**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 №5**

**з дисципліни «Безпека інформаційних систем»**

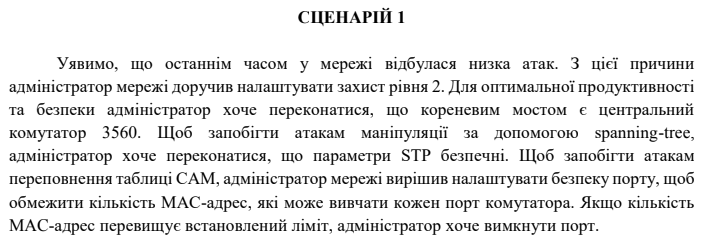
Виконав:

студент групи ТР-23

Ровний Г.О.

КИЇВ - 2024

**Мета роботи:** лабораторна робота спрямована на набуття практичних навичок роботи в емуляторі Cisco Packet Tracer та дослідженні особливостей налаштування безпеки для рівня 2 та захищеного функціонування VLAN.

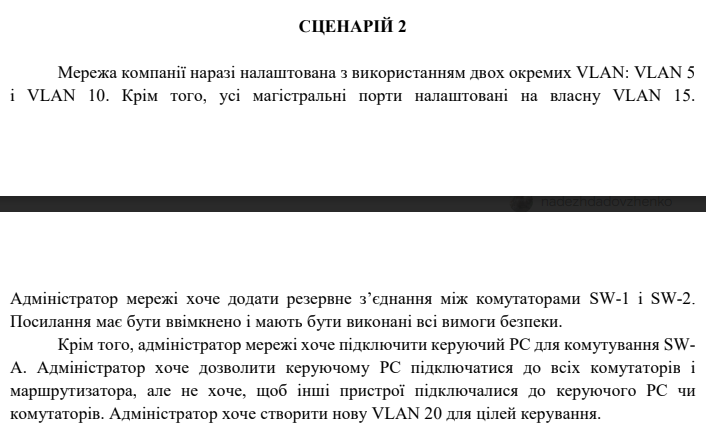
****

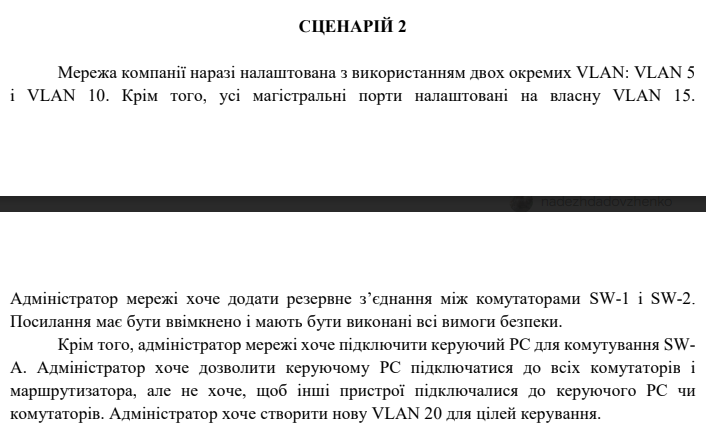
**Поставлене завдання:**

1. Призначити центральний комутатор кореневим мостом.

2. Захистити параметри spanning-tree, щоб запобігти атакам маніпуляції STP.

3. Увімкнути захист портів, щоб запобігти атакам переповнення таблиці CAM.





**Поставлене завдання:**

1. Підключити нове резервне з'єднання між SW-1 і SW-2.

2. Увімкнути транкінг і налаштувати безпеку на новому магістральному каналі між SW-1 і SW-2.

3. Створити нову мережу керування VLAN (VLAN 20) і підключити керуючий РС до цієї мережі VLAN.

4. Впровадити ACL, щоб запобігти доступу зовнішніх користувачів до VLAN керування.

**Результат виконання роботи**

**СЦЕНАРІЙ 1**

**Частина 1. Налаштувати кореневий міст**

Крок 1. Визначити поточний кореневий міст.

