

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ  
ІМ. І. СІКОРСЬКОГО”

ФАКУЛЬТЕТ ІНФОРМАТИКИ ТА ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ  
КАФЕДРА ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

ЛАБОРАТОРНА РОБОТА №6  
З курсу  
«Мобільні комп’ютерні мережі»

Виконав:  
студент групи ІП-01  
Пашковський Євгеній

Київ — 2023

**Тема:** планування міжмережових екранів.

**Мета роботи:** отримання навичок розміщення брандмауерів в підходящих місцях, що задовольняють вимогам безпеки.

### Сценарій 1. Захист мережі від хакерів.

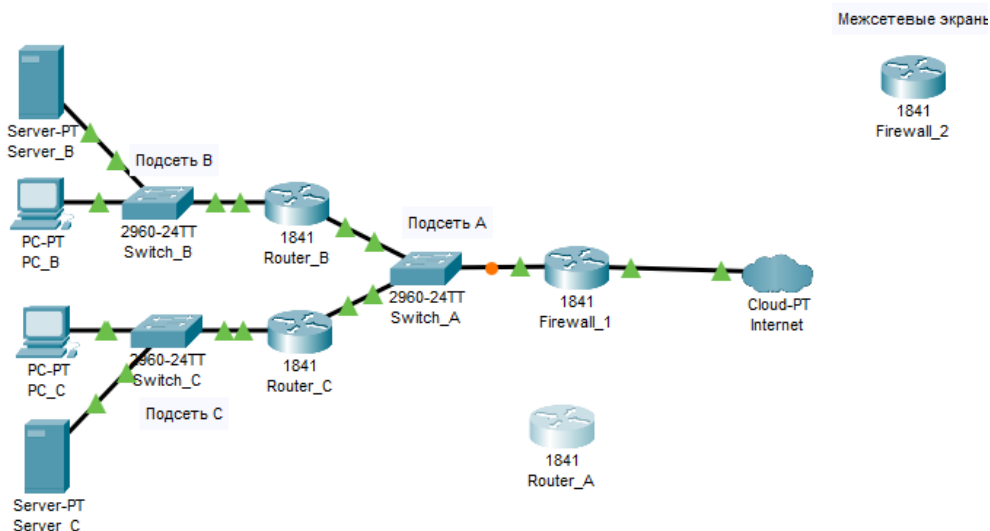
Так як в компанії підвищені вимоги до безпеки, рекомендується встановити міжмережовий екран для захисту мережі від хакерів, працюючих в Інтернеті. Дуже важливо обмежити доступ до внутрішньої мережі з Інтернету.

В міжмережевому екрані Firewall\_1 попередньо налаштовані правила для забезпечення необхідної клієнту безпеки. Встановіть цей брандмауер в мережі клієнта і перевірте правильність його функціонування.

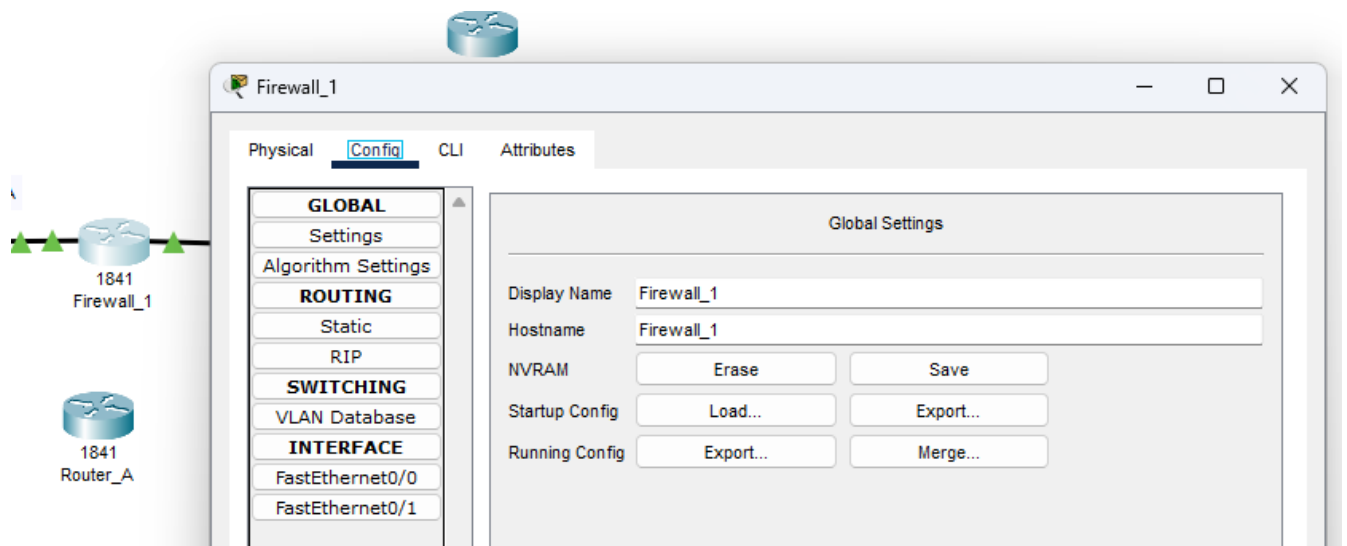
#### Крок 1. Заміна маршрутизатора Router\_A брандмауером Firewall\_1.

а. Демонтуйте маршрутизатор Router\_A і замініть його брандмауером Firewall\_1 Підключіть інтерфейс технології Fast Ethernet 0/0 брандмауера Firewall\_1 до інтерфейсу Fast Ethernet 0/1 комутатора Switch\_A.

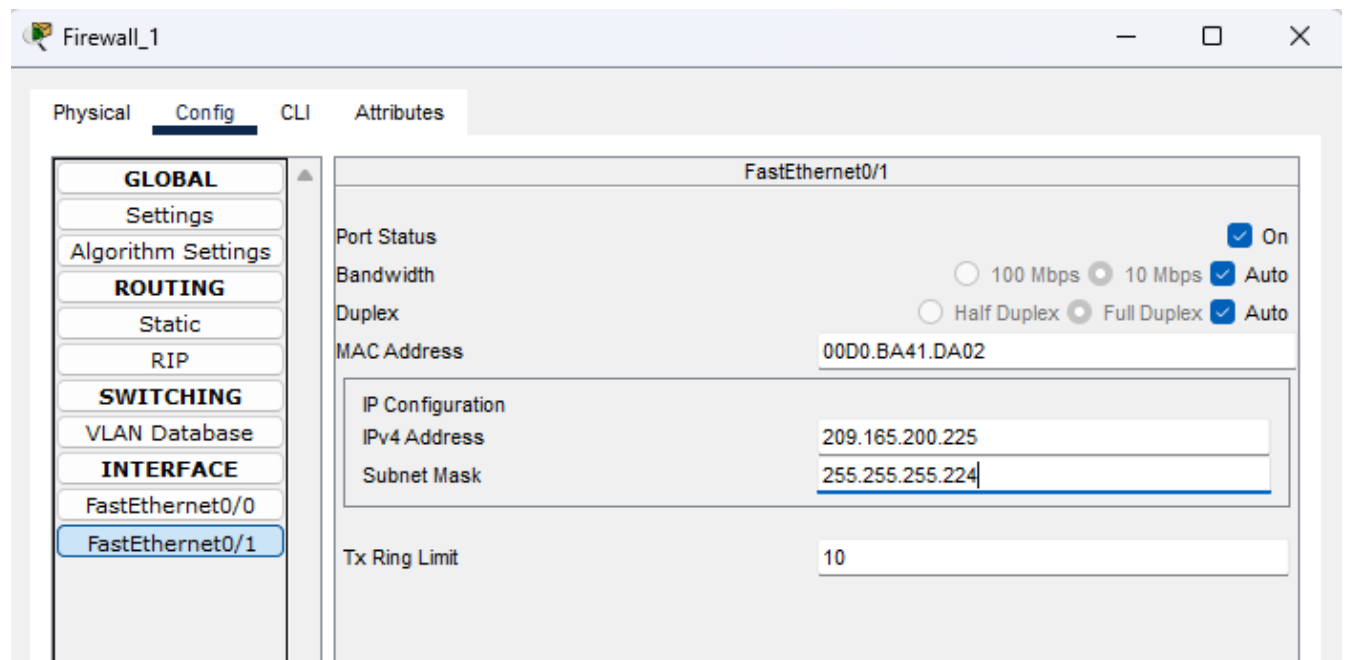
б. Підключіть інтерфейс Fast Ethernet 0/1 брандмауера Firewall\_1 до інтерфейсу Ethernet 6 хмари мережі ISP. (Використовуйте прямий кабель для обох сполук.)



