**Національний технічний університет України**

**«Київський політехнчний інститут імені Ігоря Сікорського»**

**Навчально-науковий інститут атомної та теплової енергетики**

**Кафедра цифрових технологій в енергетиці**

**Звіт**

**з лабораторної роботи №7**

**з дисципліни «Комп’ютерні мережі»**

Виконав:

студент групи ТР-23

Ровний Г.О.

КИЇВ - 2024

**Списки доступу ACL**

**Завдання 1:**

Створення стандартного списку доступу. Потрібно дозволити доступ на сервер PC1 з адресою 192.168.0.12, а PC0 з адресою 192.168.0.11 – заборонити.

**Результат виконання роботи**

Побудуємо мережу подану у завданні а також здійснимо налаштування PC0 та PC1 (потрібно налаштувати ipconfig).

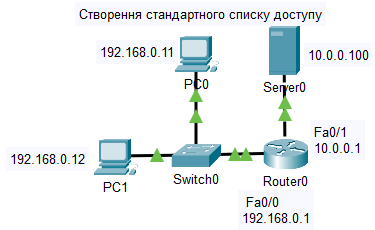


Рис 1. Побудована мережа для завдання

Тепер виконаємо налаштування R0. Інтерфейс 0/0 маршрутизатора 1841 налаштуємо на адресу 192.168.0.1 і увімкнемо наступними командами:

Router>**en**

Router#**conf t**

Router (config)#**int fa0/0**

Router (config-if)#**ip addr 192.168.0.1 255.255.255.0**

Router (config-if)#**no shut**

Router (config-if)#**exit**

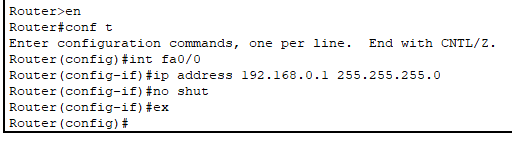
****

Рис 2. Налаштування інтерфейсу R0 (порт 0/0)

Другий інтерфейс маршрутизатора (порт 0/1) налаштуємо на адресу 10.0.0.1 і так само увімкнемо:

Router (config)#**intfa0/1**

Router (config-if)#**ip addr 10.0.0.1 255.255.255.0**

Router (config-if)#**no shut**

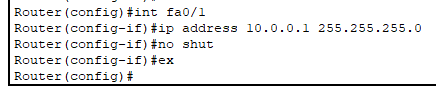


Рис 3. Налаштування інтерфейсу R0 (порт 0/1)

Тепер виконаємо налаштування Server0. Введемо параметри вказані у завданні.

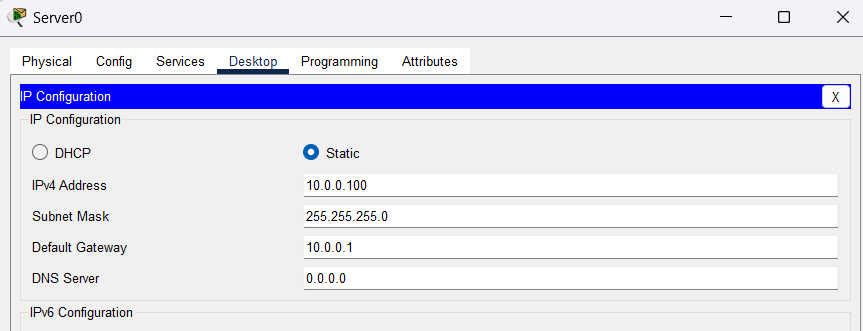


Рис 4. Перевірка наявності зв’язку за допомогою команди ping

Тепер виконуємо діагностику зв’язку ПК з різних мереж. Просто виконаємо пінгування з одного ПК на інший:

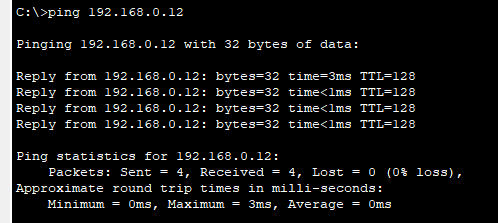


Рис 5. Перевірка наявності зв’язку за допомогою команди ping

Правило заборони і дозволу доступу будемо складати з використанням стандартних списків доступу (ACL). Поки не заданий список доступу на інтерфейсі - все дозволено (permit). Варто створити список, відразу діє механізм заборони. Немає необхідності щось забороняти (deny) - вказуємо що дозволено, а "іншим -заборонити" автоматично. За умовами завдання потрібно на R0 пропустити пакети з вузла 192.168.0.12 на сервер.

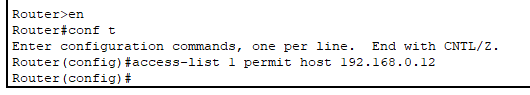


Рис 6. Створення ACL на R0, що дозволяє доступ

Далі даємо правило яке означає, що список доступу (правило з номером 1) діятиме на інтерфейсі fa0/0 на вхідному (in) від PC1 напрямку.

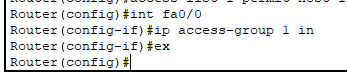


Рис 7. Створення правила для порту Fa0/0

Перевіряємо зв’язок двох ПК із сервером:

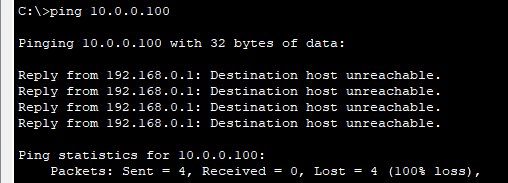


Рис 8. Перевірка наявності зв’язку з ПК0 (відмова)

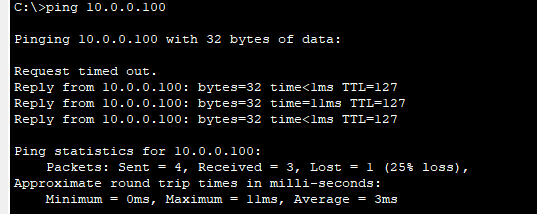


Рис 9. Перевірка наявності зв’язку з ПК1 (доступ дозволено)

Переглянемо наш ACL за допомогою #**sh** **access-lists**:

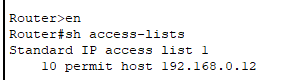


Рис 10. Перевірка ACL

Якщо потрібно додати новий вузол, наприклад, PC2 з адресою 192.168.0.13 в список ACL використаємо #**access-list 1 permit host 192.168.0.13**. Для скасування будь-якого правила - повторюємо його з приставкою "no": #**no ip access-group 1 in**, тоді ACL буде скасований і знову всі ПК можуть пінгувати сервер.

**Завдання 2:**

Розширені списки доступу ACL. Необхідно дозволити доступ до FTP сервера 10.0.1.3 для вузла 192.168.1.2 і заборонити для вузла 192.168.1.3.

**Результат виконання роботи**

Спочатку сформуйемо та налаштуємо тестову мережу задану в завданні для роботи з розширеними списками доступу.

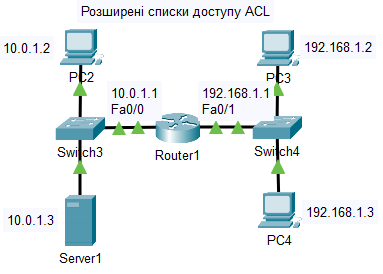


Рис 11. Тестова мережа

Створимо розширені списки доступу і заборонимо FTP трафік. Спочатку на сервері 10.0.1.3 (адреса сервера) FTP сервіс піднятий за замовчуванням зі значеннями ім'я користувача і пароль Cisco.

