

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет прикладной математики и информатики

Благодарный Артём Андреевич
(студент 3 курса 3 группы)

Краткий отчет
по лабораторной работе №12
Настройка и проверка NAPT
(вариант №8)

Минск 2025

Содержание

Исходные данные из варианта задания №8	3
Шаг 1. Подсоединение устройств.....	3
Шаг 2. Настройка основной конфигурации маршрутизатора 2.....	4
Шаг 3. Настройка маршрутизатора, используемого в качестве шлюза.....	5
Шаг 4. Настройка правильного IP-адреса, маски подсети и шлюза по умолчанию для узлов.	6
Шаг 5. Проверка работоспособности сети.	8
Шаг 6. Создание маршрута по умолчанию.....	9
Шаг 7. Создание статического маршрута.....	11
Шаг 8. Определение пула используемых публичных IP-адресов.	11
Шаг 9. Определение списка доступа, соответствующего внутренним частным IP-адресам.	12
Шаг 10. Определение NAT из списка внутренних адресов в пул внешних адресов	12
Шаг 11. Назначение интерфейсов.....	13
Шаг 12. Генерация трафика с маршрутизатора Gateway к маршрутизатору ISP	13
Шаг 13. Проверьте работоспособность NAT	14
Шаг 14. Краткий реферат по NAT и NAT	15

Исходные данные для варианта задания

Заполнить строку таблицы ниже с вашим вариантом задания

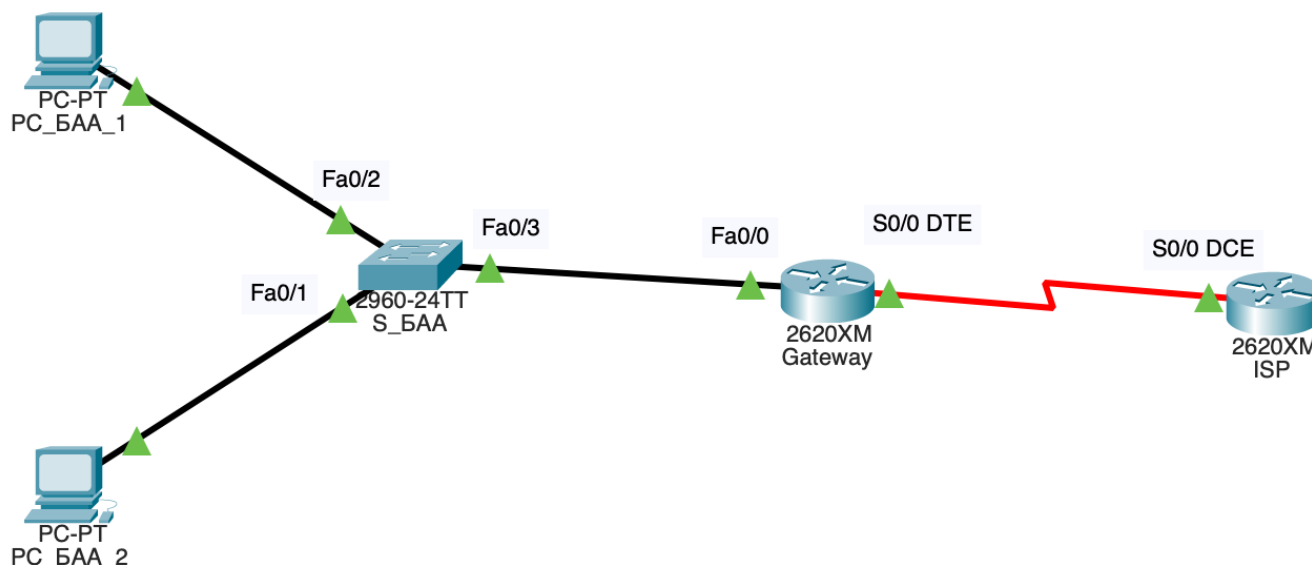
Вариант	Адреса для узлов	Маршрутизатор 1	Маршрутизатор 2	IP-адрес Loopback 1
8	192.168.30.0/24	169.166.0.1/30	169.166.0.2/30	172.16.1.8/32

Заполнить таблицу ниже.

