**МИНИСТЕРСТВО ОБРАЗОВАНИЯ**

**РЕСПУБЛИКИ БЕЛАРУСЬ**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**Факультет прикладной математики и информатики**

**Жуковский Павел Сергеевич**

**Настройка и проверка NAPT**

Отчет по лабораторной работе № 13,

Вариант 32

(“Компьютерные сети”)

студента 2-го курса 13-ой группы

**Преподаватель**

**Бубен. И.В.**

**2020 г.**

Оглавление по пунктам выполнения

**[Вариант 32](#_Toc40107253)** [3](#_Toc40107253)

[**Задания на лабораторную работу** 3](#_Toc40107254)

[1. Представить в отчете небольшой реферат о технологии NAT. 3](#_Toc40107255)

[2. Реализовать по аналогии схему сети приведенной на рисунке 1. 5](#_Toc40107256)

[3. Присвоить имена маршрутизаторам и хостам по уже принятым правилам. 5](#_Toc40107257)

[4. Выполните пункты 1-13 методических указаний к лабораторной работе. Адреса задавать согласно вашему варианту задания. 5](#_Toc40107258)

[4.1. Шаг 1. Подсоединение устройств 5](#_Toc40107259)

[4.2. Шаг 2. Настройка основной конфигурации маршрутизатора 2 5](#_Toc40107260)

[4.3. Шаг 3. Настройка маршрутизатора, используемого в качестве шлюза 7](#_Toc40107261)

[4.4. Шаг 4. Настройка правильного IP-адреса, маски подсети и шлюза по умолчанию для узлов 9](#_Toc40107262)

[4.5. Шаг 5. Проверка работоспособности сети 9](#_Toc40107263)

[4.6. Шаг 6. Создание маршрута по умолчанию 10](#_Toc40107264)

[4.7. Шаг 7. Создание статического маршрута 11](#_Toc40107265)

[4.8. Шаг 8. Определение пула используемых публичных IP-адресов 12](#_Toc40107266)

[4.9. Шаг 9. Определение списка доступа, соответствующего внутренним частным IP-адресам 12](#_Toc40107267)

[4.10. Шаг 10. Определение NAT из списка внутренних адресов в пул внешних адресов 12](#_Toc40107268)

[4.11. Шаг 11. Назначение интерфейсов 13](#_Toc40107269)

[4.12. Шаг 12. Генерация трафика с маршрутизатора Gateway к маршрутизатору ISP 13](#_Toc40107270)

[4.13. Шаг 13. Проверка работоспособности NAT 13](#_Toc40107271)

[5. В отчет включить: скриншоты с комментариями по каждому шагу работы, ответы на вопросы и при необходимости ваши выводы на полученный результат. 15](#_Toc40107272)

[6. Согласно вашему варианту задания в отчет поместите развернутый ответ на теоретический вопрос. 15](#_Toc40107273)

[Теоретический мини коллоквиум 15](#_Toc40107274)

# **Вариант 32**

| **Вариант** | Адреса для узлов | Маршрутизатор 1 | Маршрутизатор  2 | IP-адрес  Loopback 1 |
| --- | --- | --- | --- | --- |
| 32 | 10.150.1.0/24 | 187.16.64.1/30 | 187.16.64.2/30 | 172.16.1.10/32 |

# **Задания на лабораторную работу**

## 1. Представить в отчете небольшой реферат о технологии NAT.

**Технология NAT**

Преобразование сетевых адресов (NAT) - это процесс, во время которого сетевое устройство (обычно им является брандмауэр) назначает общий адрес компьютеру (или целой группе компьютеров) внутри какой-то частной сети. Основное использование NAT заключается в том, чтобы ограничивать количество общедоступных IP-адресов, которые организация или компания должны использовать как в целях безопасности, так и в целях экономии.

Наиболее распространенная форма сетевого перевода включает в себя достаточно большую частную сеть, использующую адреса в частном диапазоне (10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255 или 192.168.0 0-192.168.255.255). Можно задаться вопросом: а где эта схема может быть полезной? Схема частной адресации хорошо работает для компьютеров, которым требуется только доступ к ресурсам внутри сети, например, для рабочих станций, которым необходим доступ к файловым серверам и принтерам. Маршрутизаторы внутри частной сети также могут маршрутизировать трафик между частными адресами без каких-либо проблем. Однако для доступа к ресурсам вне сети, таким как Интернет, эти компьютеры должны иметь уже публичный адрес, чтобы ответы на их запросы возвращались к ним обратно. Вот тут-то и показывает себя технология NAT.

Интернет-запросы, которые требуют преобразования сетевых адресов (NAT), довольно сложны, но происходят настолько быстро, что конечный пользователь редко знает, что это произошло. Рабочая станция внутри сети делает запрос к компьютеру в Интернете. Позже маршрутизаторы внутри сети распознают, что запрос не относится к ресурсу внутри сети, поэтому они отправляют запрос в брандмауэр. Брандмауэр видит запрос от компьютера с внутренним IP-адресом. Затем он делает тот же запрос в Интернет, используя свой собственный публичный адрес, и возвращает ответ с Интернет-ресурса на компьютер внутри частной сети. С точки зрения ресурса в Интернете, это отправка информации по адресу брандмауэра. С точки зрения рабочей станции, кажется, что связь осуществляется непосредственно с сайтом в Интернете. Когда NAT используется таким образом, все пользователи внутри частной сети получают доступ к интернету с одним и тем же публичным IP-адресом, когда они используют интернет. Это означает, что только один публичный адрес необходим для сотен или даже тысяч пользователей.

