Министерство образования Республики Беларусь
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет прикладной математики и информатики

Бинцаровский Леонид Петрович

НАСТРОЙКА И ПРОВЕРКА NAPT

Отчет по лабораторной работе № 12,
(“Компьютерные сети”)
студента 3-го курса 3-ей группы

Преподаватель

Рафеенко Е.Д./
Рябый В.В.

2024

Содержание

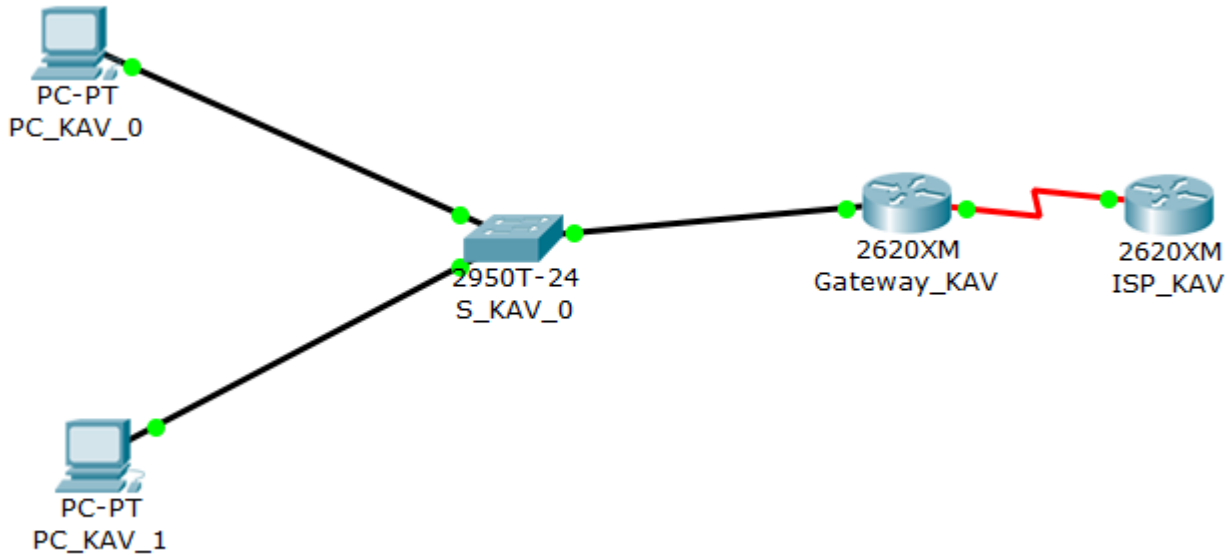
Исходные данные для варианта задания

Вариант	Адреса для узлов	Маршрутизатор 1	Маршрутизатор 2	IP-адрес Loopback 1
6	10.100.1.0/24	179.131.122.1/30	179.131.122.2/30	172.16.1.6/32

Устройство	**Имя узла**	**Маска подсети порта FastEthenet0/0**	**Тип интерфейса**	**IP-адрес порта Serial 0/0**	**IP-адрес Loopback 1**
Маршрутизатор 1	Cateway	10.100.1.1/24	DTE	179.131.122.1/30	
Маршрутизатор 2	ISP		DCE	179.131.122.2/30	172.16.1.6/32
Коммутатор 1	Switch 1				

