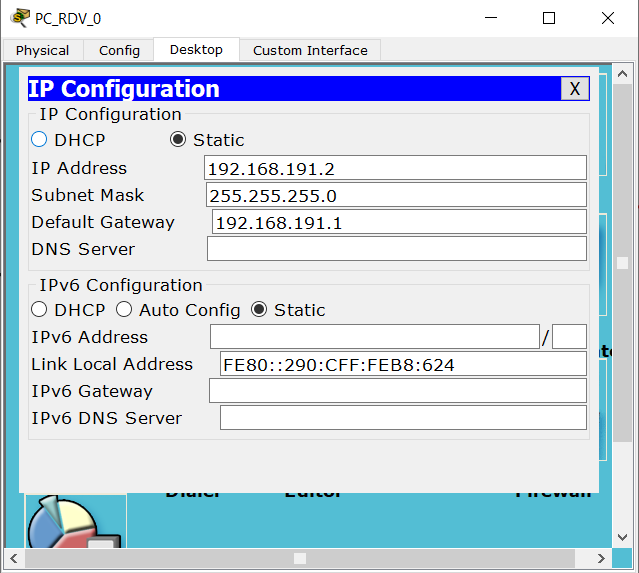


Интерфейс Serial 0/0:

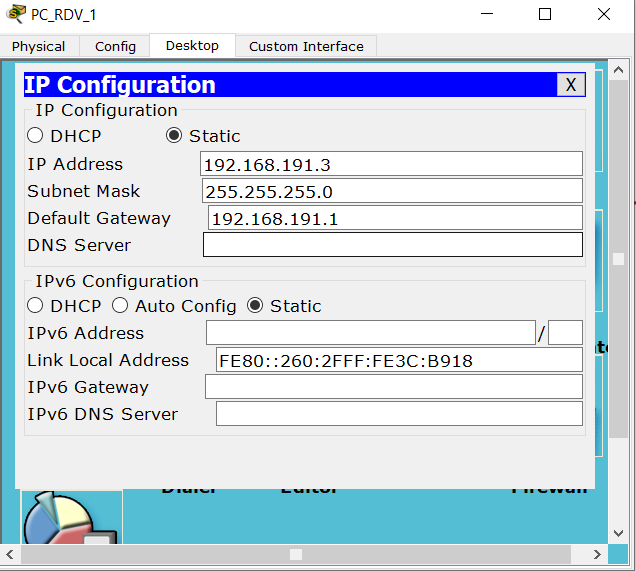


## **Шаг 4. Настройка правильного ip-адреса, маски подсети и шлюза по умолчанию.**

PC\_RDV\_0:

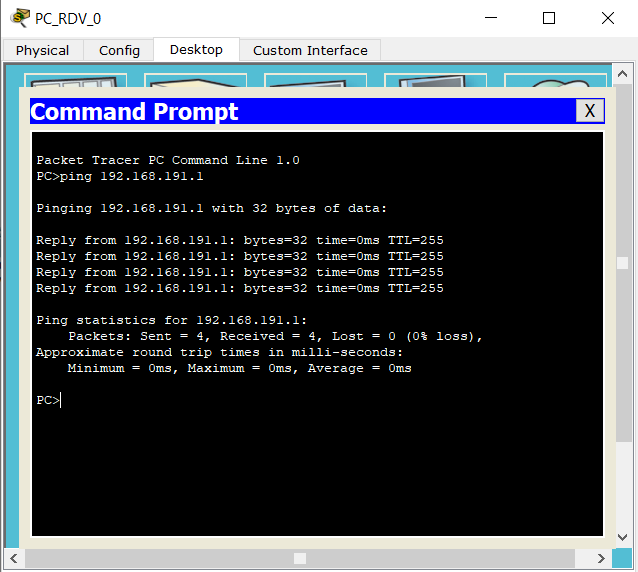


PC\_RDV\_1:

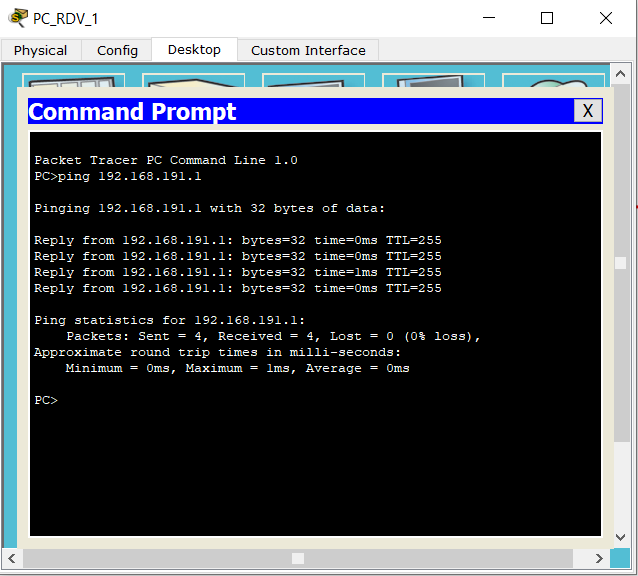


## **Шаг 5. Проверка работоспособности сети**

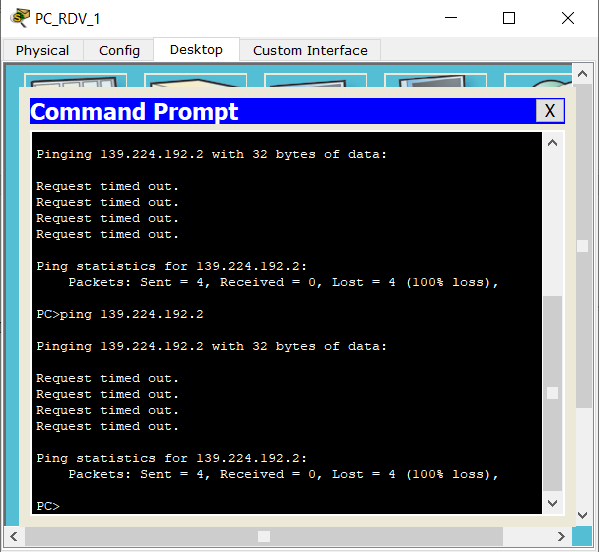
С **первого узла** на FE-интерфейс маршрутизатора:



С **второго узла** на FE-интерфейс маршрутизатора:



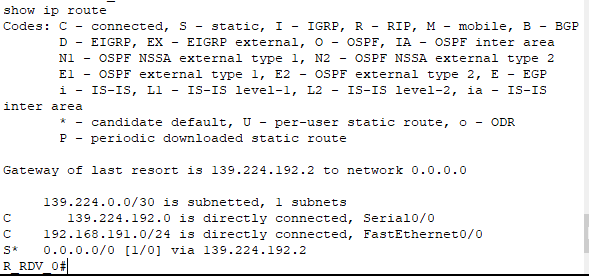
А вот интерфейс второго маршрутизатора мы пропинговать пока не можем, так как на данный момент мы ещё не настроили маршруты к нему:



## **Шаг 6. Создание маршрута по умолчанию.**

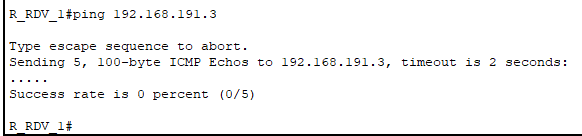


Таблица маршрутизации роутера R\_RDV\_0:



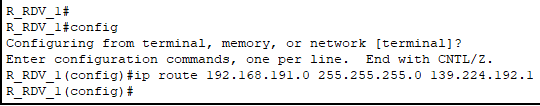
Как мы видим, здесь появился маршрут по умолчанию.

