

PC1

Physical Config Desktop Programming Attributes

Command Prompt

Packet Tracer PC Command Line 1.0

C:\>ping 64.100.201.1

Pinging 64.100.201.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 64.100.201.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

PC2

Physical Config Desktop Programming Attributes

Command Prompt

Packet Tracer PC Command Line 1.0

C:\>ping 64.100.201.1

Pinging 64.100.201.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 64.100.201.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

L1

Physical Config Desktop Programming Attributes

Command Prompt

Packet Tracer PC Command Line 1.0

C:\>ping 64.100.201.1

Pinging 64.100.201.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 64.100.201.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

L2

Physical Config Desktop Programming Attributes

Command Prompt

Packet Tracer PC Command Line 1.0

C:\>ping 64.100.201.1

Pinging 64.100.201.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 64.100.201.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

011 9.3.1.4 Packet Tracer - Verify

Файл | C:/Users/Иван/De...

2 из 2

Сценарий

Подрядчик восстановил старую настройку на новом маршрутизаторе с работающим прео NAT. Однако после создания резервной копии старой настройки сеть изменилась, и в нее добавлена новая подсеть. Ваша задача — восстановить работу сети.

Часть 1: Локализация проблемы

Отправьте эхо-запрос на Сервер 1 с ПК 1, ПК 2, L1, L2 и R2. Запишите результаты каждого запроса. В случае необходимости отправьте эхо-запрос на любой другой компьютер.

Часть 2: Отладка настроек NAT

Шаг 1: Просмотрите преобразования NAT на маршрутизаторе R2.

R2

Physical Config CLI Attributes

IOS Command Line Interface

Kubakov-R2>

Kubakov-R2>ping 64.100.201.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 64.100.201.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/5 ms

Kubakov-R2>

Ctrl+F6 to exit CLI focus

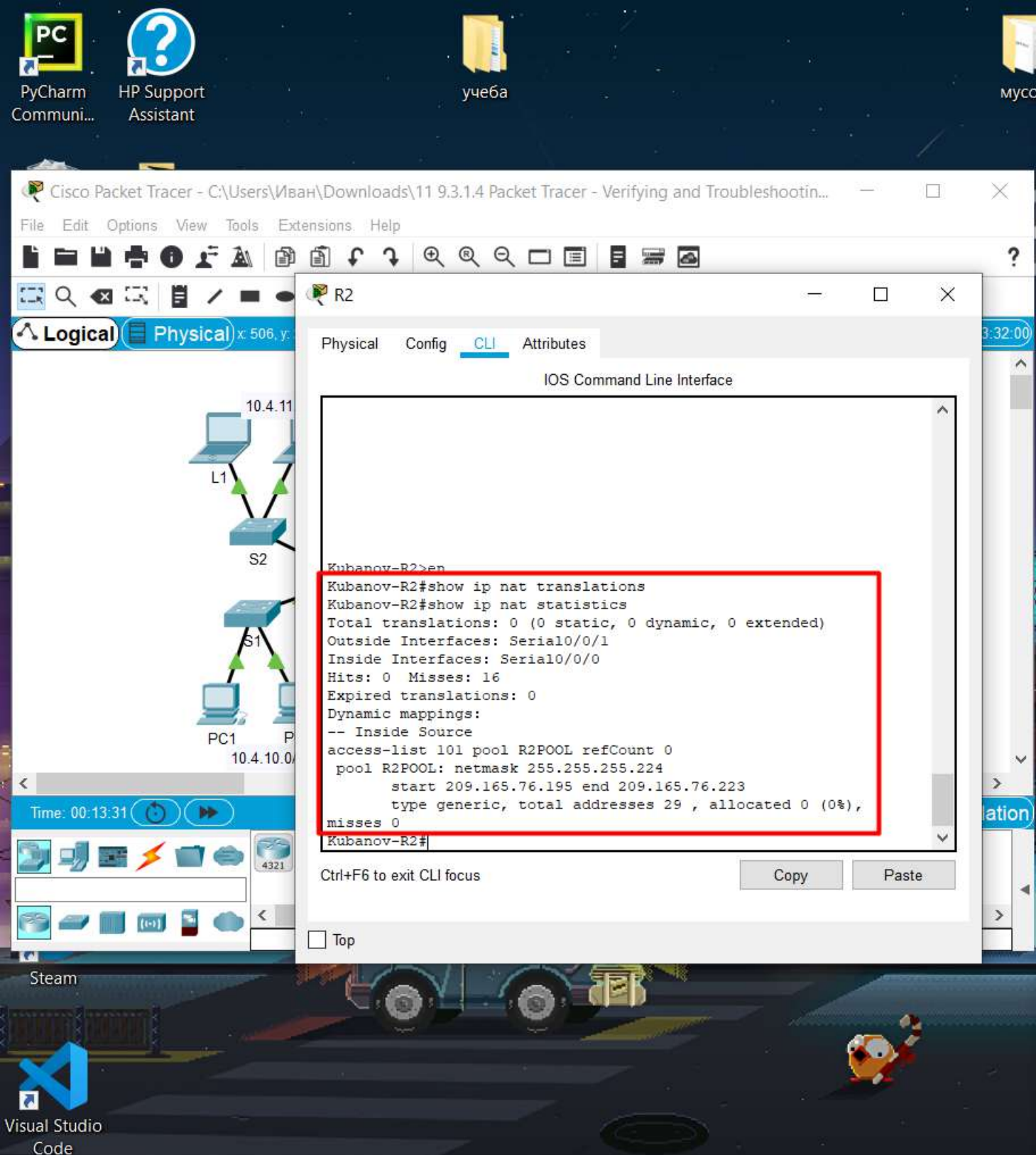
Copy Paste

ENG

18:54

31.10.2023





011 9.3.1.4 Packet Tracer - Verify

Файл | C:/Users/Иван/De...

2 из 2

### Сценарий

Подрядчик восстановил старую настройку на новом маршрутизаторе с работающим прео NAT. Однако после создания резервной копии старой настройки сеть изменилась, и в нее добавлена новая подсеть. Ваша задача — восстановить работу сети.

### Часть 1: Локализация проблемы

Отправьте эхо-запрос на **Сервер 1** с ПК 1, ПК 2, L1, L2 и R2. Запишите результаты каждого запроса. В случае необходимости отправьте эхо-запрос на любой другой компьютер.

### Часть 2: Отладка настроек NAT

#### Шаг 1: Просмотрите преобразования NAT на маршрутизаторе R2.

Если NAT работает, в таблице должны быть записи.

#### Шаг 2: Просмотрите текущую настройку маршрутизатора R2.

Внутренний порт NAT должен соответствовать частному адресу, а внешний порт NAT должен соответствовать публичному адресу.

#### Шаг 3: Исправьте настройки интерфейсов.

Примените к соответствующим портам команды `ip nat inside` и `ip nat outside`.

#### Шаг 4: Отправьте эхо-запрос на Сервер 1 с ПК 1, ПК 2, L1, L2 и R2.

Запишите результаты каждого эхо-запроса. В случае необходимости отправьте эхо-запрос на любой другой компьютер.

#### Шаг 5: Просмотрите преобразования NAT на маршрутизаторе R2.

Если NAT работает, в таблице должны быть записи.

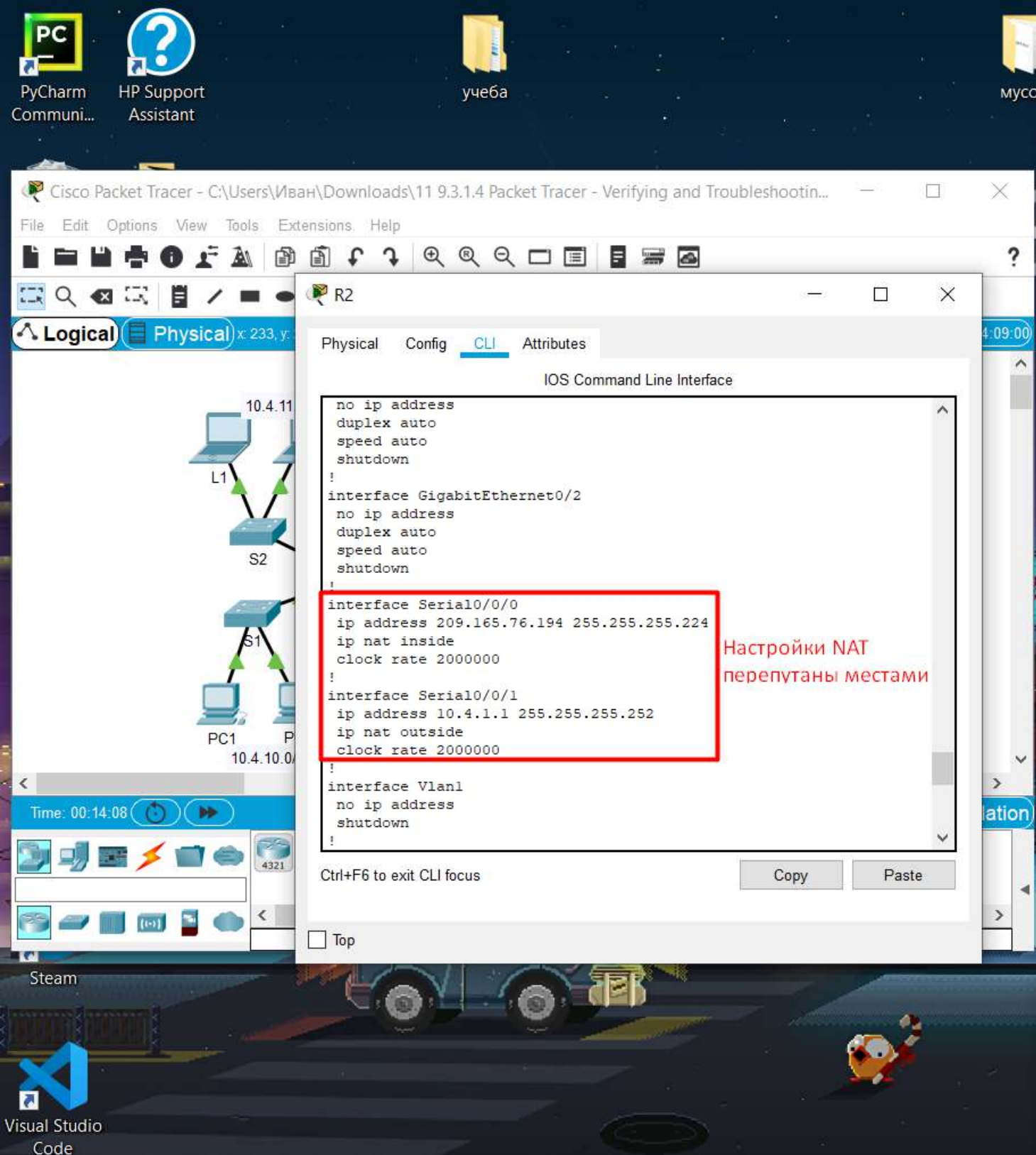
#### Шаг 6: Отобразите список контроля доступа 101 на маршрутизаторе R2.