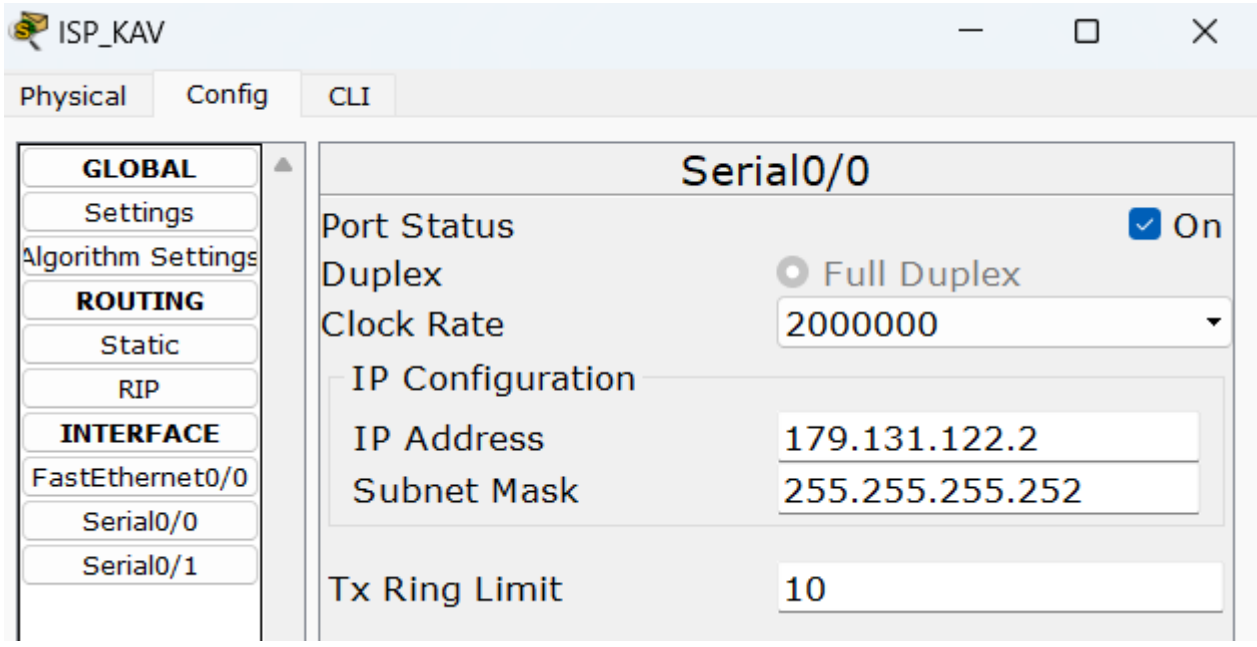
Шаг 1. Подсоединение устройств

- **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

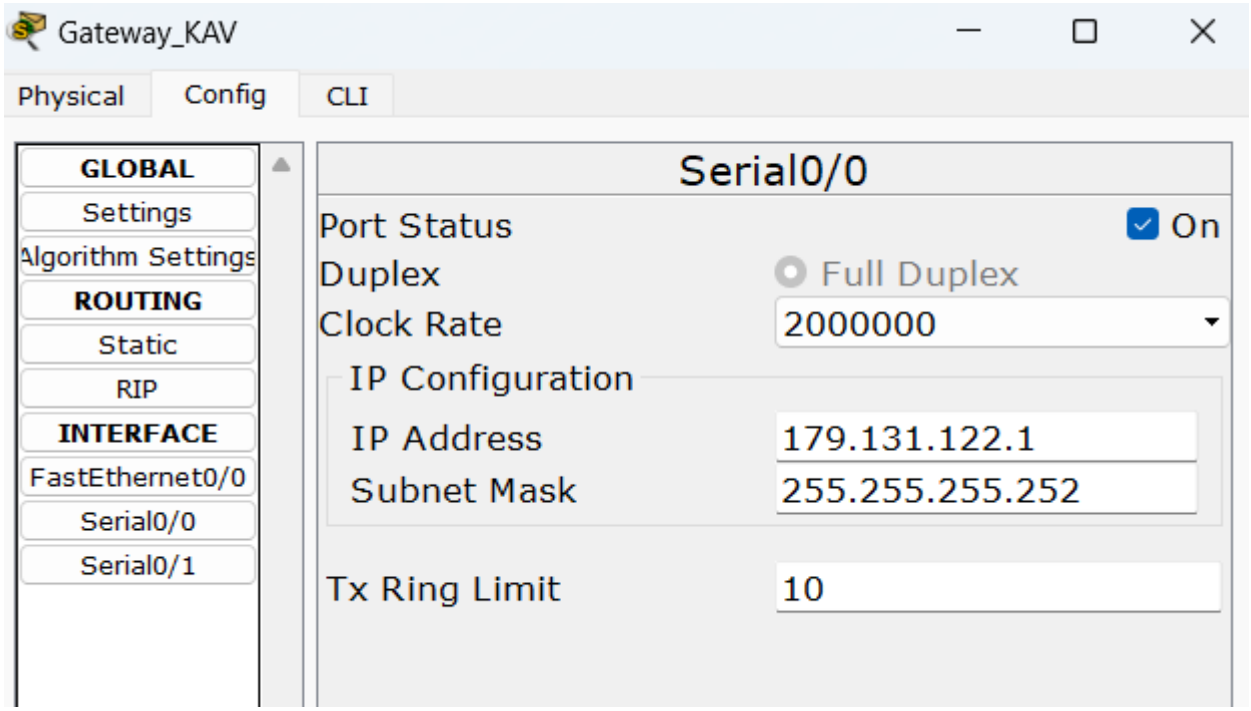
Задайте в настройках конфигурации маршрутизатора 2 (ISP) имя узла, задайте IP-адреса для интерфейсов согласно вашему варианту задания. Сохраните конфигурацию.

