

Міністерство освіти і науки України

Національний технічний університет України «КПІ

імені Ігоря Сікорського»

Факультет інформатики та обчислювальної техніки

Кафедра інформатики та програмної інженерії

## **ЗВІТ**

лабораторної роботи №6

з курсу «Мережеве управління та протоколи»

Перевірила:

Зенів І. О.

Виконав:

Студент Гр. ІІІ-01

Пашковський Є. С.

Київ 2023

## Лабораторна робота № 6.

### Списки доступу ACL

#### Практична робота 9-1.

#### Створення стандартного списку доступу

**Завдання:** створити мережу, налаштувати стандартний список доступу та перевірити правильність його роботи.

Списки доступу бувають декількох видів: стандартні, розширені, динамічні та інші. У стандартних ACL є можливість задати лише IP адресу джерела пакетів для їх заборони або дозволів.

Для виконання завдання будемо та налаштуємо мережу, що зображена на рис. 1. На ній показано дві підмережі: 192.168.0.0 і 10.0.0.0.

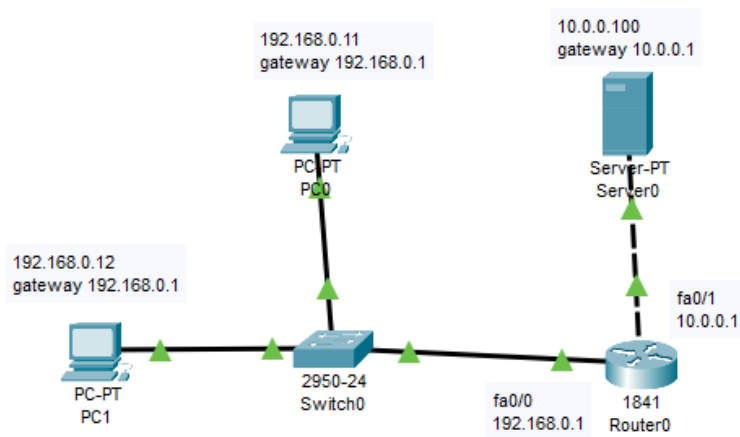


Рис. 1. Схема мережі для виконання завдання

Потрібно дозволити PC1 доступ на сервер з адресою 192.168.0.12, а PC0 з адресою 192.168.0.11 - заборонити.

#### Діагностика мережі

Перевіряємо зв'язок ПК з різних мереж (рис. 2).