Большинство современных брандмауэров являются статусными – то есть они способны устанавливать соединение между внутренней рабочей станцией и Интернет-ресурсом. Они могут отслеживать детали соединения, такие как порты, порядок пакетов и соответствующие IP-адреса. Это называется отслеживанием состояния соединения. Таким образом, они могут отслеживать сеанс, состоящий из связи между рабочей станцией и брандмауэром, а также брандмауэр с Интернетом. Когда сеанс заканчивается, брандмауэр удаляет всю информацию о соединении.

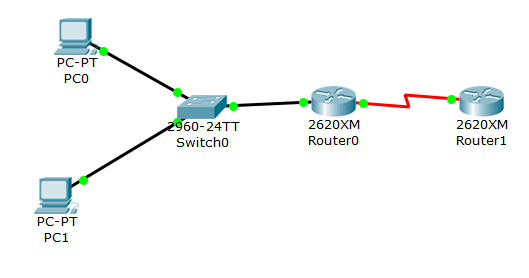
Помимо вышесказанного, существуют и другие способы преобразования сетевых адресов (NAT), помимо простого предоставления доступа к интернету рабочим станциям с внутренними IP-адресами. В больших сетях некоторые серверы могут выступать в качестве веб-серверов и требуют доступа из интернета. Этим серверам назначаются общедоступные IP-адреса в брандмауэре, что позволяет общественности получать доступ к серверам только через этот IP-адрес. Однако в качестве дополнительного уровня безопасности брандмауэр выступает в качестве посредника между внешним миром и защищенной внутренней сетью. Можно добавить дополнительные правила, включая то, к каким портам можно получить доступ по этому IP-адресу. Использование NAT таким образом позволяет сетевым инженерам более эффективно направлять внутренний сетевой трафик к тем же ресурсам и разрешать доступ к большему количеству портов, ограничивая доступ через брандмауэр. Он также позволяет детализировать протоколирование сообщений между сетью и внешним миром.

Кроме того, NAT можно использовать и для обеспечения селективного доступа к внешней части сети. Рабочие станции или другие компьютеры, требующие специального доступа вне сети, могут быть назначены определенные внешние IP-адреса с помощью NAT, что позволяет им взаимодействовать с компьютерами и приложениями, требующими уникального публичного IP-адреса. Опять же, брандмауэр выступает в качестве посредника и может управлять сеансом в обоих направлениях, ограничивая доступ к порту и протоколам.

Подытожив, можно сказать, что NAT – это очень важный аспект безопасности брандмауэра. Он сохраняет количество общедоступных адресов, используемых в организации, и позволяет более строго контролировать доступ к ресурсам по обе стороны брандмауэра.

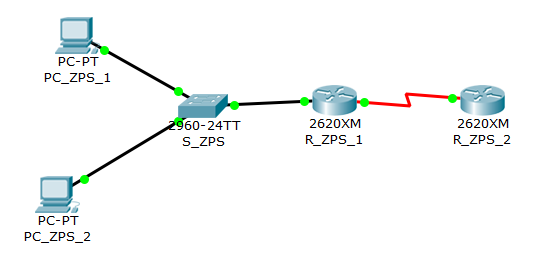
## 2. Реализовать по аналогии схему сети приведенной на рисунке 1.

Реализовал схему:



## 3. Присвоить имена маршрутизаторам и хостам по уже принятым правилам.

Присвоил имена маршрутизаторам и хостам (а также свитчу) на схеме:



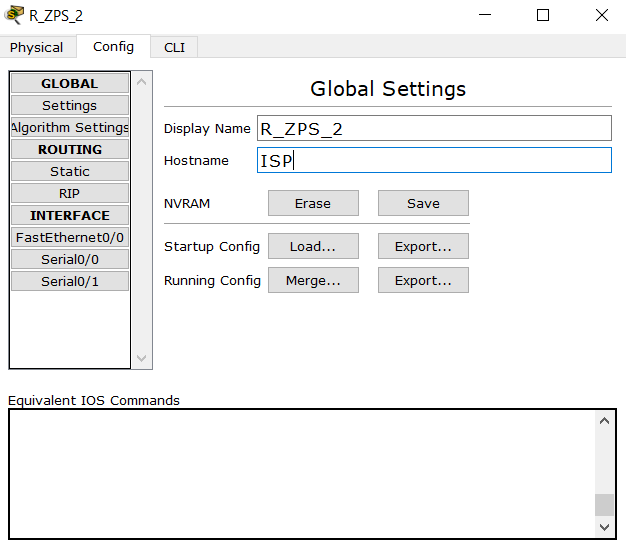
## 4. Выполните пункты 1-13 методических указаний к лабораторной работе. Адреса задавать согласно вашему варианту задания.