Шаблонная маска должна охватывать сети 10.4.10.0 и 10.4.11.0.

#### Шаг 7: Внесите изменения в список контроля доступа.

Удалите список контроля доступа `access-list 101` и замените его похожим списком длиной запись. Единственным отличием должна быть шаблонная маска.





011 9.3.1.4 Packet Tracer - Verify

Файл | C:/Users/Иван/De...

2 из 2

### Сценарий

Подрядчик восстановил старую настройку на новом маршрутизаторе с работающим прео NAT. Однако после создания резервной копии старой настройки сеть изменилась, и в нее добавлена новая подсеть. Ваша задача — восстановить работу сети.

### Часть 1: Локализация проблемы

Отправьте эхо-запрос на **Сервер 1** с ПК 1, ПК 2, L1, L2 и R2. Запишите результаты каждого запроса. В случае необходимости отправьте эхо-запрос на любой другой компьютер.

### Часть 2: Отладка настроек NAT

#### Шаг 1: Просмотрите преобразования NAT на маршрутизаторе R2.

Если NAT работает, в таблице должны быть записи.

#### Шаг 2: Просмотрите текущую настройку маршрутизатора R2.

Внутренний порт NAT должен соответствовать частному адресу, а внешний порт NAT должен соответствовать публичному адресу.

#### Шаг 3: Исправьте настройки интерфейсов.

Примените к соответствующим портам команды `ip nat inside` и `ip nat outside`.

#### Шаг 4: Отправьте эхо-запрос на Сервер 1 с ПК 1, ПК 2, L1, L2 и R2.

Запишите результаты каждого эхо-запроса. В случае необходимости отправьте эхо-запрос на любой другой компьютер.

#### Шаг 5: Просмотрите преобразования NAT на маршрутизаторе R2.

Если NAT работает, в таблице должны быть записи.

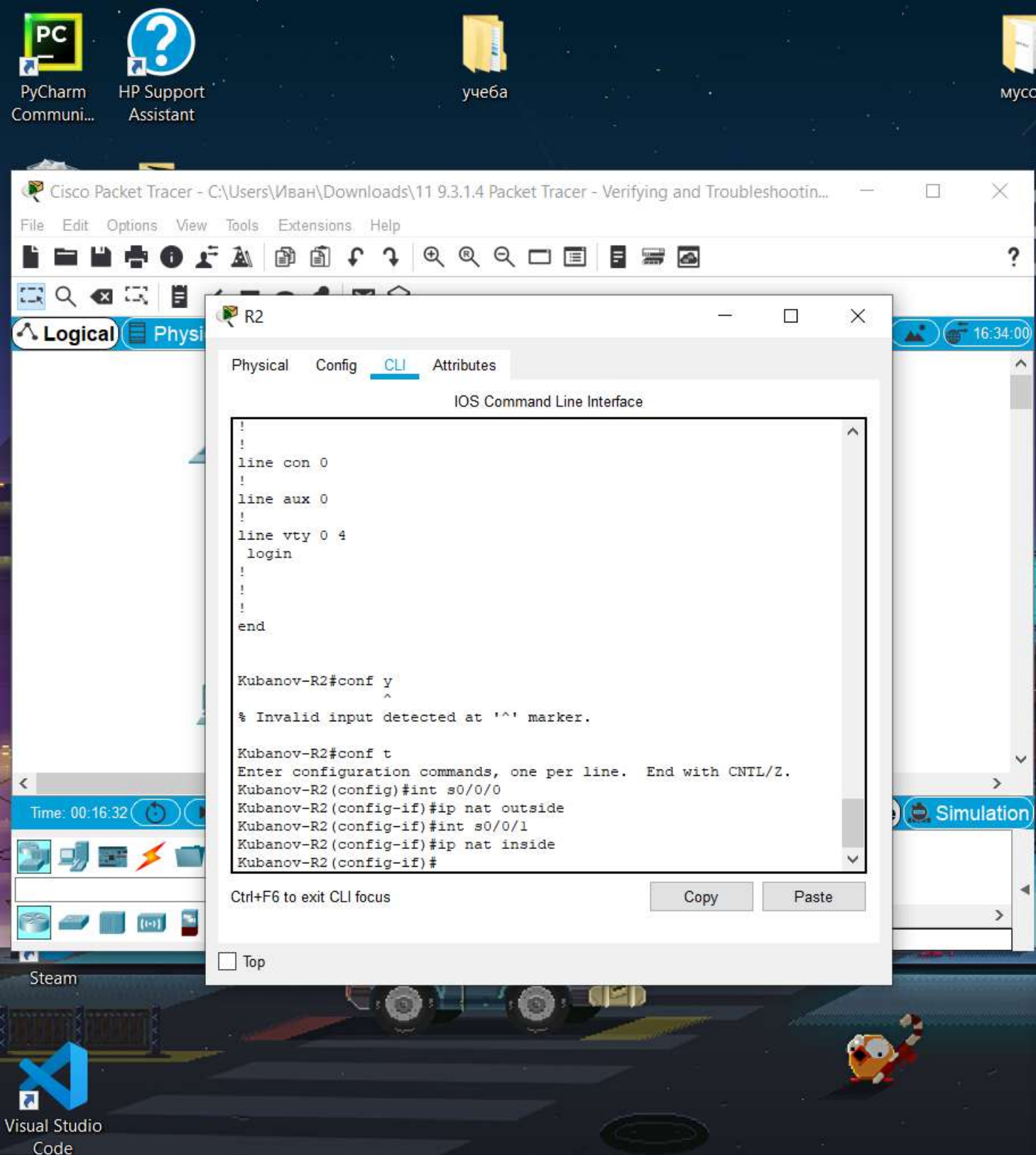
#### Шаг 6: Отобразите список контроля доступа 101 на маршрутизаторе R2.

Шаблонная маска должна охватывать сети 10.4.10.0 и 10.4.11.0.

#### Шаг 7: Внесите изменения в список контроля доступа.

Удалите список контроля доступа `access-list 101` и замените его похожим списком длиной запись. Единственным отличием должна быть шаблонная маска.





011 9.3.1.4 Packet Tracer - Verify

Файл | C:/Users/Иван/De...

2 из 2

### Сценарий

Подрядчик восстановил старую настройку на новом маршрутизаторе с работающим прео NAT. Однако после создания резервной копии старой настройки сеть изменилась, и в нее добавлена новая подсеть. Ваша задача — восстановить работу сети.

### Часть 1: Локализация проблемы

Отправьте эхо-запрос на **Сервер 1** с ПК 1, ПК 2, L1, L2 и R2. Запишите результаты каждого запроса. В случае необходимости отправьте эхо-запрос на любой другой компьютер.

### Часть 2: Отладка настроек NAT

#### Шаг 1: Просмотрите преобразования NAT на маршрутизаторе R2.

Если NAT работает, в таблице должны быть записи.

#### Шаг 2: Просмотрите текущую настройку маршрутизатора R2.

Внутренний порт NAT должен соответствовать частному адресу, а внешний порт NAT должен соответствовать публичному адресу.

#### Шаг 3: Исправьте настройки интерфейсов.

Примените к соответствующим портам команды `ip nat inside` и `ip nat outside`.

#### Шаг 4: Отправьте эхо-запрос на Сервер 1 с ПК 1, ПК 2, L1, L2 и R2.

Запишите результаты каждого эхо-запроса. В случае необходимости отправьте эхо-запрос на любой другой компьютер.

#### Шаг 5: Просмотрите преобразования NAT на маршрутизаторе R2.

Если NAT работает, в таблице должны быть записи.