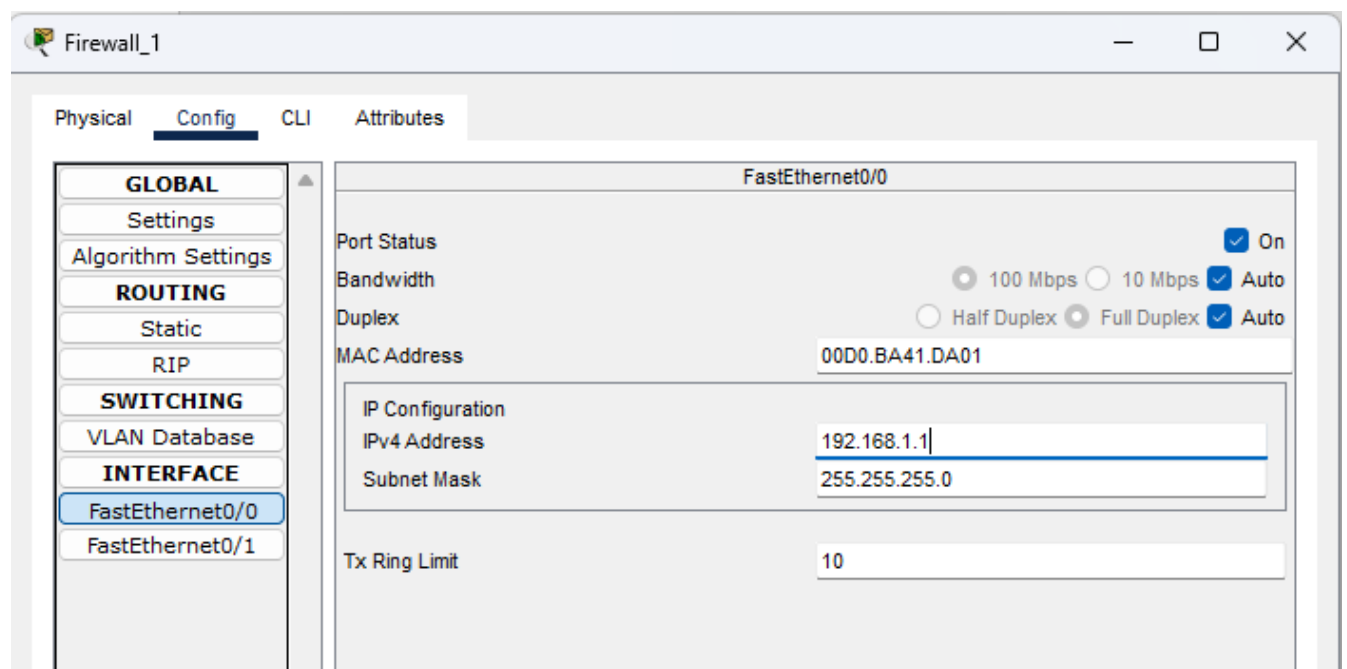
в. Підтвердіть ім'я мережевого вузла для Firewall\_1 - "Firewall\_1".



г. На Firewall\_1 налаштуйте IP-адресу глобальної мережі та маску підмережі для інтерфейсу Fast Ethernet 0/1 209.165.200.225 і 255.255.255.224, відповідно.

