

Сергиенко Лев

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Сергиенко Лев Эдуардович

(студент 3 курса **12** группа)

НАСТРОЙКА И ПРОВЕРКА NART

**Краткий отчет
по лабораторной работе №11**

(вариант №15)

Минск 2024

Содержание

РЕФЕРАТ.....	3
Исходные данные для варианта задания.....	5
Шаг 1. Подсоединение устройств.....	5
Шаг 2. Настройка основной конфигурации маршрутизатора 2.....	5
Шаг 3. Настройка маршрутизатора, используемого в качестве шлюза.....	7
Шаг 4. Настройка правильного IP-адреса, маски подсети и шлюза по умолчанию для узлов.....	9
Шаг 5. Проверка работоспособности сети.....	9
Шаг 6. Создание маршрута по умолчанию.....	11
Шаг 7. Создание статического маршрута.....	13
Шаг 8. Определение пула используемых публичных IP-адресов.....	15
Шаг 9. Определение списка доступа, соответствующего внутренним частным IP-адресам.....	16
Шаг 10. Определение NAT из списка внутренних адресов в пул внешних адресов.....	16
Шаг 11. Назначение интерфейсов.....	17
Шаг 12. Генерация трафика с маршрутизатора Gateway к маршрутизатору ISP.....	17
Шаг 13. Проверьте работоспособность NAT.....	18

РЕФЕРАТ

Network Address Translation (NAT) — это технология, позволяющая изменять IP-адреса в сетевых пакетах, проходящих через маршрутизатор или другое сетевое устройство. Она широко используется для обеспечения гибкости в управлении адресным пространством, повышения безопасности и подключения локальных сетей к Интернету через один или несколько публичных IP-адресов.

Основное назначение NAT

NAT был разработан как решение проблемы ограниченного количества IPv4-адресов. Поскольку IPv4 предоставляет около $4,3 \cdot 10^9$ уникальных адресов, этого оказалось недостаточно для всех устройств, подключенных к Интернету. NAT позволяет скрыть внутренние IP-адреса локальной сети за одним (или несколькими) общедоступными адресами. Основные задачи NAT включают:

1. **Сохранение IPv4-адресов:** Устройства внутри локальной сети используют частные IP-адреса, которые не требуют регистрации в глобальном реестре.
2. **Безопасность:** Скрытие внутренней топологии сети повышает защищенность, так как устройства локальной сети становятся недоступными для прямого доступа извне.
3. **Подключение к Интернету:** Устройства с частными IP-адресами могут взаимодействовать с внешними сетями через общий публичный IP.

Принцип работы NAT

При использовании NAT маршрутизатор или другое устройство изменяет IP-адреса и порты в заголовках сетевых пакетов. Существует несколько видов NAT:

1. **Static NAT (статический):** Однозначное сопоставление между внутренним и внешним IP-адресом. Этот тип используется, если требуется постоянный доступ извне к конкретному устройству в сети.
2. **Dynamic NAT (динамический):** Маршрутизатор выбирает публичный IP-адрес из заранее заданного пула. Этот подход полезен для временных подключений.
3. **PAT (Port Address Translation):** Частный IP-адрес сопоставляется с публичным через уникальные номера портов. Это наиболее распространенный тип NAT, известный как *маскарадинг*. Он позволяет десяткам или даже сотням устройств в локальной сети использовать один публичный IP-адрес.

Пример работы NAT

Предположим, компьютер в локальной сети с IP-адресом 192.168.1.10 отправляет HTTP-запрос на сервер в Интернете. Процесс проходит следующие этапы:

1. Исходящий пакет покидает компьютер и поступает на маршрутизатор.
2. NAT на маршрутизаторе заменяет частный IP (192.168.1.10) на публичный (например, 203.0.113.1) и записывает соответствие в таблицу NAT.
3. Пакет отправляется на целевой сервер с публичным IP.
4. Сервер отправляет ответ на публичный IP-адрес маршрутизатора.
5. NAT на маршрутизаторе по таблице сопоставления определяет, какому устройству в локальной сети отправить пакет, и заменяет IP обратно.

Заключение

NAT остается важной технологией в эпоху IPv4, несмотря на внедрение IPv6, которое решает проблему нехватки адресов. Благодаря NAT миллионы устройств могут подключаться к Интернету, обеспечивая гибкость, экономичность и защиту локальных сетей.

Исходные данные для варианта задания

Вариант	Адреса для узлов	Маршрутизатор 1	Маршрутизатор 2	IP-адрес Loopback 1
15	192.168.15.0/24	132.101.22.1/30	132.101.22.2/30	172.16.1.15/32

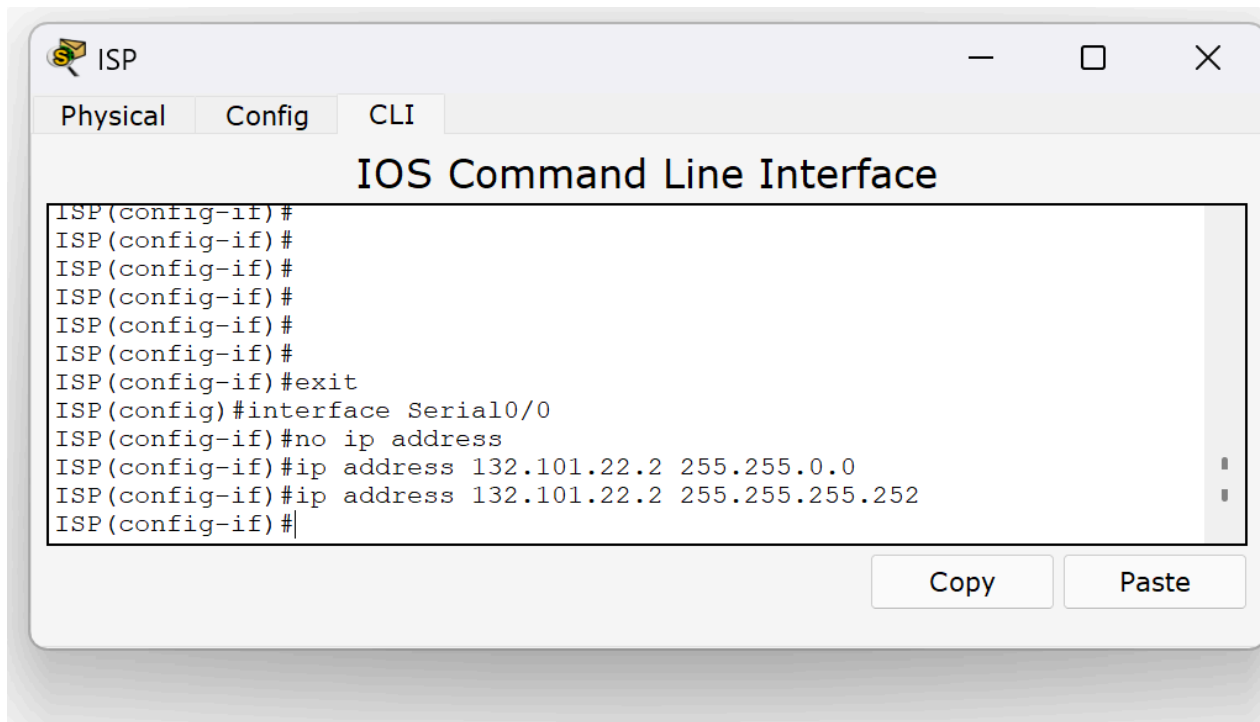
Устройство	Имя узла	Маска подсети порта FastEthernet0/0	Тип интерфейса	IP-адрес порта Serial 0/0	IP-адрес Loopback 1
Маршрутизатор 1	Cateway	192.168.15.0/24	DTE	132.101.22.1	
Маршрутизатор 2	ISP	Нет	DCE	132.101.22.2	172.16.1.15/32
Коммутатор 1	Switch 1				