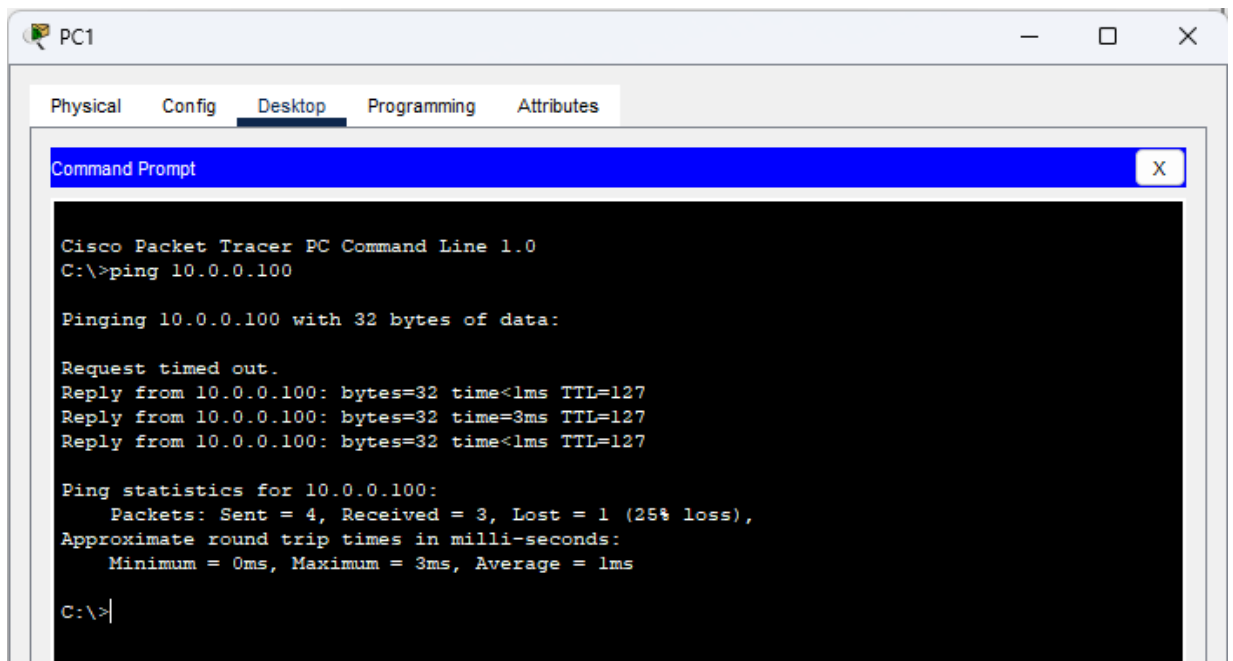


Рис. 2. ПК з різних мереж можуть отримувати доступ до сервера

Переходимо до вирішення завдання. Правило заборони і дозволу доступу будемо складати з використанням стандартних списків доступу (ACL). Поки не заданий список доступу на інтерфейсі все дозволено (permit). Але, варто створити список, відразу діє механізм "Все, що не дозволено, то заборонено". Тому немає необхідності щось забороняти (deny) - вказуємо що дозволено, а "іншим - заборонити" мається на увазі автоматично. За умовами завдання нам потрібно на Router0 пропустити пакети з вузла 192.168.0.12 на сервер (рис. 3).

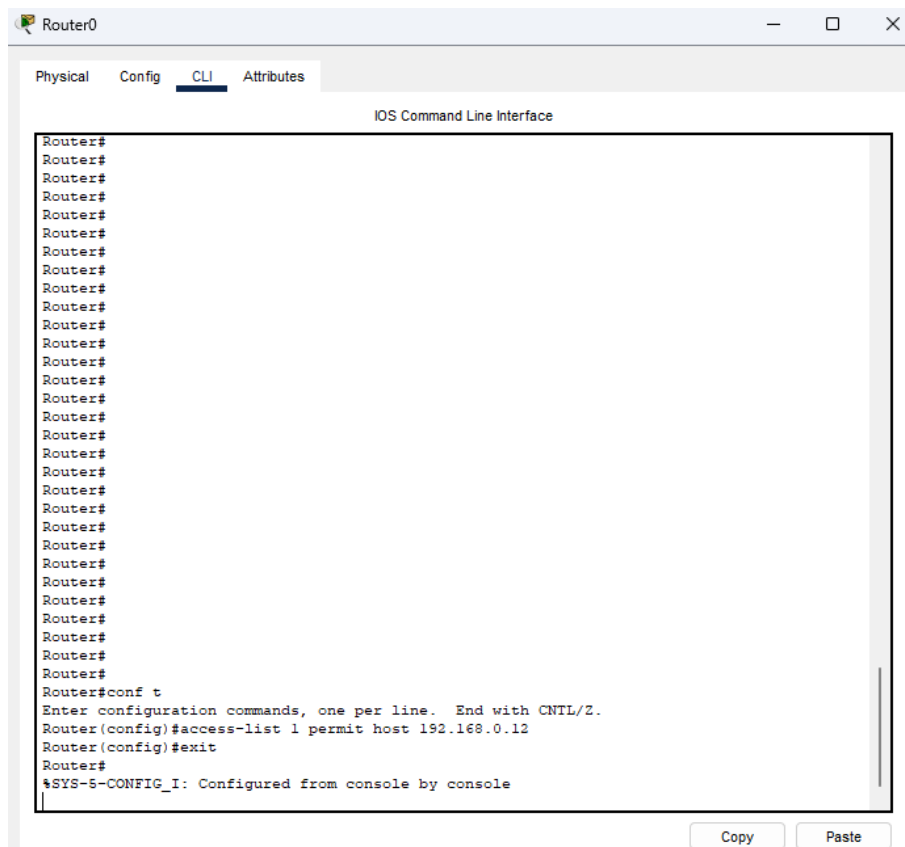


Рис. 3. Створення дозволу ACL на Router0

Застосовується дане правило на інтерфейс в залежності від напрямку (PC1 розташований з боку порту fa0/0) - рис. 4. Ця установка означає, що список доступу (правило з номером 1) діятиме на інтерфейсі fa0/0 на вхідному (in) від PC1 напрямку.