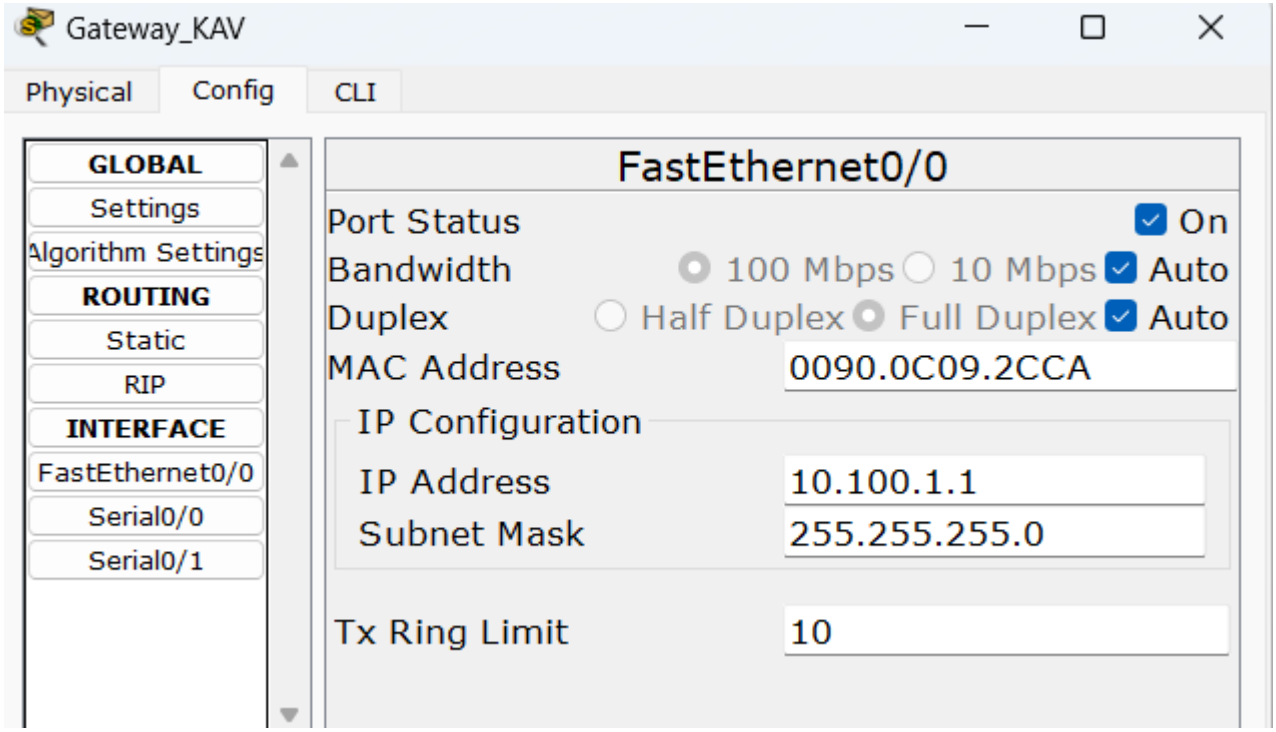


```
ISP_KAV(config)#interface loopback 1

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

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