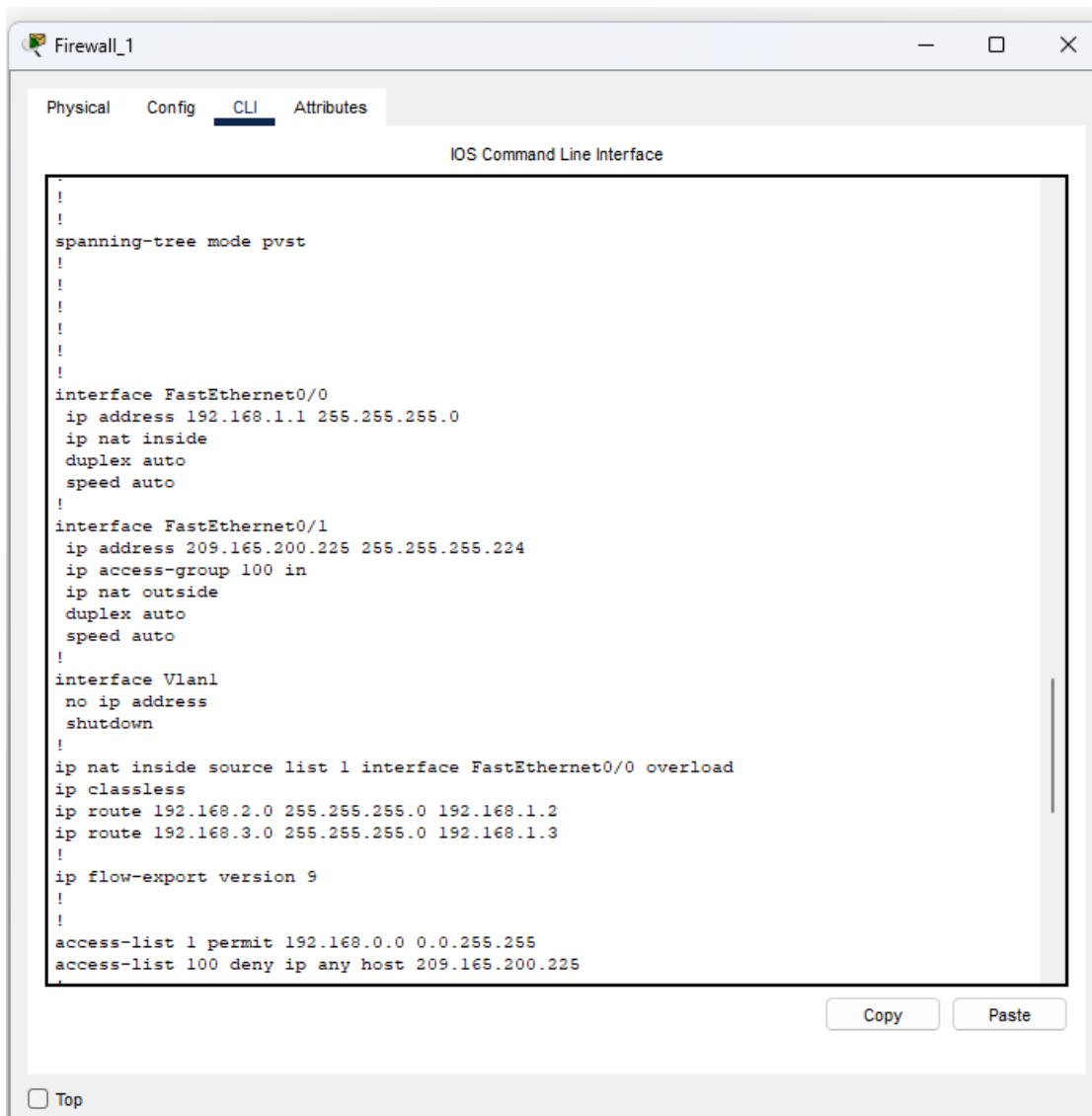


д. На брандмауері Firewall\_1 виберіть IP-адресу глобальної мережі та маску підмережі для інтерфейсу Fast Ethernet 0/0: 192.168.1.1 і 255.255.255.0.

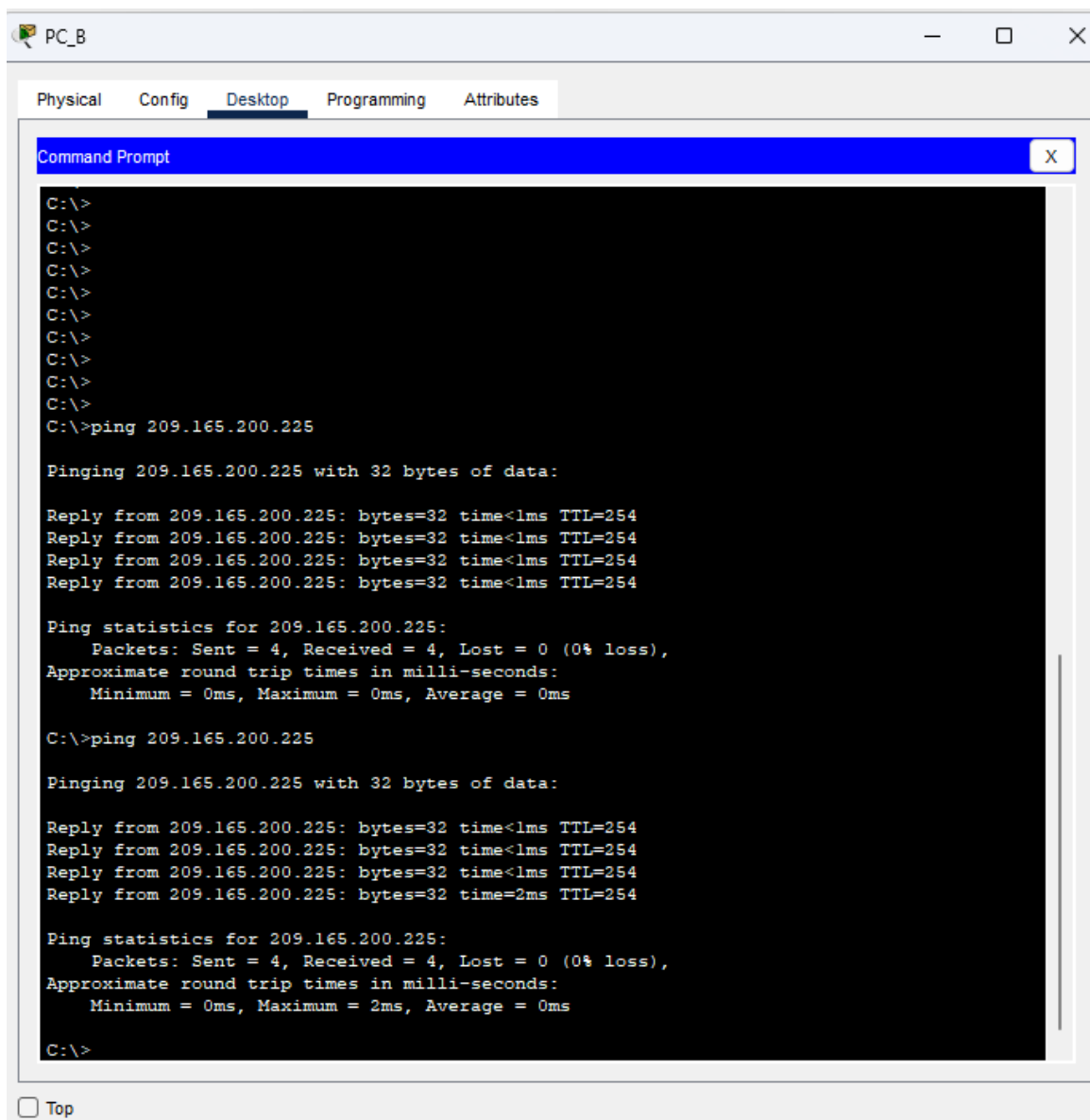


## Крок 2. Перевірка конфігурації брандмауера Firewall\_1

Для перевірки настройки використовуйте команду **show run**.



З комп'ютера ПК\_В, відправте ехо-запит 209.165.200.225, щоб переконатися, що у внутрішнього комп'ютера мається доступ в Інтернет.



The screenshot shows a window titled "PC\_B" with a menu bar containing "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active. Inside the window is a "Command Prompt" window with a blue title bar and a close button. The command prompt shows the following text:

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

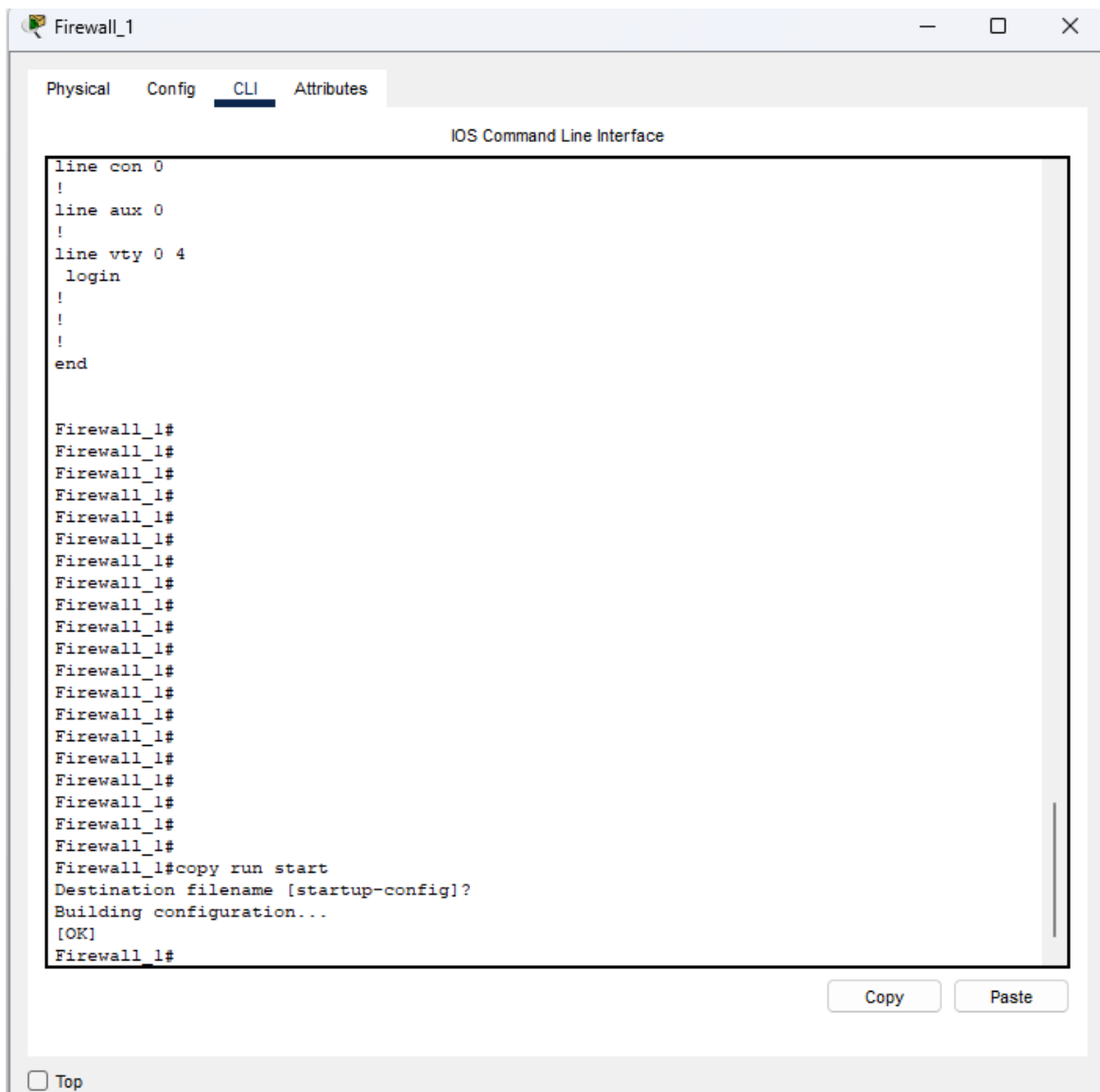
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=2ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>
```

At the bottom left of the window, there is a checkbox labeled "Top".

В привілейованому режимі ЕХЕС брандмауера Firewall\_1 збережить поточну конфігурацію в початкову за допомогою команди `copy run start`.



## Сценарій 2. Захист мережі відділу досліджень і розробок

Тепер, коли вся мережа захищена від трафіку, що надходить з Інтернету, прийшов час захистити мережу відділу досліджень і розробок (підмережа Subnet C) від можливих проникнень з внутрішньої області мережі. Для проведення досліджень науково-дослідницькій групі необхідний доступ до серверів, розташованих в підмережі B, і до Інтернету. Комп'ютерам підмережі B повинно бути відмовлено в доступі до підмережі науково-дослідного відділу.