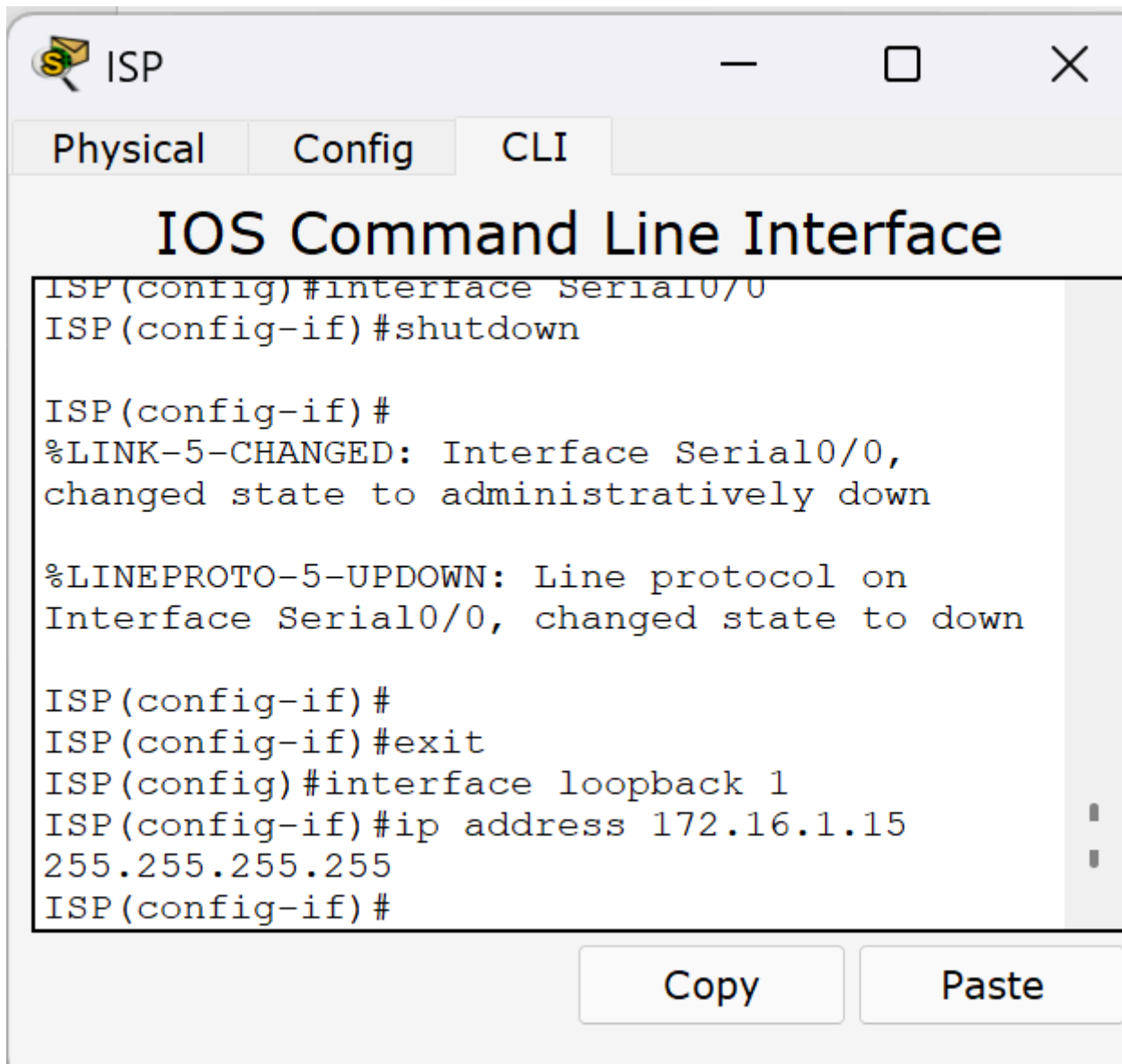
Шаг 1. Подсоединение устройств

- 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

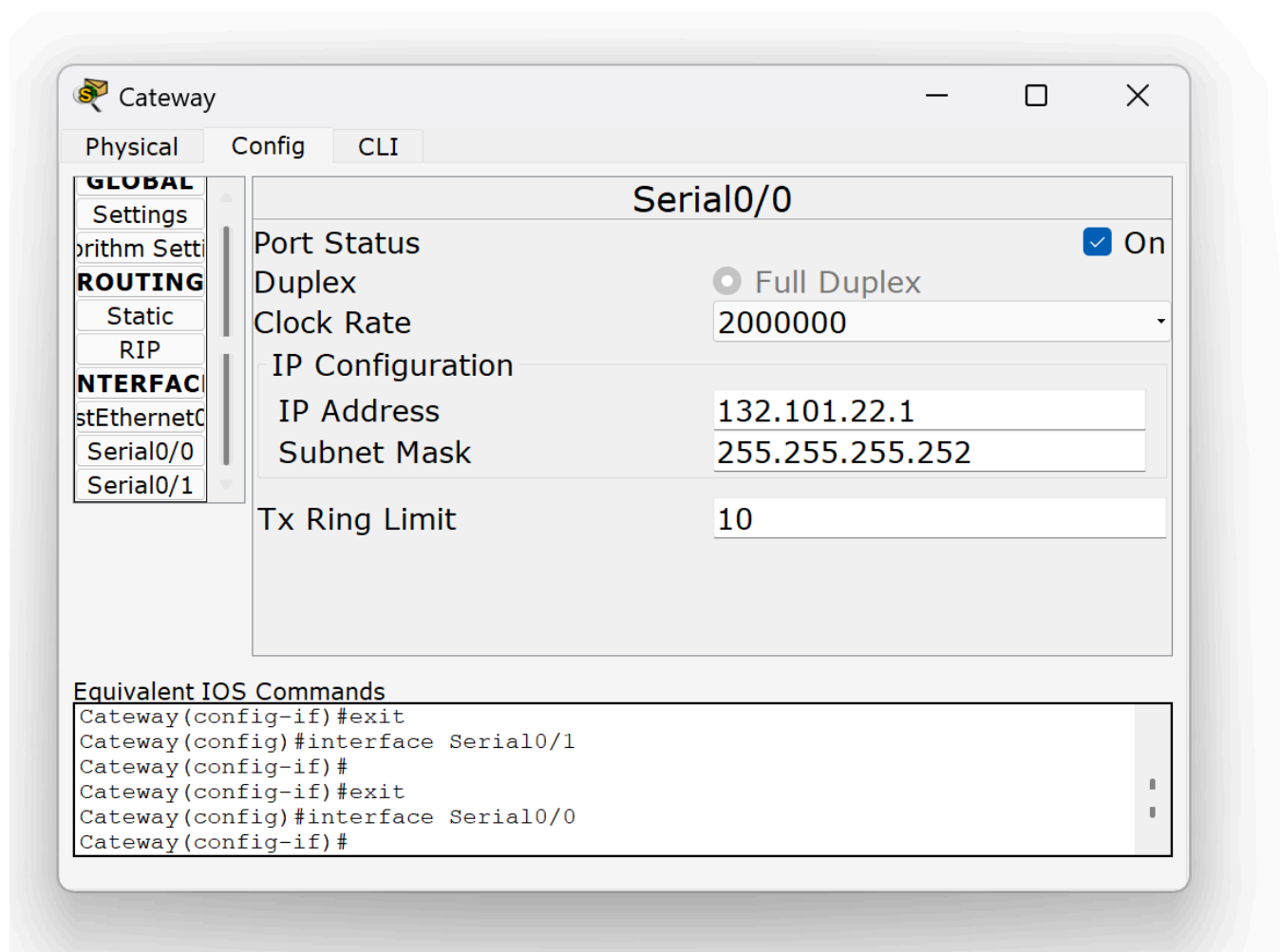
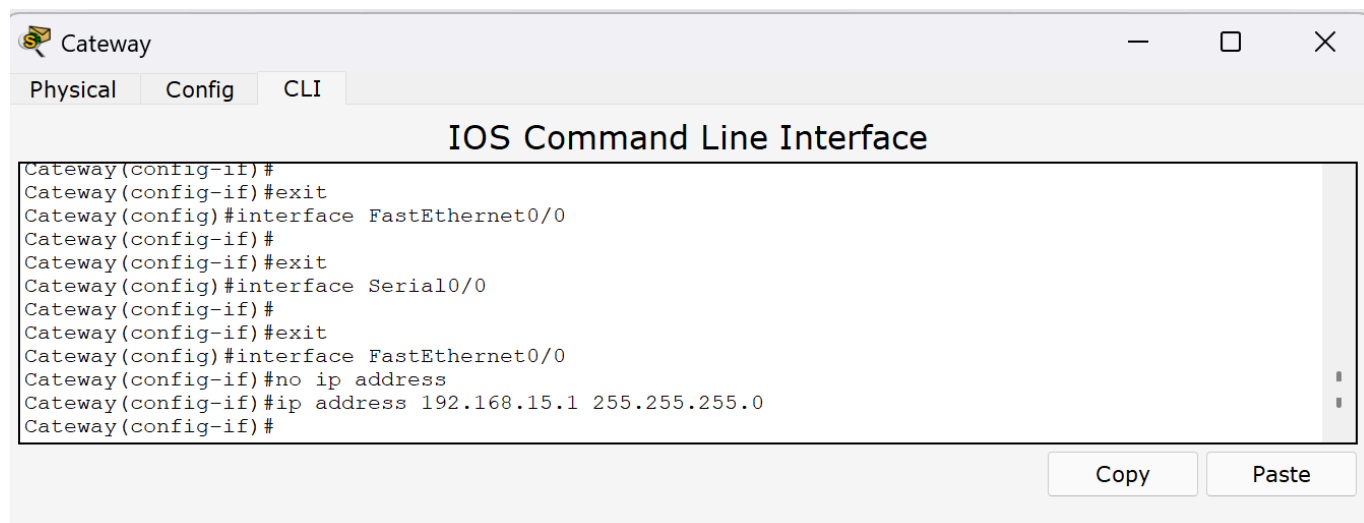
Задайте в настройках конфигурации маршрутизатора 2 (ISP) имя узла, задайте IP-адреса для интерфейсов согласно вашему варианту задания. Сохраните конфигурацию.