### 4.1. Шаг 1. Подсоединение устройств

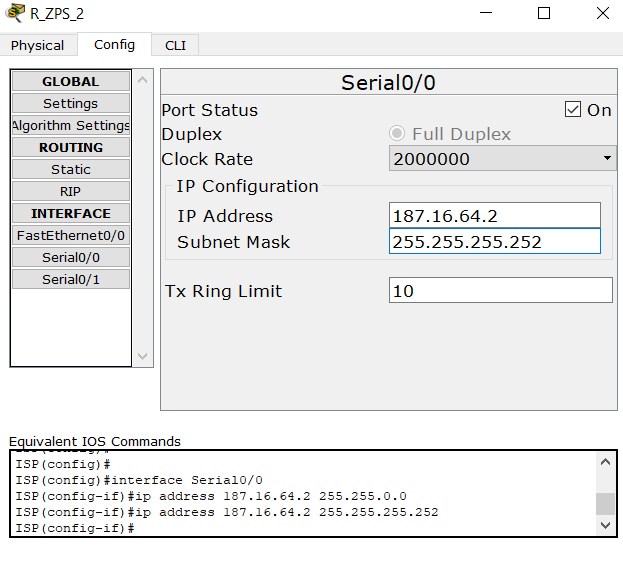
Мы подсоединил устройства так, как показано на схеме выше.

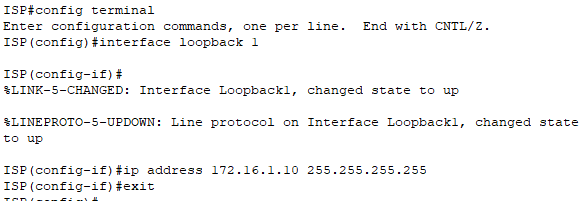
### 4.2. Шаг 2. Настройка основной конфигурации маршрутизатора 2

Задал в настройках конфигурации 2-ого маршрутизатора имя узла – ISP:

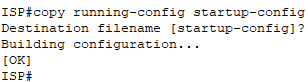


Задал IP-адреса для интерфейсов маршрутизатора согласно 32-ому варианту:



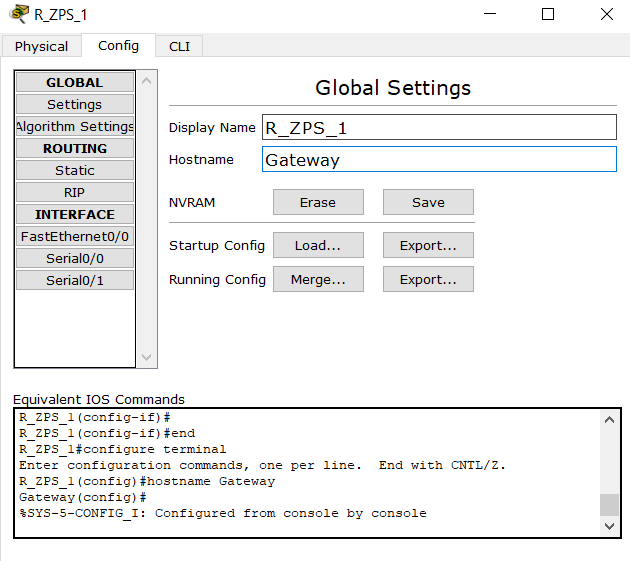


Сохранение конфигурации:

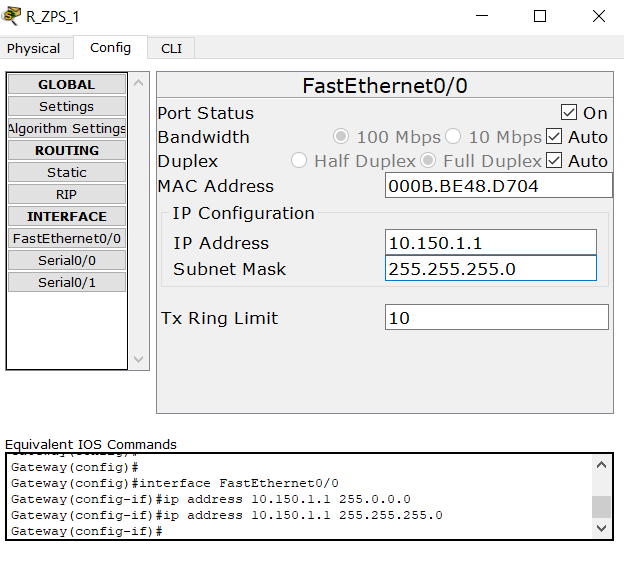


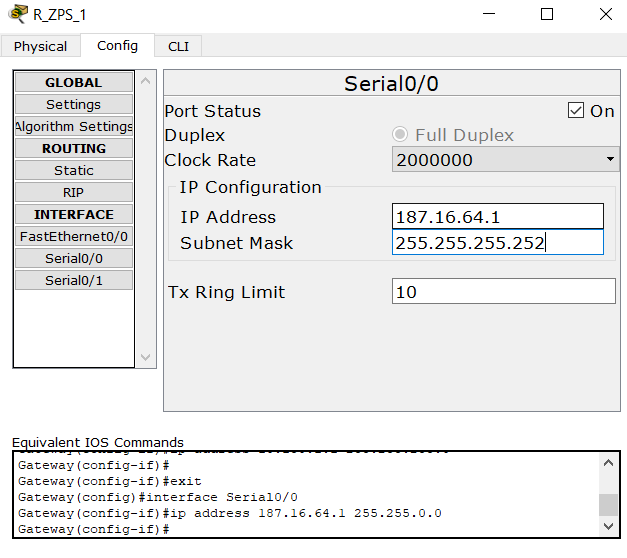
### 4.3. Шаг 3. Настройка маршрутизатора, используемого в качестве шлюза