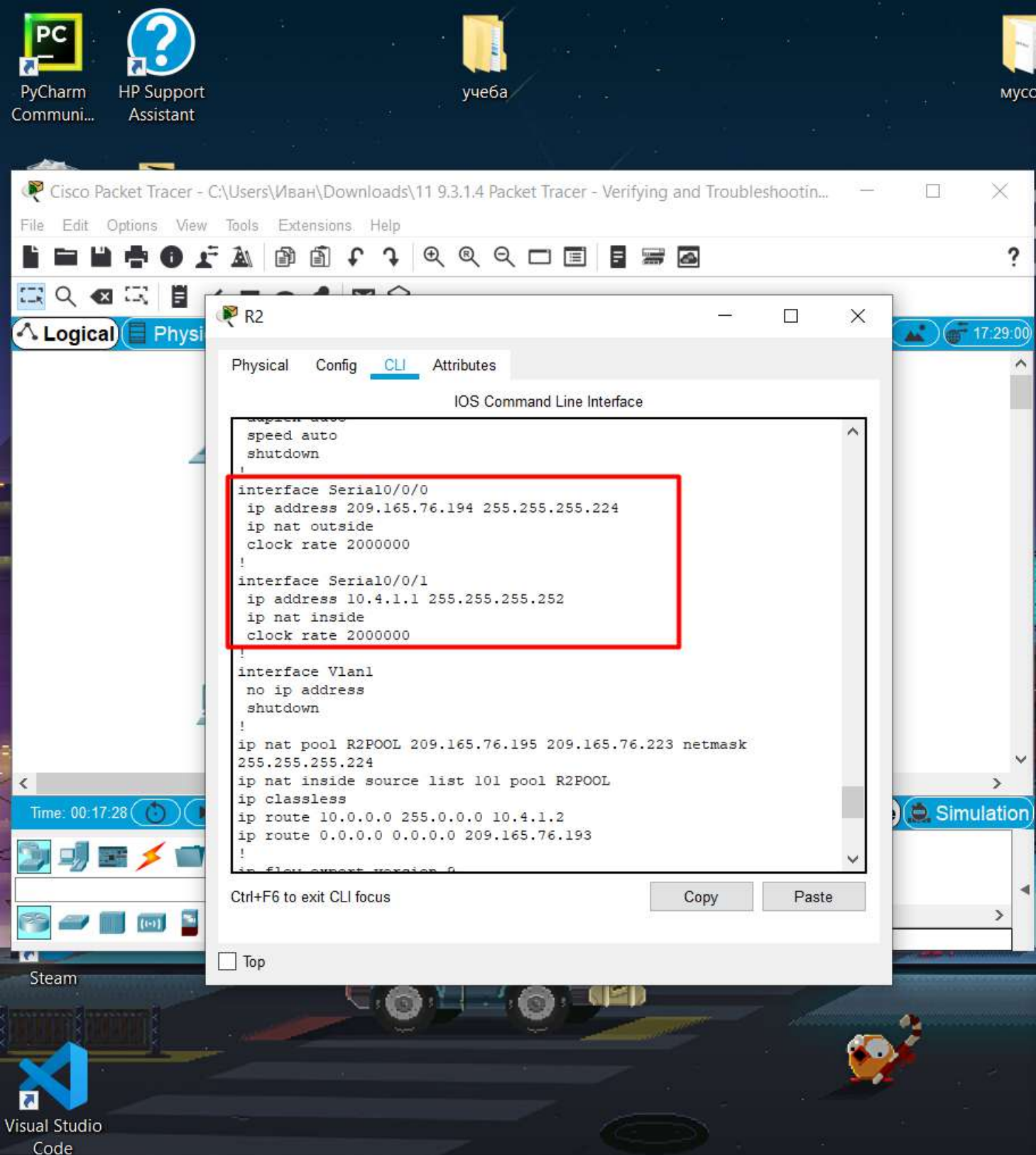
#### Шаг 6: Отобразите список контроля доступа 101 на маршрутизаторе R2.

Шаблонная маска должна охватывать сети 10.4.10.0 и 10.4.11.0.

#### Шаг 7: Внесите изменения в список контроля доступа.

Удалите список контроля доступа `access-list 101` и замените его похожим списком длиной запись. Единственным отличием должна быть шаблонная маска.





011 9.3.1.4 Packet Tracer - Verify

Файл | C:/Users/Иван/De...

2 из 2

### Сценарий

Подрядчик восстановил старую настройку на новом маршрутизаторе с работающим прео NAT. Однако после создания резервной копии старой настройки сеть изменилась, и в нее добавлена новая подсеть. Ваша задача — восстановить работу сети.

### Часть 1: Локализация проблемы

Отправьте эхо-запрос на **Сервер 1** с ПК 1, ПК 2, L1, L2 и R2. Запишите результаты каждого запроса. В случае необходимости отправьте эхо-запрос на любой другой компьютер.

### Часть 2: Отладка настроек NAT

#### Шаг 1: Просмотрите преобразования NAT на маршрутизаторе R2.

Если NAT работает, в таблице должны быть записи.

#### Шаг 2: Просмотрите текущую настройку маршрутизатора R2.

Внутренний порт NAT должен соответствовать частному адресу, а внешний порт NAT должен соответствовать публичному адресу.

#### Шаг 3: Исправьте настройки интерфейсов.

Примените к соответствующим портам команды `ip nat inside` и `ip nat outside`.

#### Шаг 4: Отправьте эхо-запрос на Сервер 1 с ПК 1, ПК 2, L1, L2 и R2.

Запишите результаты каждого эхо-запроса. В случае необходимости отправьте эхо-запрос другой компьютер.

#### Шаг 5: Просмотрите преобразования NAT на маршрутизаторе R2.

Если NAT работает, в таблице должны быть записи.

#### Шаг 6: Отобразите список контроля доступа 101 на маршрутизаторе R2.

Шаблонная маска должна охватывать сети 10.4.10.0 и 10.4.11.0.

#### Шаг 7: Внесите изменения в список контроля доступа.

Удалите список контроля доступа `access-list 101` и замените его похожим списком длиной запись. Единственным отличием должна быть шаблонная маска.



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 64.100.201.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 64.100.201.1

Pinging 64.100.201.1 with 32 bytes of data:

Reply from 64.100.201.1: bytes=32 time=6ms TTL=253
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253
Reply from 64.100.201.1: bytes=32 time=3ms TTL=253
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253

Ping statistics for 64.100.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 6ms, Average = 3ms
```

```
L1
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 64.100.201.1 with 32 bytes of data:

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

Ping statistics for 64.100.201.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 64.100.201.1

Pinging 64.100.201.1 with 32 bytes of data:

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

Ping statistics for 64.100.201.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 64.100.201.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 64.100.201.1

Pinging 64.100.201.1 with 32 bytes of data:

Reply from 64.100.201.1: bytes=32 time=6ms TTL=253
Reply from 64.100.201.1: bytes=32 time=7ms TTL=253
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253
Reply from 64.100.201.1: bytes=32 time=5ms TTL=253

Ping statistics for 64.100.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 7ms, Average = 5ms
```

```
L2
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 64.100.201.1 with 32 bytes of data:

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

Ping statistics for 64.100.201.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 64.100.201.1

Pinging 64.100.201.1 with 32 bytes of data:

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

Ping statistics for 64.100.201.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

```
R2
Physical Config CLI Attributes
IOS Command Line Interface

!
!
line con 0
!
line aux 0
!
line vty 0 4
    login
!
!
end

Kubnov-R2#ping 64.100.201.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.100.201.1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
3/9/32 ms

Kubnov-R2#
```

## Сценарий

Подготовка  
NAT  
документации

## Часть 1

Отправка  
запроса

## Часть 2

### Шаг 1:

Если

### Шаг 2:

Внутренний  
соединение

### Шаг 3: Исправьте настройки интерфейсов.

Примените к соответствующим портам команды `ip nat inside` и `ip nat outside`.

### Шаг 4: Отправьте эхо-запрос на Сервер 1 с ПК 1, ПК 2, L1, L2 и R2.

Запишите результаты каждого эхо-запроса. В случае необходимости отправьте эхо-запрос с другого компьютера.

### Шаг 5: Просмотрите преобразования NAT на маршрутизаторе R2.

Если NAT работает, в таблице должны быть записи.

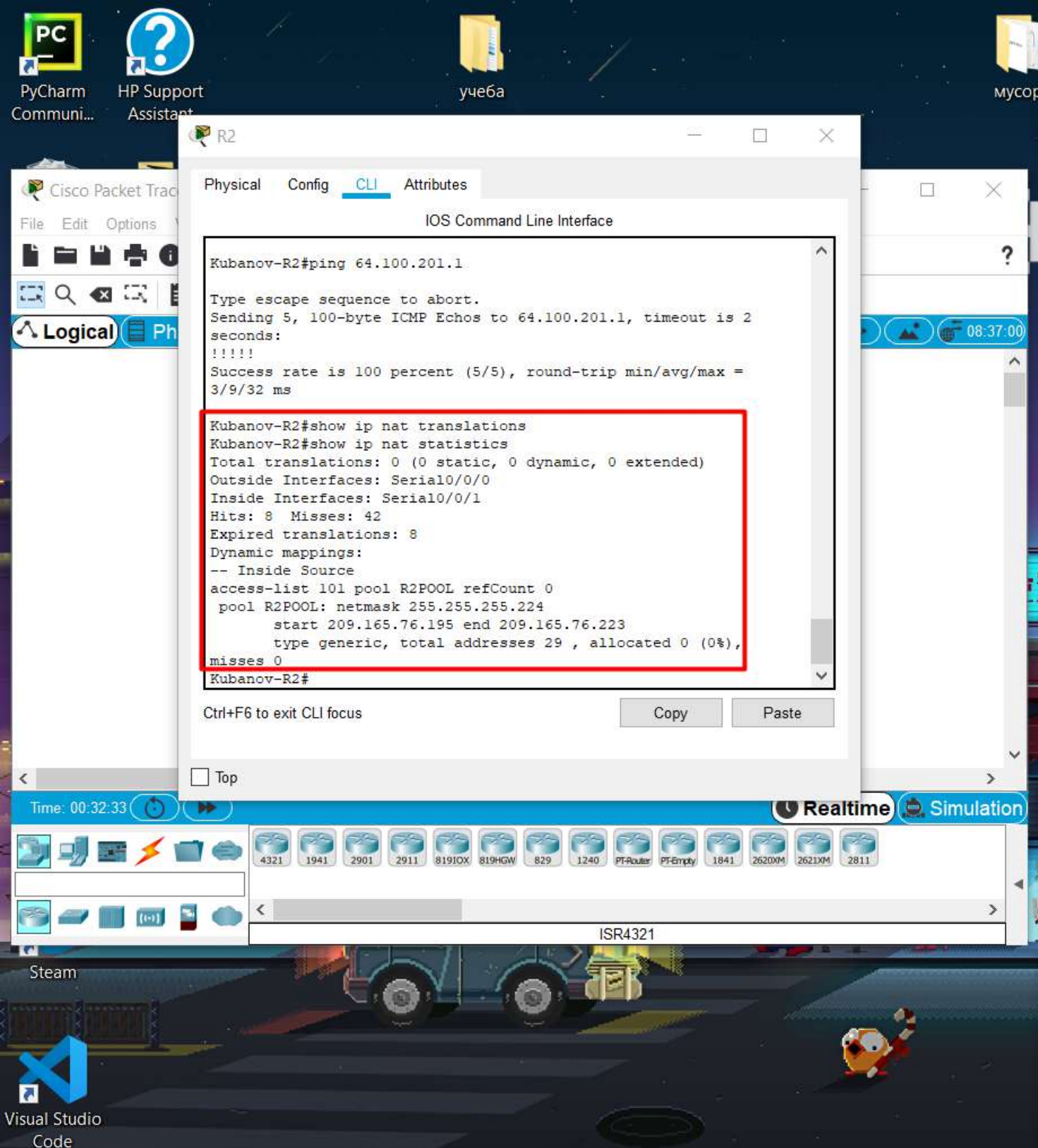
### Шаг 6: Отобразите список контроля доступа 101 на маршрутизаторе R2.