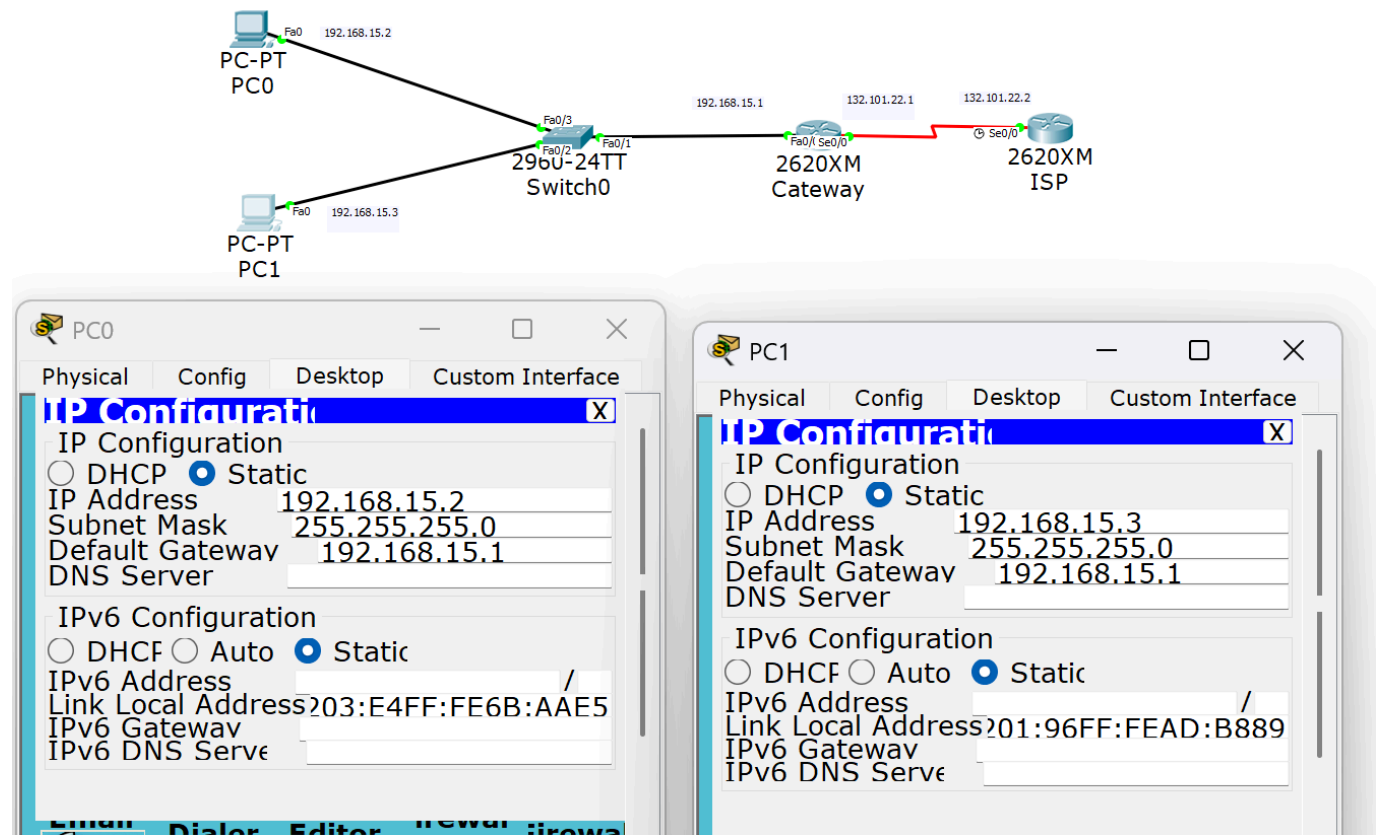
Шаг 3. *Настройка маршрутизатора, используемого в качестве шлюза*

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



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. Шлюзом по умолчанию должен быть IP-адрес интерфейса FastEthernet маршрутизатора с именем Gateway.



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

Внутренние IP-адреса используются внутри локальной сети (например, в доме или офисе) для идентификации устройств, таких как компьютеры, смартфоны и принтеры. Эти адреса не видны в интернете и обеспечивают связь между устройствами внутри сети.

Внешние IP-адреса назначаются интернет-провайдером и используются для идентификации вашей сети в интернете. Они позволяют устройствам внутри вашей локальной сети общаться с внешними ресурсами и получать доступ к интернету.