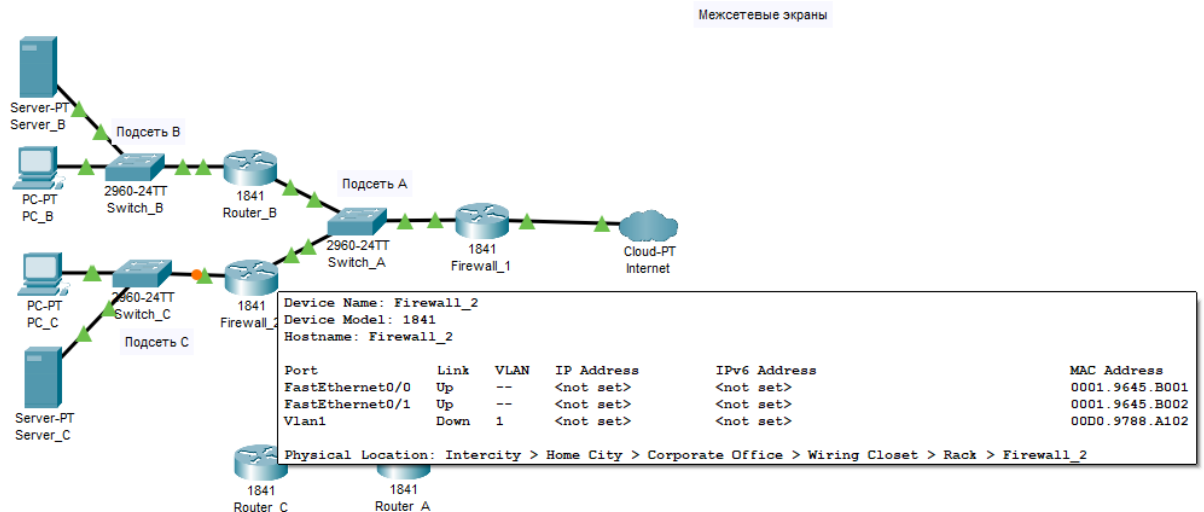
В міжмережевому екрані Firewall\_2 попередньо налаштовані правила для забезпечення необхідної клієнту безпеки. Встановіть цей брандмауер в мережі клієнта. Перевірте правильність його функціонування.

### Крок 1. Заміна маршрутизатора Router\_C брандмауером Firewall\_2.

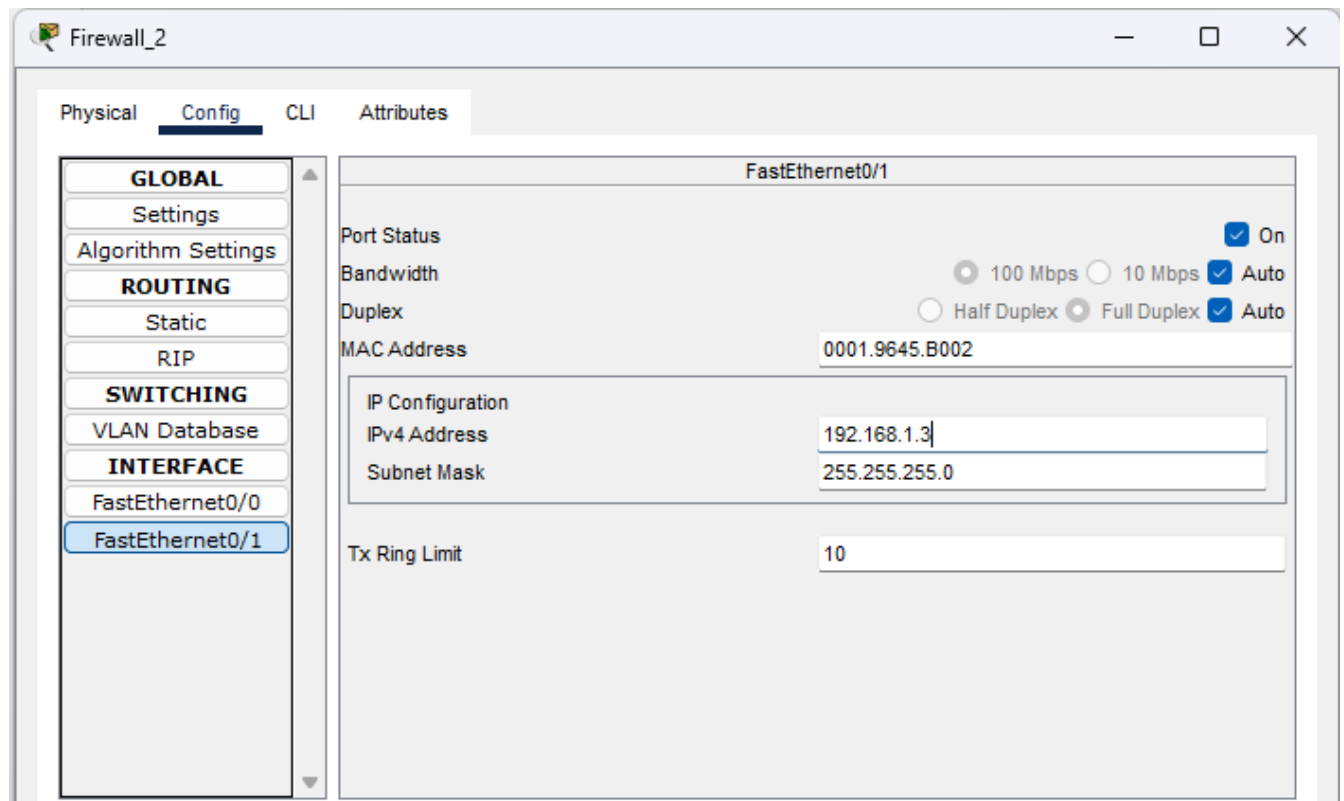
а. Видаліть маршрутизатор Router\_C і замініть його брандмауером Firewall\_2.

б. Підключіть інтерфейс Fast Ethernet 0/1 брандмауера Firewall\_2 до інтерфейсу Fast Ethernet 0/3 комутатора Switch\_A. Підключіть інтерфейс Fast Ethernet 0/0 брандмауера Firewall\_2 до інтерфейсу Fast Ethernet 0/1 комутатора Switch\_C. (Використовуйте прямий кабель для обох сполук.)