ISP_KAV(config-if)#ip address 172.16.1.6 255.255.255.255
ISP_KAV(config-if)#^Z
ISP_KAV#
%SYS-5-CONFIG_I: Configured from console by console

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

Шаг 3. Настройка маршрутизатора, используемого в качестве шлюза

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

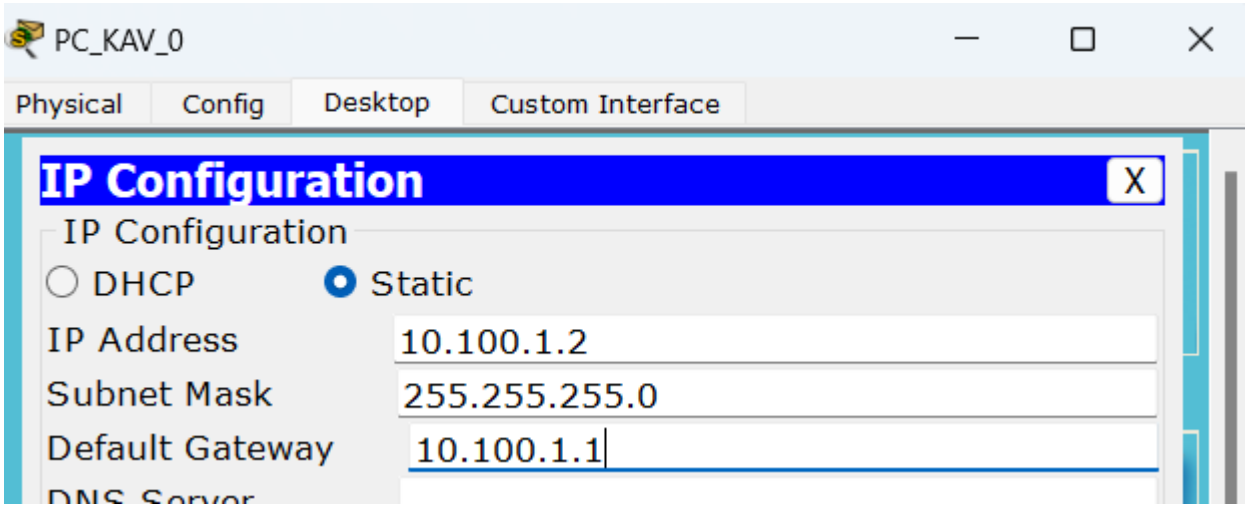


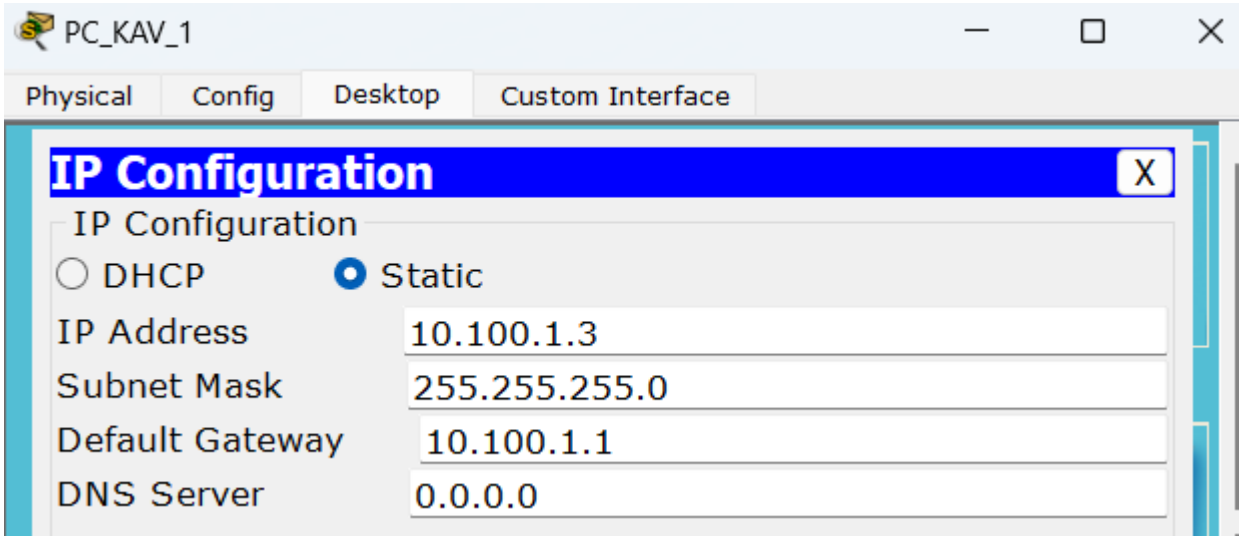


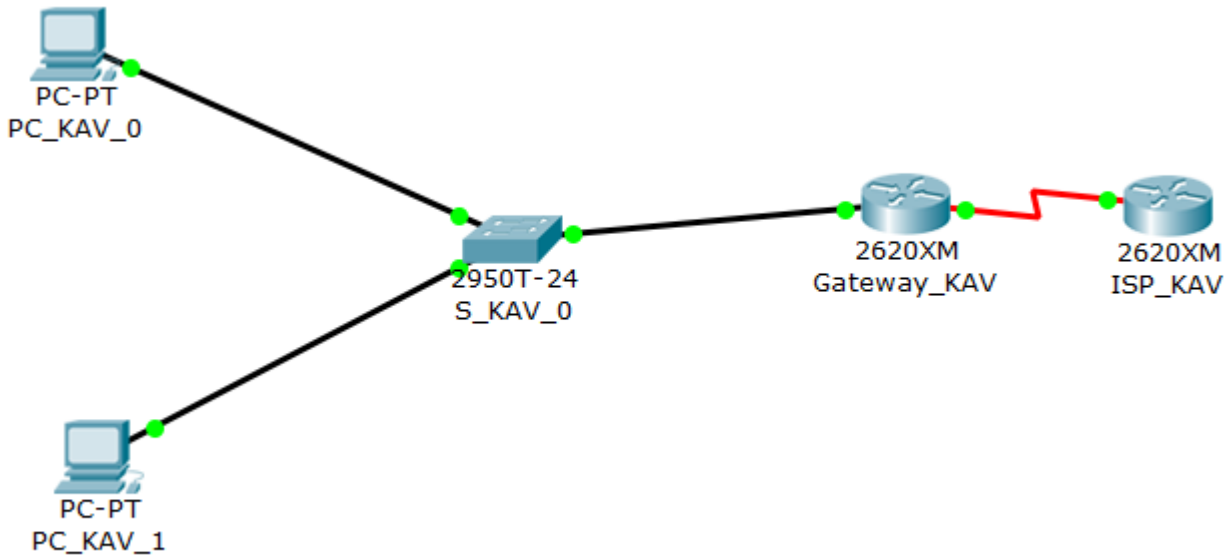