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

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

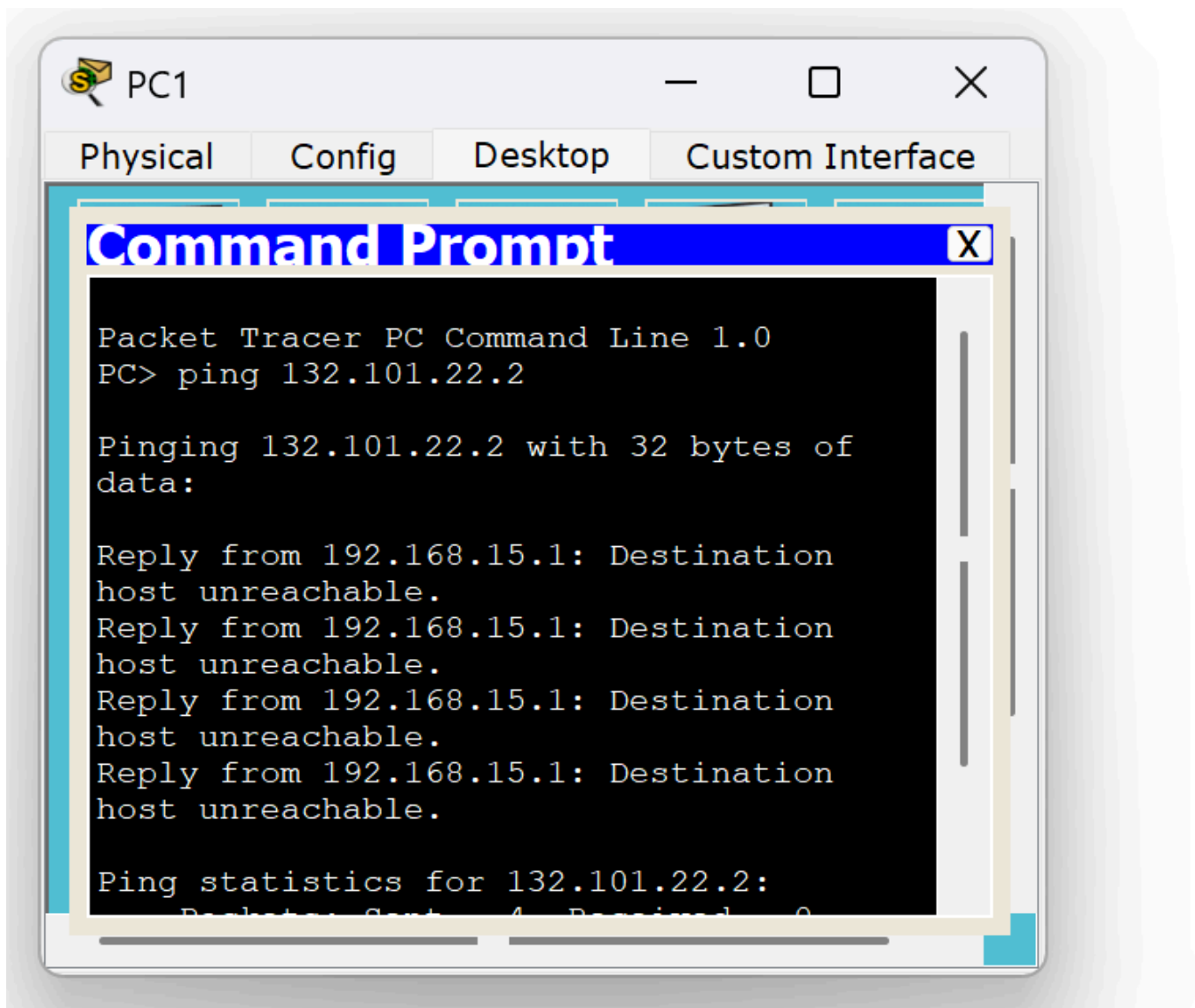
Fire	Last Sta	Sou	Destination	Type	Col	Time(s)	Peric	Nu	Edi	Delete
	Succe...	PC0	Gateway	ICMP		0.000	N	0	(e...	
	Succe...	PC1	Gateway	ICMP		0.000	N	1	(e...	

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.

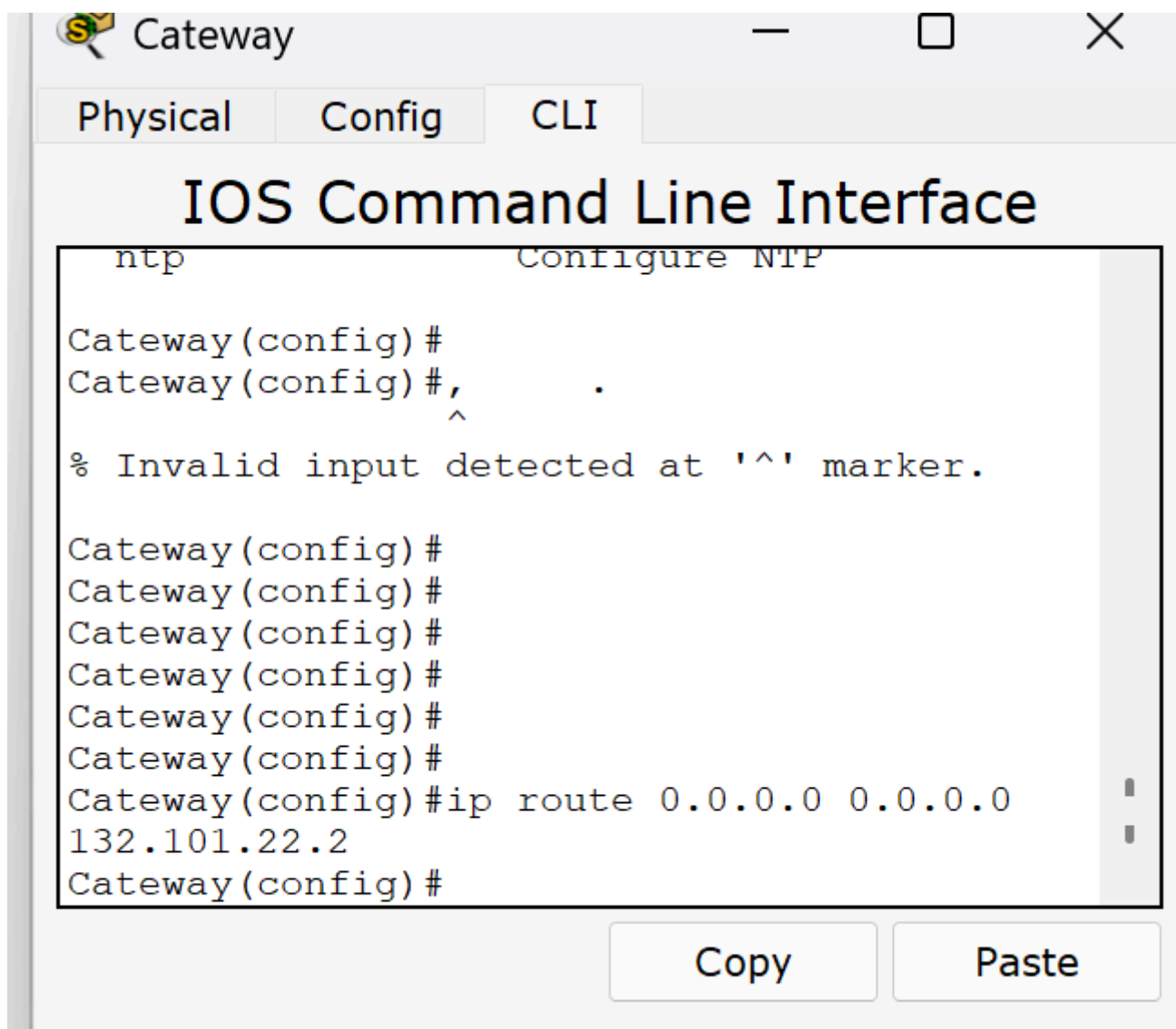


Эхо-запрос не успешен, т.к. нет маршрута до данного адреса.

Узлы не могут достичь IP-адреса 132.101.22.2, поскольку на маршрутизаторе Gateway отсутствует маршрут к этой сети, и маршрутизатор ISP не знает о сети 192.168.15.0/24.

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.