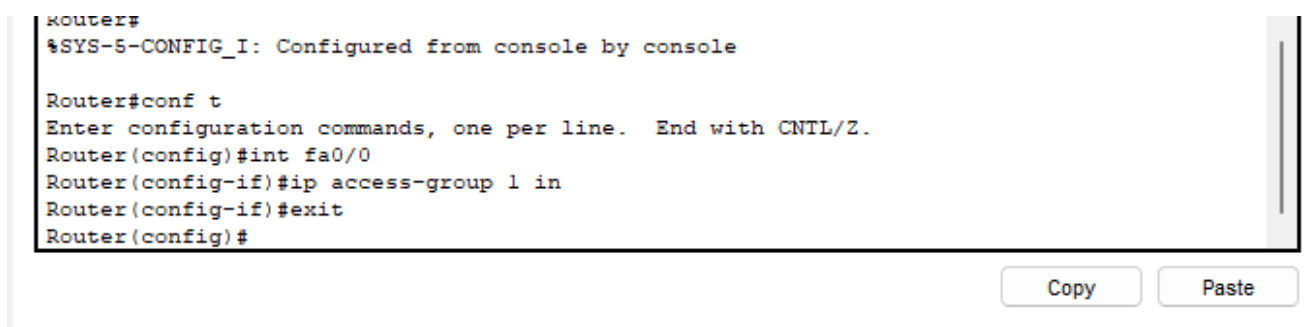


Рис. 4. Застосовування створеного правила до порту fa0/0 Router0

Перевіряємо зв'язок ПК з сервером (рис. 5 и рис. 6).