Устройство	Имя узла	Маска подсети порта FastEthernet0/0	Тип интерфейса	IP-адрес порта Serial 0/0	IP-адрес Loopback 1
Маршрутизатор 1	Cateway	255.255.255.0	DTE	169.166.0.1	
Маршрутизатор 2	ISP		DCE	169.166.0.2	172.16.1.8/32
Коммутатор 1	Switch 1				

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

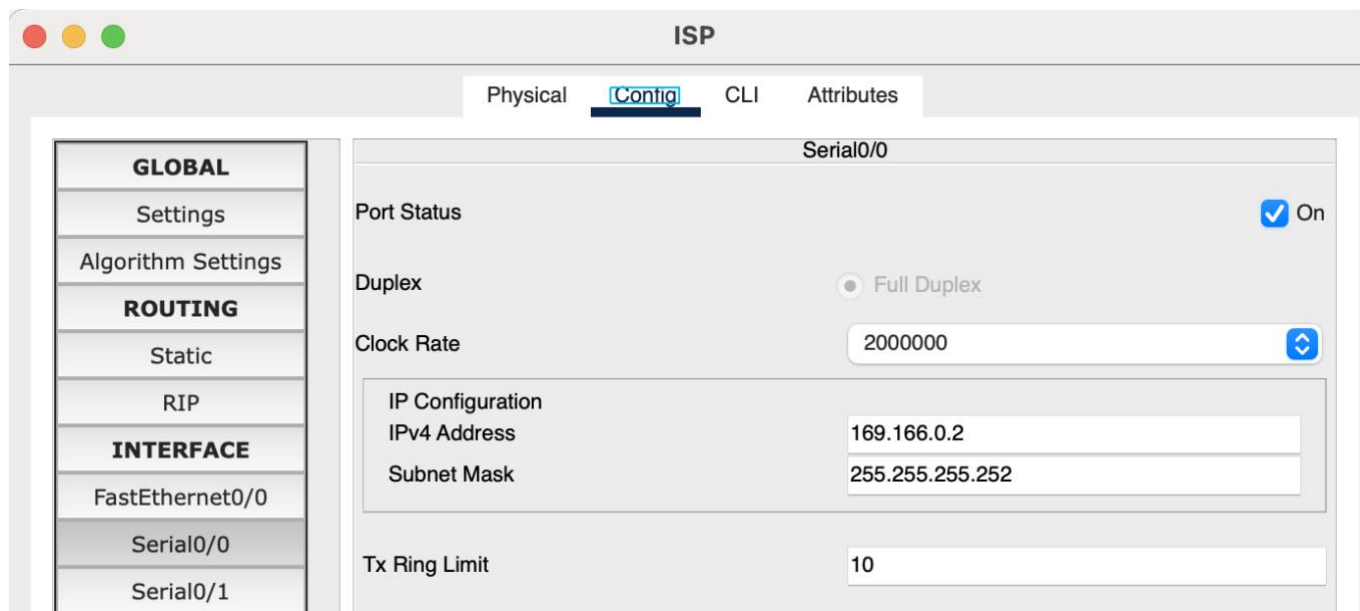


Шаг 2. Настройка основной конфигурации маршрутизатора 2

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

Вставить скриншот процесса конфигурирования

Настройка интерфейса Serial0/0:



Настройка интерфейса Loopback 1 и сохранение конфигурации:

```
ISP>enable
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#interface loopback 1

ISP(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

ISP(config-if)#ip address 172.16.1.8 255.255.255.255
ISP(config-if)#exit
ISP(config)#exit
ISP#
%SYS-5-CONFIG_I: Configured from console by console

ISP#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#
```

