**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 №2**

**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 автентифікації ААА на маршрутизаторах Cisco.

**Поставлене завдання:**

1. Налаштувати локальний обліковий запис користувача на R1 та налаштувати автентифікацію на консолі та лінії vty за допомогою локального AAA.

2. Перевірити локальну автентифікацію AAA з консолі R1 і клієнта PC-A.

3. Налаштувати серверну автентифікацію AAA за допомогою TACACS+.

4. Перевірити автентифікацію AAA на сервері від клієнта PC-B.

5. Налаштувати автентифікацію AAA на основі сервера за допомогою RADIUS.

6. Перевірити автентифікацію AAA на сервері від клієнта PC-C.

**Результат виконання роботи**

1. Для початку здійснимо перевірку підключення. Для цього потрібно здійснити пінгування з PC-A на PC-B, з PC-A на PC-C та з PC-B на PC-C. Скористаємось командою ping <ip address>:

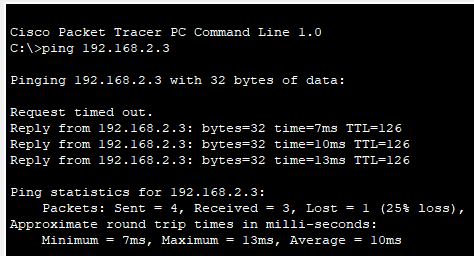


Рис.1.Пінгування з PC-A на PC-B

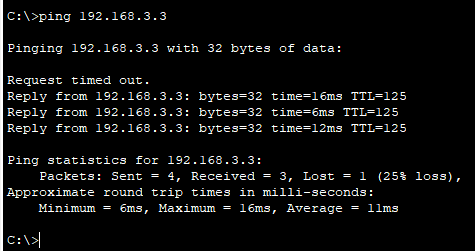


Рис.2.Пінгування з PC-A на PC-C

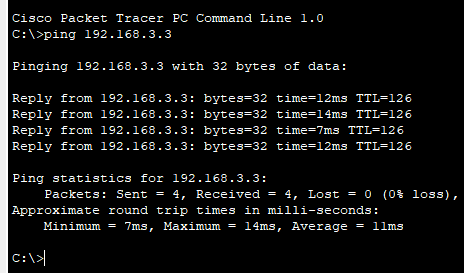


Рис.3.Пінгування з PC-B на PC-C

Далі виконуємо налаштування локального імені користувача на R1(CLI). Потрібно налаштувати ім’я користувача **Admin1** із секретним паролем **admin1pa55**. Для цього скористаємось командою **R1#configure terminal** та **R1(config)# username Admin1 secret admin1pa55**.

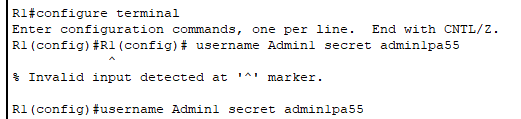


Рис.4.Налаштування локального імені користувача на R1

Вмикаємо AAA (aaa new-model) на R1 і налаштовуємо автентифікацію AAA (aaa authentication login default local) для входу в консоль для використання локальної БД.



Рис.5.Увімкнення та налаштування автентифікації ААА на R1

Вмикаємо AAA (line console 0) на R1 і налаштуйте автентифікацію AAA для входу в лінійну консоль (login authentication default), щоб використовувати список методів за замовчуванням.



Рис.6.Налаштування лінійної консолі на R1

Виконуємо перевірку методу автенифікації ААА, перед цим перезавантаживши роутер (reload):

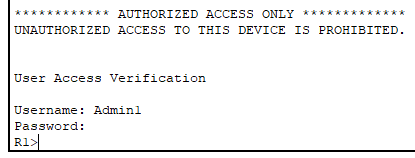


Рис.7.Перевірка автентифікації

1. Перейдемо до налаштування локальної автентифікації на R1 для лінії vty. Будемо використовувати **ccnasecurity.com** як доменне ім’я на R1 (**# ip domain-name ccnasecurity.com**).