```
Gateway_KAV#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

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 (напомнаю, вам необходимо задать адреса согласно вашему варианту задания). Шлюзом по умолчанию должен быть IP-адрес интерфейса FastEthernet маршрутизатора с именем Gateway.







Что означают термины внутренние IP-адреса, внешние IP-адреса?

Внутренний IP-адрес – это уникальный адрес, который используется для идентификации устройства в локальной сети, например, в вашей домашней сети или офисной сети. Такие адреса не маршрутизируются в интернете, к ним нельзя напрямую обратиться извне.

Внешний IP-адрес – это уникальный адрес, который присваивается вашему интернет-провайдеру и используется для идентификации вашей сети в глобальной сети, то есть в интернете.

Шаг 5. Проверка работоспособности сети.

1. С присоединенных узлов отправьте эхо-запрос на интерфейс FastEthernet маршрутизатора, используемого в качестве шлюза по умолчанию.

```
PC>ping 10.100.1.1

Pinging 10.100.1.1 with 32 bytes of data:

Reply from 10.100.1.1: bytes=32 time=2ms TTL=255
Reply from 10.100.1.1: bytes=32 time=0ms TTL=255
Reply from 10.100.1.1: bytes=32 time=0ms TTL=255
Reply from 10.100.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.100.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

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

```
PC>ping 10.100.1.1

Pinging 10.100.1.1 with 32 bytes of data:

Reply from 10.100.1.1: bytes=32 time=0ms TTL=255
Reply from 10.100.1.1: bytes=32 time=0ms TTL=255
Reply from 10.100.1.1: bytes=32 time=0ms TTL=255
Reply from 10.100.1.1: bytes=32 time=0ms TTL=255

Ping statistics for 10.100.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

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

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 с хостов на IP-адрес маршрутизатора ISP.**

Какой получили результат.

```
PC>ping 179.131.122.2

Pinging 179.131.122.2 with 32 bytes of data:

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

Ping statistics for 179.131.122.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PC>ping 179.131.122.2

Pinging 179.131.122.2 with 32 bytes of data:

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

Ping statistics for 179.131.122.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Запрос не прошел, потому что 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.**

```
Gateway_KAV>enable
Gateway_KAV#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Gateway_KAV(config)#ip route 0.0.0.0 0.0.0.0 179.131.122.2
```

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

```
Gateway_KAV#
%SYS-5-CONFIG_I: Configured from console by console

Gateway_KAV#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 179.131.122.2 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.100.1.0 is directly connected, FastEthernet0/0
     179.131.0.0/30 is subnetted, 1 subnets
C       179.131.122.0 is directly connected, Serial0/0
S*   0.0.0.0/0 [1/0] via 179.131.122.2
Gateway KAV#
```

Статический маршрут находится в ТМ (S*)

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

```
PC>ping 179.131.122.2

Pinging 179.131.122.2 with 32 bytes of data:

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

Ping statistics for 179.131.122.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Запрос не прошел.

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.

```
ISP_KAV>enable
ISP_KAV#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
ISP_KAV(config)#ip route 10.100.1.0 255.255.255.0 179.131.122.1
```

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

```
PC>ping 179.131.122.2

Pinging 179.131.122.2 with 32 bytes of data:

Reply from 179.131.122.2: bytes=32 time=2ms TTL=254
Reply from 179.131.122.2: bytes=32 time=1ms TTL=254
Reply from 179.131.122.2: bytes=32 time=1ms TTL=254
Reply from 179.131.122.2: bytes=32 time=1ms TTL=254

Ping statistics for 179.131.122.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Запрос прошел успешно

- **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.

```
Gateway_KAV>enable
Gateway_KAV#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Gateway_KAV(config)#ip nat pool public_access 179.131.122.1 179.131.122.2 netmask 255.255.255.252
```

Публичные адреса - это уникальные адреса, которые присваиваются вашему интернет-провайдеру и используются для идентификации вашей сети в глобальной сети.

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

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

```
Gateway_KAV(config)#access-list 1 permit 10.100.1.0 0.0.0.255
```

Список доступа – списки, которые используются для фильтрации трафика.

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

Для определения NAT используйте команду ip nat inside source.

Команда нужна чтобы осуществлялась трансляция частных адресов в публичный адрес.