З Central виконуємо команду show spanning-tree, щоб визначити поточний кореневий міст, побачити порти, що використовуються та побачити їхній статус. (STP) - це протокол мережі, який створює безпетлеву топологію для Ethernet-мереж. Це досягається шляхом вибору одного комутатора як “кореневого мосту” і визначення найкоротшого шляху від кожного комутатора до кореневого мосту. В даному випадку кореневим мостом є VLAN0001.

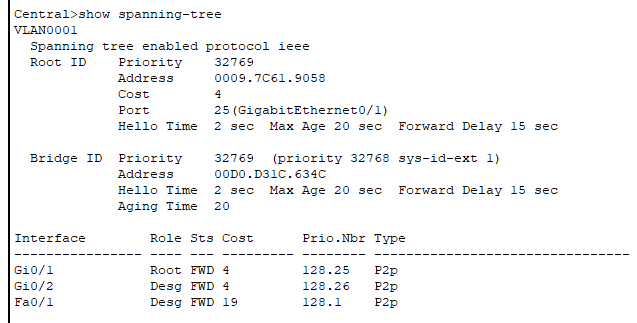


Рис.1. Визначення поточного кореневого місту

Крок 2. Призначити Central основним кореневим мостом.

На Central переходимо до режиму глобальної конфігурації. Використовуючи команду spanning-tree vlan 1 root призначаємо Central як кореневий міст.

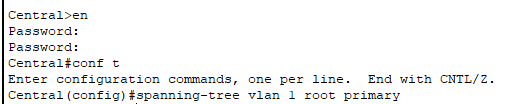


Рис.2. Призначення Central основним кореневим мостом

Крок 3. Призначити SW-1 як вторинний кореневий міст.

Переходимо до режиму глобальної конфігурації на комутаторі SW-1. Призначаємо SW-1 вторинним кореневим мостом за допомогою команди spanning-tree vlan 1 root secondary.



Рис.3. Призначення SW-1 як вторинний кореневий міст

Крок 4. Перевірити spanning tree конфігурацію.

Виконаємо команду show spanning-tree на Central, щоб переконатися, що Central є кореневим мостом. Як бачимо, цей міст є кореневим мостом.

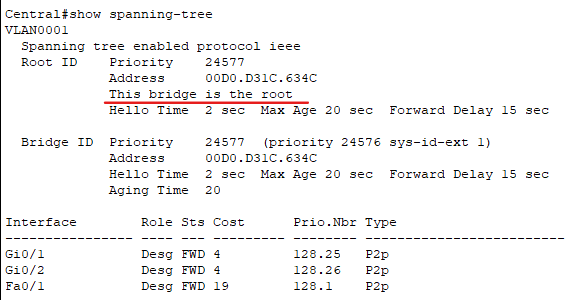


Рис.4. Перевірка spanning tree конфігурації

**Частина 2. Захист від атак STP.**

Крок 1. Увімкнути PortFast на всіх портах доступу.

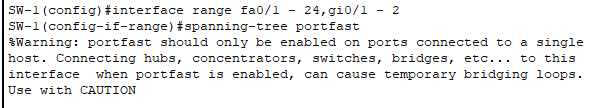


Рис.5. Увімнкнення PortFast на SW-1

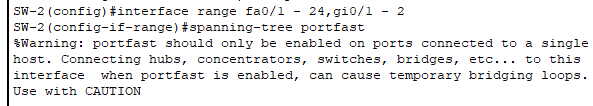


Рис.6. Увімнкнення PortFast на SW-2

Крок 2. Увімкнути захист BPDU на всіх портах доступу.