Задал в настройках конфигурации 1-ого маршрутизатора имя узла – Gateway:

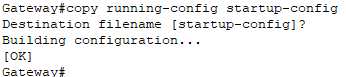


Задал IP-адреса для интерфейсов:



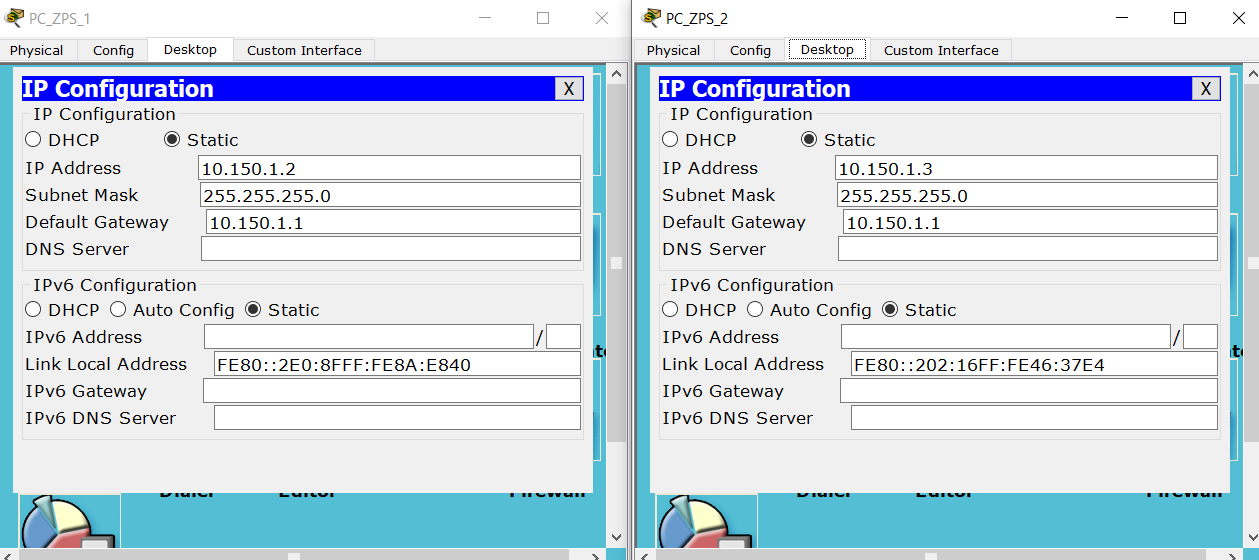


Сохранение конфигурации:



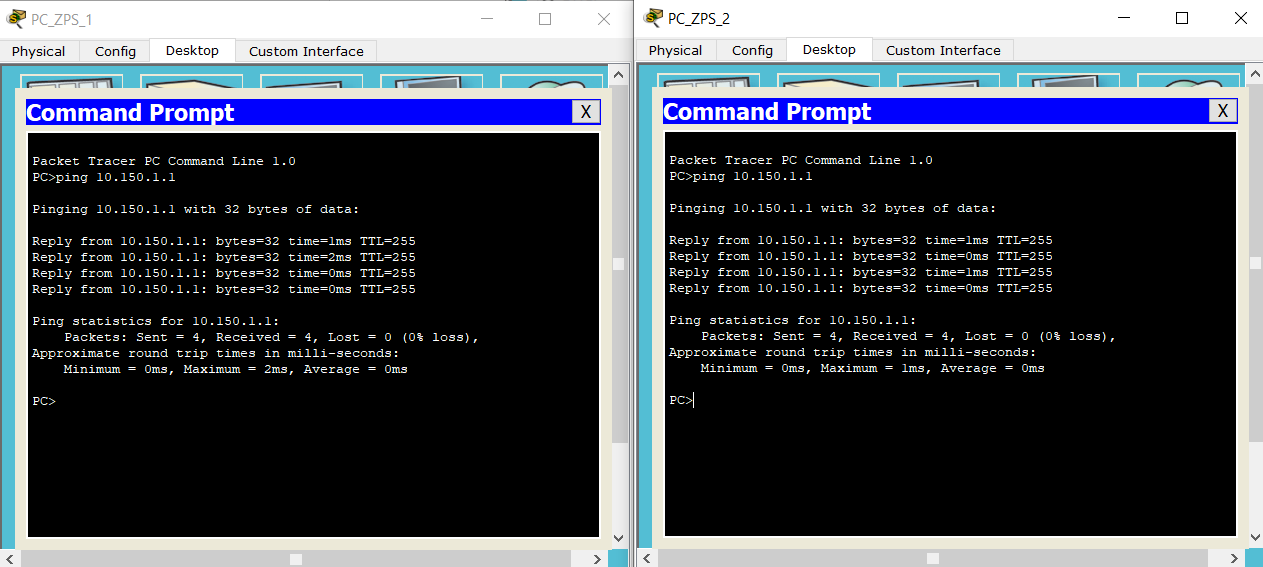
### 4.4. Шаг 4. Настройка правильного IP-адреса, маски подсети и шлюза по умолчанию для узлов

Присвоил каждому узлу соответствующий IP-адрес из 32-ого варианта, а также соответствующую маску подсети и шлюз по умолчанию:



### 4.5. Шаг 5. Проверка работоспособности сети

Отправил эхо-запрос на интерфейс FastEthernet0/0 маршрутизатора, используемого в качестве шлюза по умолчанию, с обоих подключённых узлов:



Ответил на следующие вопросы:

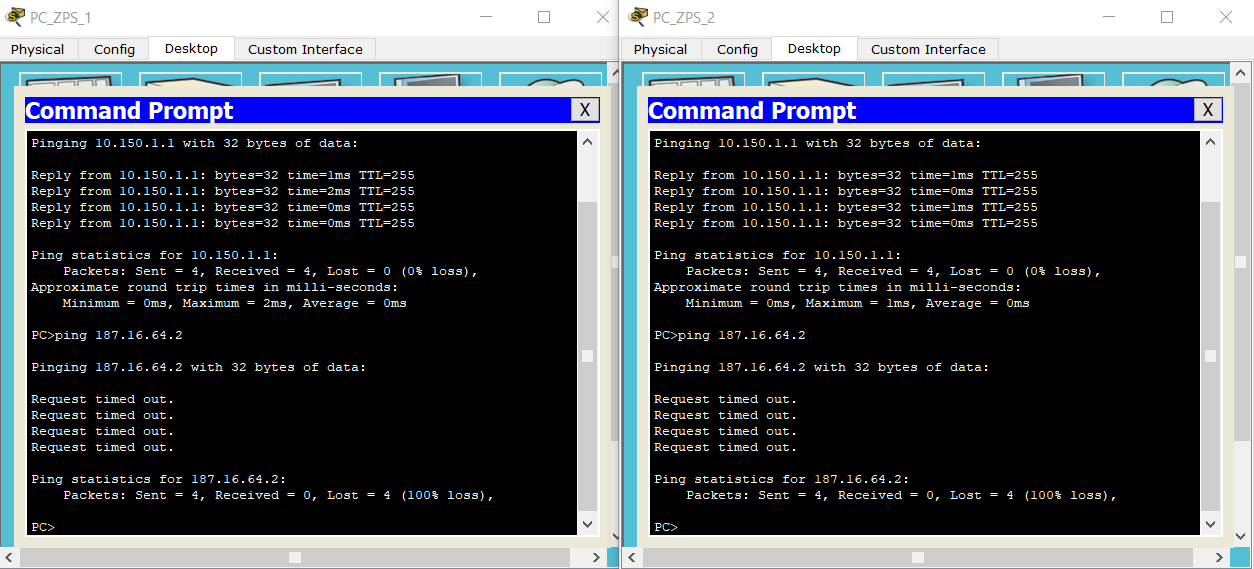
1) Успешно ли выполнен эхо-запрос с 1-ого узла?

Да, успешно, без потерь пакетов.

2) Успешно ли выполнен эхо-запрос со 2-ого узла?

Да, успешно, без потерь пакетов.

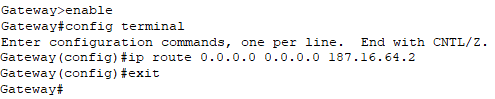
Отправил также эхо-запросы на IP-адрес маршрутизатора ISP с обоих узлов:



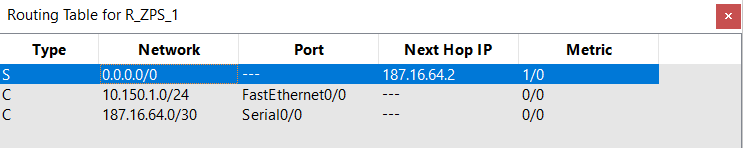
После получения результатов (они показаны выше) я пришел к выводу, что эхо-запросы прошли с полной потерей всех пакетов. Предположительно, это случилось потому, что мы еще не настроили маршрутизацию между подсетями маршрутизаторов и узлов. Другими словами, маршрутизатор с именем ISP пока не обладает информацией о том, куда отправить пакеты с данными.

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

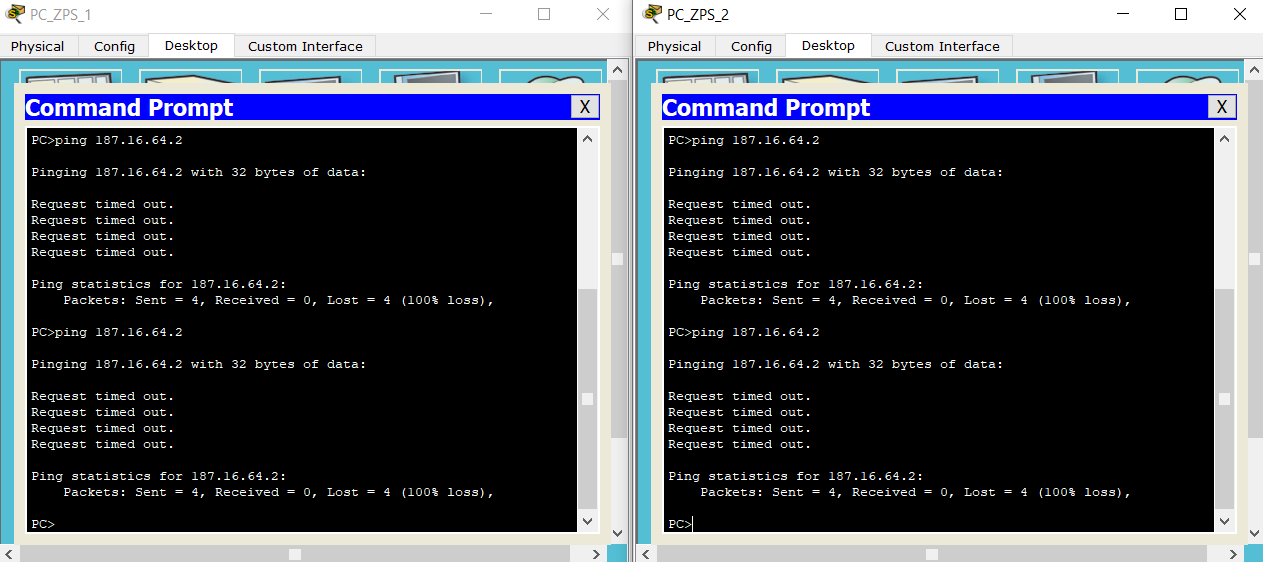
С маршрутизатора, который используется в качестве шлюза по умолчанию, я создал статический маршрут к маршрутизатору поставщика услуг Интернета в сети 0.0.0.0 0.0.0.0 с помощью команды **ip route**:



Проверил маршрут по умолчанию, который мы только что настроили, в таблице маршрутизации маршрутизатора Gateway и убедился в том, что данный статический маршрут там действительно появился:



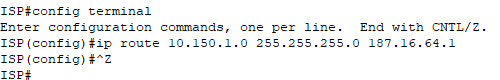
Вновь попробовал отправить эхо-запросы от наших узлов к адресу второго маршрутизатора ISP:



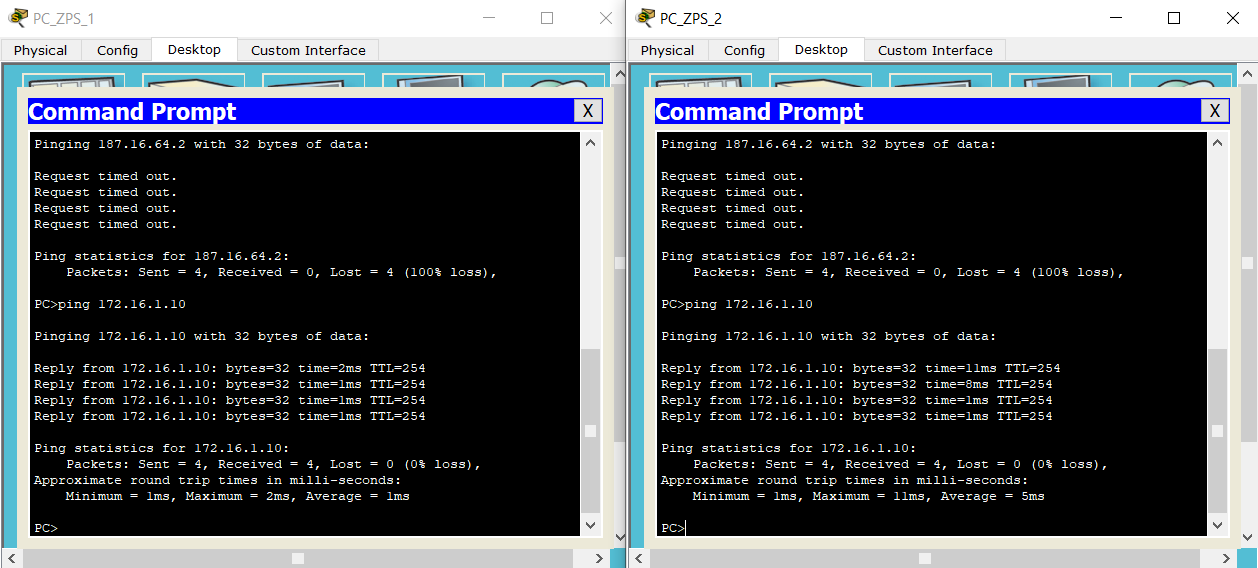
Видно, что маршрутизатор ISP пока не обладает информацией об узлах.

### 4.7. Шаг 7. Создание статического маршрута

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



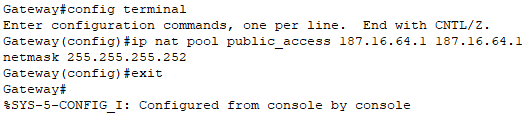
Попробовал отправить эхо-запросы с узлов на адрес интерфейс Loopback 2-ого маршрутизатора ISP:



Можно наблюдать, что эхо-запросы успешно выполнены, т.к. нету потерь пакетов.