Шаг 3. Настройка маршрутизатора, используемого в качестве шлюза

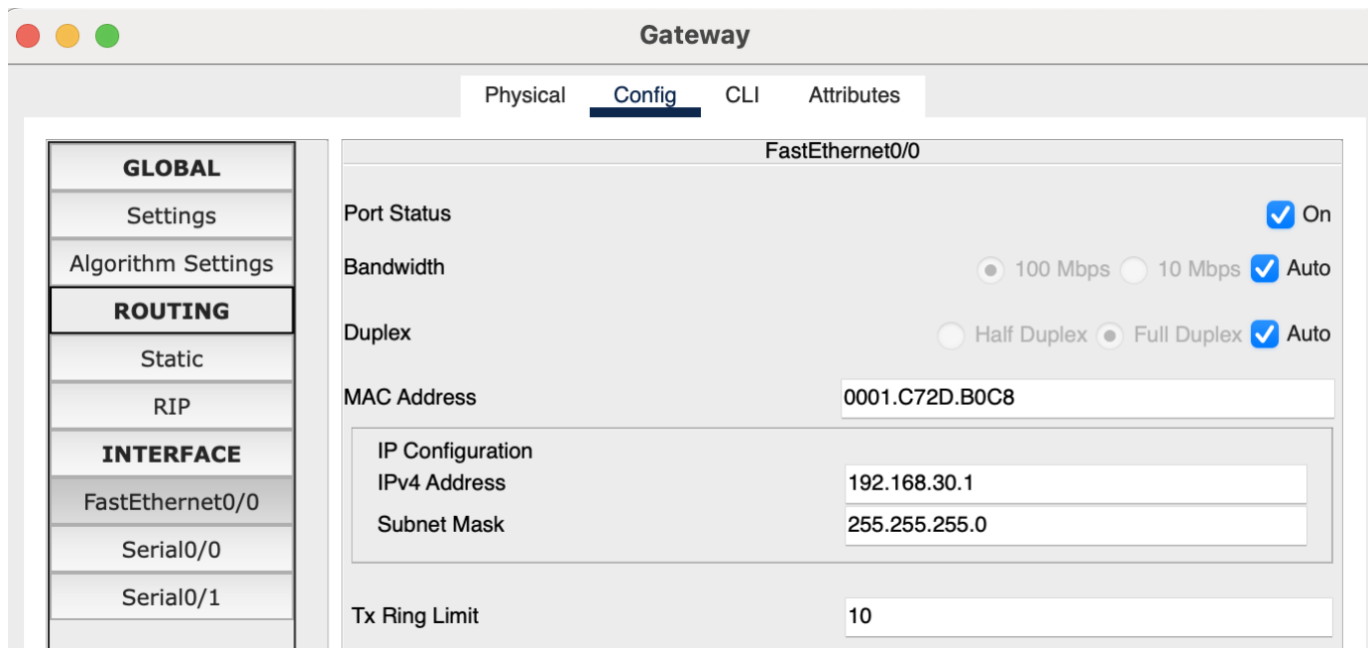
Задайте в настройках основной конфигурации маршрутизатора 1 имя узла (Gateway), задайте IP-адреса для интерфейсов. Сохраните конфигурацию.

Вставить скриншот процесса настройки

Настройка интерфейса Serial0/0:

The screenshot shows the 'Gateway' configuration window with the 'Config' tab selected. On the left, a sidebar lists configuration categories: GLOBAL (Settings, Algorithm Settings), ROUTING (Static, RIP), and INTERFACE (FastEthernet0/0, Serial0/0, Serial0/1). The 'Serial0/0' interface is selected. The main configuration area for Serial0/0 includes: Port Status (checked, On), Duplex (Full Duplex selected), Clock Rate (1200), IP Configuration (IPv4 Address: 169.166.0.1, Subnet Mask: 255.255.255.252), and Tx Ring Limit (10).