Попытка эхо-запроса не удалась:

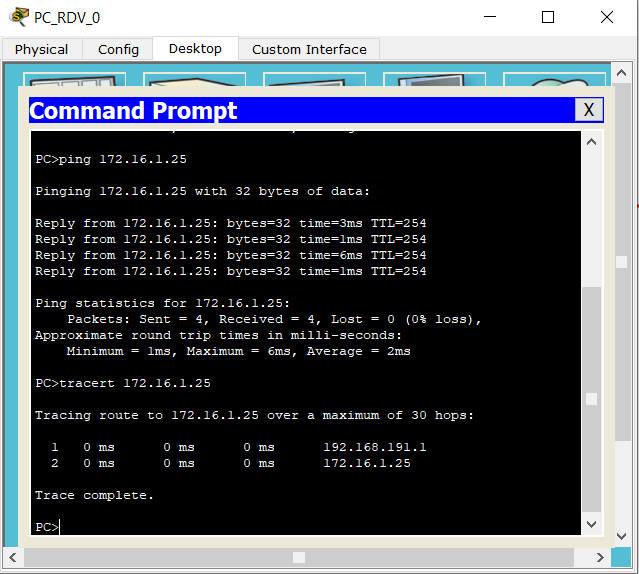


Так как у нас есть маршрут по умолчанию, однако нет статического маршрута между 1-ым и 2-ым роутерами.

## **Шаг 7. Создание статического маршрута.**



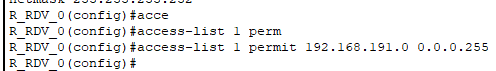
После настройки маршрутизации, эхо-запрос с узла PC\_RDV\_0 на loopback-интерфейс роутера выполнен успешно:



## **Шаг 8. Создание пула используемых публичных адресов.**



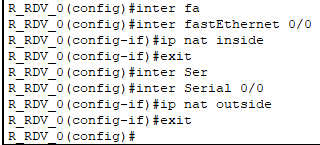
## **Шаг 9. Определение списка доступа, соответствующего внутренним частным IP-адресам.**