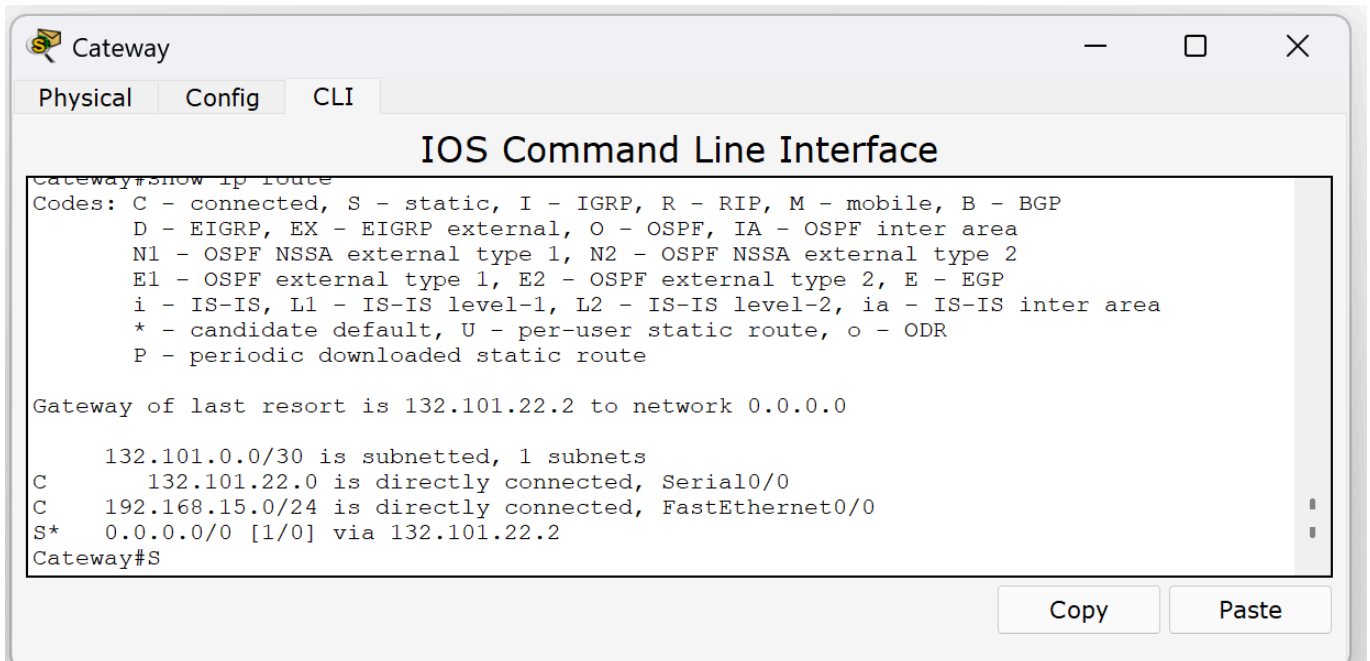


Как вы понимаете термин «шлюз последней надежды»?

Сергиенко Лев

Это маршрут по умолчанию, используемый для отправки пакетов к неизвестным сетям через указанный шлюз.

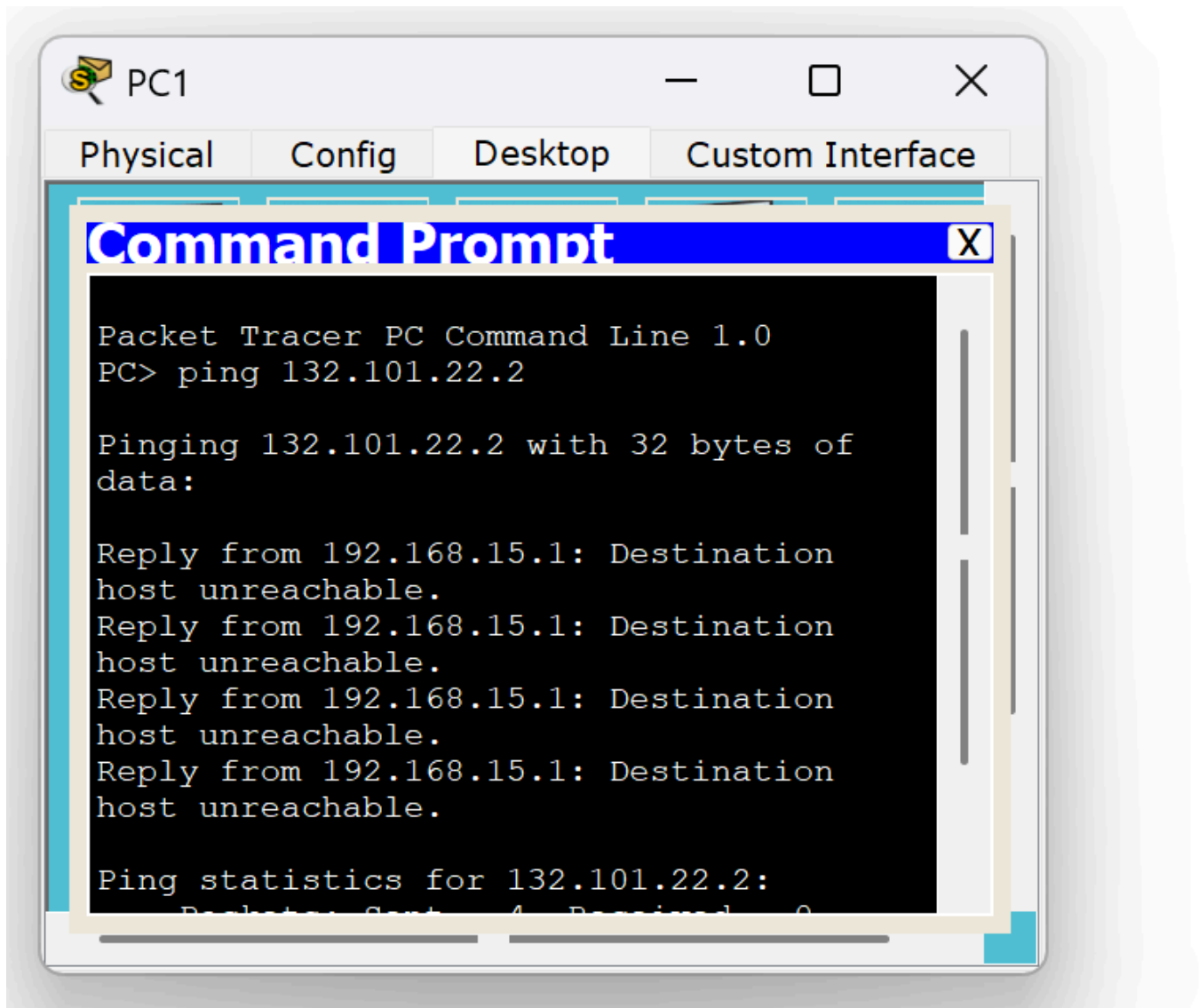
- Проверьте маршрут по умолчанию по таблице маршрутизации маршрутизатора Gateway.



Находится ли статический маршрут в таблице маршрутизации?

Да, статический маршрут по умолчанию присутствует.