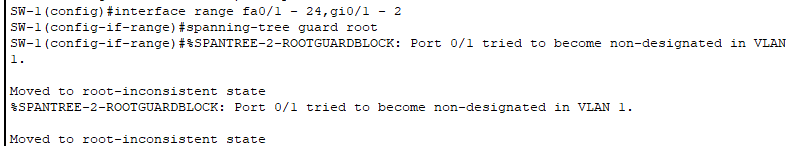
Необхідно увімкнути захист BPDU на портах доступу SW-A та SW-B. Захист BPDU spanning-tree можна ввімкнути на кожному окремому порту за допомогою команди spanning-tree bpduguard enable у режимі конфігурації інтерфейсу або команди spanning-tree portfast bpduguard за замовчуванням у режимі глобальної конфігурації.





Рис.7. Увімнкнення захисту BRUD на всіх портах доступу SW-A та SW-B

Крок 3. Увімкнути root guard.



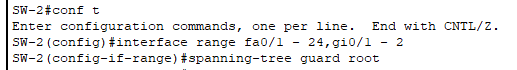


Рис.8. Увімкнення root guard

**Частина 3. Налаштування захисту портів і вимкнення невикористовуваних портів.**

Крок 1. Налаштування базової безпеки на всіх портах, підключених до хост-пристроїв. Зазначену процедуру слід виконати на всіх портах доступу на SW-A та SW-B. Необхідно встановити максимальну кількість отриманих MAC-адрес на 2, дозволити динамічне визначення MAC-адреси та встановити примусове вимкнення при порушеннях. Порт комутатора має бути налаштований як порт доступу, щоб увімкнути захист порту.

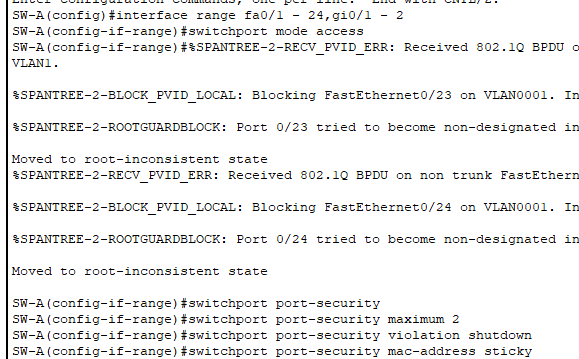


Рис.9. Налаштування базової безпеки на SW-A

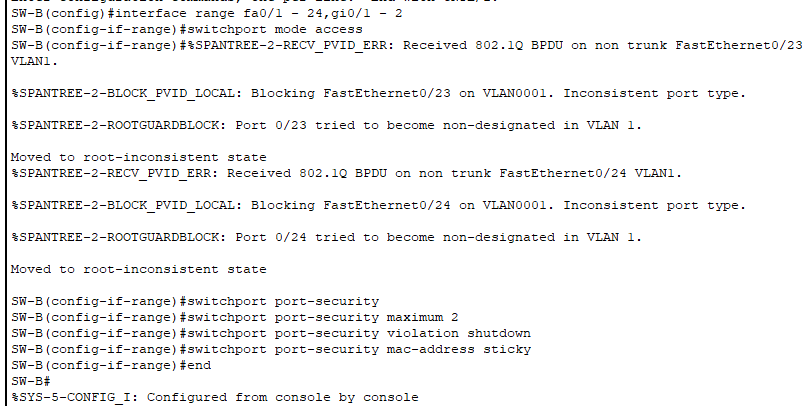


Рис.10. Налаштування базової безпеки на SW-B

Крок 2. Перевірка безпеки порту.

На SW-A виконуємо команду show port-security interface f0/1, щоб переконатися, що безпеку порту налаштовано.

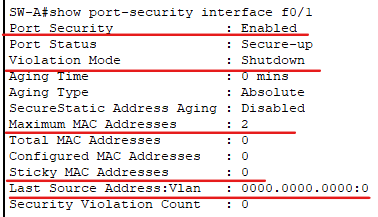
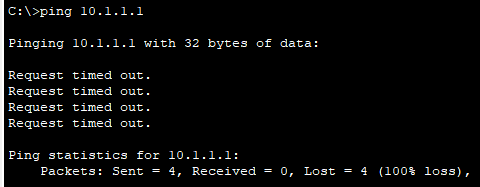


Рис.11. Перевірки безпеки порту на SW-A

Виконаємо тестування від C1 до C2 і знову виконуємо команду show port-security interface f0/1, щоб переконатися, що комутатор отримав MAC-адресу для C1.