в. Підтвердіть ім'я мережевого вузла для Firewall\_2 - "Firewall\_2".

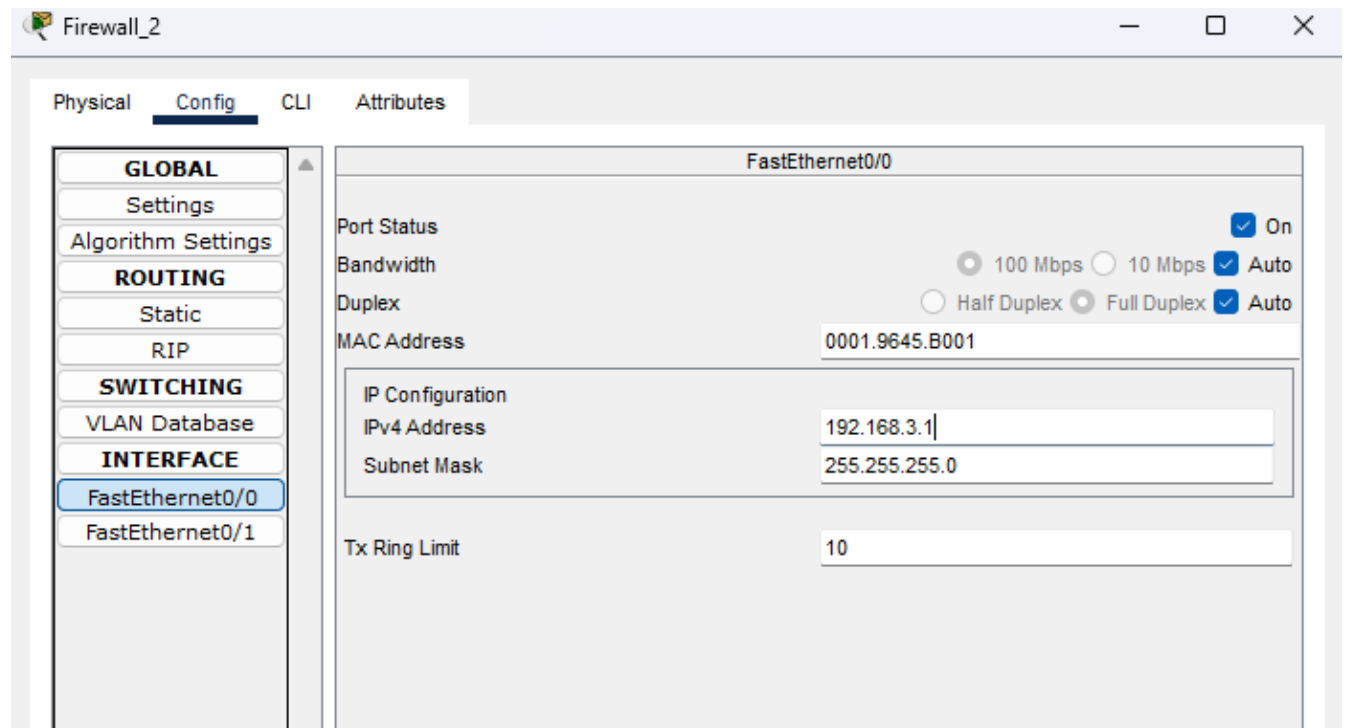


г. На Firewall\_2 налаштуйте IP-адресу глобальної мережі та маску підмережі для інтерфейсу Fast Ethernet 0/1: 192.168.1.3 і 255.255.255.0, відповідно.



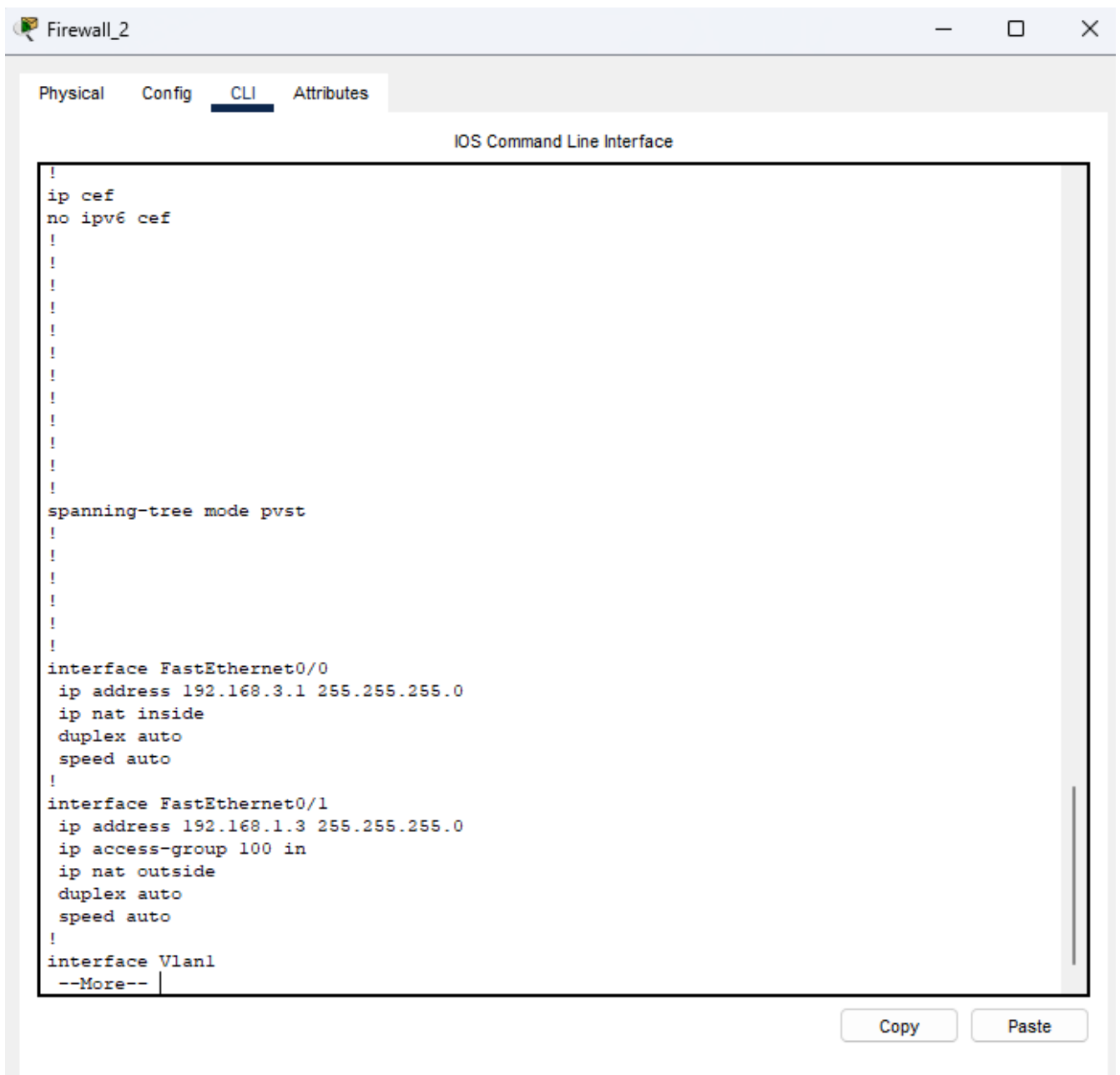


д. На брандмауері Firewall\_1 виберіть IP-адресу локальної мережі та маску підмережі для інтерфейсу FastEthernet 0/0: 192.168.3.1 і 255.255.255.0.

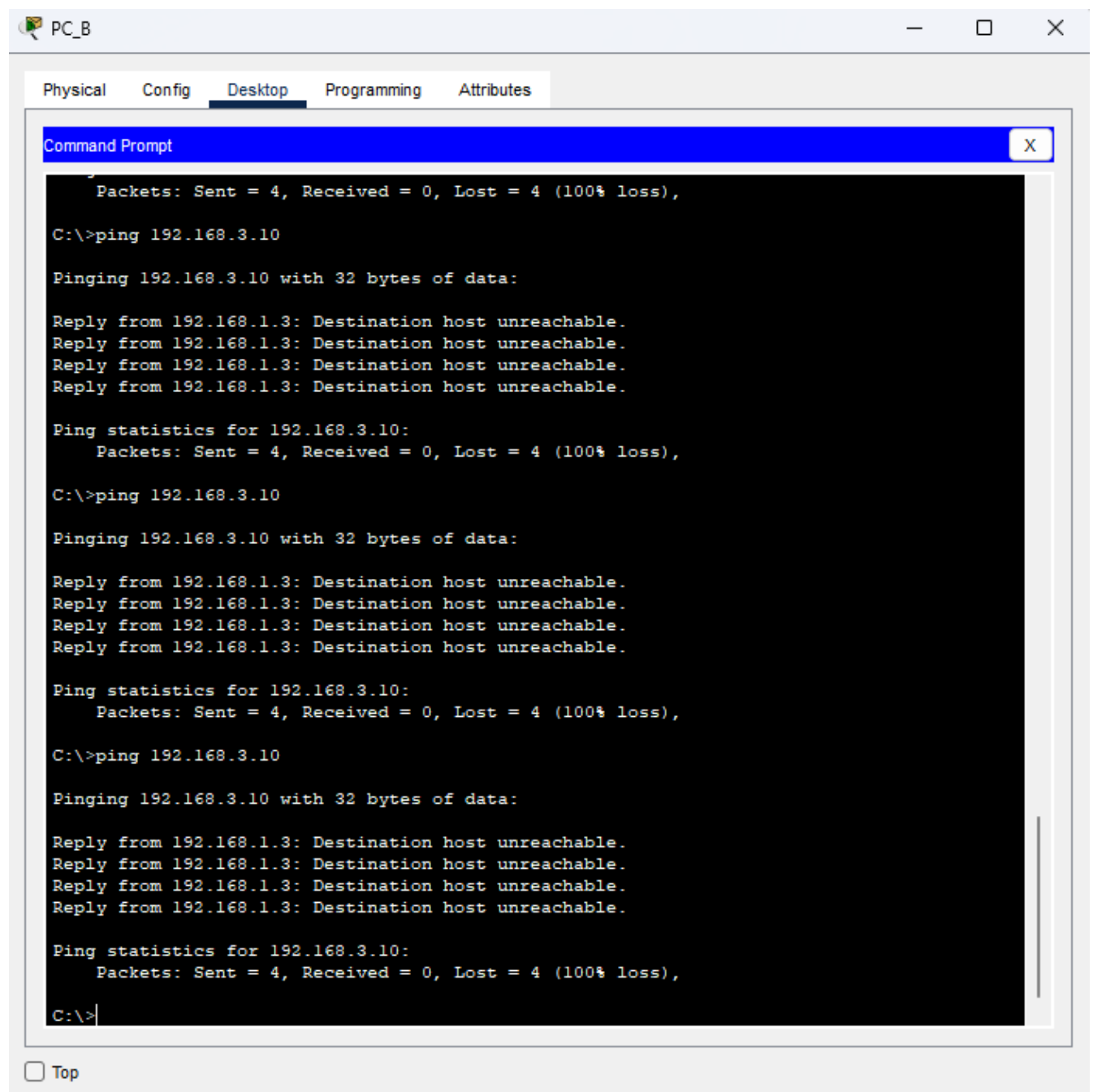


## Крок 2. Проверка конфигурации брандмауэра Firewall\_2

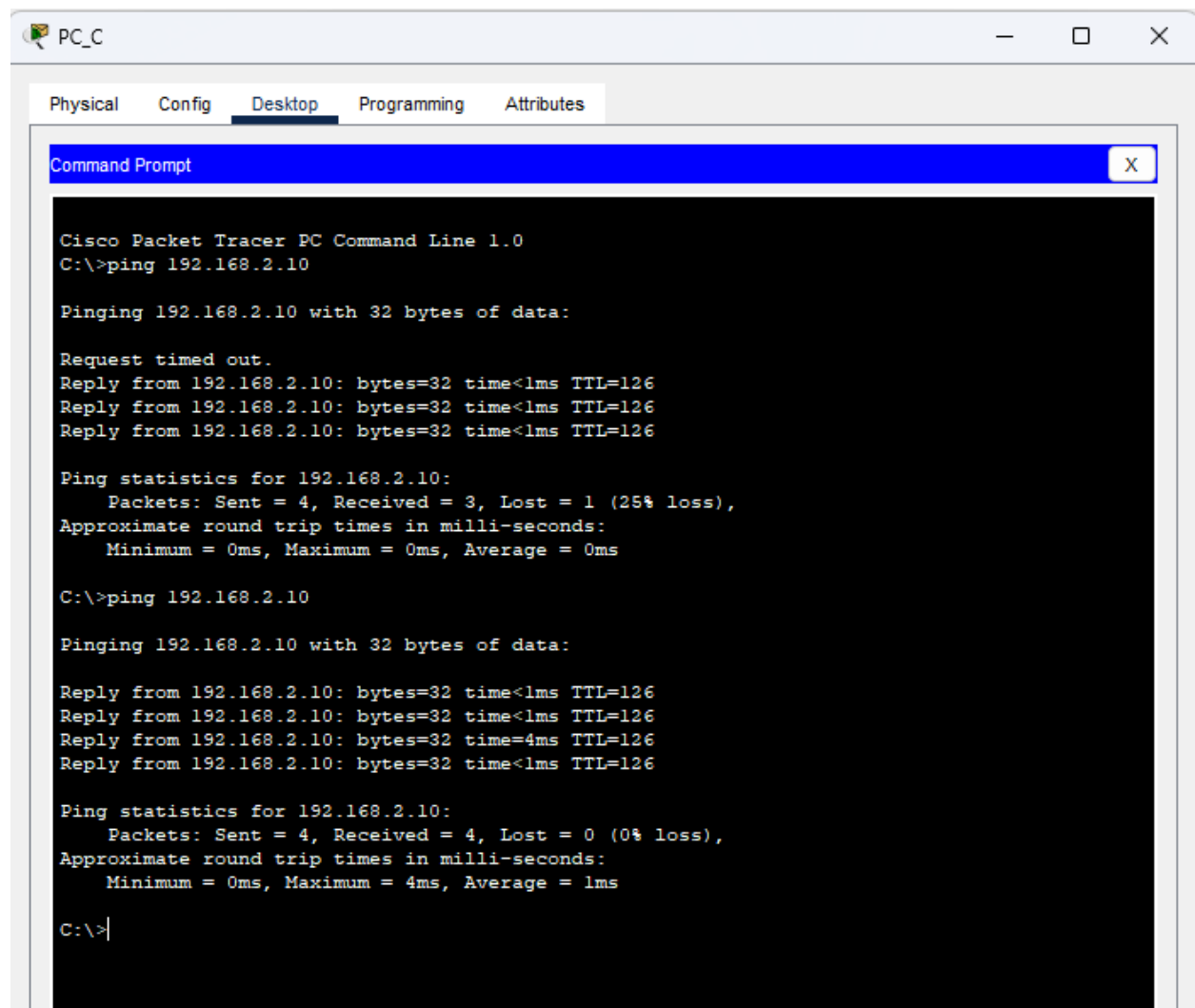
Для перевірки налаштувань використовуйте команду "show run". Далі представлена частина вихідних даних.



За запитом команди на ПК\_В використовуйте команду `ping`, щоб переконатися, що комп'ютери в підмережі Subnet B не можуть отримати доступ до комп'ютерів в підмережі Subnet C.