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

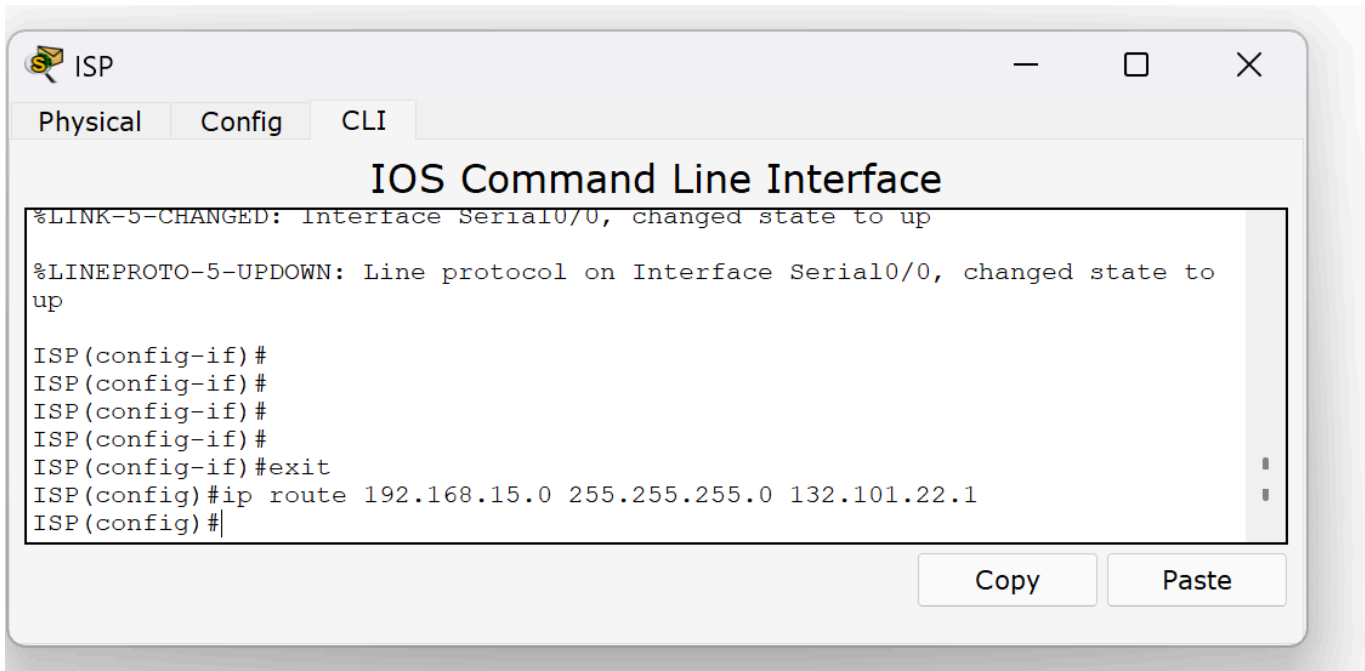


Успешно ли выполнен эхо-запрос?

Нет, поскольку маршрутизатор ISP не имеет обратного маршрута.

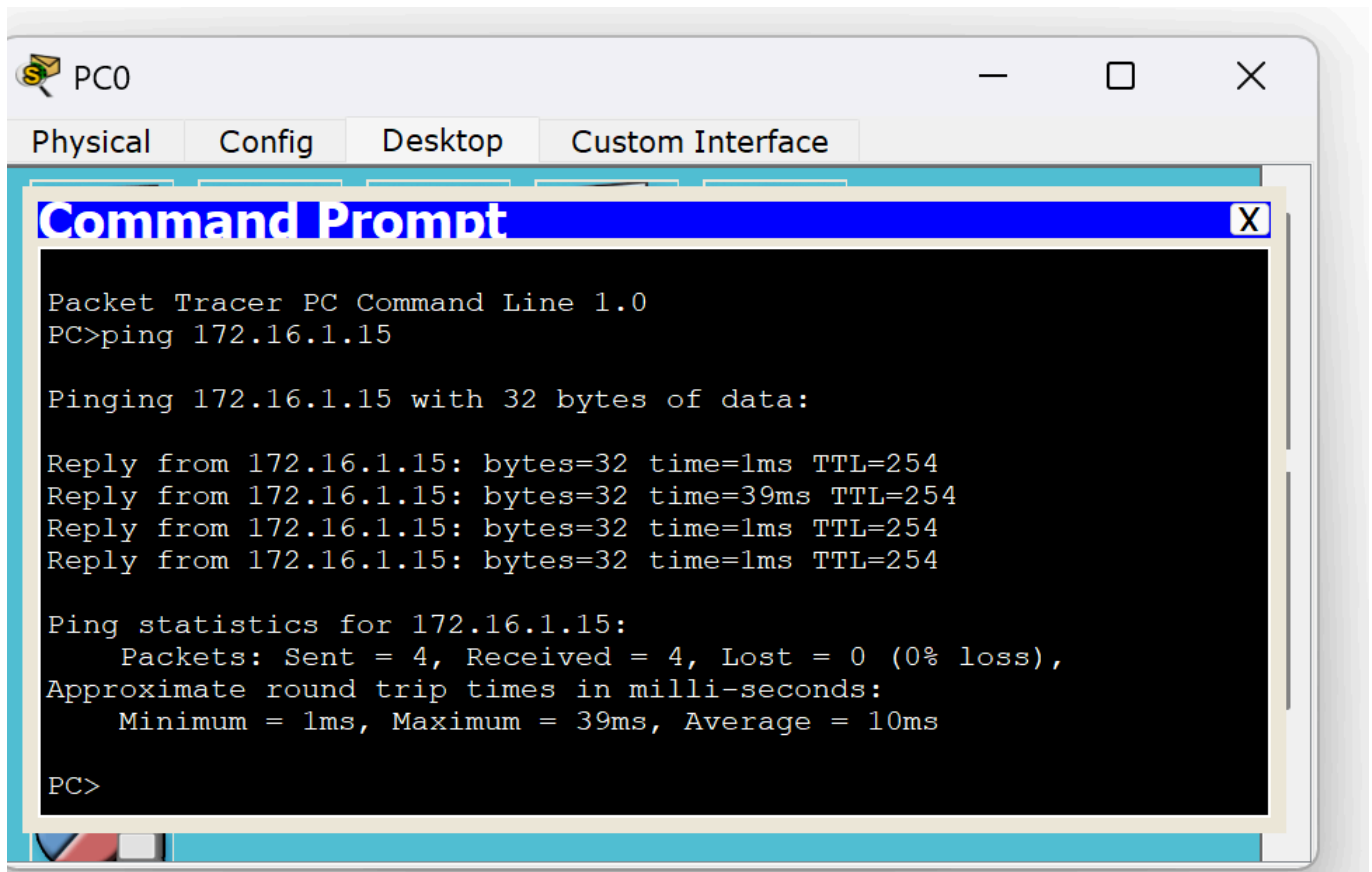
Шаг 7. Создание статического маршрута

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



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

Routing Table for Gateway					
Type	Network	Port	Next Hop IP	Metric	
S	0.0.0.0/0	---	132.101.22.2	1/0	
C	132.101.22...	Serial0/0	---	0/0	
C	192.168.15...	FastEthern...	---	0/0	