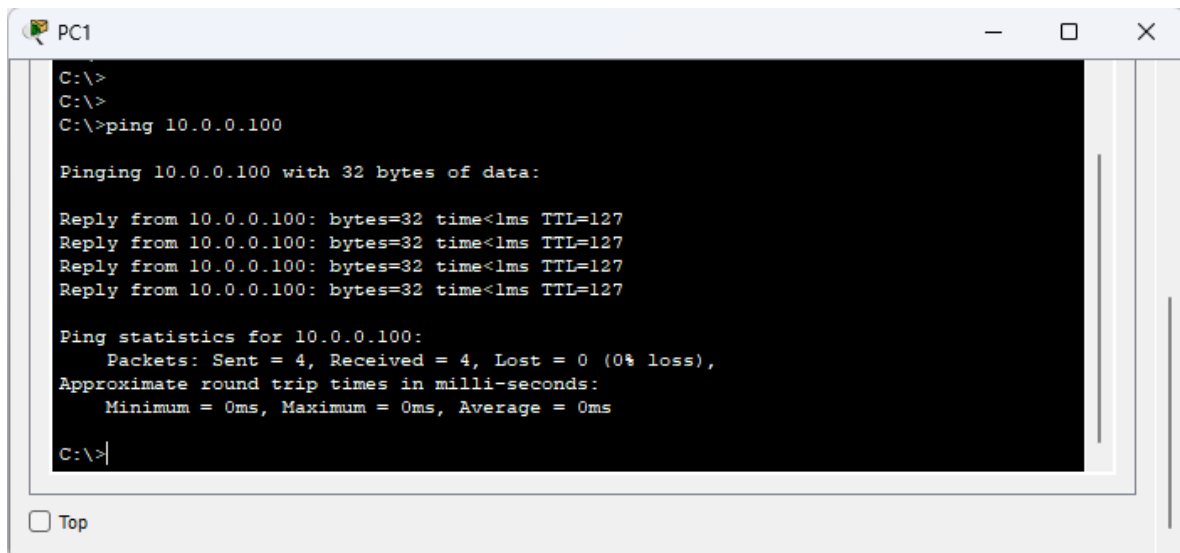


Рис. 5. Для PC1 сервер доступний

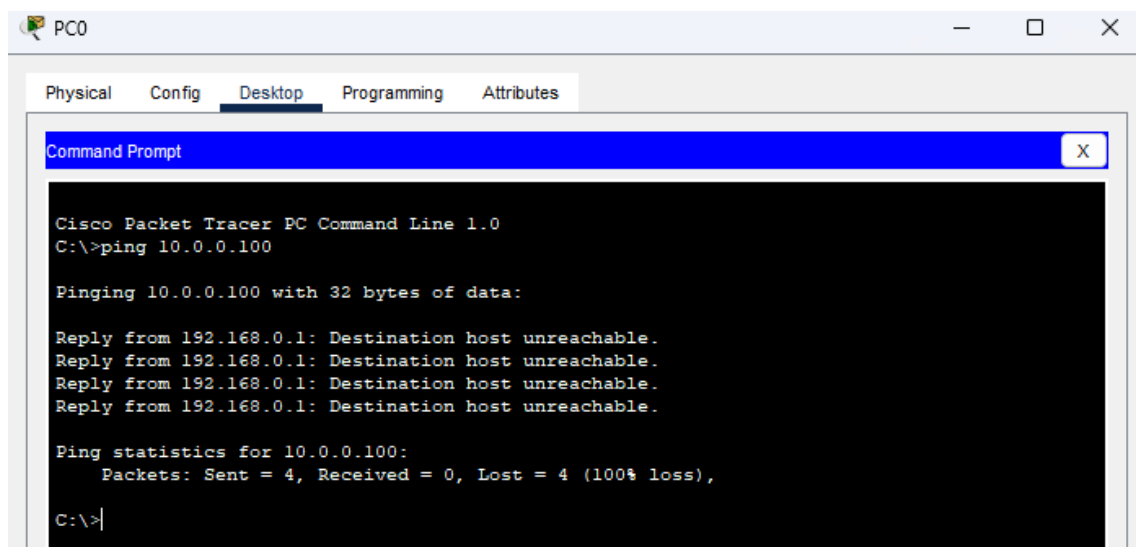


Рис. 6. Для PC0 сервер не доступний

Давайте подивимось на налаштування ACL (рис. 7).

```
Router#sh access-lists
Standard IP access list 1
    10 permit host 192.168.0.12 (4 match(es))
Router#
```

Рис. 7. Перегляд налаштувань ACL

**Висновки:** у межах цієї практичної роботи було побудовано і налаштовано мережу, налаштовано дозвіл ACL на маршрутизаторі та перевірено роботу такої мережі.

## Практична робота 9-2-1.

### Розширені списки доступу ACL

**Завдання:** налаштувати та дослідити роботу розширених списків доступу ACL.

Зберемо схему мережі, показану на рис. 8.

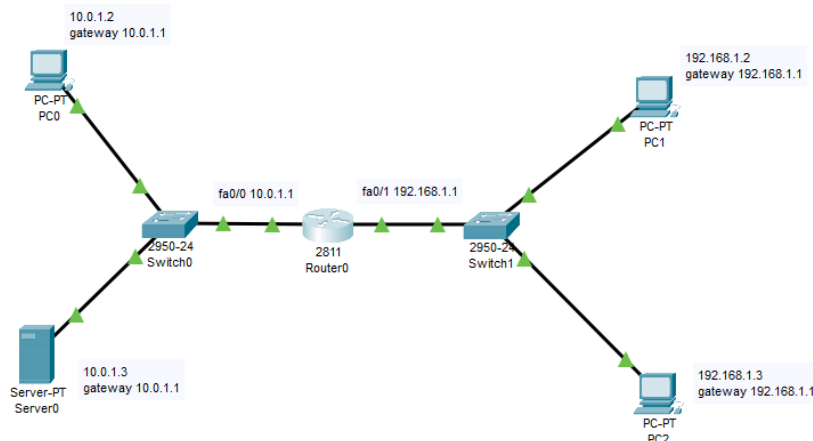


Рис. 8. Схема мережі для виконання завдання

Нам треба дозволити доступ до FTP-сервера 10.0.1.3 для вузла 192.168.1.2 і заборонити для вузла 192.168.1.3.

**Створюємо розширені списки доступу і забороняємо FTP трафік.**

Спочатку на сервері 10.0.1.3 FTP сервіс піднято за замовчуванням зі значеннями ім'я користувача Cisco, пароль Cisco. Переконаємося, що вузол Server0 доступний і FTP працює, для цього заходимо на PC1 і зв'язуємося з сервером (рис. 9). Виконуємо будь-які команди, наприклад, DIR - читання директорії.