```
Gateway_KAV(config)#ip nat inside source list 1 pool public_access overload
```

Шаг 11. Назначение интерфейсов

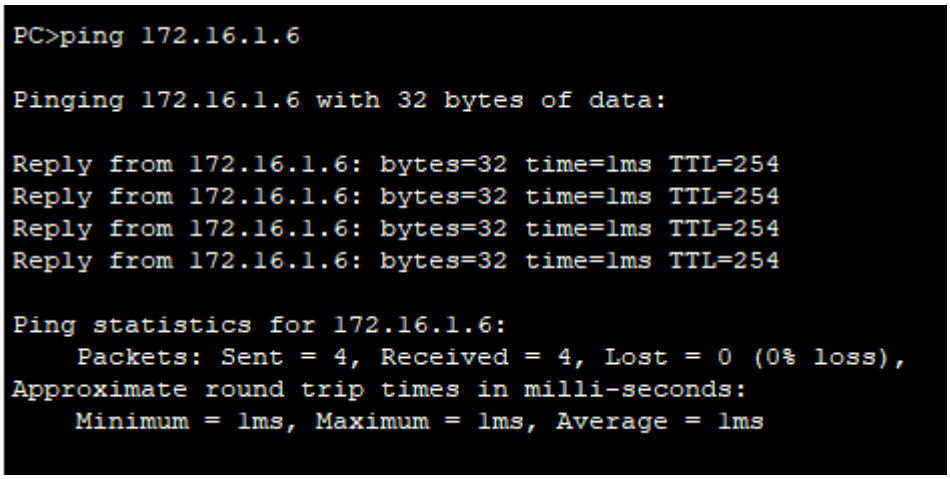
Активные интерфейсы маршрутизатора следует определить в качестве внутреннего или внешнего интерфейса в отношении к NAT. Для этого используйте команду *ip nat inside* или ***ip nat outside***.

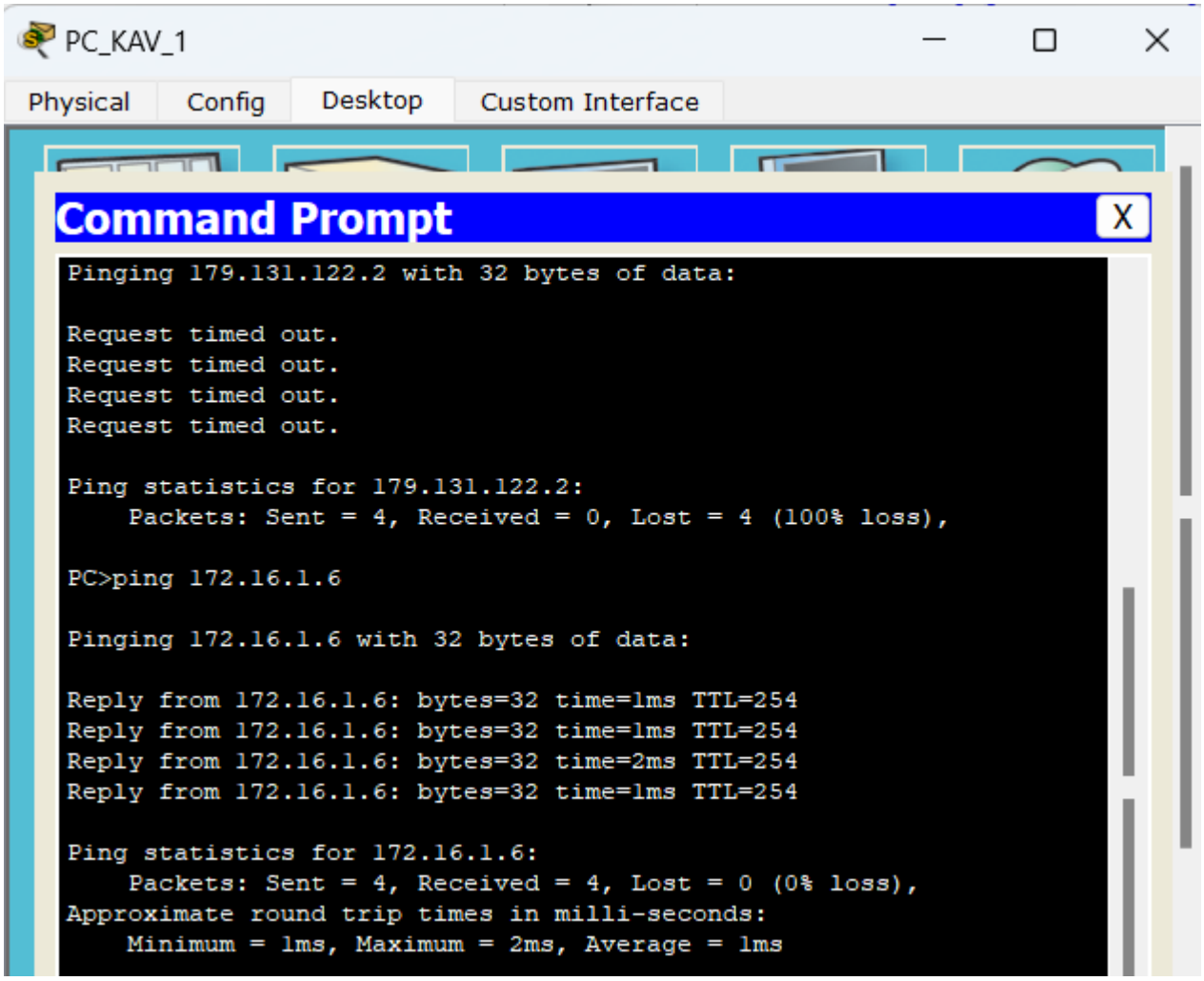
Внутренний интерфейс взаимодействует с частыми адресами, а внешний взаимодействует с публичными

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

Шаг 12. Генерация трафика с маршрутизатора Gateway к маршрутизатору ISP

Отправьте эхо-запросы с узлов 1 и 2 на адрес 172.16.1.6.





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.