## **Шаг 10. Определение NAT из списка внутренних адресов в пул внешних адресов.**

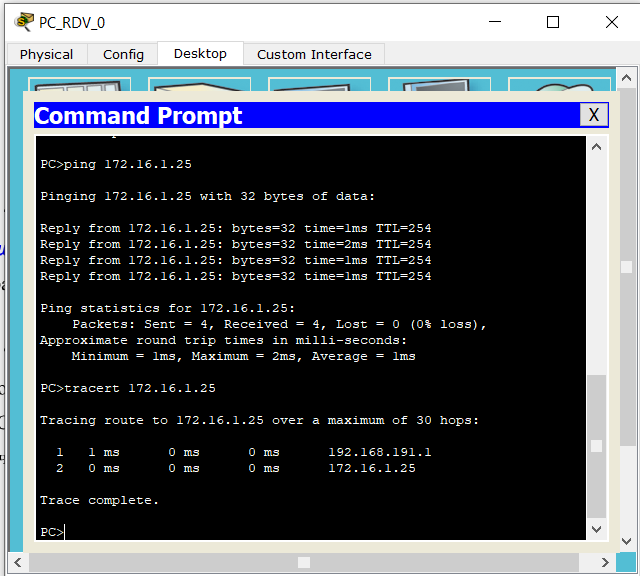


## **Шаг 11. Назначение интерфейсов.**

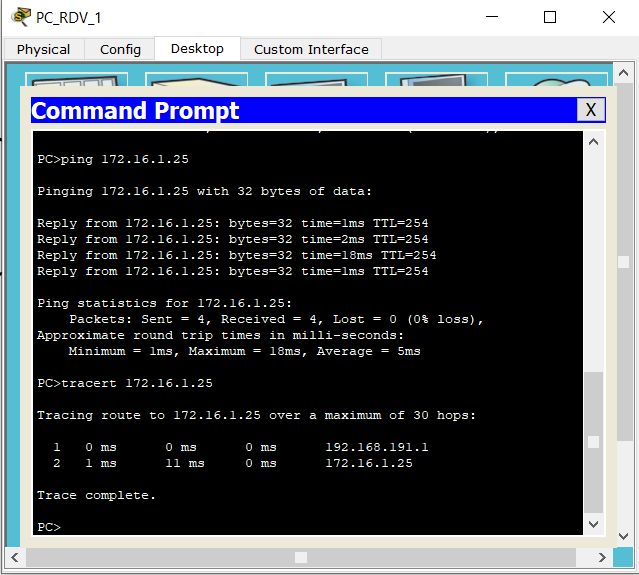


## **Шаг 12. Генерация трафика с маршрутизатора Gateway к маршрутизатору ISP.**

C PC\_RDV\_0:

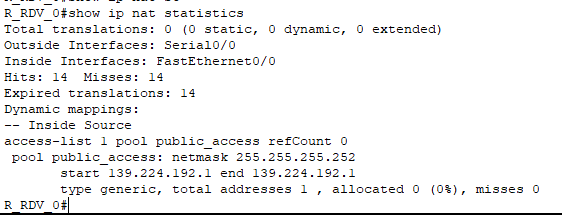


C PC\_RDV\_1:



## **Шаг 13. Проверьте работоспособность NAPT**

Результат выполнения команды **show ip nat stat**:



*Сколько активных преобразований выполенено?*

Выполнено 0 активных преобразований (total translations).

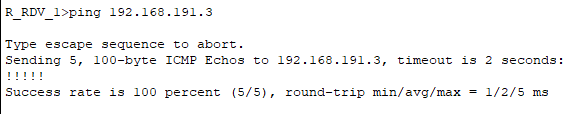
*Сколько адресов имеется в пуле?*

В пуле имеется 1 адрес (total addresses).

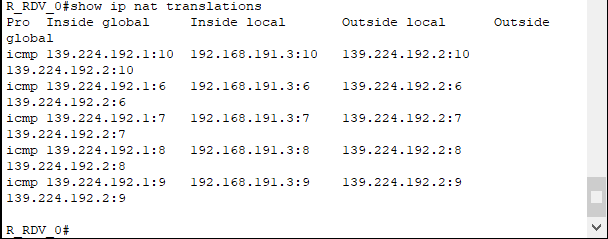
*Сколько адресов уже выделено?*

Выделено 0 адресов (allocated).

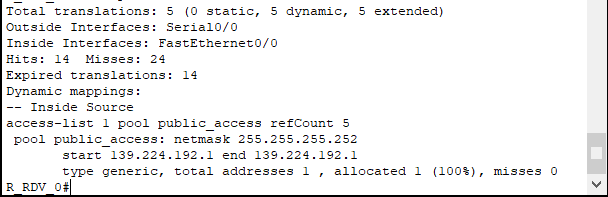
**Выполнение эхо-запроса с R\_RDV\_1 на PC\_RDV\_0:**



**Преобразование NAT:**



Выполнение команды show ip nat stat:



Как мы можем заметить, total translations сразу стало равняться пяти, а также allocated стало равняться 1.

**Реферат на тему «технология NAPT»**

## **Немного о NAT.**

Одной из причин популярности технологии NAT можно назвать дефицит IP-адресов. Если сеть предприятия автономна, то в ней могут быть использованы любые IP-адреса, лишь бы они были синтаксически правильными. Совпадение адресов в не связанных между собой сетях не вызовет никаких отрицательных последствий. Однако для всех сетей, подключенных к Internet, необходимы глобальные IP-адреса, т. е. позволяющие однозначно определить сетевые интерфейсы в пределах всей составной сети. Их уникальность гарантируется централизованной, иерархически организованной системой их распределения. Главным органом регистрации глобальных адресов в 1998 г. стал Internet Corporation for Assigned Names and Numbers (ICANN) — неправительственная некоммерческая организация, управляемая Советом директоров. Она координирует работу региональных отделов, чья деятельность охватывает большие географические зоны: ARIN — Америка, RIPE — Европа, APNIC — Азия и Тихоокеанский регион. Региональные отделы выделяют блоки глобальных адресов крупным провайдерам, те в свою очередь присваивают их клиентам, среди которых могут быть и более мелкие провайдеры.