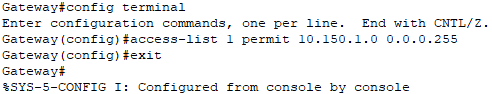
### 4.8. Шаг 8. Определение пула используемых публичных IP-адресов

Определил пул используемых публичных IP-адресов с помощью команды **ip nat pool**:



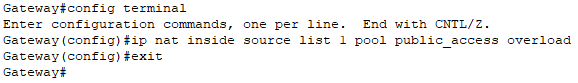
### 4.9. Шаг 9. Определение списка доступа, соответствующего внутренним частным IP-адресам

Определил список доступа, который соответствует внутренним частным IP-адресам, с помощью команды **access-list:**

****

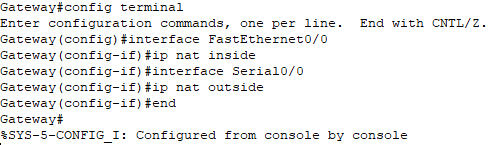
### 4.10. Шаг 10. Определение NAT из списка внутренних адресов в пул внешних адресов

Определил NAT из списка внутренних адресов в пул внешних адресов командой **ip nat inside source**:



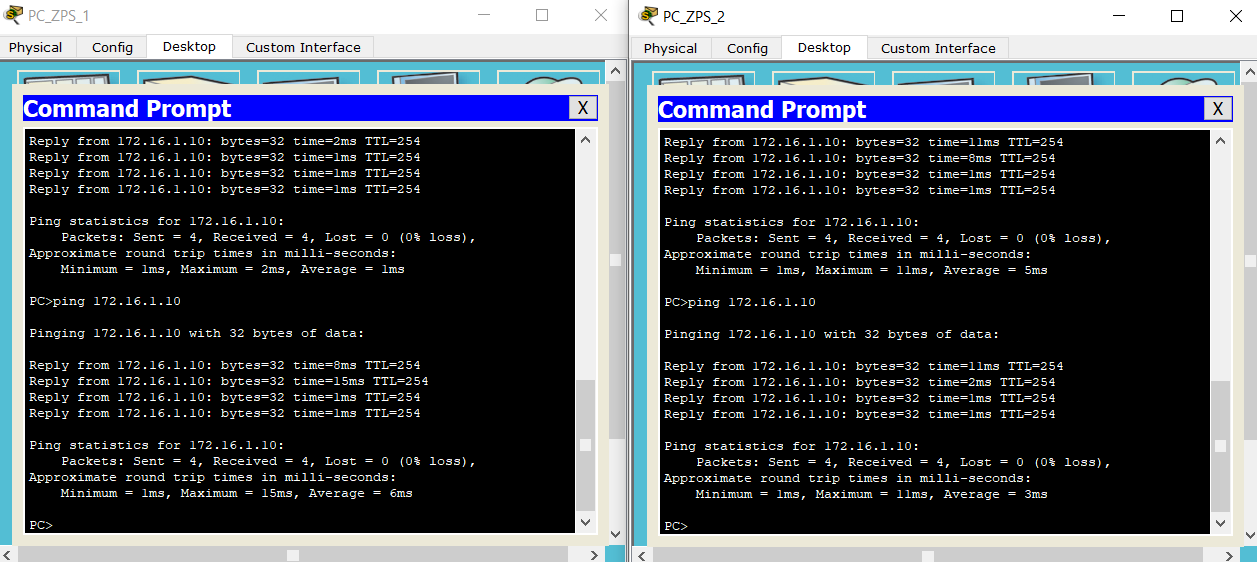
### 4.11. Шаг 11. Назначение интерфейсов

С помощью команд **ip nat inside** и **ip nat outside** определил активные интерфейсы маршрутизатора в качестве внутреннего/внешнего интерфейса в отношении к NAT:



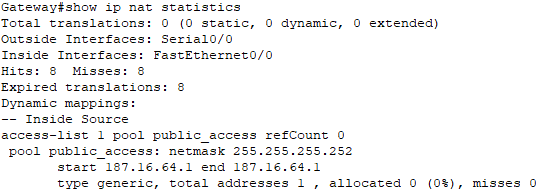
### 4.12. Шаг 12. Генерация трафика с маршрутизатора Gateway к маршрутизатору ISP

Отправил с обоих узлов по одному эхо-запросу на IP-адрес 172.16.1.10 для генерации трафика:



### 4.13. Шаг 13. Проверка работоспособности NAT

Отобразил статистику NAPT, введя в приглашение привилегированного режима EXEC маршрутизатора Gateway команду **show ip nat statistics**:



Тщательно проанализировав полученные данные, ответил на следующие вопросы:

1) Сколько активных преобразований выполнено?

Всего было выполнено 8 активных преобразований.

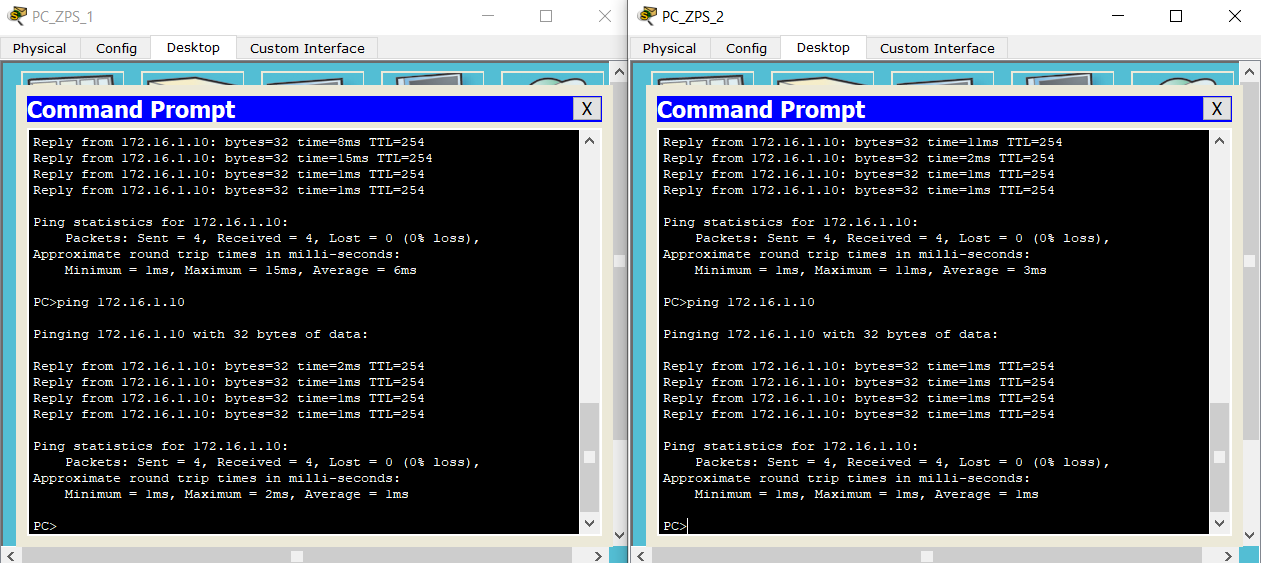
2) Сколько адресов имеется в пуле?