```
Gateway_KAV#show ip nat statistics
Total translations: 3 (0 static, 3 dynamic, 3 extended)
Outside Interfaces: Serial0/0
Inside Interfaces: FastEthernet0/0
Hits: 3  Misses: 9
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 3
 pool public_access: netmask 255.255.255.252
       start 179.131.122.1 end 179.131.122.2
       type generic, total addresses 2 , allocated 1 (50%), misses 0
```

1. **Сколько активных преобразований выполнено? 0**
2. **Сколько адресов имеется в пуле? 2**
3. **Сколько адресов уже выделено? 1**

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

Шаг 14. Краткий реферат по NAT и NAPT

NAT (Network Address Translation) и NAPT (Network Address and Port Translation) - это технологии, которые используются для перевода сетевых адресов в IP-сетях. Они предназначены для решения проблем с нехваткой IPv4-адресов и обеспечения безопасности сети.

NAT является простой техникой, которая позволяет скрыть внутренние IP-адреса от внешнего интернета, заменяя их на один общий внешний адрес. Это особенно полезно в домашних сетях или офисах, где устройства внутри сети имеют частные IP-адреса, но нуждаются в доступе к интернету. NAT выполняет преобразование адресов в IP-заголовках пакетов, пересылаемых через маршрутизатор, что позволяет внутренним устройствам коммуницировать с внешними ресурсами.

NAPT расширяет функциональность NAT, добавляя перевод портов к переводу адресов. В отличие от NAT, где каждому внутреннему устройству назначается только один внешний адрес, NAPT использует комбинацию IP-адреса и порта для идентификации каждого устройства. Это позволяет одному внешнему адресу поддерживать множество внутренних устройств, что значительно увеличивает эффективность использования доступных IP-адресов.

Обе технологии, NAT и NAPT, широко применяются в современных компьютерных сетях для управления сетевыми ресурсами, обеспечения безопасности и поддержки работы сети при ограниченном числе доступных IP-адресов. Они играют ключевую роль в обеспечении связности и безопасности сетевого трафика в сетях любого масштаба.