Если по каким-либо причинам предприятию не удается получить у провайдера нужное количество глобальных IP-адресов, оно может прибегнуть к технологии NAT. В этом случае для адресации внутренних узлов применяются специально зарезервированные для подобных целей так называемые частные (private) адреса:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

Приведенные выше диапазоны адресов составляют огромное адресное пространство, достаточное для нумерации узлов сетей практически любых размеров. Эти адреса исключены из множества централизованно распределяемых, а значит, пакеты с такими адресами назначения будут проигнорированы маршрутизаторами на магистралях Internet. Для того чтобы узлы с частными адресами могли связываться друг с другом через Internet или с любыми другими узлами, необходимо использовать технологию NAT.

Потребность в трансляции IP-адресов возникает и тогда, когда предприятие из соображений безопасности желает скрыть адреса узлов своей сети, чтобы не позволить злоумышленникам составить представление о ее структуре и масштабах, а также о структуре и интенсивности исходящего и входящего трафика.

Технология трансляции сетевых адресов имеет несколько разновидностей, наиболее популярная из которых — **традиционный NAT** (Traditional NAT) — позволяет узлам из частной сети прозрачным для пользователей образом получать доступ к узлам во внешних сетях. Сеансы традиционного NAT однонаправленные и инициируются изнутри частной сети. (Направление сеанса определяется положением инициатора: если обмен данными инициируется приложением, работающим на узле внутренней сети, такой сеанс называется исходящим, несмотря на то что в рамках указанного сеанса в сеть могут поступать данные извне.) В виде исключения традиционный NAT допускает сеансы обратного направления, посредством статического отображения адресов для некоторого ограниченного, заранее заданного набора узлов, для которых устанавливается взаимно однозначное соответствие между внутренними и внешними адресами.

**Традиционный NAT** подразделяется на **Basic Network Address Translation (Basic NAT)** — метод, использующий для отображения только IP-адреса, и **Network Address Port Translation (NAPT)** — когда для отображения привлекаются еще и так называемые транспортные идентификаторы, в качестве которых чаще всего выступают порты TCP/UDP.

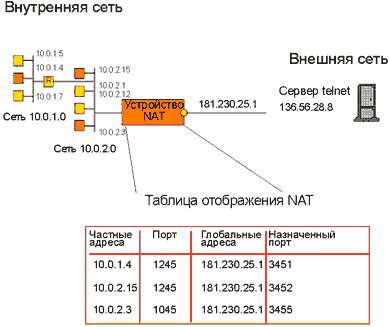
Но так как нам более интересен NAPT, рассмотрим подробнее именно эту технологию.

## **Непосредственно NAPT**

Допустим, что некоторая организация имеет частную сеть IP и соединение с провайдером Internet. Внешнему интерфейсу пограничного маршрутизатора назначен глобальный адрес, а остальным узлам сети — частные адреса. NAPT позволяет всем узлам внутренней сети одновременно взаимодействовать с внешними сетями с помощью одного-единственного зарегистрированного IP-адреса. Каким же образом внешние пакеты, поступающие в ответ на запросы из сети, находят узел-отправитель, ведь в поле адреса источника всех пакетов, отправляющихся во внешнюю сеть, помещается один и тот же адрес внешнего интерфейса? Для идентификации узла отправителя можно привлечь дополнительную информацию — номер порта UDP или TCP. Но и это не вносит полной ясности, поскольку из внутренней сети может исходить несколько запросов с совпадающими номерами портов отправителя, и опять возникает вопрос об однозначности отображения единственного глобального адреса на набор внутренних адресов. Решение состоит в том, что при прохождении пакета из внутренней во внешнюю сеть каждой паре {внутренний частный адрес; номер порта TCP/IP отправителя} ставится в соответствие другая пара {глобальный IP-адрес внешнего интерфейса; назначенный номер порта TCP/IP}. Назначенный номер порта выбирается произвольно, но он должен быть уникальным в пределах всех узлов, получающих выход во внешнюю сеть. Соответствие фиксируется в таблице.