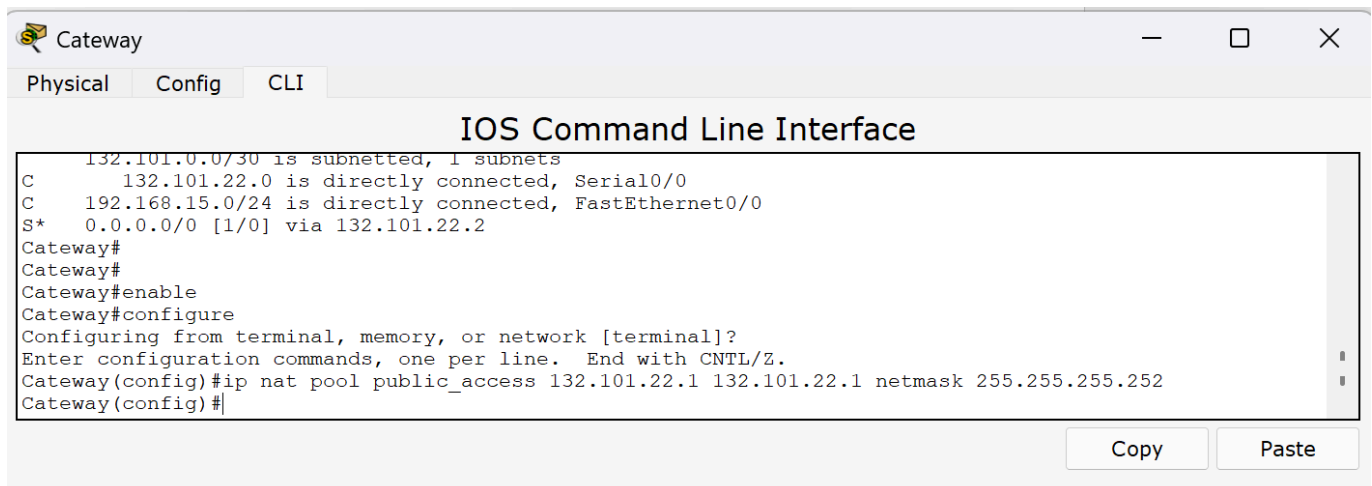


Успешно ли выполнен эхо-запрос?

Да, эхо-запрос успешен.

Шаг 8. Определение пула используемых публичных IP-адресов

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



Что вы понимаете под термином — публичные адреса, частные адреса?

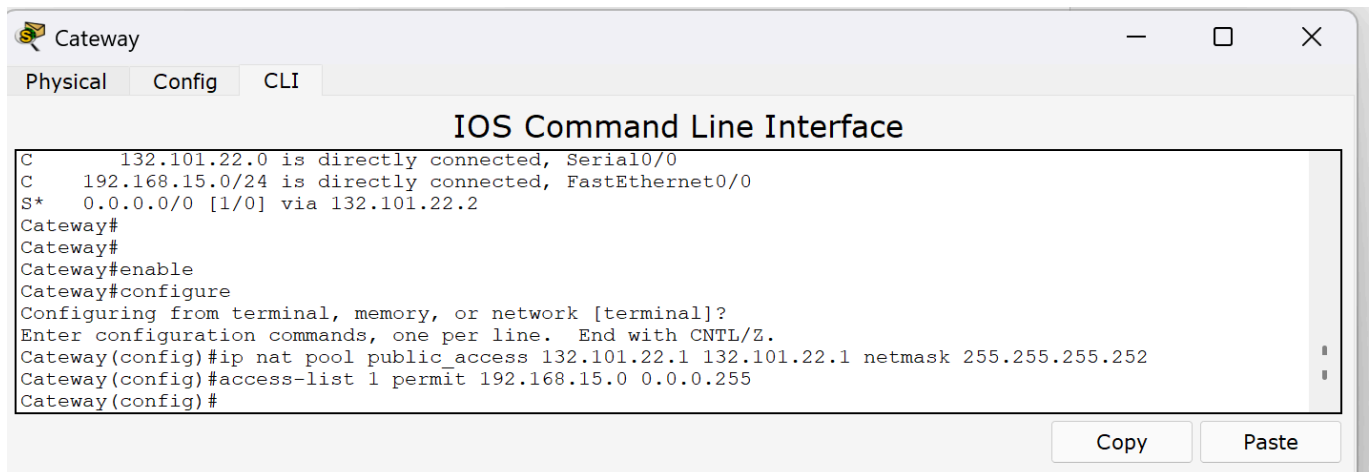
Публичные адреса — IP-адреса, доступные в глобальном интернете.

Сергиенко Лев

Частные адреса — IP-адреса, используемые в локальных сетях и не маршрутизируемые в интернете.

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

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




```
C 132.101.22.0 is directly connected, Serial0/0
C 192.168.15.0/24 is directly connected, FastEthernet0/0
S* 0.0.0.0/0 [1/0] via 132.101.22.2
Gateway#
Gateway#
Gateway#enable
Gateway#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#ip nat pool public_access 132.101.22.1 132.101.22.1 netmask 255.255.255.252
Gateway(config)#access-list 1 permit 192.168.15.0 0.0.0.255
Gateway(config)#
```

Прокомментируйте термин “список доступа”.

Список доступа (ACL) — набор правил для контроля трафика и обеспечения безопасности в сети.

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

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



```
C 192.168.15.0/24 is directly connected, FastEthernet0/0
S* 0.0.0.0/0 [1/0] via 132.101.22.2
Gateway#
Gateway#
Gateway#enable
Gateway#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#ip nat pool public_access 132.101.22.1 132.101.22.1 netmask 255.255.255.252
Gateway(config)#access-list 1 permit 192.168.15.0 0.0.0.255
Gateway(config)#ip nat inside source list 1 pool public_access overload
Gateway(config)#
```

Пояснение

Это позволяет множеству внутренних адресов использовать ограниченный пул внешних адресов, осуществляя трансляцию адресов и портов.

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*.

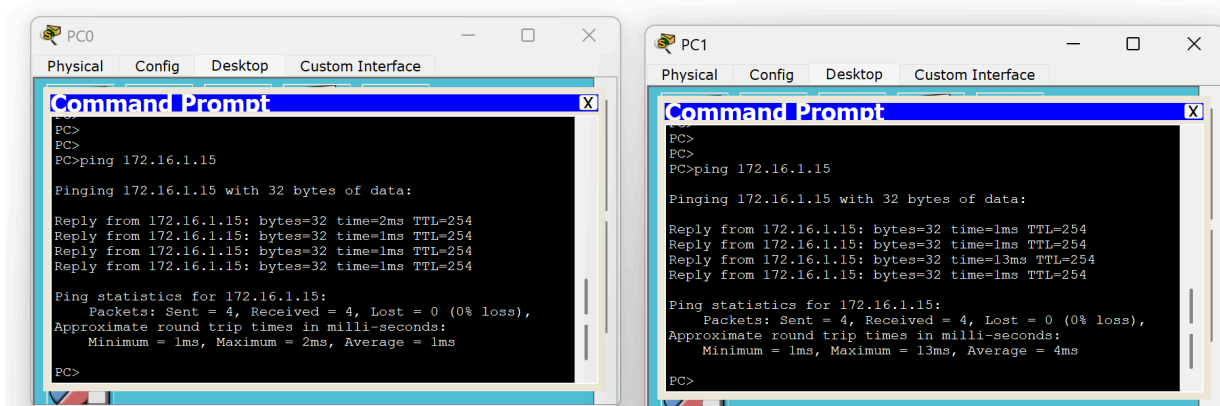


В данном контексте, что такое внутренние и внешние интерфейсы?

- Внутренний интерфейс — подключен к локальной сети (LAN).
- Внешний интерфейс — подключен к внешней сети или интернету (WAN).

