**Министерство образования Республики Беларусь**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**Факультет прикладной математики и информатики**

Никончик даниил викторович

Настройка и проверка NAPT

Отчет по лабораторной работе № 13,

вариант 19

(“Компьютерные сети”)

студента 2-го курса 13-ой группы

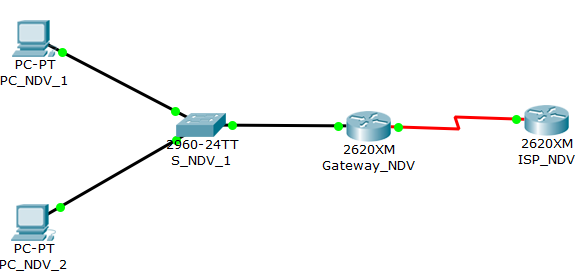
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | | **Преподаватель** | | |
|  | | | **Бубен И. В.** | | |
|  | | | | | | | | |
| **2021 г.** | | | | | | | | |
| **Вариант** | Адреса для узлов | | Маршрутизатор 1 | Маршрутизатор 2 | | IP-адрес  Loopback 1 |
| **19** | 10.64.30.0/24 | | 11.62.112.1/30 | 11.62.112.2/30 | | 172.16.1.19/32 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Устройство | Имя узла | Маска подсети порта FastEthenet0/0 | Тип интерфейса | IP-адрес порта Serial 0/0 | IP-адрес Loopback 1 |
| Gateway\_NDV | Gateway | 10.64.30.0/24 | DTE | 11.62.112.1/30 |  |
| ISP\_NDV | ISP | нет | DCE | 11.62.112.2/30 | 172.16.1.19/32 |
| S\_NDV\_1 | S\_NDV\_1 |  |  |  |  |

1. **Последовательность выполнения работы**

**Шаг 1. Подсоединение устройств.**

* Подсоедините интерфейс Serial 0/0 маршрутизатора 1 к интерфейсу Serial 0/0 маршрутизатора 2 с помощью последовательного кабеля.
* Подсоедините интерфейс Fa0/0 маршрутизатора 1 к интерфейсу Fa0/1 коммутатора 1 с помощью прямого кабеля.
* Подсоедините оба узла к порту Fa0/2 и Fa0/3 коммутатора с помощью прямых кабелей.
* Как уже было принято, подписать устройства сети.

****

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

* Зашел в настройках конфигурации маршрутизатора 2 имя узла (ISP), задайте IP-адреса для интерфейсов согласно вашему варианту задания. Сохранил конфигурацию.

****

* Конфигурирование Loopback интерфейса



**Шаг 3. Настройка маршрутизатора, используемого в качестве шлюза(Gateway).**

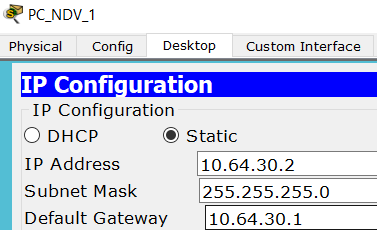
* Задал в настройках основной конфигурации маршрутизатора 1 имя узла (Gateway), задайте IP-адреса для интерфейсов. Сохранил конфигурацию.



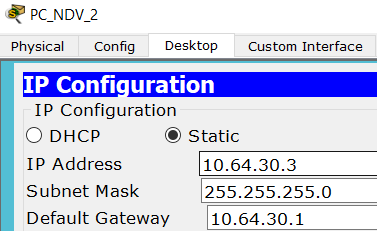
**Шаг 4. Настройки правильного IP-адреса, маски подсети и шлюза по умолчанию для узлов.**

* Присвоил каждому узлу соответствующий IP-адрес, маску подсети и шлюз по умолчанию. Оба узла должны получить внутренние частные IP-адреса в сети 10.64.30.0/24. Шлюзом по умолчанию должен быть IP-адрес интерфейса FastEthernet маршрутизатора с именем Gateway.