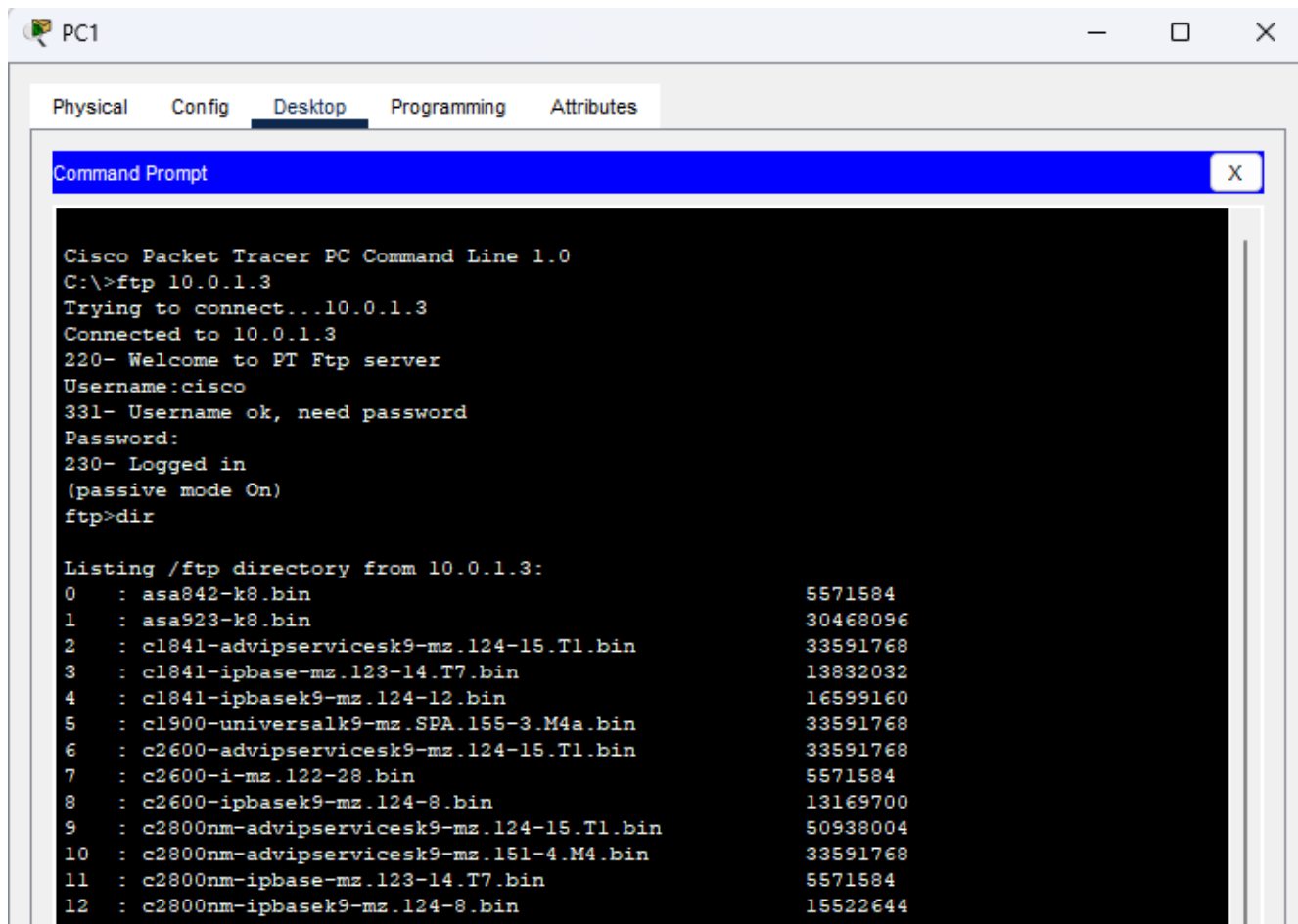


Рис. 9. FTP сервер доступний

Тепер створимо список правил з номером 101 в якому вкажемо 2 дозволяючих і по 2 забороняючих правила для портів сервера 21 і 20 (ці порти служать для FTP - передачі команд і даних) – рис. 10.

