НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«Київський політехнічний інститут імені Ігоря Сікорського» Факультет інформатики та обчислювальної техніки Кафедра технічної кібернетики

Звіти до комп’ютерних практикумів з кредитного модуля “Мережеве управління та протоколи”

Виконав

Студенти групи ІТ-02 Терешкович М.О.

Перевірила:

Зенів І. О.

Київ – 2023

# Завдання 6-1:

A computer network diagram with words and numbers

Description automatically generated with medium confidence

**Виконання**

Побудуємо схему за заданим малюнком.

A diagram of a computer network

Description automatically generated

**Налаштування R0**

A screenshot of a computer program

Description automatically generated

**Налаштування сервера**

A screenshot of a computer

Description automatically generated

Перевіряємо зв'язок ПК з різних мереж

A computer screen shot of a program

Description automatically generated

**Переходимо до вирішення завдання**Правило заборони і дозволу доступу будемо складати з використанням стандартних списків доступу (ACL).

A close-up of a white background

Description automatically generated

**Рис. 9.5.**Створюємо на R0 дозволяє ACL

Застосовується дане правило на інтерфейс в залежності від напрямку (PC1 розташований з боку порту Fa0 / 0). Ця установка означає, що список доступу (правило з номером 1) діятиме на інтерфейсі fa0 / 0 на вхідному (in) від PC1 напрямку.

A black text on a white background

Description automatically generated

Перевіряємо зв'язок ПК з сервером

ПК1

A screenshot of a computer screen

Description automatically generated

ПК0

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

# Висновок 6-1:

У ході виконання даної лабораторної роботи було розглянуто процес створення стандартного списку доступу (ACL) на маршрутизаторі R0 з метою керування доступом до сервера з різних вузлів мережі. Задачею було дозволити доступ на сервер PC1 з IP-адресою 192.168.0.12 та заборонити доступ PC0 з IP-адресою 192.168.0.11.

Важливим етапом було налаштування мережевих інтерфейсів маршрутизатора та сервера з використанням відповідних IP-адрес. Далі було використано стандартний ACL для встановлення правил доступу на маршрутизаторі R0. При цьому використовувались команди конфігурації інтерфейсів та створення ACL.

Список доступу був налаштований таким чином, що дозволяв доступ з вузла 192.168.0.12 і блокував доступ з вузла 192.168.0.11. Після застосування цих правил, була проведена діагностика мережі для перевірки результатів. Виявлено, що PC1 має доступ до сервера, тоді як PC0 не має.

Крім того, було розглянуто питання розширених списків доступу (ACL), які надають більше можливостей для фільтрації трафіку, зокрема за протоколами та портами.

У висновку, використання ACL є важливим елементом в мережевому адмініструванні для контролю доступу до ресурсів та забезпечення безпеки мережі. Правильна конфігурація ACL дозволяє здійснювати ефективне керування мережевим трафіком та захищати систему від небажаних з'єднань.

# Завдання 6-2:

A diagram of a computer network

Description automatically generated

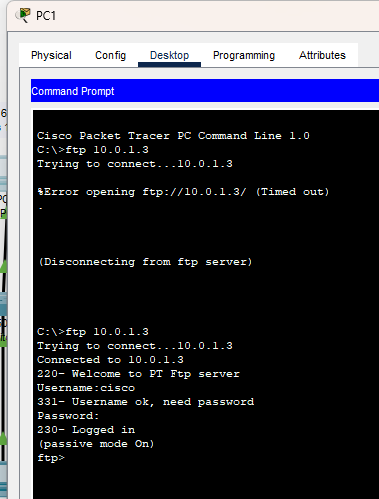
**Виконання**

Створимо схему як показано на малюнку.

A diagram of a computer network

Description automatically generated

Налаштувавши інтерфейси на Роутері0 зробимо ftp запит на сервер увійшовши при паролі Cisco і такім же логіном. Виконаємо команду для читання директорії Dir.



A screenshot of a computer program

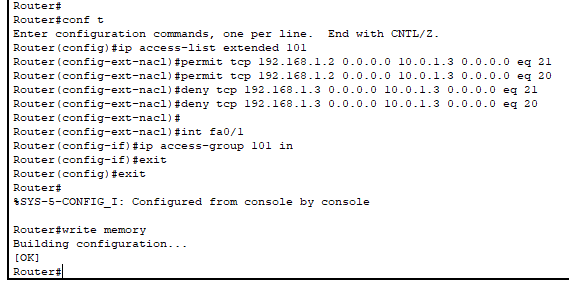
Description automatically generated

Отже 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)

A black and white text on a white background

Description automatically generated

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



Перевіряємо зв'язок сервера з PC2

A screenshot of a computer program

Description automatically generated

Перевіряємо зв'язок сервера з PC1

A screen shot of a computer

Description automatically generated

# Висновок 6-2:

У процесі виконання даної лабораторної роботи було розглянуто застосування розширених списків доступу (ACL) для керування трафіком в мережі. Задачею було дозволити доступ до FTP-сервера з IP-адресою 10.0.1.3 для вузла з IP-адресою 192.168.1.2 і заборонити для вузла 192.168.1.3.

Для досягнення цієї мети було створено розширений список доступу з номером 101, в якому вказані дозволяючі та забороняючі правила для портів FTP-сервера (21 і 20). Цей список був застосований на вхідний інтерфейс Fa0/1 маршрутизатора.

Діагностика мережі вказала, що після застосування ACL, PC1 має доступ до FTP-сервера, а PC2 – ні, що відповідає задачам, поставленим в завданні.

Важливим було перевірити роботу FTP-сервера, а також впевнитися в правильності написання та застосуванні правил у розширеному списку доступу.

Застосування розширених списків доступу в мережах дозволяє більш гнучко регулювати трафік, враховуючи конкретні протоколи та порти, що є важливим елементом забезпечення безпеки та ефективності роботи мережі.