Для PC\_NDV\_1:



Для PC\_NDV\_2:



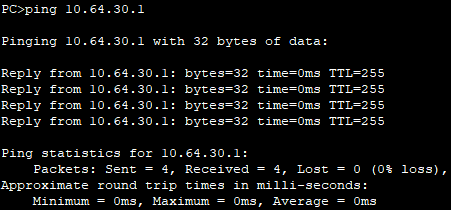
Для Gateway\_NDV:



**Шаг 5. Проверка работоспособности сети.**

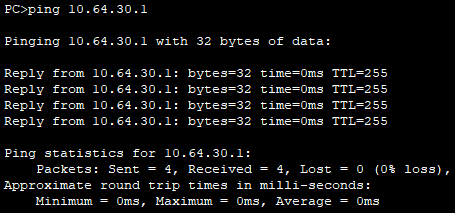
1. С присоединенных узлов отправьте эхо-запрос на интерфейс FastEthernet маршрутизатора, используемого в качестве шлюза по умолчанию. Ответьте на следующие вопросы.
2. Успешно ли выполнен эхо-запрос с узла 1?

Ответ: да



1. Успешно ли выполнен эхо-запрос с узла 2?

Ответ: да



1. Ответы на оба вопроса положительны.
2. Отправьте эхо-запросы на IP-адрес маршрутизатора ISP. Какой получили результат. Поясните свой ответ.

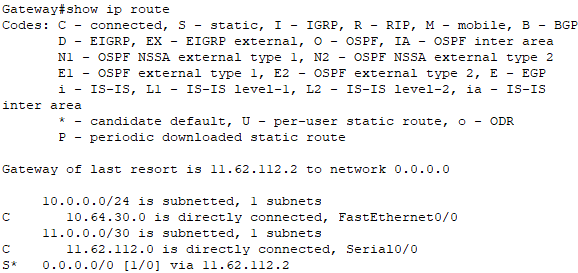
Ответ: запрос не удался, так как еще не настроена маршрутизация

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

* С маршрутизатора, использующегося в качестве шлюза по умолчанию, создайте статический маршрут к маршрутизатору поставщика услуг Интернета в сети 0.0.0.0 0.0.0.0 с помощью команды ***ip route***. Это вызовет трафик к любому неизвестному адресу назначения через поставщика услуг Интернета путем настройки шлюза «последней надежды» на маршрутизаторе, использующемся в качестве шлюза по умолчанию



* Проверьте маршрут по умолчанию по таблице маршрутизации маршрутизатора Gateway. Находится ли статический маршрут в таблице маршрутизации.



Ответ: статический маршрут находится в таблице маршрутизации.

* Попробуйте отправить эхо-запрос с одной с рабочих станций на IP-адрес последовательного интерфейса маршрутизатора поставщика услуг Интернета. Успешно ли выполнен эхо-запрос?

Ответ: нет, эхо-запрос был выполнен неудачно.

**Шаг 7. Создание статического маршрута.**

Создал статический маршрут от маршрутизатора ISP к частной сети, присоединенной к маршрутизатору Gateway. Создал статический маршрут с помощью команды ***ip route.***



* Отправьте эхо-запрос с узла 1 на адрес интерфейса loopback маршрутизатора ISP. Успешно ли выполнен эхо-запрос?

Ответ: да

* Если эхо-запрос не выполнен, проверьте правильность конфигурации маршрутизатора и узла и повторите тестирование связи.

**Шаг 8. Определение пула используемых публичных IP-адресов.**

Для определения пула используемых публичных IP-адресов используйте команду **ip nat pool.**



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

Для определения списка доступа, соответствующего, внутренним частным адресам, использовал команду **access-list.**



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

Для определения NAT использовал команду **ip nat inside source.**



**Шаг 11. Назначение интерфейсов.**

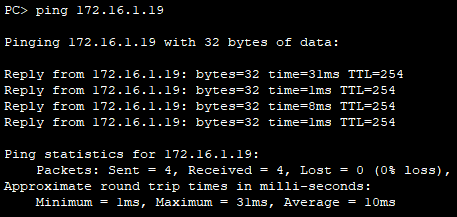
Активные интерфейсы маршрутизатора следует определить в качестве внутреннего или внешнего интерфейса в отношении к NAT. Для этого использовал одну из команд ***ip nat inside*** или ***ip nat outside***



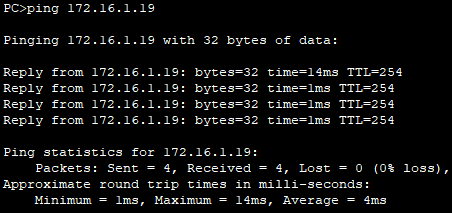
**Шаг 12. Генерация трафика с маршрутизатором Gateway к маршрутизатору ISP.**

Отправьте эхо-запросы с узлов 1 и 2 на адрес 172.16.1.19.