В пуле адресов мы можем наблюдать только один адрес.

3) Сколько адресов уже выделено?

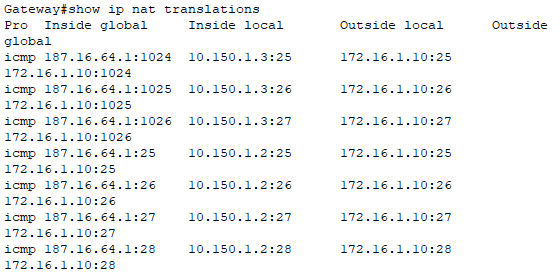
Также можно заметить, что выделен лишь один адрес.

Вновь отправил эхо-запросы с обоих хостов по адресу 172.16.1.10:



Эхо-запросы вновь прошли успешно, без потери пакетов.

Сразу после совершения эхо-запросов отобразил преобразование NAT на маршрутизаторе Gateway с помощью команды **show ip nat translations**:



## 5. В отчет включить: скриншоты с комментариями по каждому шагу работы, ответы на вопросы и при необходимости ваши выводы на полученный результат.

В отчёт включены скриншоты с комментариями по каждому шагу работы, а также ответы на вопросы с выводами на полученный результат.

## 6. Согласно вашему варианту задания в отчет поместите развернутый ответ на теоретический вопрос.

Развёрнутый ответ на теоретический вопрос будет описан ниже.

### Теоретический мини коллоквиум

Согласно варианту задания ответить на теоретический вопрос (можно ***письменно, главное чтобы текст был читабельным) и вставить*** в отчет (Своего рода реферат).

Так как у меня 32-ой вариант, а тем в списке всего 29, то я взял тему с номером остатка 29 по модулю 32, а именно я взял 3-ю тему, потому что 32 (mod 29) = 3.

**3. Технология Ethernet с общей шиной**

Ethernet – это семейство компьютерных сетевых технологий, которые обычно используются в локальных сетях (они же LAN), столичных сетях (они же Man) и широкополосных сетях (их называют WAN). Как я узнал из электронных источников, эта технология была коммерчески представлена в 1980 году и впервые стандартизирован в 1983 году как IEEE 802.3. С тех пор Ethernet сохранил большую часть обратной совместимости и был усовершенствован для поддержки более высоких скоростей передачи битов, а также большего числа узлов и более длинных расстояний соединения. Со временем Ethernet в значительной степени вытеснил конкурирующие технологии проводной локальной сети. Среди них можно выделить такие технологии, как как: Token Ring, FDDI, ARCNET и др.

Оригинальный 10BASE5 Ethernet использует коаксиальный кабель в качестве общей среды, в то время как более новые варианты Ethernet используют витую пару и волоконно-оптические линии связи в сочетании с коммутаторами. Поразительно, но за свою историю скорость передачи данных Ethernet была увеличена с первоначальных 2,94 мегабит в секунду (Мбит/с) до последних 400 гигабит в секунду (Гбит/с). К тому же, стандарты Ethernet включают в себя несколько вариантов подключения и сигнализации физического уровня OSI, используемого с Ethernet.

Системы, взаимодействующие через Ethernet, разделяют поток данных на более короткие фрагменты, которые также называются кадрами. Каждый такой кадр содержит адреса источника и назначения, а также данные проверки ошибок, так что поврежденные кадры могут быть обнаружены и отброшены. Зачастую протоколы более высокого уровня запускают повторную передачу потерянных кадров. В соответствии с моделью OSI Ethernet предоставляет услуги вплоть до уровня канала передачи данных. Я также нашел информацию и том, что 48-битный MAC-адрес был принят другими сетевыми стандартами IEEE 802, включая IEEE 802.11 Wi-Fi, а также FDDI. В добавок, значения EtherType также используются в заголовках протокола доступа к подсети (SNAP).

В заключение можно сказать, что технология Ethernet широко используется в домах и промышленности, а также хорошо взаимодействует с Wi-Fi. Интернет-протокол обычно передается черезEthernet, и поэтому он считается одной из ключевых технологий, составляющих интернет. Даже я сам, у себя дома, использую эту технология для поддержания своей сети.