Настройка интерфейса FastEthernet0/0:



Сохранение конфигурации:

```
Gateway>enable
Gateway#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Gateway#
```

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

Присвойте каждому узлу соответствующий IP-адрес, маску подсети и шлюз по умолчанию. Оба узла должны получить внутренние частные IP-адреса в сети 10.10.10.0/24 (напоимную, **вам необходимо задать адреса согласно вашему варианту задания**). Шлюзом по умолчанию должен быть IP-адрес интерфейса FastEthernet маршрутизатора с именем Gateway.

Вставить скриншот процесса настройки

Вставить схему сети с подписями как ранее.

Соблюдайте правила именования устройств и их интерфейсов

PC_БАА_1

PhysicalConfigDesktopProgrammingAttributes

IP Configuration

InterfaceFastEthernet0

IP Configuration

DHCP

Static

IPv4 Address

192.168.30.2

Subnet Mask

255.255.255.0

Default Gateway

192.168.30.1

DNS Server

0.0.0.0

PC_БАА_2

PhysicalConfigDesktopProgrammingAttributes

IP Configuration

InterfaceFastEthernet0

IP Configuration

DHCP

Static

IPv4 Address

192.168.30.3

Subnet Mask

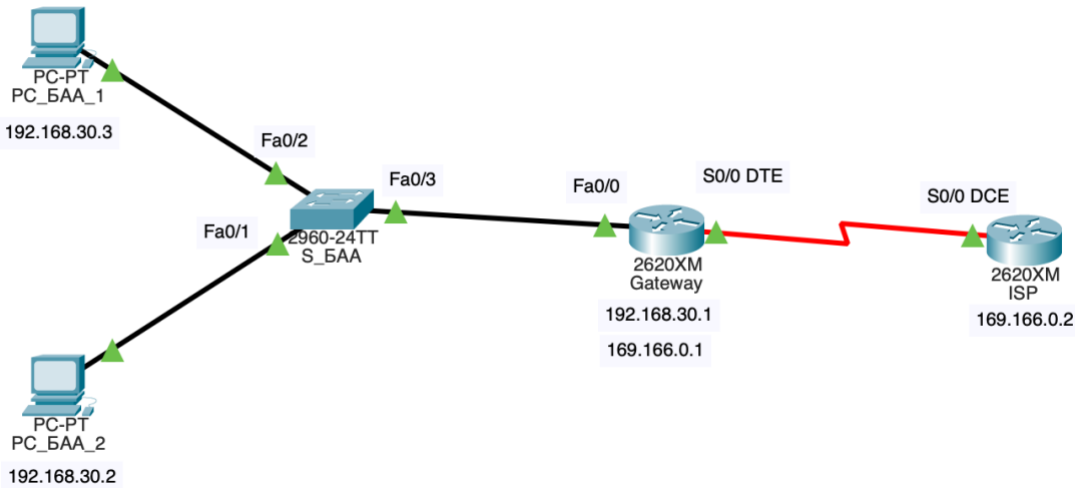
255.255.255.0

Default Gateway

192.168.30.1

DNS Server

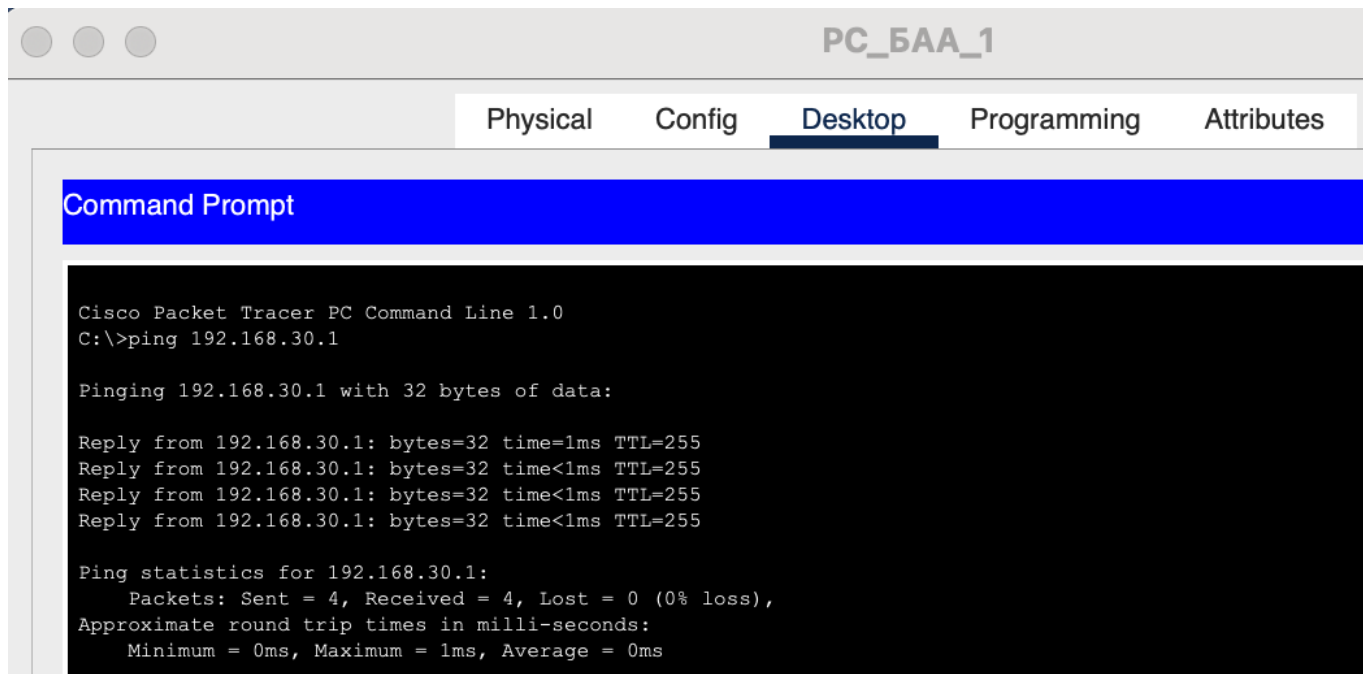
0.0.0.0



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.

а). Успешно ли выполнен эхо-запрос с узла 1? _____да_____



The screenshot shows a Cisco Packet Tracer PC window titled "PC_BAA_1". The "Desktop" tab is selected, displaying a "Command Prompt" window. The text in the command prompt is as follows:

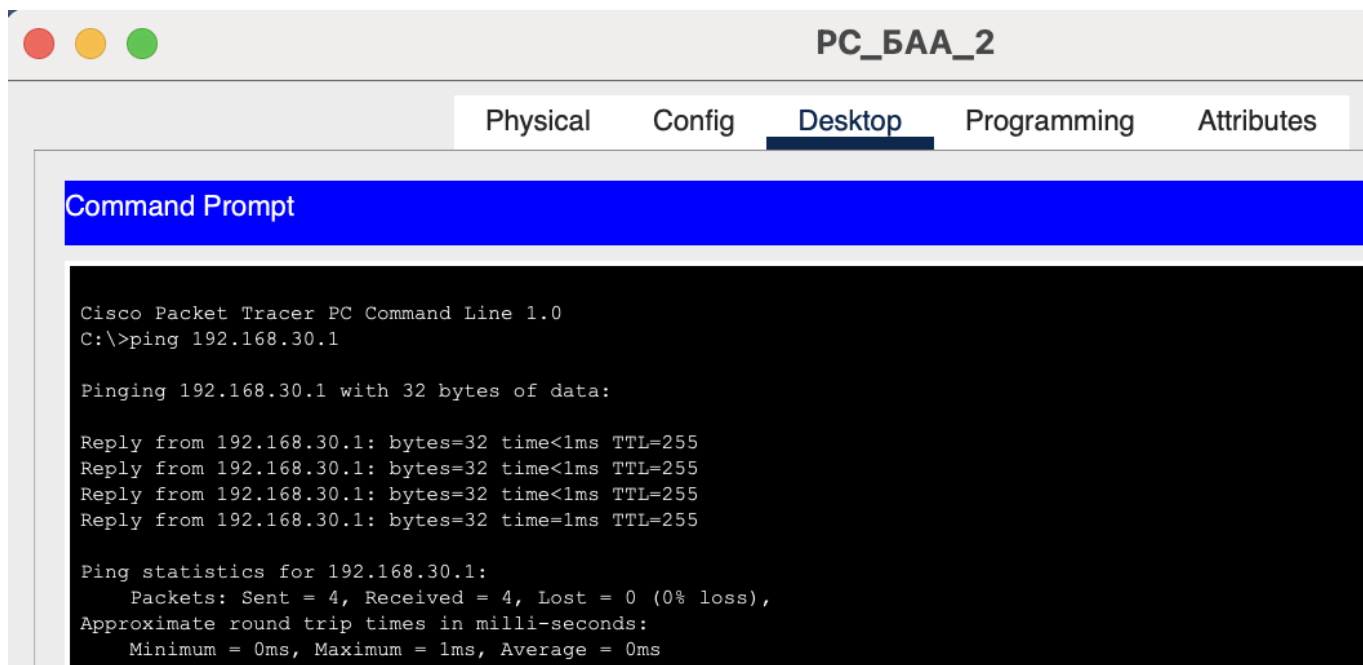
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time=1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