С первого узла:

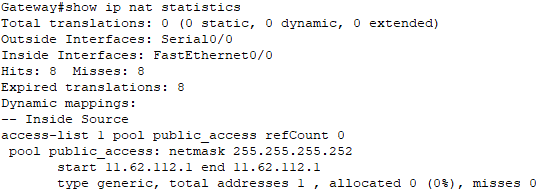


Со второго узла:



**Шаг 13. Проверьте работоспособность NAPT.**

Для отображения статистики NAРT введите в приглашение привилегированного режима EXEC маршрутизатора Gateway команду ***show ip nat statistics***.



Проанализируйте полученную информацию и дать ответ на следующие вопросы.

1. Сколько активных преобразований выполнено?

Ответ: 8

1. Сколько адресов имеется в пуле?

Ответ: 1

1. Сколько адресов уже выделено?

Ответ:0

Эхо-запрос выполнился успешно, отобразил преобразование NAT на маршрутизаторе Gateway с помощью команды **show ip nat translations**



**Технология NAT**

**Трансляция сетевых адресов (NAT)** - это процесс, в котором один или несколько частных IP-адресов преобразуются в один или несколько публичных IP-адресов и наоборот, чтобы обеспечить доступ в Интернет для локальных узлов.

Кроме того, **NAT выполняет преобразование номеров портов**, то есть маскирует номер порта хоста другим номером порта в пакете, который будет направлен в пункт назначения. При этом NAT не только сохраняет пул общедоступных IP-адресов, но и скрывает схему адресации вашей сети. Затем он вносит соответствующие записи IP-адреса и номера порта в таблицу NAT.

Алгоритм работы технологии состоит в том, что **когда клиент в сети отправляет какой-то запрос в Интернет, маршрутизатор пересылает запрос специальному устройству**. NAT преобразует адрес отправителя в общедоступный IP-адрес устройства перед пересылкой запроса в Интернет и для дальнейшего получения информации с сервера.

Когда ответ получен от внешнего источника, **NAT преобразует общедоступный IP-адрес в частный IP-адрес** перед самой пересылкой пакета клиенту. Для этого NAT создает сопоставление между парой PrivateSrcIP, PrivateSrcPort и парой PublicSrcIP, PublicSrcPort, чтобы знать наверняка, как преобразовать IP-адрес назначения и номер порта назначения возвращающегося трафика. NAT обычно работает на маршрутизаторе или межсетевом экране.

**Принцип работы NAT.**

Основной принцип работы NAT заключается в том, что когда IP-пакеты, передаваемые между хостом частной сети и хостом общедоступной сети, проходят через шлюз NAT, исходный IP или IP-адрес назначения в пакете IP находятся в частном IP и NAT. Конвертировать между публичными IP-адресами. Шлюз NAT имеет 2 сетевых порта, а IP-адрес порта общедоступной сети представляет собой общедоступный IP-адрес с единообразным назначением, равный 202.204.65.2, а IP-адрес порта частной сети - зарезервированный адрес, равный 192.168.1.1. Хост 192.168.1.2 в частной сети отправил 1 пакет IP на хост 166.111.80.200 в публичной сети (Des = 166.111.80.200, Src = 192.168.1.2). Когда IP-пакет проходит через шлюз NAT, NAT преобразует исходный IP-адрес IP-пакета в общедоступный IP-адрес NAT и перенаправляет его в общедоступную сеть. В настоящее время IP-пакет (Des = 166.111.80.200, Src = 202.204.65.2) не содержит никаких Информация о частной сети IP. Поскольку исходный IP-адрес IP-пакета был преобразован в общедоступный IP-адрес NAT, отвечающий IP-пакет (Des = 202.204.65.2, Src = 166.111.80.200) будет отправлен в NAT. В это время NAT преобразует IP-адрес назначения IP-пакета в IP-адрес хоста в частной сети, а затем пересылает IP-пакет (Des = 192.168.1.2, Src = 166.111.80.200) в частную сеть. Для обеих сторон общения этот процесс преобразования адресов полностью прозрачен.