За запитом команди на ПК\_C використовуйте команду ping, щоб переконатися, що комп'ютери в підмережі Subnet C мають доступ до сервера в підмережі Subnet B.



The screenshot shows a window titled "PC\_C" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the output of two ping commands to 192.168.2.10. The first command shows a 25% loss (1 packet lost), and the second command shows 0% loss (0 packets lost).

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.2.10

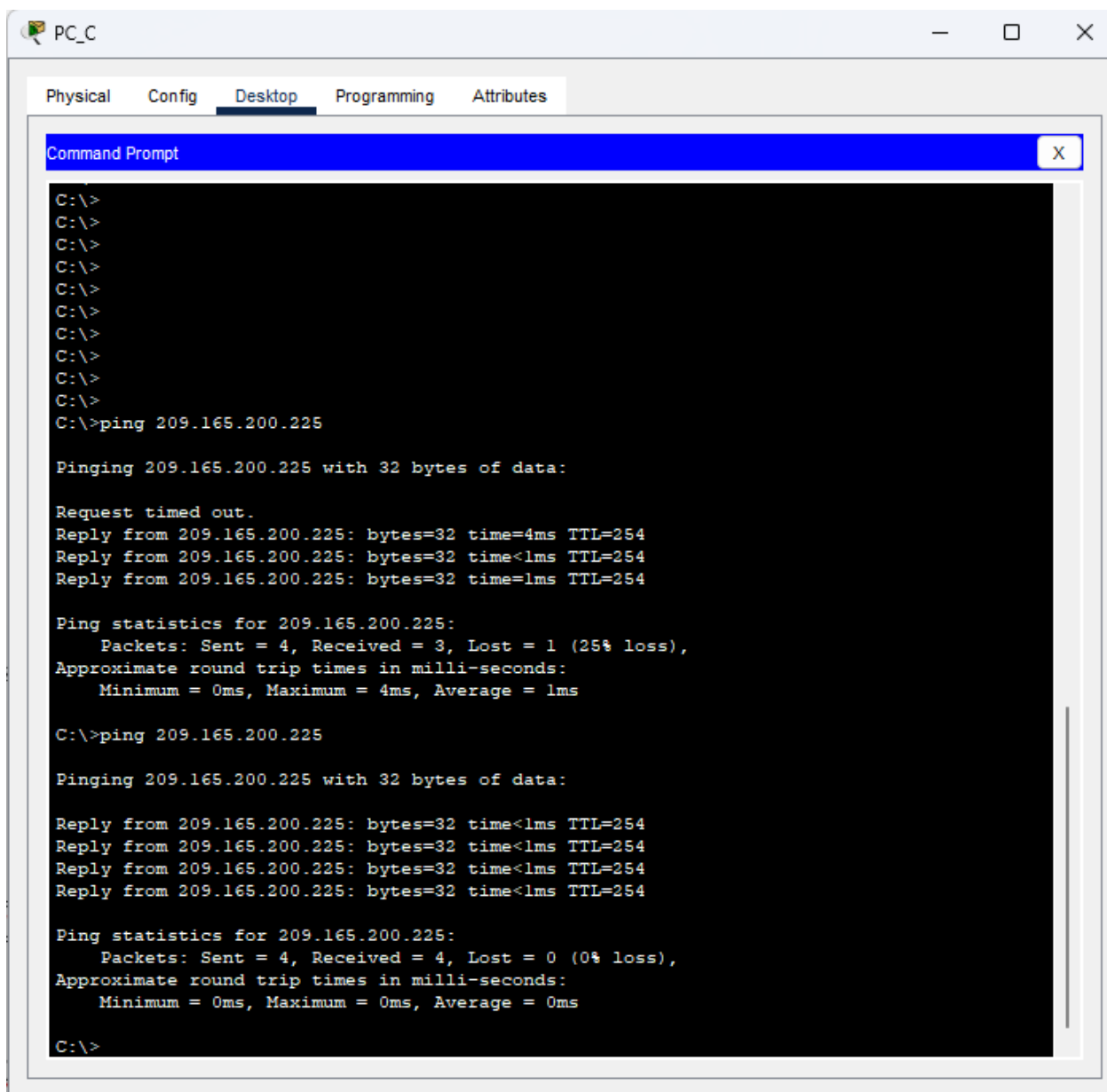
Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time<1ms TTL=126
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126
Reply from 192.168.2.10: bytes=32 time=4ms TTL=126
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>|
```