Эта модель удовлетворяет требованиям большинства сетей средних размеров для доступа к внешним сетям с помощью единственного зарегистрированного IP-адреса, полученного от провайдера.

На **рисунке ниже** приведен пример, когда тупиковая сеть А использует внутренние адреса из блока 10.0.0.0/8. Внешнему интерфейсу маршрутизатора этой сети провайдером назначен адрес 181.230.25.1



Когда хост 10.0.1.4 сети А посылает пакет сервиса telnet хосту 136.56.28.8 во внешней сети, то он в качестве адреса назначения указывает глобальный адрес 136.56.28.8 и направляет пакет маршрутизатору. Маршрутизатор знает путь к сети 136.56.0.0/16, поэтому передает пакет на внешний интерфейс. Но при этом NAPT маршрутизатора транслирует адрес отправителя 10.0.1.4 и его порт TCP 1245 в глобально уникальный адрес 181.230.25.1 и уникально назначенный порт TCP, например 3451. Генерирующий ответное сообщение получатель в качестве адреса назначения указывает единственный зарегистрированный глобальный адрес сети А (адрес внешнего интерфейса устройства NAPT), а также назначенный номер порта TCP/UDP, который он берет из поля порта отправителя пришедшего пакета. При поступлении ответного пакета на устройство NAPT сети А именно по номеру порта в таблице трансляции выбирается нужная строка. Из нее определяется внутренний IP-адрес соответствующего узла и действительный номер порта. Эта процедура трансляции полностью прозрачна для конечных узлов.

В варианте NAPT разрешаются только исходящие из частной сети сеансы TCP/UDP. Однако нередки ситуации, когда нужно обеспечить доступ извне к некоторому узлу внутренней сети. В простейшем случае, если сервис зарегистрирован, т. е. ему присвоен «хорошо известный» номер порта (например, Web или DNS) и, кроме того, этот сервис представлен во внутренней сети в единственном экземпляре, задача решается достаточно просто. Сервис и узел, на котором он работает, однозначно определяются на основании «хорошо известного» зарегистрированного номера порта сервиса.

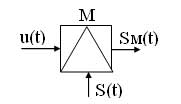
**Теоретический мини-коллоквиум**

**Вопрос:** *Модуляция сигналов. Основные типы аналоговой модуляции.*

**Ответ:** Начнём с определения. **Модуляцией** называют процесс преобразования одной либо нескольких характеристик модулирующего высокочастотного колебания при воздействии управляющего низкочастотного сигнала. В итоге спектр управляющего сигнала перемещается в высокочастотную область, где передача высоких частот является более эффективной.

Модуляция выполняется с целью передачи информации посредством [электромагнитного излучения](https://pue8.ru/ekologiya/406-vliyanie-elektromagnitnykh-polej-na-cheloveka.html). Передаваемые данные содержатся в управляющем сигнале. А функцию переносчика осуществляет высокочастотное колебание, именуемое несущим. В роли несущего колебания могут быть использованы колебания разнообразной формы: пилообразные, прямоугольные и др., но обычно используют гармонические синусоидальные.