Шаблонная маска должна охватывать сети 10.4.10.0 и 10.4.11.0.

### Шаг 7: Внесите изменения в список контроля доступа.

Удалите список контроля доступа `access-list 101` и замените его похожим списком длиной 1 запись. Единственным отличием должна быть шаблонная маска.





011 9.3.1.4 Packet Tracer - Verify

Файл | C:/Users/Иван/De...

2 из 2

### Сценарий

Подрядчик восстановил старую настройку на новом маршрутизаторе с работающим прео NAT. Однако после создания резервной копии старой настройки сеть изменилась, и в нее добавлена новая подсеть. Ваша задача — восстановить работу сети.

### Часть 1: Локализация проблемы

Отправьте эхо-запрос на **Сервер 1** с ПК 1, ПК 2, L1, L2 и R2. Запишите результаты каждого запроса. В случае необходимости отправьте эхо-запрос на любой другой компьютер.

### Часть 2: Отладка настроек NAT

#### Шаг 1: Просмотрите преобразования NAT на маршрутизаторе R2.

Если NAT работает, в таблице должны быть записи.

#### Шаг 2: Просмотрите текущую настройку маршрутизатора R2.

Внутренний порт NAT должен соответствовать частному адресу, а внешний порт NAT дог соответствовать публичному адресу.

#### Шаг 3: Исправьте настройки интерфейсов.

Примените к соответствующим портам команды `ip nat inside` и `ip nat outside`.

#### Шаг 4: Отправьте эхо-запрос на Сервер 1 с ПК 1, ПК 2, L1, L2 и R2.

Запишите результаты каждого эхо-запроса. В случае необходимости отправьте эхо-запрс другой компьютер.

#### Шаг 5: Просмотрите преобразования NAT на маршрутизаторе R2.

Если NAT работает, в таблице должны быть записи.

#### Шаг 6: Отобразите список контроля доступа 101 на маршрутизаторе R2.

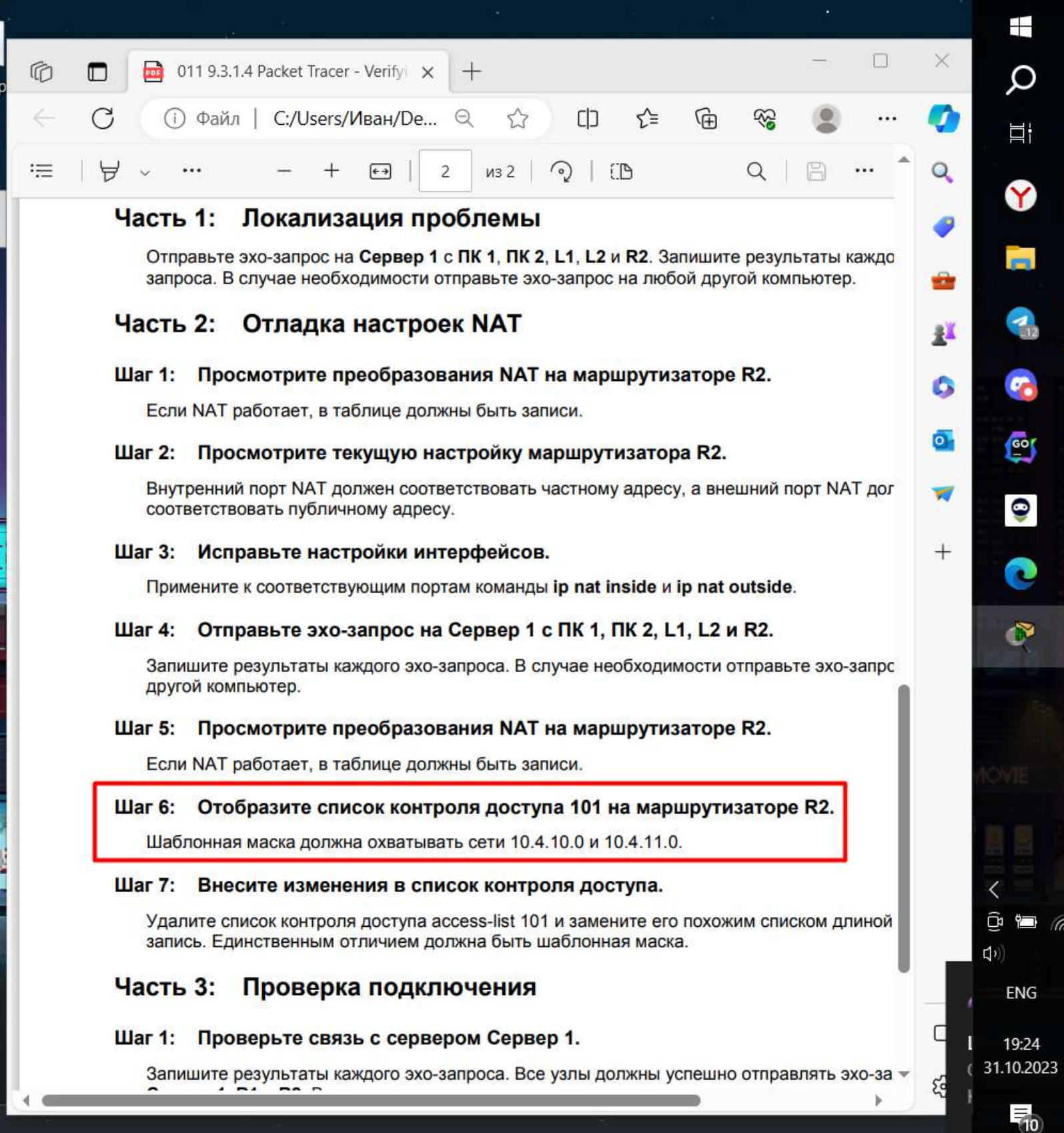
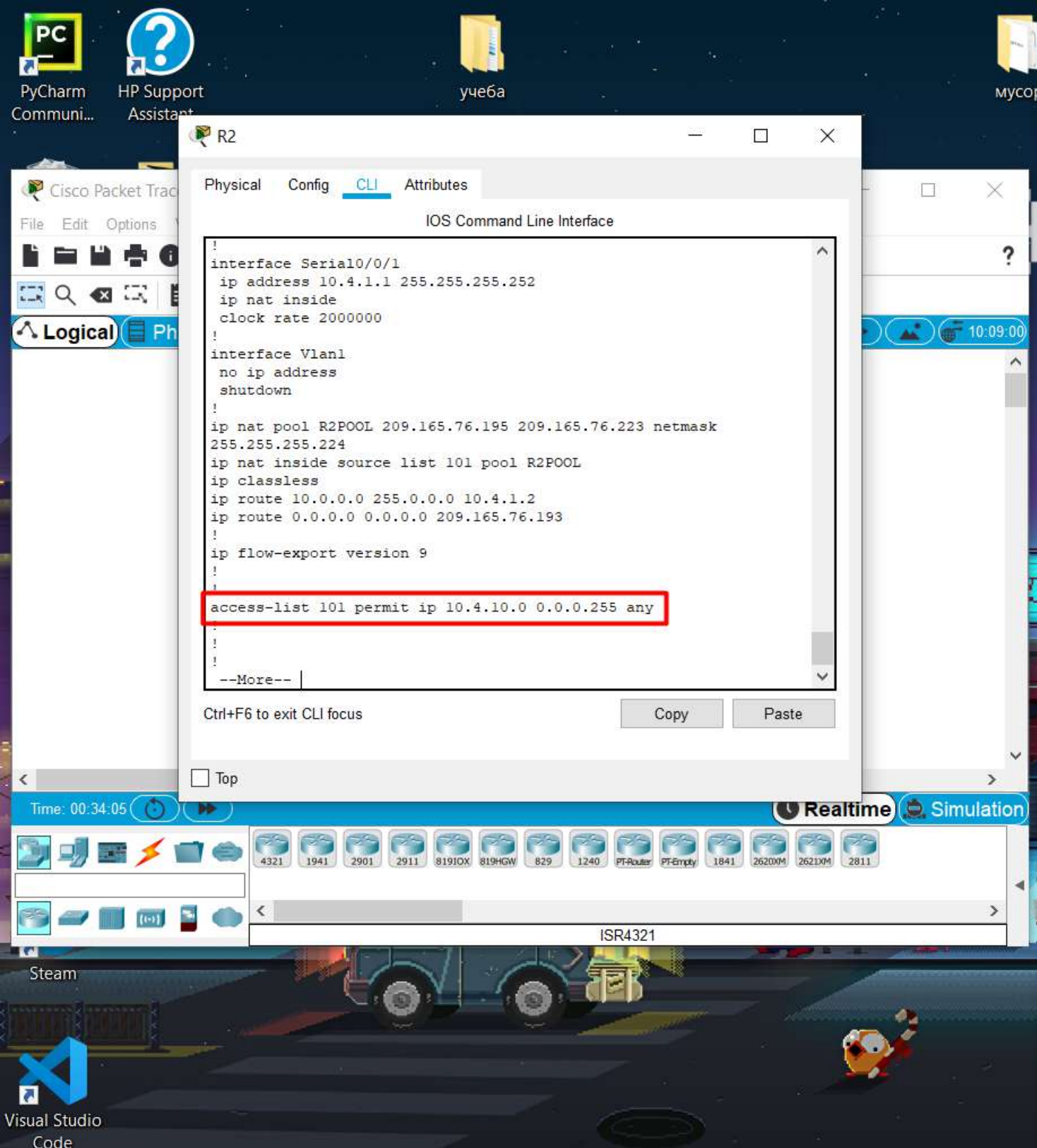
Шаблонная маска должна охватывать сети 10.4.10.0 и 10.4.11.0.