За запитом команди на ПК\_C використовуйте команду ping, щоб переконатися, що комп'ютери в підмережі Subnet C мають доступ до Інтернету.



The screenshot shows a window titled "PC\_C" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the execution of a ping command to 209.165.200.225. The first attempt shows a 25% packet loss (1 out of 4 packets lost). The second attempt shows 0% packet loss (0 out of 4 packets lost).

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Request timed out.
Reply from 209.165.200.225: bytes=32 time=4ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>ping 209.165.200.225

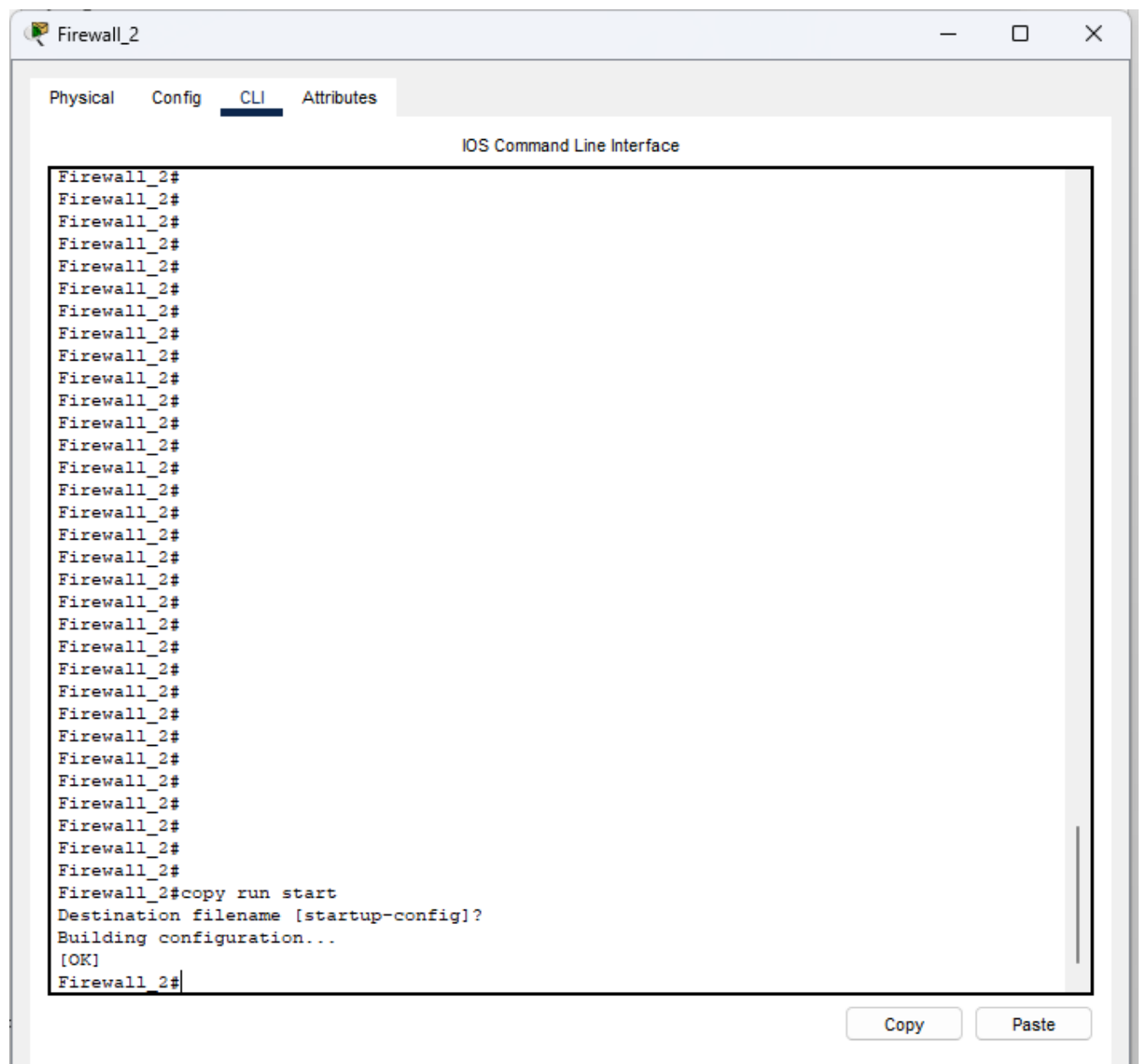
Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254

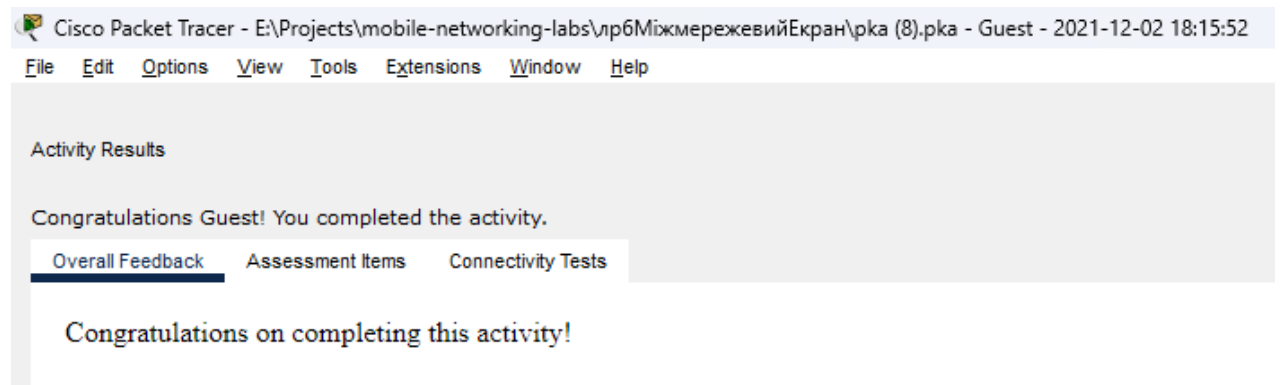
Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

д. В привілейованому режимі EXEC брандмауера Firewall\_2 збережіть поточну конфігурацію в початкову за допомогою команди copy run start.



е. Для перевірки зробленої роботи натисніть кнопку Check Results (Перевірити результати) в нижній частині вікна інструкцій.



## **Висновки**

У межах цієї роботи було досліджено роботу міжмережевих екранів.