Шаг 12. Генерация трафика с маршрутизатора Gateway к маршрутизатору ISP

Отправьте эхо-запросы с узлов 1 и 2 на адрес 172.16.1.15

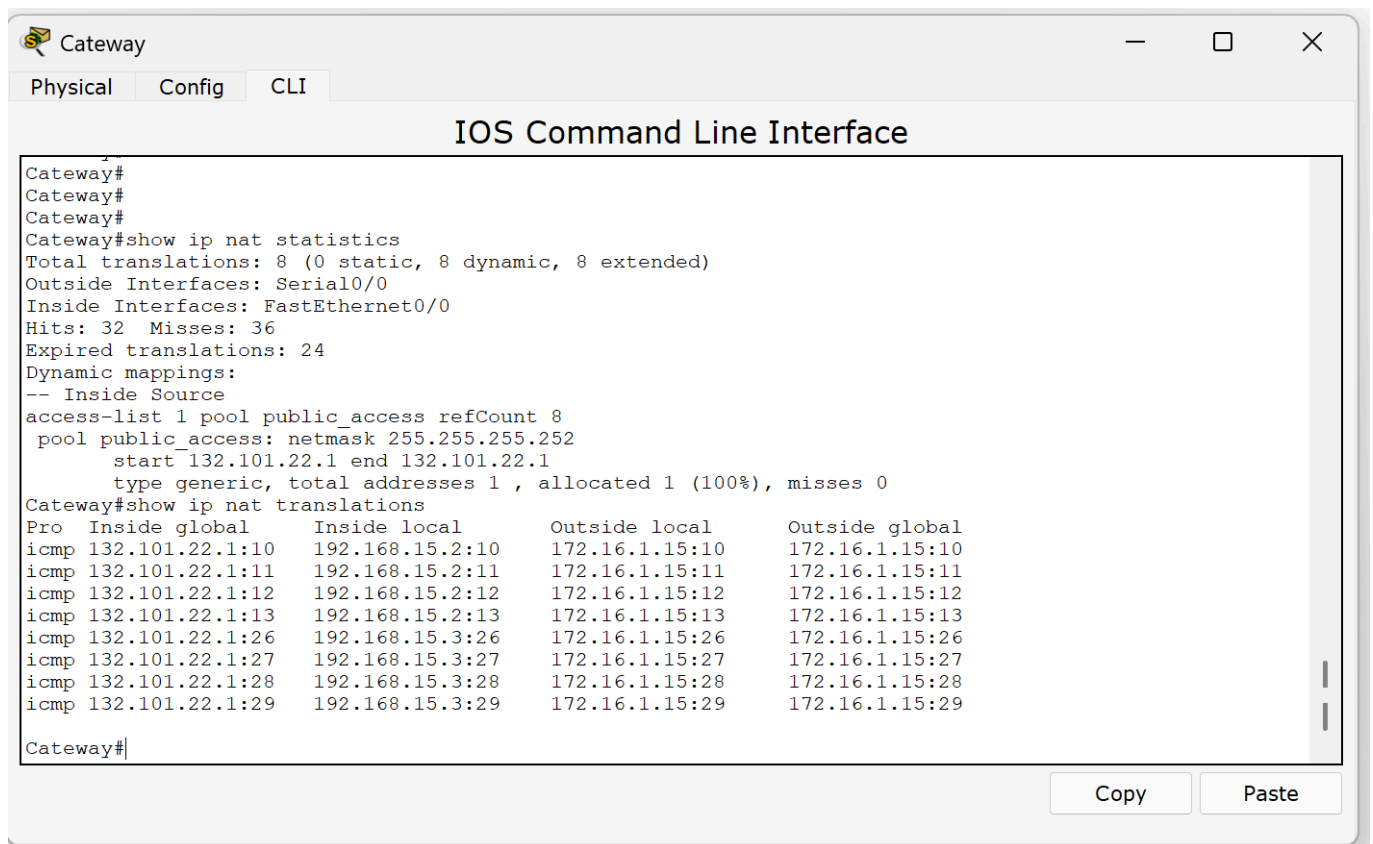


Шаг 13. Проверьте работоспособность NAPT

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?
2. Сколько адресов имеется в пуле?
3. Сколько адресов уже выделено?

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



```
Gateway
Gateway#
Gateway#
Gateway#show ip nat statistics
Total translations: 8 (0 static, 8 dynamic, 8 extended)
Outside Interfaces: Serial0/0
Inside Interfaces: FastEthernet0/0
Hits: 32 Misses: 36
Expired translations: 24
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 8
 pool public_access: netmask 255.255.255.252
   start 132.101.22.1 end 132.101.22.1
   type generic, total addresses 1 , allocated 1 (100%), misses 0
Gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 132.101.22.1:10    192.168.15.2:10   172.16.1.15:10     172.16.1.15:10
icmp 132.101.22.1:11    192.168.15.2:11   172.16.1.15:11     172.16.1.15:11
icmp 132.101.22.1:12    192.168.15.2:12   172.16.1.15:12     172.16.1.15:12
icmp 132.101.22.1:13    192.168.15.2:13   172.16.1.15:13     172.16.1.15:13
icmp 132.101.22.1:26    192.168.15.3:26   172.16.1.15:26     172.16.1.15:26
icmp 132.101.22.1:27    192.168.15.3:27   172.16.1.15:27     172.16.1.15:27
icmp 132.101.22.1:28    192.168.15.3:28   172.16.1.15:28     172.16.1.15:28
icmp 132.101.22.1:29    192.168.15.3:29   172.16.1.15:29     172.16.1.15:29
Gateway#
```

1. Сколько активных преобразований выполнено?

Из вывода команды `show ip nat statistics`:

Total translations: 8 (0 static, 8 dynamic, 8 extended)

Ответ:

Всего выполнено **8 активных динамических преобразований.**

2. Сколько адресов имеется в пуле?

Из раздела `Dynamic mappings`:

pool public_access: netmask 255.255.255.252

start 132.101.22.1 end 132.101.22.1

type generic, total addresses 1 , allocated 1 (100%), misses 0

Ответ:

В пуле NAT public_access имеется **1 публичный IP-адрес** (132.101.22.1).

3. Сколько адресов уже выделено?

Из того же раздела:

allocated 1 (100%)

Ответ:

Из пула уже **выделен 1 адрес**, что составляет **100%** доступных адресов.

Анализ и Пояснения

1. Активные преобразования (Total translations):

- о **8 динамических преобразований** указывает на то, что 8 внутренних IP-адресов были успешно преобразованы для доступа к внешней сети.

2. Пул NAT (public_access):

- о **Только 1 публичный IP-адрес** в пуле ограничивает количество одновременных преобразований. В текущей конфигурации это соответствует количеству выделенных адресов (1 из 1).

3. Статистика HIT/MISS и Expired translations:

- о **Hits: 32, Misses: 36:** Это показывает количество успешных и неуспешных попыток использования существующих NAT-преобразований.
- о **Expired translations: 24:** Указывает на количество завершенных или истекших преобразований, которые уже не используются.

4. Таблица NAT-преобразований (show ip nat translations):

```
Pro Inside global Inside local Outside local Outside global
icmp 132.101.22.1:10 192.168.15.2:10 172.16.1.15:10 172.16.1.15:10
icmp 132.101.22.1:11 192.168.15.2:11 172.16.1.15:11 172.16.1.15:11
icmp 132.101.22.1:12 192.168.15.2:12 172.16.1.15:12 172.16.1.15:12
icmp 132.101.22.1:13 192.168.15.2:13 172.16.1.15:13 172.16.1.15:13
icmp 132.101.22.1:26 192.168.15.3:26 172.16.1.15:26 172.16.1.15:26
icmp 132.101.22.1:27 192.168.15.3:27 172.16.1.15:27 172.16.1.15:27
icmp 132.101.22.1:28 192.168.15.3:28 172.16.1.15:28 172.16.1.15:28
icmp 132.101.22.1:29 192.168.15.3:29 172.16.1.15:29 172.16.1.15:29
```

- **Inside global:** Публичный IP-адрес из пула (132.101.22.1) с уникальными портами.

Сергиенко Лев

- **Inside local:** Внутренние IP-адреса узлов (192.168.15.2 и 192.168.15.3) с соответствующими портами.
- **Outside local и Outside global:** IP-адреса внешних ресурсов (в данном случае 172.16.1.15) с портами.

Пояснение:

Эти преобразования подтверждают, что внутренние узлы успешно взаимодействуют с внешними ресурсами через настроенный пул NAT.

Заключение:

Я успешно настроил и проверил работоспособность NAT в сети. Все активные преобразования отражены в таблице NAT-преобразований, что подтверждает корректную работу механизма трансляции адресов.