#### Шаг 7: Внесите изменения в список контроля доступа.

Удалите список контроля доступа access-list 101 и замените его похожим списком длиной запись. Единственным отличием должна быть шаблонная маска.

РУС 19:23 31.10.2023











PyCharm Communi... HP Support Assistant

учеба

мусор

Cisco Packet Tracer

Physical Config CLI Attributes

IOS Command Line Interface

```
!
interface Serial10/0/1
 ip address 10.4.1.1 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
ip nat pool R2POOL 209.165.76.195 209.165.76.223 netmask 255.255.255.224
ip nat inside source list 101 pool R2POOL
ip classless
ip route 10.0.0.0 255.0.0.0 10.4.1.2
ip route 0.0.0.0 0.0.0.0 209.165.76.193
!
ip flow-export version 9
!
access-list 101 permit ip 10.4.10.0 0.0.1.255 any
!
!
--More--
```

Ctrl+F6 to exit CLI focus

Copy Paste

Time: 00:37:13

Realtime Simulation

ISR4321

Steam

Visual Studio Code

011 9.3.1.4 Packet Tracer - Verify

Файл C:/Users/Иван/De...

2 из 2

### Шаг 1: Просмотрите преобразования NAT на маршрутизаторе R2.

Если NAT работает, в таблице должны быть записи.

### Шаг 2: Просмотрите текущую настройку маршрутизатора R2.

Внутренний порт NAT должен соответствовать частному адресу, а внешний порт NAT должен соответствовать публичному адресу.

### Шаг 3: Исправьте настройки интерфейсов.

Примените к соответствующим портам команды `ip nat inside` и `ip nat outside`.

### Шаг 4: Отправьте эхо-запрос на Сервер 1 с ПК 1, ПК 2, L1, L2 и R2.

Запишите результаты каждого эхо-запроса. В случае необходимости отправьте эхо-запрос на любой другой компьютер.

### Шаг 5: Просмотрите преобразования NAT на маршрутизаторе R2.

Если NAT работает, в таблице должны быть записи.

### Шаг 6: Отобразите список контроля доступа 101 на маршрутизаторе R2.

Шаблонная маска должна охватывать сети 10.4.10.0 и 10.4.11.0.

### Шаг 7: Внесите изменения в список контроля доступа.

Удалите список контроля доступа `access-list 101` и замените его похожим списком длиной также в одну запись. Единственным отличием должна быть шаблонная маска.

## Часть 3: Проверка подключения

### Шаг 1: Проверьте связь с сервером Сервер 1.

Запишите результаты каждого эхо-запроса. Все узлы должны успешно отправлять эхо-запросы на Сервер 1, R1 и R2. В случае непрохождения эхо-запросов выполните отладку.

### Шаг 2: Просмотрите преобразования NAT на маршрутизаторе R2.

Таблица NAT должна содержать несколько записей.

ENG

19:27 31.10.2023



PC1

Physical Config Desktop Programming Attributes

Command Prompt

Reply from 64.100.201.1: bytes=32 time=3ms TTL=253  
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253

Ping statistics for 64.100.201.1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 2ms, Maximum = 6ms, Average = 3ms

C:\>ping 64.100.201.1

Pinging 64.100.201.1 with 32 bytes of data:

Reply from 64.100.201.1: bytes=32 time=2ms TTL=253  
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253  
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253  
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253

Ping statistics for 64.100.201.1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 2ms, Maximum = 2ms, Average = 2ms

PC2

Physical Config Desktop Programming Attributes

Command Prompt

Reply from 64.100.201.1: bytes=32 time=2ms TTL=253  
Reply from 64.100.201.1: bytes=32 time=5ms TTL=253

Ping statistics for 64.100.201.1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 2ms, Maximum = 7ms, Average = 5ms

C:\>ping 64.100.201.1

Pinging 64.100.201.1 with 32 bytes of data:

Reply from 64.100.201.1: bytes=32 time=2ms TTL=253  
Reply from 64.100.201.1: bytes=32 time=8ms TTL=253  
Reply from 64.100.201.1: bytes=32 time=6ms TTL=253  
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253

Ping statistics for 64.100.201.1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 2ms, Maximum = 8ms, Average = 4ms

L1

Physical Config Desktop Programming Attributes

Command Prompt

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

Ping statistics for 64.100.201.1:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 64.100.201.1

Pinging 64.100.201.1 with 32 bytes of data:

Reply from 64.100.201.1: bytes=32 time=16ms TTL=253  
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253  
Reply from 64.100.201.1: bytes=32 time=7ms TTL=253  
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253

Ping statistics for 64.100.201.1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 2ms, Maximum = 16ms, Average = 6ms

C:\>

L2

Physical Config Desktop Programming Attributes

Command Prompt

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

Ping statistics for 64.100.201.1:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 64.100.201.1

Pinging 64.100.201.1 with 32 bytes of data:

Reply from 64.100.201.1: bytes=32 time=9ms TTL=253  
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253  
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253  
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253

Ping statistics for 64.100.201.1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 2ms, Maximum = 9ms, Average = 3ms

C:\>

011 9.3.1.4 Packet Tracer - Verify

Файл | C:/Users/Иван...

2 из 2

Внутренний порт NAT должен соответствовать частному адресу, а внешний порт N. соответствовать публичному адресу.

**Шаг 3: Исправьте настройки интерфейсов.**  
Примените к соответствующим портам команды `ip nat inside` и `ip nat outside`.

**Шаг 4: Отправьте эхо-запрос на Сервер 1 с ПК 1, ПК 2, L1, L2 и R2.**  
Запишите результаты каждого эхо-запроса. В случае необходимости отправьте эхо-запрос с другого компьютера.

**Шаг 5: Просмотрите преобразования NAT на маршрутизаторе R2.**  
Если NAT работает, в таблице должны быть записи.

**Шаг 6: Отобразите список контроля доступа 101 на маршрутизаторе R2.**  
Шаблонная маска должна охватывать сети 10.4.10.0 и 10.4.11.0.

**Шаг 7: Внесите изменения в список контроля доступа.**  
Удалите список контроля доступа `access-list 101` и замените его похожим списком с записью. Единственным отличием должна быть шаблонная маска.

**Часть 3: Проверка подключения**

**Шаг 1: Проверьте связь с сервером Сервер 1.**  
Запишите результаты каждого эхо-запроса. Все узлы должны успешно отправлять эхо-запросы на Сервер 1, R1 и R2. В случае непрохождения эхо-запросов выполните отладку.