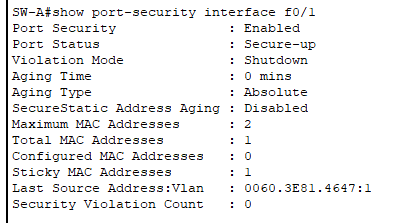
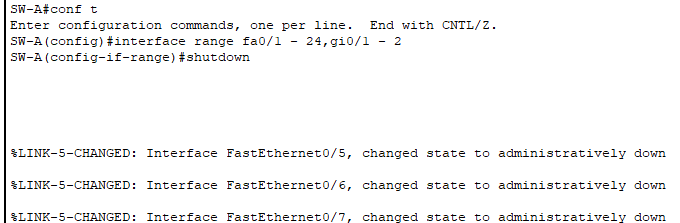


Рис.12. Тестування та перевірка отримання комутатором MAC-адреси

Крок 3. Відключення портів, що не використовуються.

Скористаємось командою shutdown в режимі глобальної конфігурації для того, щоб відключити невикористані порти на комутаторах SW-A та SW-B.



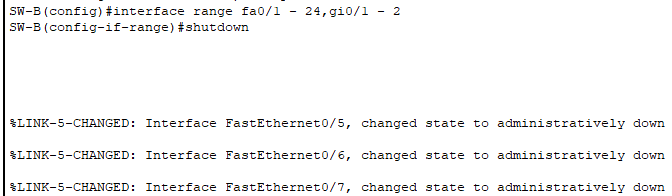


Рис.13. Відключення портів, що не використовуються на SW-A та SW-B

Виконуємо перевірку результатів виконання сценарію1.

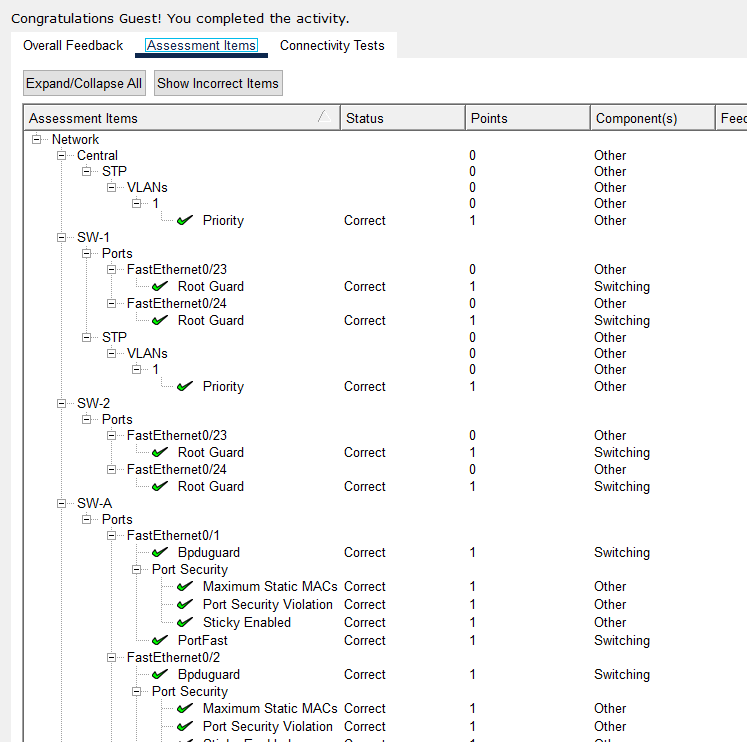




Рис.14. Перевірка результатів виконання сценарію 1

**СЦЕНАРІЙ 2**

**Частина 1. Перевірка підключення.**

Крок 1. Перевірити підключення між C2 (VLAN 10) і C3 (VLAN 10)