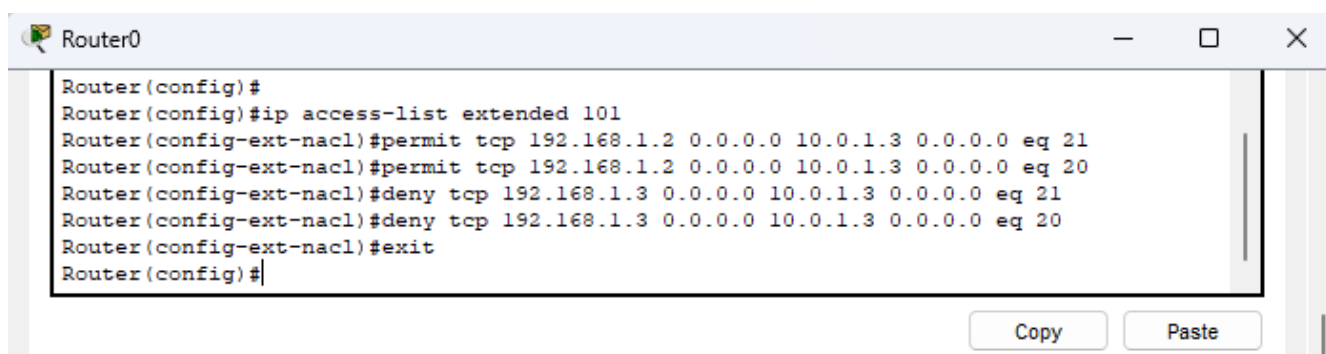


Рис. 10. Складаємо розширені списки доступу

А тепер застосовуємо наш список з номером 101 на вхід (in) fa0/1 тому, що трафік входить на цей порт роутера з боку мережі 192.168.1.0 (рис. 11).

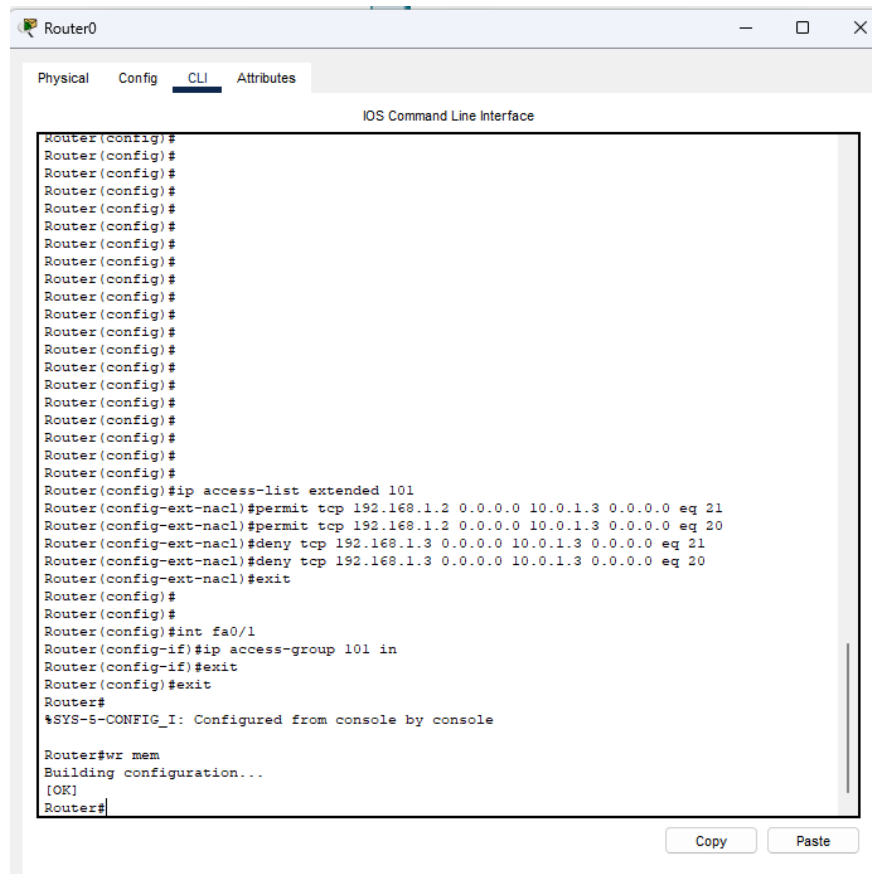


Рис. 11. Застосовуємо правило з номером 101 до порту 0/1 роутера  
Перевіряємо зв'язок сервера з PC2 (рис. 12).