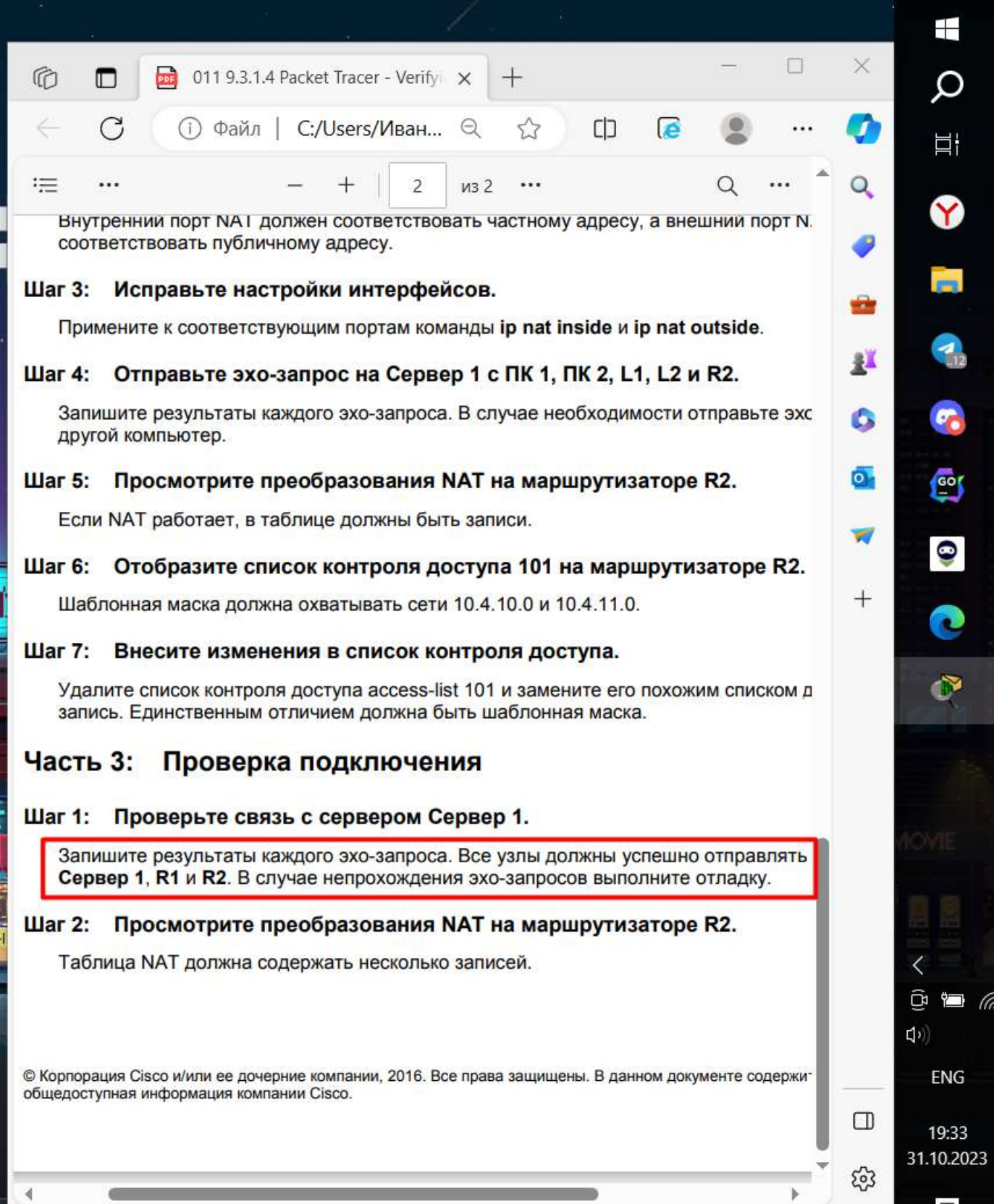
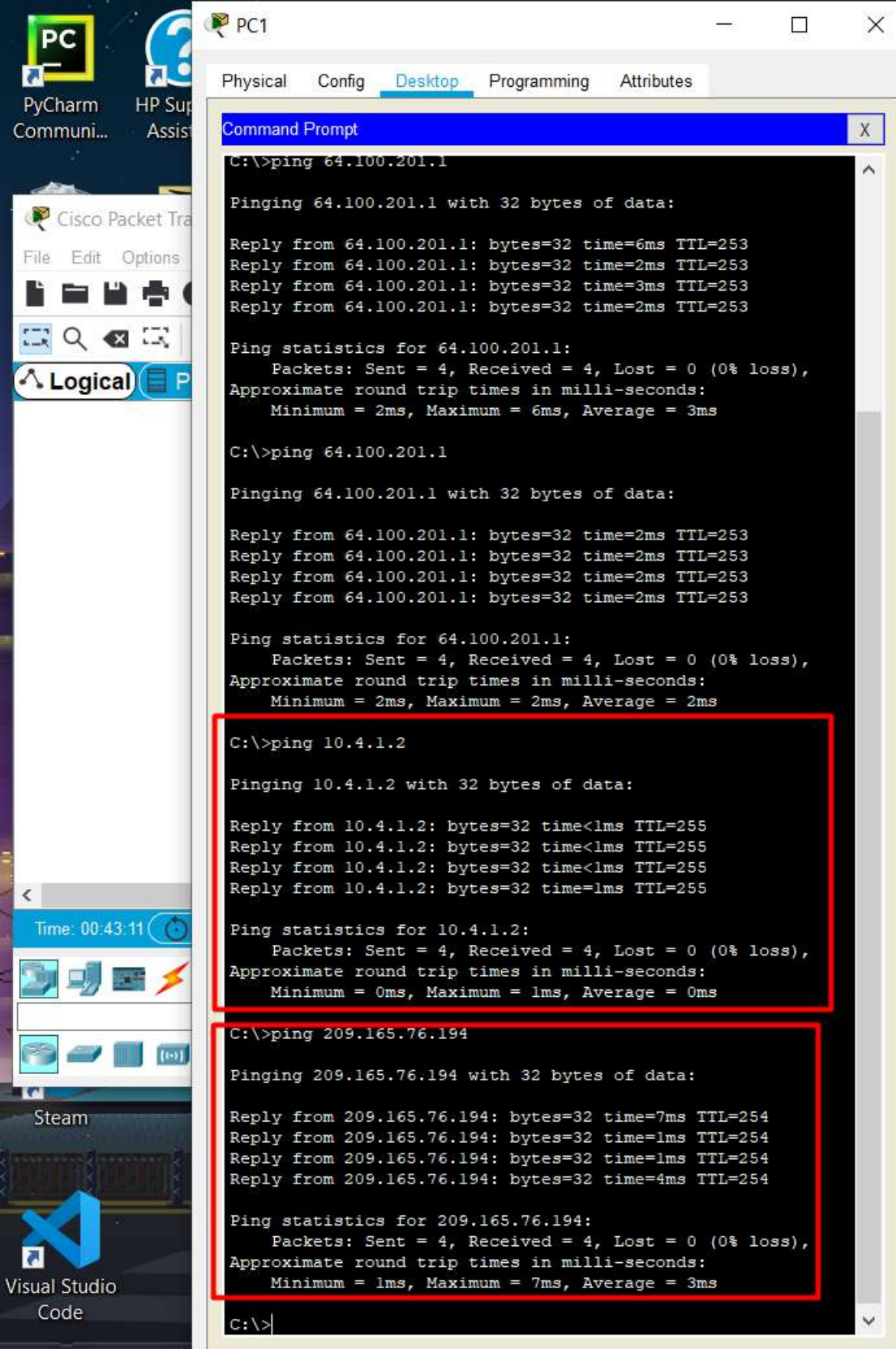
**Шаг 2: Просмотрите преобразования NAT на маршрутизаторе R2.**  
Таблица NAT должна содержать несколько записей.

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

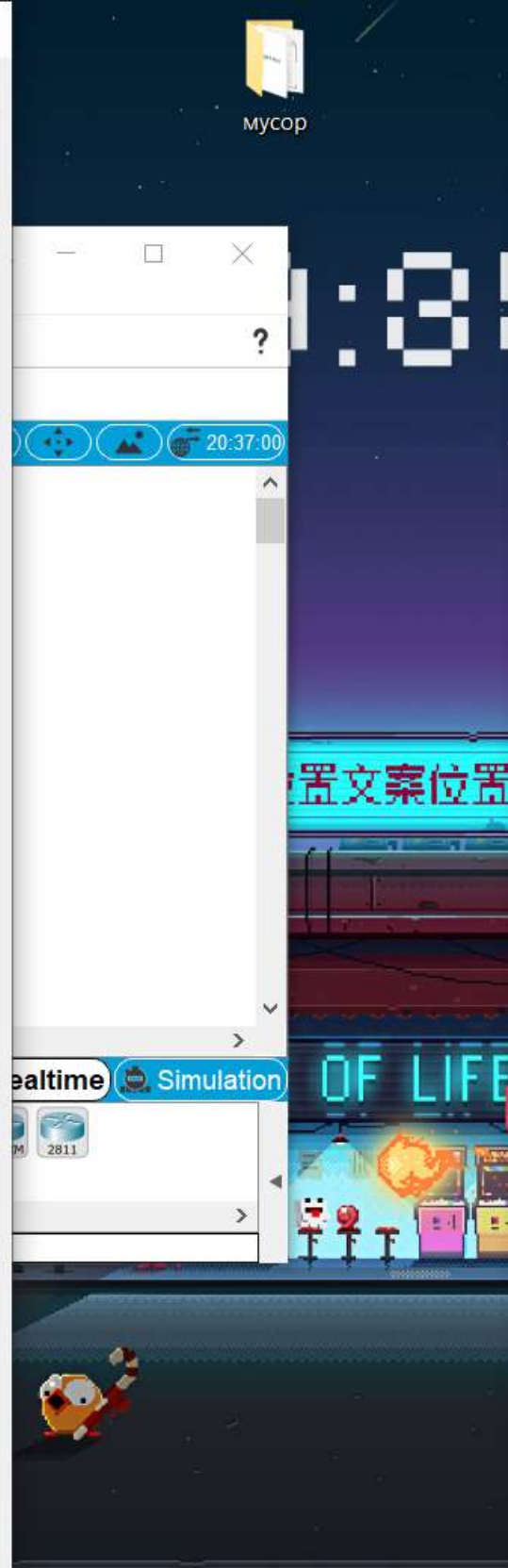
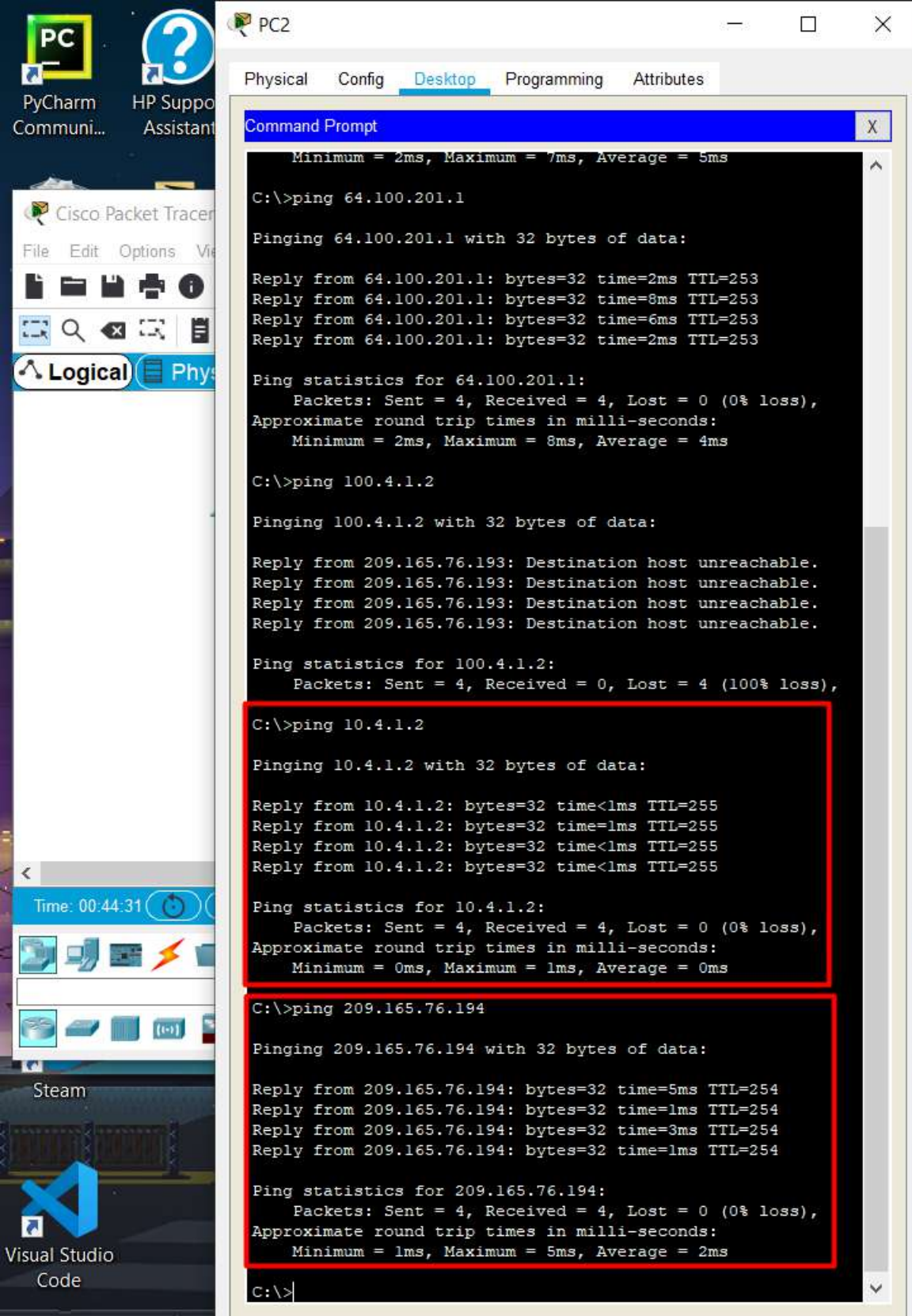
ENG

19:31  
31.10.2023









011 9.3.1.4 Packet Tracer - Verify

Файл | C:/Users/Иван...