Модуляция осуществляется в устройствах *модуляторах*. Условное графическое обозначение модулятора имеет вид:



При модуляции на вход модулятора подаются сигналы:

u(t) — *модулирующий*, данный сигнал является информационным и низкочастотным (его частоту обозначают W или F);

S(t) — *модулируемый (несущий)*, данный сигнал является неинформационным и высокочастотным (его частота обозначается w0 или f0);

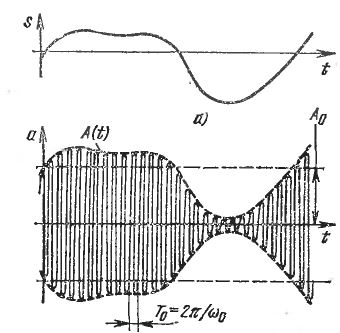
Sм(t) — *модулированный сигнал*, данный сигнал является информационным и высокочастотным.

Различают **аналоговую модуляцию** следующих видов (основных):

* Амплитудная модуляция
* Амплитудная модуляция c одной боковой полосой
* Частотная модуляция
* Линейно-частотная модуляция
* Фазовая модуляция
* Дифференциально-фазовая модуляция

**Амплитудная модуляция**

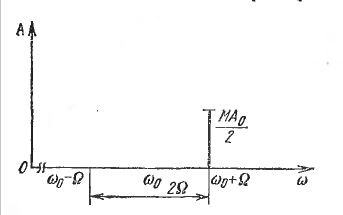
При амплитудной модуляции, огибающая амплитуд несущего колебания изменяется по закону, совпадающему с законом передаваемого сообщения. Частота и фаза несущего колебания при этом не меняется.



Одним из основных параметров АМ, является коэфициент модуляции(M).  
Коэффициент модуляции — это отношение разности между максимальным и минимальным значениями амплитуд модулированного сигнала к сумме этих значений(%).  
 Проще говоря, этот коэффициент показывает, насколько сильно значение амплитуда несущего колебания в данный момент отклоняется от среднего значения.  
При коэффициенте модуляции больше 1, возникает эффект перемодуляции, в результате чего происходит искажение сигнала.

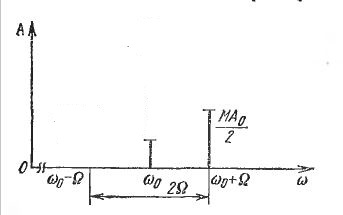
**Амплитудная модуляция с одной боковой полосой**

В связи с неэффективностью классической амплитудной модуляции, была придумана амплитудная модуляция с одной боковой полосой. Суть ее заключается в удалении из спектра несущей и одной из боковых полос, при этом вся необходимая информация передается по оставшейся боковой полосе.



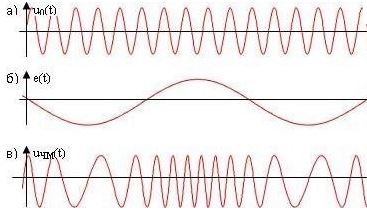
Но в чистом виде в бытовом радиовещании этот вид не прижился, т.к. в приемнике нужно синтезировать несущую с очень высокой точностью. Используется в аппаратуре уплотнения и любительском радио.

В радиовещании чаще используют АМ с одной боковой полосой и частично подавленной несущей:



**Частотная модуляция**

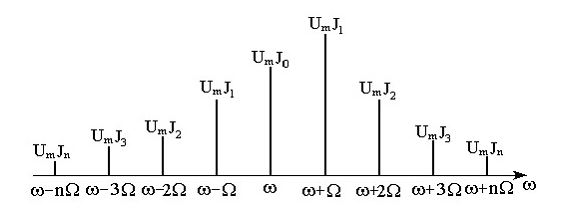
Вид аналоговой модуляции, при которой, частота несущей изменяется по закону модулирующего низкочастотного сигнала. Амплитуда при этом остается постоянной.