б) Успешно ли выполнен эхо-запрос с узла 2? _____да_____



The screenshot shows a Cisco Packet Tracer PC window titled "PC_BAA_2". The "Desktop" tab is selected, displaying a "Command Prompt" window. The text in the command prompt is as follows:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

2. Если ответы на оба вопроса отрицательны, выполните поиск и устранение ошибок в конфигурации маршрутизатора и узлов. Тестируйте соединение до тех пор, пока эхо-запросы не будут успешными.

3. Отправьте эхо-запросы на IP-адрес маршрутизатора ISP. Какой получили результат. Поясните свой ответ.

Вставить скриншоты проверки

Ответить на вопросы,

Пояснить ответы

```
C:\>ping 169.162.0.2

Pinging 169.162.0.2 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 169.162.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

```
C:\>ping 169.162.0.2

Pinging 169.162.0.2 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Request timed out.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 169.162.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

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, используемом в качестве шлюза по умолчанию.

Как вы понимаете выражение шлюз последней надежды?

Вставить скриншот команды IP route

Шлюз последней надежды я понимаю как маршрут по умолчанию, к которому отправляется весь трафик, если не найдено точного маршрута в таблице маршрутизации.

```
Gateway>enable
Gateway#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#ip route 0.0.0.0 0.0.0.0 169.166.0.2
Gateway(config)#exit
Gateway#
```

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

Вывести скриншот ТМ.

Ответить на заданный вопрос

```
Gateway>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 169.166.0.2 to network 0.0.0.0

    169.166.0.0/30 is subnetted, 1 subnets
C       169.166.0.0 is directly connected, Serial0/0
C       192.168.30.0/24 is directly connected, FastEthernet0/0
S*     0.0.0.0/0 [1/0] via 169.166.0.2
```

Да, находится (S*)

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

Скриншот эхо-запроса и комментарий

```
C:\>ping 169.162.0.2

Pinging 169.162.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 169.162.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Нет, запрос был выполнен неудачно.

Шаг 7. Создание статического маршрута

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

Скриншот команды IP route

```
ISP(config)#ip route 192.168.30.0 255.255.255.0 169.166.0.1
ISP(config)#
```

- Отправьте эхо-запрос с узла 1 на адрес интерфейса loopback маршрутизатора ISP. Успешно ли выполнен эхо-запрос?
- Если эхо-запрос не выполнен, проверьте правильность конфигурации маршрутизатора и узла и повторите тестирование связи.

Вывести скриншот ТМ.

Скриншоты эхо-запросов.

Ответить на заданные вопросы