Внутренний порт NAT должен соответствовать частному адресу, а внешний порт N. соответствовать публичному адресу.

**Шаг 3: Исправьте настройки интерфейсов.**

Примените к соответствующим портам команды `ip nat inside` и `ip nat outside`.

**Шаг 4: Отправьте эхо-запрос на Сервер 1 с ПК 1, ПК 2, L1, L2 и R2.**

Запишите результаты каждого эхо-запроса. В случае необходимости отправьте эхс другой компьютер.

**Шаг 5: Просмотрите преобразования NAT на маршрутизаторе R2.**

Если NAT работает, в таблице должны быть записи.

**Шаг 6: Отобразите список контроля доступа 101 на маршрутизаторе R2.**

Шаблонная маска должна охватывать сети 10.4.10.0 и 10.4.11.0.

**Шаг 7: Внесите изменения в список контроля доступа.**

Удалите список контроля доступа `access-list 101` и замените его похожим списком д запись. Единственным отличием должна быть шаблонная маска.

**Часть 3: Проверка подключения**

**Шаг 1: Проверьте связь с сервером Сервер 1.**

Запишите результаты каждого эхо-запроса. Все узлы должны успешно отправлять **Сервер 1, R1 и R2**. В случае непрохождения эхо-запросов выполните отладку.

**Шаг 2: Просмотрите преобразования NAT на маршрутизаторе R2.**

Таблица NAT должна содержать несколько записей.

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержи- общедоступная информация компании Cisco.

ENG

19:35  
31.10.2023





```
Physical Config Desktop Programming Attributes
Command Prompt
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 64.100.201.1
Pinging 64.100.201.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 64.100.201.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 64.100.201.1
Pinging 64.100.201.1 with 32 bytes of data:
Reply from 64.100.201.1: bytes=32 time=16ms TTL=253
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253
Reply from 64.100.201.1: bytes=32 time=7ms TTL=253
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253
Ping statistics for 64.100.201.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 16ms, Average = 6ms
C:\>ping 10.4.1.2
Pinging 10.4.1.2 with 32 bytes of data:
Reply from 10.4.1.2: bytes=32 time<1ms TTL=255
Reply from 10.4.1.2: bytes=32 time<1ms TTL=255
Reply from 10.4.1.2: bytes=32 time<1ms TTL=255
Reply from 10.4.1.2: bytes=32 time<1ms TTL=255
Ping statistics for 10.4.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 209.165.76.194
Pinging 209.165.76.194 with 32 bytes of data:
Reply from 209.165.76.194: bytes=32 time=5ms TTL=254
Reply from 209.165.76.194: bytes=32 time=4ms TTL=254
Reply from 209.165.76.194: bytes=32 time=2ms TTL=254
Reply from 209.165.76.194: bytes=32 time=1ms TTL=254
Ping statistics for 209.165.76.194:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 5ms, Average = 3ms
C:\>
```



011 9.3.1.4 Packet Tracer - Verify

Файл | C:/Users/Иван...

Внутренний порт NAT должен соответствовать частному адресу, а внешний порт N. соответствовать публичному адресу.

**Шаг 3: Исправьте настройки интерфейсов.**

Примените к соответствующим портам команды `ip nat inside` и `ip nat outside`.

**Шаг 4: Отправьте эхо-запрос на Сервер 1 с ПК 1, ПК 2, L1, L2 и R2.**

Запишите результаты каждого эхо-запроса. В случае необходимости отправьте эхс другой компьютер.

**Шаг 5: Просмотрите преобразования NAT на маршрутизаторе R2.**

Если NAT работает, в таблице должны быть записи.

**Шаг 6: Отобразите список контроля доступа 101 на маршрутизаторе R2.**

Шаблонная маска должна охватывать сети 10.4.10.0 и 10.4.11.0.

**Шаг 7: Внесите изменения в список контроля доступа.**

Удалите список контроля доступа `access-list 101` и замените его похожим списком д запись. Единственным отличием должна быть шаблонная маска.

**Часть 3: Проверка подключения**

**Шаг 1: Проверьте связь с сервером Сервер 1.**

Запишите результаты каждого эхо-запроса. Все узлы должны успешно отправлять Сервер 1, R1 и R2. В случае непрохождения эхо-запросов выполните отладку.

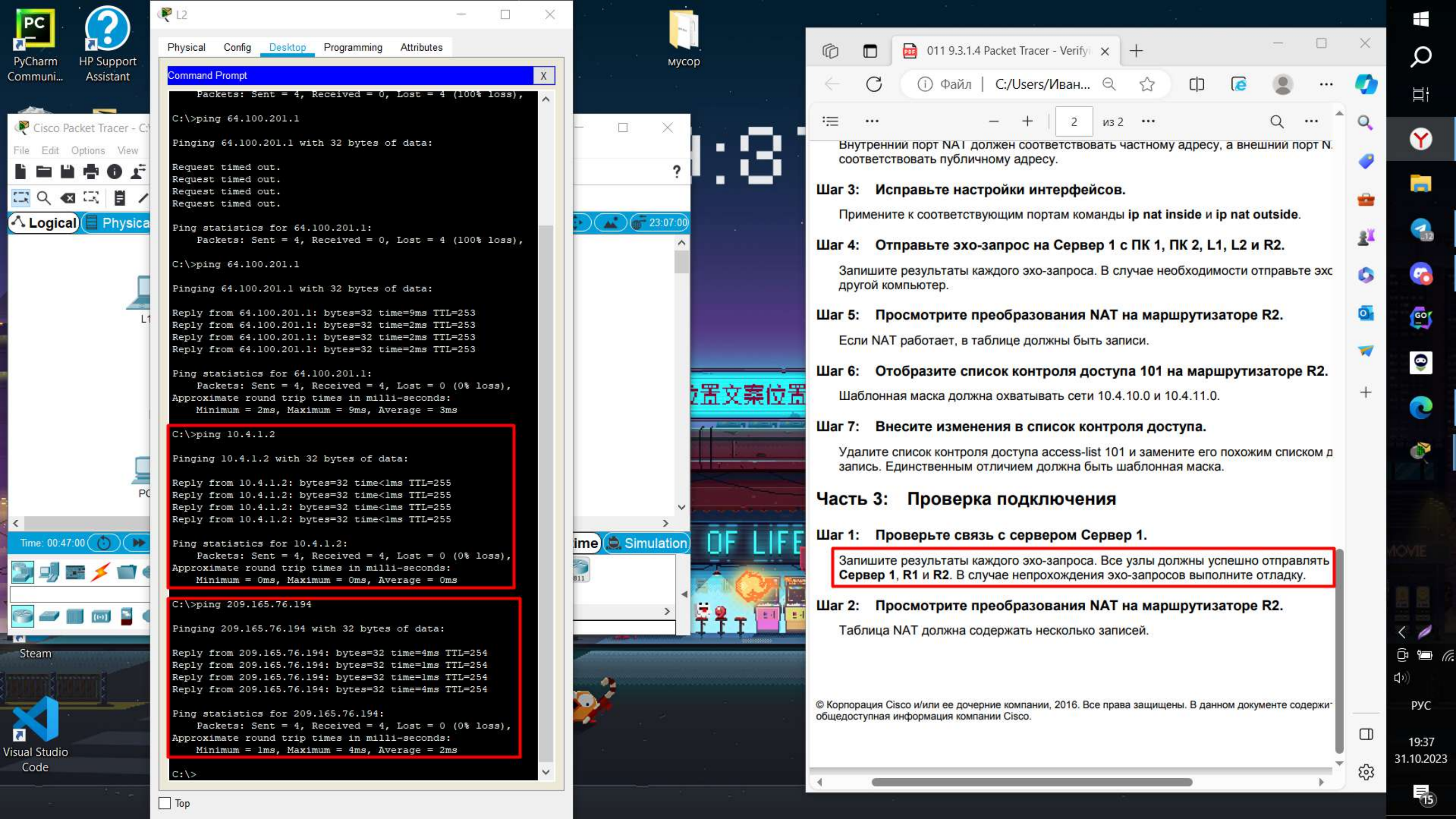
**Шаг 2: Просмотрите преобразования NAT на маршрутизаторе R2.**

Таблица NAT должна содержать несколько записей.

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержи общедоступная информация компании Cisco.