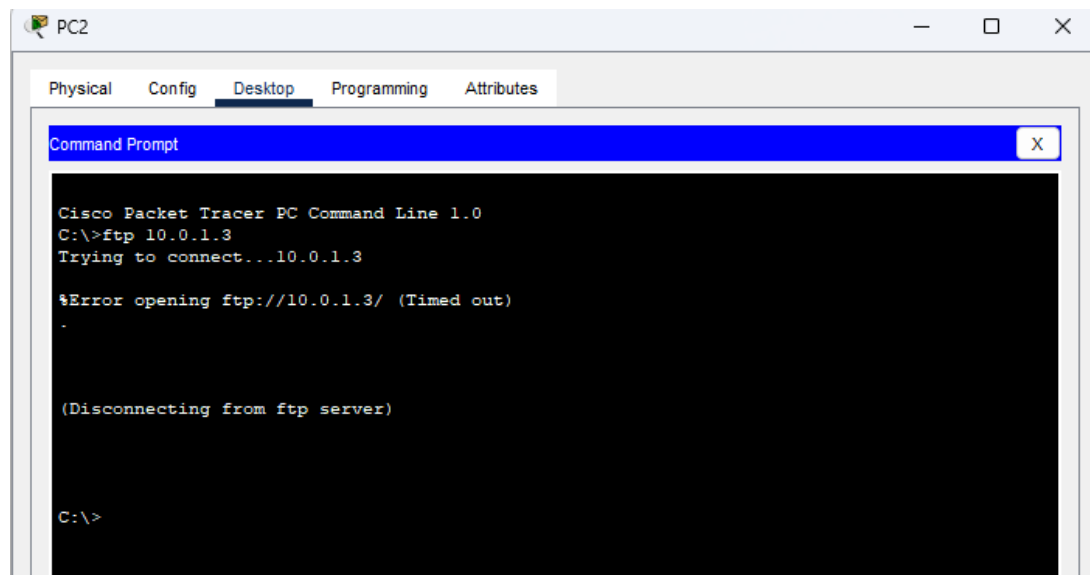
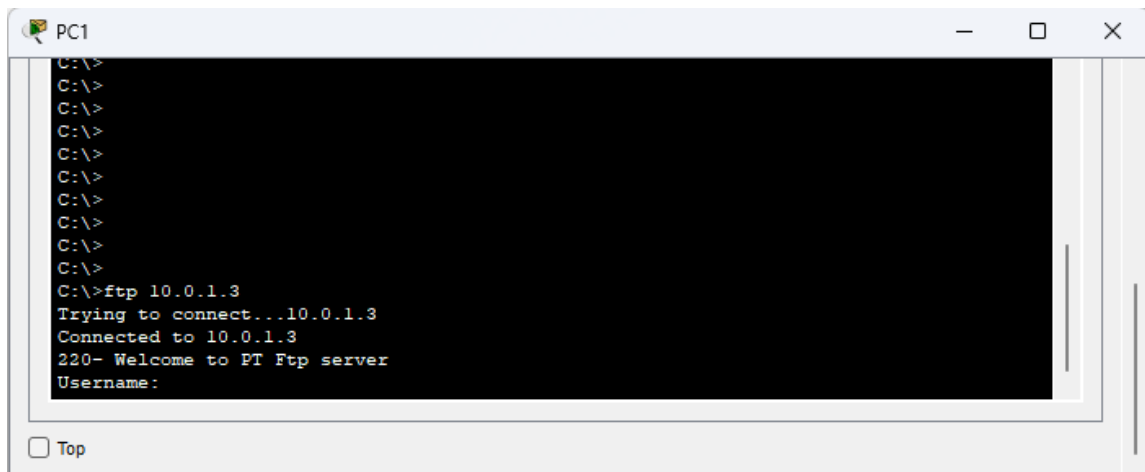


Рис. 12. Для PC2 FTP сервер недоступний  
Перевіряємо зв'язок сервера з PC1 (рис. 13).





```
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>ftp 10.0.1.3  
Trying to connect...10.0.1.3  
Connected to 10.0.1.3  
220- Welcome to PT Ftp server  
Username:
```

Рис. 13. Для PC1 FTP сервер доступний

**Висновки:** під час виконання цієї практичної роботи було досліджено роботу розширених списків доступу на прикладі мережі доступом до ftp сервера.

## **Висновки**

Отже, під час виконання лабораторної роботи було налаштовано та досліджено роботу мереж із застосуванням списків доступу (ACL). Було досягнуто часткового доступу до певних хостів за вказаними правилами, вказаними за допомогою стандартного та розширеного списку доступу.