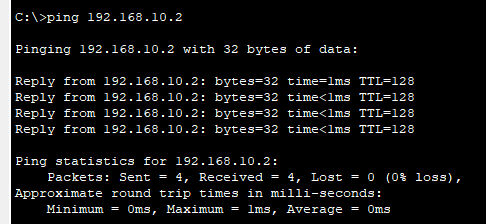


Рис.15. Перевірка підключення між C2 (VLAN 10) і C3 (VLAN 10)

Крок 2. Перевірити підключення між C2 (VLAN 10) і D1 (VLAN 5).

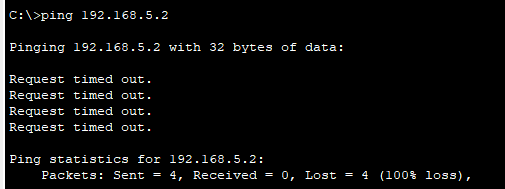


Рис.15. Перевірка підключення між C2 (VLAN 10) і D1 (VLAN 5)

**Частина 2. Створення резервного зв’язку між SW-1 і SW-2.**

Крок 1. З’єднання SW-1 і SW-2.

За допомогою перехресного кабелю з’єднуємо порт F0/23 на SW-1 з портом F0/23 на SW-2.

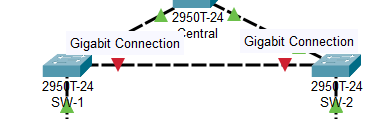


Рис.16. З’єднання SW-1 і SW-2

Крок 2. Увімкнути транкінг, включаючи всі механізми безпеки магістралі на каналі іж SW-1 і SW-2.







Рис.17. Увімкнення тракінгу на каналах між SW-1 та SW-2

**Частина 3. Увімкнути VLAN 20 як VLAN керування.**

Крок 1. Увімкнути VLAN керування (VLAN 20) на SW-A.

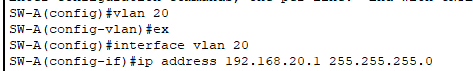
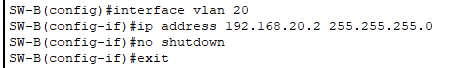
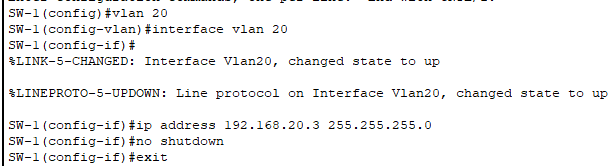


Рис.18. Увімкнення VLAN 20 на SW-A

Крок 2. Увімкнути ту саму VLAN керування на всіх інших комутаторах.





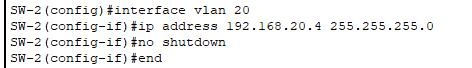


Рис.19. Увімкнення VLAN 20 на всіх інших комутаторах

Крок 3. Підключити і налаштувати керуючий РС до порту SW-A F0/1.

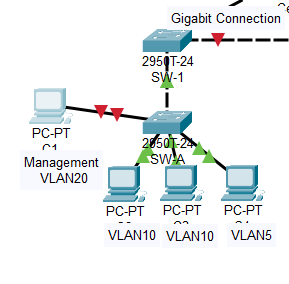


Рис.20. Підключення і налаштування керуючого PC до SW-A F0/1

Крок 4. На SW-A переконатися, що керуючий РС є частиною VLAN 20.