Physical Config **Desktop** Programming Attributes

Command Prompt X

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 64.100.201.1

Pinging 64.100.201.1 with 32 bytes of data:

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

Ping statistics for 64.100.201.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 64.100.201.1

Pinging 64.100.201.1 with 32 bytes of data:

Reply from 64.100.201.1: bytes=32 time=9ms TTL=253
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253
Reply from 64.100.201.1: bytes=32 time=2ms TTL=253

Ping statistics for 64.100.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 9ms, Average = 3ms

C:\>ping 10.4.1.2

Pinging 10.4.1.2 with 32 bytes of data:

Reply from 10.4.1.2: bytes=32 time<1ms TTL=255
Reply from 10.4.1.2: bytes=32 time<1ms TTL=255
Reply from 10.4.1.2: bytes=32 time<1ms TTL=255
Reply from 10.4.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.4.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 209.165.76.194

Pinging 209.165.76.194 with 32 bytes of data:

Reply from 209.165.76.194: bytes=32 time=4ms TTL=254
Reply from 209.165.76.194: bytes=32 time=1ms TTL=254
Reply from 209.165.76.194: bytes=32 time=1ms TTL=254
Reply from 209.165.76.194: bytes=32 time=4ms TTL=254

Ping statistics for 209.165.76.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\>
```

011 9.3.1.4 Packet Tracer - Verify X

Файл | C:/Users/Иван...

2 из 2

Внутренний порт NAT должен соответствовать частному адресу, а внешний порт N. соответствовать публичному адресу.

**Шаг 3: Исправьте настройки интерфейсов.**

Примените к соответствующим портам команды `ip nat inside` и `ip nat outside`.

**Шаг 4: Отправьте эхо-запрос на Сервер 1 с ПК 1, ПК 2, L1, L2 и R2.**

Запишите результаты каждого эхо-запроса. В случае необходимости отправьте эхс другой компьютер.

**Шаг 5: Просмотрите преобразования NAT на маршрутизаторе R2.**

Если NAT работает, в таблице должны быть записи.

**Шаг 6: Отобразите список контроля доступа 101 на маршрутизаторе R2.**

Шаблонная маска должна охватывать сети 10.4.10.0 и 10.4.11.0.

**Шаг 7: Внесите изменения в список контроля доступа.**

Удалите список контроля доступа `access-list 101` и замените его похожим списком д запись. Единственным отличием должна быть шаблонная маска.

### Часть 3: Проверка подключения

**Шаг 1: Проверьте связь с сервером Сервер 1.**

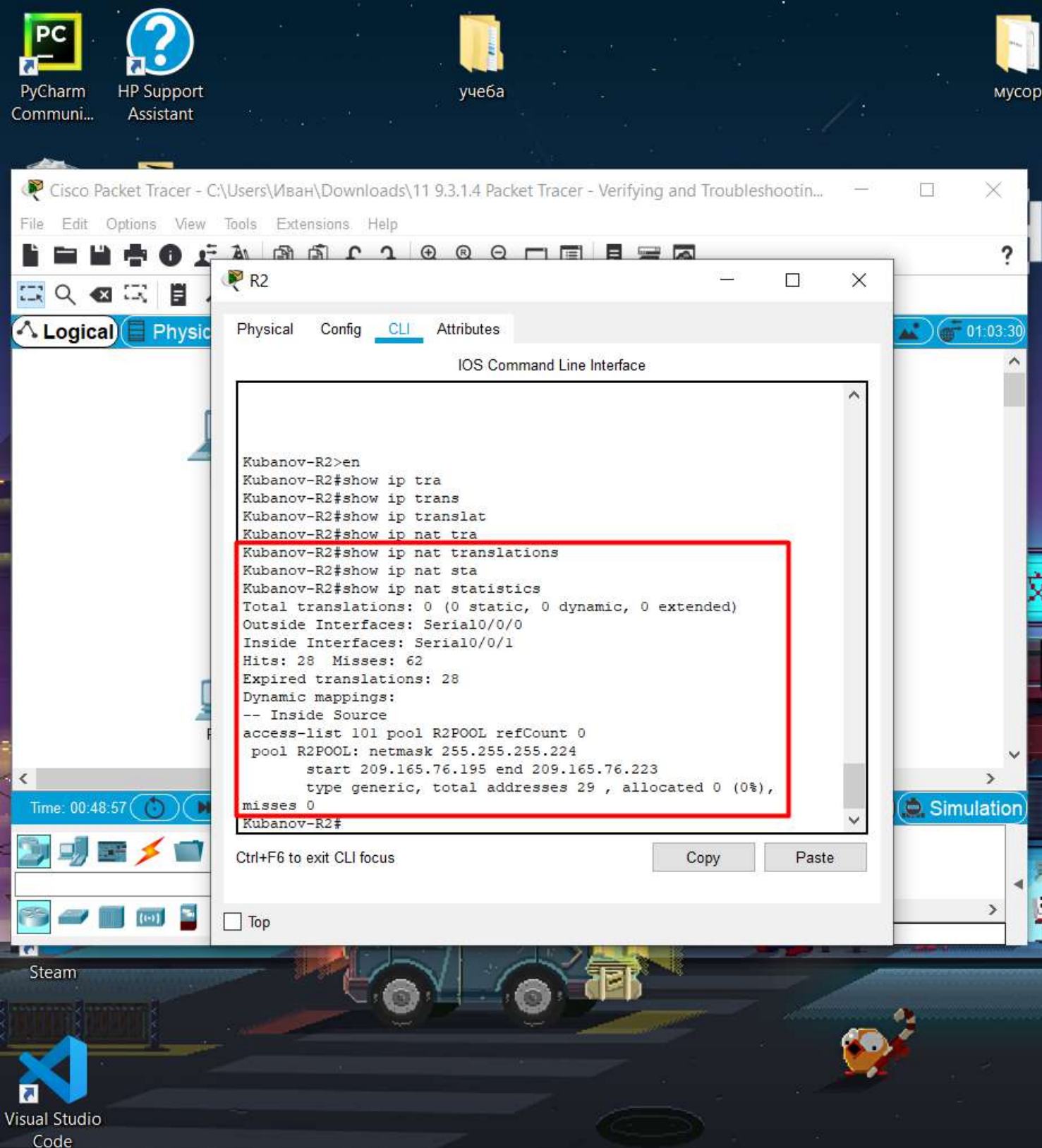
Запишите результаты каждого эхо-запроса. Все узлы должны успешно отправлять **Сервер 1, R1 и R2**. В случае непрохождения эхо-запросов выполните отладку.

**Шаг 2: Просмотрите преобразования NAT на маршрутизаторе R2.**

Таблица NAT должна содержать несколько записей.

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержи- общедоступная информация компании Cisco.





011 9.3.1.4 Packet Tracer - Verify x +

Файл | C:/Users/Иван... 2 из 2

Внутренний порт NAT должен соответствовать частному адресу, а внешний порт N. соответствовать публичному адресу.

**Шаг 3: Исправьте настройки интерфейсов.**

Примените к соответствующим портам команды `ip nat inside` и `ip nat outside`.

**Шаг 4: Отправьте эхо-запрос на Сервер 1 с ПК 1, ПК 2, L1, L2 и R2.**

Запишите результаты каждого эхо-запроса. В случае необходимости отправьте эхо другой компьютер.

**Шаг 5: Просмотрите преобразования NAT на маршрутизаторе R2.**

Если NAT работает, в таблице должны быть записи.

**Шаг 6: Отобразите список контроля доступа 101 на маршрутизаторе R2.**

Шаблонная маска должна охватывать сети 10.4.10.0 и 10.4.11.0.

**Шаг 7: Внесите изменения в список контроля доступа.**

Удалите список контроля доступа `access-list 101` и замените его похожим списком д запись. Единственным отличием должна быть шаблонная маска.

**Часть 3: Проверка подключения**

**Шаг 1: Проверьте связь с сервером Сервер 1.**

Запишите результаты каждого эхо-запроса. Все узлы должны успешно отправлять **Сервер 1, R1 и R2**. В случае непрохождения эхо-запросов выполните отладку.

**Шаг 2: Просмотрите преобразования NAT на маршрутизаторе R2.**

Таблица NAT должна содержать несколько записей.

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержи- общедоступная информация компании Cisco.

ENG 19:39 31.10.2023



PyCharm Communi... HP Support Assistant

учеба мусор

Cisco Packet Tracer - C:\Users\Иван\Downloads\11 9.3.1.4 Packet Tracer - Verifying and Troubleshootin...

File Edit Options View Tools Extensions Help

Logical Physical x: 875, y: 81 [Root] 02:18:30

PT Activity: 00:50:19

Packet Tracer. Проверка и отладка настроек NAT

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
R1	G0/0	10.4.10.254	255.255.255.0
	G0/1	10.4.11.254	255.255.255.0
	S0/0/1	10.4.1.2	255.255.255.252

Time Elapsed: 00:50:19 Completion: 100/100

1/1

Time: 00:50:12 Realtime Simulation

4321 1941 2901 2911 8191OX 8191GW 829 1240 PTF-Router PTF-Empty 1841 2620XM 2621XM 2811

2621XM

Steam Visual Studio Code

011 9.3.1.4 Packet Tracer - Verify x +

Файл | C:/Users/Иван...

2 из 2

Внутренний порт NAT должен соответствовать частному адресу, а внешний порт N. соответствовать публичному адресу.

**Шаг 3: Исправьте настройки интерфейсов.**

Примените к соответствующим портам команды `ip nat inside` и `ip nat outside`.

**Шаг 4: Отправьте эхо-запрос на Сервер 1 с ПК 1, ПК 2, L1, L2 и R2.**

Запишите результаты каждого эхо-запроса. В случае необходимости отправьте эхс другой компьютер.

**Шаг 5: Просмотрите преобразования NAT на маршрутизаторе R2.**

Если NAT работает, в таблице должны быть записи.

**Шаг 6: Отобразите список контроля доступа 101 на маршрутизаторе R2.**

Шаблонная маска должна охватывать сети 10.4.10.0 и 10.4.11.0.

**Шаг 7: Внесите изменения в список контроля доступа.**

Удалите список контроля доступа `access-list 101` и замените его похожим списком д запись. Единственным отличием должна быть шаблонная маска.

**Часть 3: Проверка подключения**

**Шаг 1: Проверьте связь с сервером Сервер 1.**

Запишите результаты каждого эхо-запроса. Все узлы должны успешно отправлять **Сервер 1, R1 и R2**. В случае непрохождения эхо-запросов выполните отладку.

**Шаг 2: Просмотрите преобразования NAT на маршрутизаторе R2.**

Таблица NAT должна содержать несколько записей.

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержи общедоступная информация компании Cisco.

ENG 19:40 31.10.2023