**Преимущества и особенности NAT.**

Из преимуществ и особенностей NAT можно выделить:

1. Скрывает внутреннюю структуру сети от посторонних глаз, неавторизованные пользователи не могут просматривать какие-либо системы, находящиеся за NAT, тем самым повышает безопасность сети.
2. решает частично вопрос в заканчиванием адресов типа IPv4.
3. предоставляет возможность использования одного IP-адреса для всей внутренней сети при подключении к Интернету.

**Недостатки NAT.**

К недостаткам этой технологии можно отнести:

1. что изменение IP-адреса может привести к усложнению поиска и решения созданной проблемы в сети.
2. некоторые службы TCP/IP плохо взаимодействуют с NAT.
3. Протоколы туннелирования усложняются по мере того, как NAT изменяет значения в заголовках пакетов, что влияет на проверку целостности этих протоколов.
4. Поскольку внутренние адреса скрыты за одним общедоступным адресом, внешний узел не сможет инициировать связь с внутренним узлом без специальной настройки брандмауэра для разрешения этого.
5. Приложения, использующие VoIP (VoIP), видеоконференции и другие пиринговые функции, должны использовать NAT-обратный путь, чтобы они функционировали.

Важная часть использования NAT - это выбор типа трансляции адресов. Всего существует три типа трансляции адресов:

* **Статический NAT** - сопоставляет один частный IP-адрес в один общедоступный (один к одному). Публичный IP-адрес всегда один и тот же.
* Динамический NAT - сопоставляет частный IP-адрес с пулом общедоступных IP-адресов (один к многим).
* **Преобразование портов адресов (PAT)** - относится к типу динамического NAT, который выполняет сопоставление нескольких частных IP-адресов одному общедоступному IP-адресу с использованием разных портов.
* Перенаправление порта - этот тип NAT позволяет одному публичному IP-адресу иметь доступ к нескольким разным серверам.

Применение NAT сейчас очень популярно в сетях поскольку оно поддерживается практически всеми операционными системами, брандмауэрами и приложениями. Если говорить об операционных системах, оптимальным выбором есть семейство UNIX.

Часто клиенты [“ГиперХост”](https://hyperhost.ua/ru) интересуются о запуске VPN на VPS/VDS с технологией NAT и спрашивают принцип доступа на наших серверах. Если Вам необходим NAT и Вы используете [VPS](https://hyperhost.ua/ru/vps-vds), для открытия доступа и выполнения настроек, вам сначала необходимо открыть просто тикет с запросом в тех.поддержку. На же клиент сразу может начать использовать и проделать необходимые ему настройки системы. Поэтому VDS сервер является лучшим решением для разворачивания такого типа VPN.

С течением времени, технология NAT сформировала различные производные и инновации из своей первой эволюции. Он предлагает две функции: сохранение адресов и безопасность, которые обычно реализуются в средах удаленного доступа. Перевод сетевых адресов является очень важным аспектом безопасности брандмауэра. Он ограничивает количество публичных адресов, используемых в организации, что позволяет более строго контролировать доступ к ресурсам по обе стороны брандмауэра.

**Функциональность NAT.**

Этот процесс изначально применялся как метод перенаправления пакетов при передаче данных по отдельным хост-сетям. В настоящее время она рассматривается как глобальное решение проблемы отсутствия доступных адресов IPv4. Он работает над оптимизацией использования доступных IP-адресов, позволяя нескольким устройствам быть доступными с одного публичного IP-адреса. Затем для перенаправления пакетов данных в пределах локальной сети используется частный IP-адрес.

Другими словами, NAT позволяет конкретному устройству, такому как маршрутизатор, а также другим устройствам, функционировать в качестве модератора между публичной сетью, такой как Интернет, и локальной или частной сетью, такой как домашняя или офисная сеть. Это позволяет одному уникальному в глобальном масштабе IP-адресу представлять всю частную сеть, включая все подключенные к ней устройства.

Эта система была создана для решения вопросов, возникших в связи с ростом популярности и использования Интернета. В основном, доступные IP-адреса не могли поддерживать потребность во всемирном соединении, так как все больше и больше людей стали использовать Интернет. Хотя изначально NAT разрабатывалась как временное решение, она широко использовалась и применялась всеми сетевыми провайдерами, производителями оборудования и технологическими компаниями.

Преобразования NAT имеет важную особенность с точки зрения обеспечения безопасности: трансляция частных IP-адресов в публичные из пула маршрутизатора, позволяет скрыть топологию внутренней сети от внешних пользователей, что затрудняет несанкционированный доступ к ресурсам сети.