```
C:\>ping 172.16.1.8

Pinging 172.16.1.8 with 32 bytes of data:

Reply from 172.16.1.8: bytes=32 time=2ms TTL=254
Reply from 172.16.1.8: bytes=32 time=2ms TTL=254
Reply from 172.16.1.8: bytes=32 time=4ms TTL=254
Reply from 172.16.1.8: bytes=32 time=4ms TTL=254

Ping statistics for 172.16.1.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 3ms
```

Да, успешно

Шаг 8. Определение пула используемых публичных IP-адресов

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

Скриншот определения пула адресов

Что вы понимаете под термином – публичные адреса,
частные адреса.

Публичные IP-адреса — это уникальные адреса, которые используются для подключения устройств к интернету. Они доступны извне и назначаются провайдерами или организациям, чтобы, например, сайты и серверы были видимы в интернете.

Частные IP-адреса используются внутри локальных сетей (домашних, офисных) и не видны в интернете. Для выхода таких устройств в интернет применяется технология NAT, которая заменяет частный адрес на публичный.

```
Gateway>enable
Gateway#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#ip nat pool pub_access 169.166.0.2 169.166.0.2 netmask 255.255.255.252
Gateway(config)#
```

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

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

Скриншот определения списка доступа.

Прокомментируйте термин “список доступа”.

Список доступа — это набор правил на маршрутизаторе или коммутаторе, который разрешает или запрещает трафик по определённым IP-адресам, протоколам или портам. Он используется для фильтрации пакетов, настройки NAT и обеспечения безопасности сети.

```
Gateway(config)#access-list 1 permit 192.168.30.0 0.0.0.255
Gateway(config)#
```

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

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

Скриншот команды `ip nat inside source`

Прокомментируйте. С какой целью вы выполняете шаг 10

Шаг 10 выполняется для того, чтобы сопоставить внутренние (частные) IP-адреса с внешними (публичными) адресами через NAT.

```
Gateway(config)#ip nat inside source list 1 pool pub_access overload
Gateway(config)#
```

Шаг 11. Назначение интерфейсов

Активные интерфейсы маршрутизатора следует определить в качестве внутреннего или внешнего интерфейса в отношении к NAT. Для этого используйте команду *ip nat inside* или *ip nat outside*.

Скриншоты назначения интерфейсов.

В данном контексте, что такое внутренние и внешние интерфейсы ?

Внутренний интерфейс (inside) — это интерфейс маршрутизатора, подключённый к локальной сети с частными IP-адресами.

Внешний интерфейс (outside) — это интерфейс маршрутизатора, подключённый к внешней сети или интернету, через который происходит выход в глобальную сеть.

```
Gateway(config)#interface FastEthernet0/0
Gateway(config-if)#ip nat inside
Gateway(config-if)#interface Serial0/0
Gateway(config-if)#ip nat outside
Gateway(config-if)#
Gateway(config-if)#
```

Шаг 12. Генерация трафика с маршрутизатора Gateway к маршрутизатору ISP

Отправьте эхо-запросы с узлов 1 и 2 на адрес 172.16.1.1.

Представить скриншоты

```
C:\>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Эхо-запросы с узлов 1 и 2 на адрес 172.16.1.8

```
C:\>ping 172.16.1.8

Pinging 172.16.1.8 with 32 bytes of data:

Reply from 172.16.1.8: bytes=32 time=2ms TTL=254
Reply from 172.16.1.8: bytes=32 time=1ms TTL=254
Reply from 172.16.1.8: bytes=32 time=1ms TTL=254
Reply from 172.16.1.8: bytes=32 time=1ms TTL=254

Ping statistics for 172.16.1.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

```
C:\>ping 172.16.1.8

Pinging 172.16.1.8 with 32 bytes of data:

Reply from 172.16.1.8: bytes=32 time=2ms TTL=254
Reply from 172.16.1.8: bytes=32 time=1ms TTL=254
Reply from 172.16.1.8: bytes=32 time=1ms TTL=254
Reply from 172.16.1.8: bytes=32 time=1ms TTL=254

Ping statistics for 172.16.1.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Шаг 13. Проверьте работоспособность NAPT

Для отображения статистики NAPT 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? 16
2. Сколько адресов имеется в пуле? 1
3. Сколько адресов уже выделено? 0

Если эхо-запрос выполнен успешно, отобразите преобразование NAT на маршрутизаторе Gateway с помощью команды *show ip nat translations*.