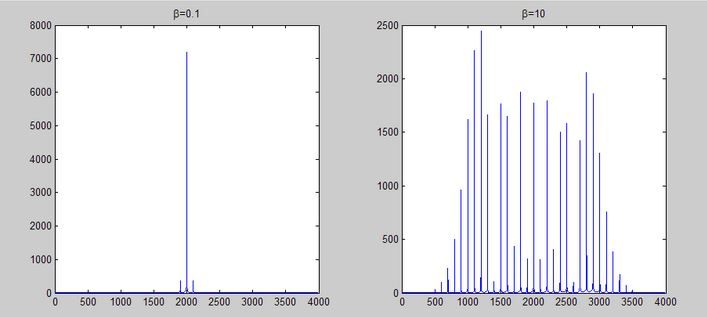


а) - несущая частота; б) модулирующий сигнал; в) результат модуляции

Наибольшее отклонение частоты от среднего значения, называется девиацией.  
В идеальном варианте, девиация должна быть прямо пропорционально амплитуде модулирующего колебания.

Спектр при частотной модуляции выглядит следующим образом:

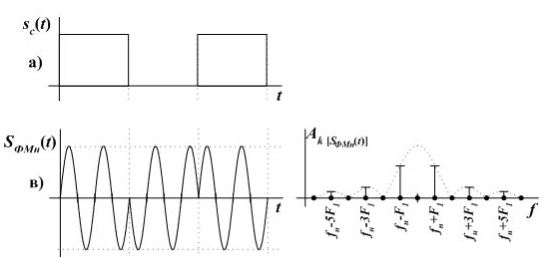


Состоит из несущей и симметрично отстающей от нее вправо и влево гармоник боковых полос, на частоту кратную частоте модулирующего колебания.  
Данный спектр представляет гармоническое колебание. В случае реальной модуляции, спектр имеет более сложные очертания.  
Различают широкополосную и узкополосную ЧМ модуляцию.  
В широкополосной — спектр частот, значительно превосходит частоту модулирующего сигнала. Применяется в ЧМ радиовещании.  
В радиостанциях применяют в основном узкополосную ЧМ модуляцию, требующую более точной настройки приемника и соответственно более защищенную от помех.  
Спектры широкополосной и узкополосной ЧМ представлены ниже:

Спектр узкополосной ЧМ напоминает амплитудную модуляцию, но если учесть фазу боковых полос, то окажется, что эти волны имеют постоянную амплитуду и переменную частоту, а не постоянную частоту и переменную амплитуду (AM). При широкополосной ЧМ амплитуда несущей может быть очень малой, что обусловливает высокую эффективность ЧМ; это значит, что большая часть передаваемой энергии содержится в боковых частотах, несущих информацию.  
  
 Основные преимущества ЧМ, перед АМ — энергоэффективность и помехоустойчивость.

**Фазовая модуляция**

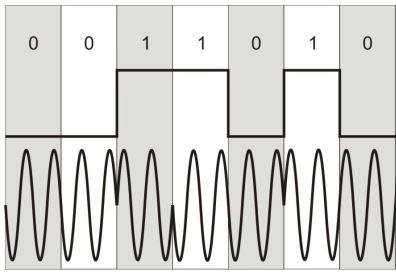
В реальности, больше применяют термин фазовая манипуляция, т.к. в основном производят модуляцию дискретных сигналов.  
 Смысл ФМ таков, что фаза несущей, изменяется скачкообразно, при приходе очередного дискретного сигнала, отличного от предыдущего.



Из спектра можно видеть, почти полное отсутствие несущей, что указывают на высокую энергоэффективность.  
 Недостаток данной модуляции в том, что ошибка в одном символе, может привести к некорректному приему всех последующих.

**Дифференциально-фазовая манипуляция**

В случае этой модуляции, фаза меняется не при каждом изменении значения модулирующего импульса, а при изменении разности. В данном примере при приходе каждой «1».



Преимущество этого вида модуляции в том, что в случае возникновения случайной ошибки в одном символе, это не влечет дальнейшую цепочку ошибок.  
  
 Стоит отметить, что существуют также фазовые манипуляции такие как квадратурная, где используется изменение фазы в пределах 90 градусов и ФМ более высоких порядков, но их рассмотрение выходит за рамки данной статьи.