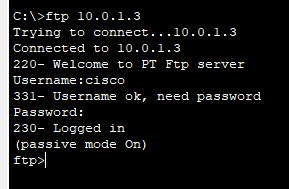


Рис 12. Підключення до ftp сервера

Переконаємося, що вузол S0 доступний і FTP працює, для цього заходимо на PC1 і зв'язуємося з сервером (виконаємо команду, наприклад DIR – читання директорії).

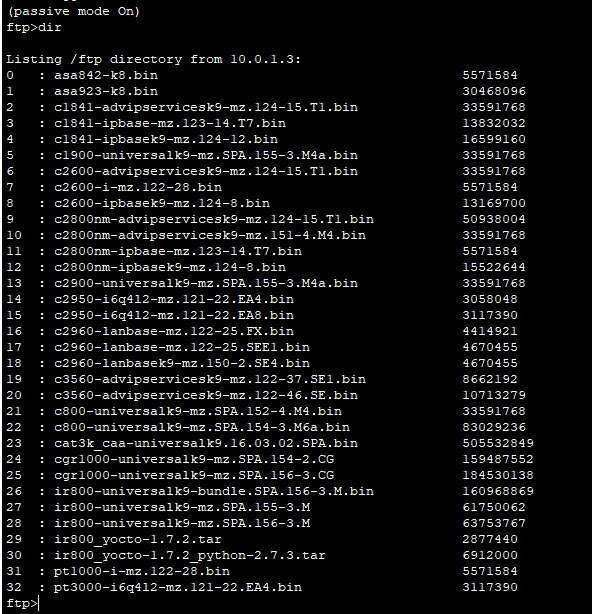


Рис 13. FTP сервер доступний

Створимо список правил з номером 101, у якому вказуємо 2 дозволених і 2 заборонених правила для портів сервера 21 і 20.

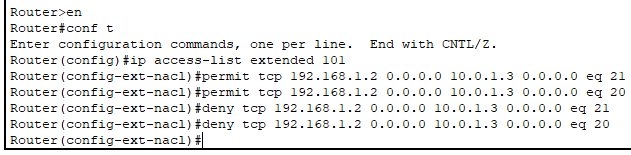


Рис 14. Створення розширеного ACL

Застосуємо список з номером 101 на вхід (in) Fa0/1 тому що трафік входить на цей порт роутера з боку мережі 192.168.1.0.

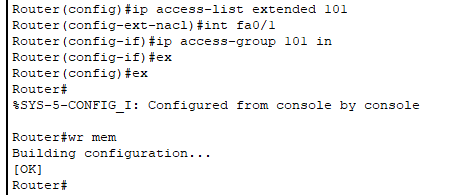


Рис 15. Застосування ACL до порту Fa0/1

Перевіримо зв'язок сервера з PC4 (для PC4 FTP сервер не доступний):

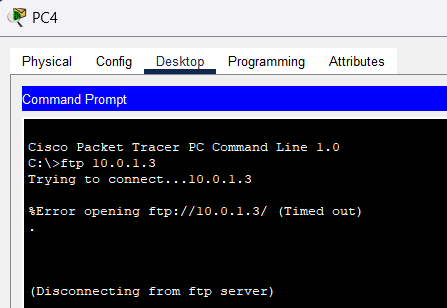


Рис 16. Перевірка доступу до FTP з PC4

Перевіримо зв'язок сервера з PC3 (для PC3 FTP сервер доступний):

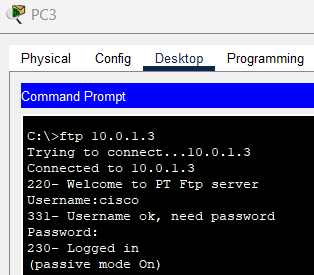


Рис 17. Перевірка доступу до FTP з PC3

**Висновок:**

У результаті виконання лабораторної роботи було отримано практичні навички роботи зі створенням стандартного та розширеного списків доступів. Було налаштовано доступ до FTP сервера для різних вузлів та перевірено підключення др FTP сервера з різних ПК.