Надо подтвердить выполнение шага 13.

Дать ответы на все вопросы

```
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0
Inside Interfaces: FastEthernet0/0
Hits: 12 Misses: 20
Expired translations: 16
Dynamic mappings:
-- Inside Source
access-list 1 pool pub_access refCount 0
 pool pub_access: netmask 255.255.255.252
   start 169.166.0.2 end 169.166.0.2
   type generic, total addresses 1 , allocated 0 (0%), misses 0
```

```
Gateway#show ip nat translations
Gateway#
```

Шаг 14. Краткий реферат по NAT и NAPT

Вставить краткий реферат по NAT и NAPT

Network Address Translation (NAT) — это метод, используемый для преобразования частных IP-адресов в публичные и наоборот. Этот процесс осуществляется на маршрутизаторе, который действует как посредник между локальной сетью и интернетом. Основной задачей NAT является скрывание внутренней сети от внешнего мира, что улучшает безопасность, а также позволяет множеству устройств внутри локальной сети использовать один публичный IP-адрес для выхода в интернет.

Основные типы NAT:

1. **Static NAT:** Преобразование одного частного IP-адреса в один публичный. Этот тип NAT обычно используется для серверов, которым нужно иметь постоянный публичный адрес.
2. **Dynamic NAT:** Преобразует частные IP-адреса в публичные из заранее определённого пула. Этот метод используется для автоматического присваивания публичных адресов устройства при выходе в интернет.
3. **PAT (Port Address Translation):** В рамках этого метода несколько устройств внутри сети могут использовать **один публичный IP-адрес**, но с разными номерами портов. Это называется трансляцией адресов с учётом портов и используется для экономии публичных IP-адресов.

Network Address Port Translation (NAPT) — это расширение технологии NAT, которое использует **один публичный IP-адрес** для трансляции множества внутренних IP-адресов, различая их не только по IP, но и по номерам портов. NAPT позволяет создавать уникальные трансляции для каждого соединения с помощью различных портов на одном публичном адресе.

Пример:

Когда несколько пользователей внутри сети (например, с адресами 192.168.1.10, 192.168.1.11 и т.д.) выходят в интернет, маршрутизатор с использованием NAPT преобразует их IP-адреса в один публичный IP, но для каждого подключения будет использовать свой уникальный номер порта.

Преимущества NAT и NAPT:

- **Экономия IP-адресов:** NAT и NAPT позволяют использовать один или несколько публичных IP-адресов для множества устройств внутри частной сети.
- **Увеличение безопасности:** Частные IP-адреса скрыты от внешнего мира, что затрудняет прямые атаки на устройства в локальной сети.
- **Гибкость:** NAT и NAPT позволяют легко управлять подключениями в сети, предоставляя возможность использовать разные схемы преобразования адресов.

Недостатки:

- **Задержки и сложность:** NAT и NAPT могут вводить дополнительные задержки в обработке трафика из-за необходимости преобразования адресов.
- **Проблемы с некоторыми приложениями:** Некоторые протоколы и приложения (например, VoIP или P2P) могут испытывать трудности с работой через NAT, так как они могут не поддерживать трансляцию портов корректно.

Заключение: NAT и NAPT играют ключевую роль в современном управлении сетями, обеспечивая экономию адресного пространства и улучшение безопасности, но также могут создавать определённые сложности в случае работы с определёнными приложениями.