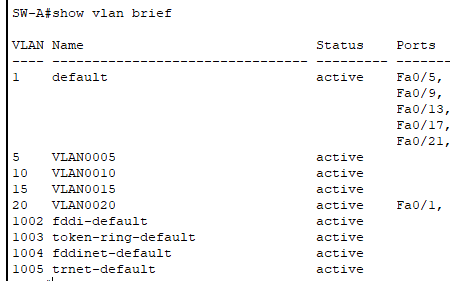
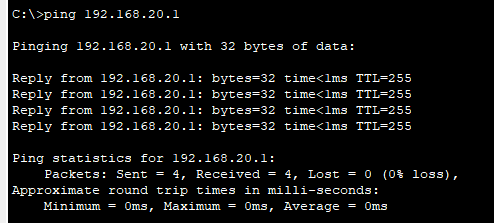


Рис.21. Переконуємось, що керуючий PC є частиною VLAN 20

Крок 5. Перевірити підключення керуючого РС до всіх комутаторів.



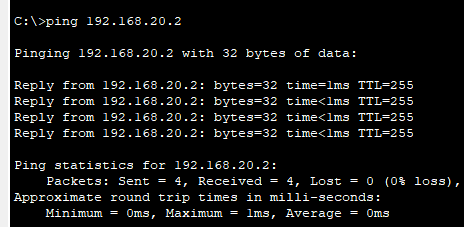


Рис.22. Перевіряємо, що керуючий PC з’єднаний з комутаторами

**Частина 4. Увімкнути керуючий РС для доступу до маршрутизатора R1.**

Крок 1. Увімкнути новий підінтерфейс на маршрутизаторі R1.

Створюємо підінтерфейс g0/0.3 і встановити інкапсуляцію на dot1q 20 для обліку VLAN 20.

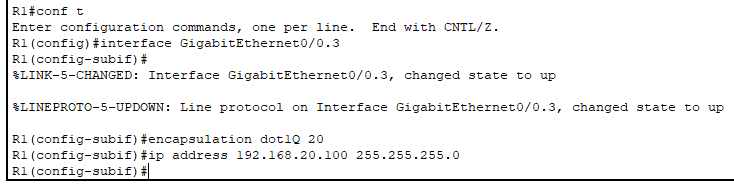


Рис.23. Увімкнення підінтерфейсу на R1

Крок 2. Перевірити з’єднання між РС керування та R1.

Перевіряємо шляхом пінгування на ip-адресу R1.

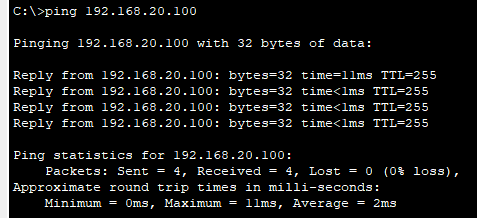


Рис.24. Перевірка з’єднання між PC та R1

Крок 3. Увімкнути захист.

Хоча керуючий РС повинен мати доступ до маршрутизатора, жоден інший РС не повинен мати доступ до керуючої VLAN. Тому Створюємо ACL, який надає доступ до маршрутизатора лише керуючому РС. Застосувати ACL до належного інтерфейсу.

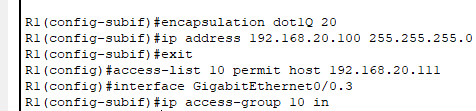


Рис.25. Увімкнення захисту

Крок 4. Перевірка безпеки.

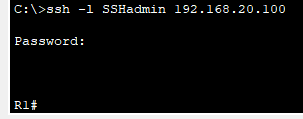


Рис.26. Перевірка безпеки

Крок 5. Перевірка результатів.

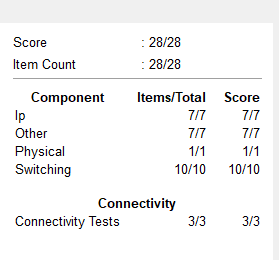


Рис.27. Перевірка результатів

**Висновок:**

У результаті виконання лабораторної роботи було набуто практичні навички в емуляторі Cisco Packet Tracer та досліджено особливості налаштування безпеки рівня 2 та захищеного функціонування VLAN 20.