Рис.8.Установка доменного імені

Після чого можна створити криптографічний RSA ключ 1024 біт (**crypto key generate rsa**).

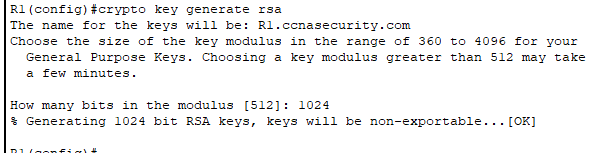


Рис.9.Створення криптографічного RSA ключа

Тепер можемо налаштувати метод автентифікації іменованого списку та vty-лінії.

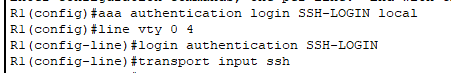


Рис.10.Налаштування автентифікації та vty-лінії

Виконаємо перевірку методу автентифікації, через PC-A:



Рис.11.Перевірка методу автентифікації

1. Налаштуємо автентифікації ААА за допомогою TACAS+ на R2. Спочатку налаштуємо резервний запис локальної бази даних Admin. Для резервного копіювання налаштуємо локальне ім’я Admin і пароль admin2pa55

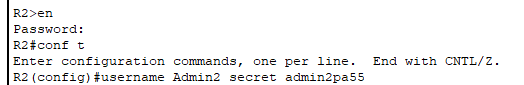


Рис.12.Створення та налаштування резервного облікового запису

Перевіримо конфігурацію сервера TACACS+. Для цього ЛКМ => Server-PC TACACS+ => Services => AAA.

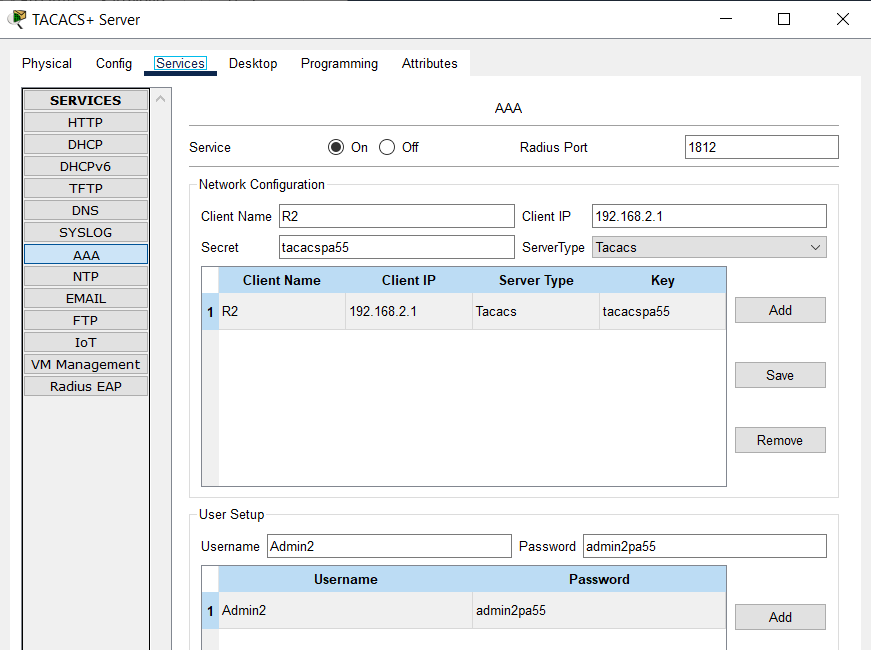


Рис.13.Перевірка конфігурації TACACS+ сервера

Налаштуємо IP-адресу сервера TACACS+ ААА (**tacacs-server host 192.168.2.2**) і ключ на R2(**tacacs-server key tacacspa55**).

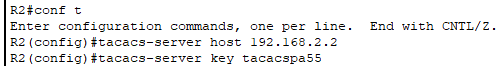


Рис.14.Налаштування IP-адреса Tacacs+

Тепер потрібно на R2 AAA налаштувати всі входи для автентифікації за допомогою сервера AAA TACACS+.



Рис.15.Налаштування консольного входу на R2

Залишилось налаштувати лінійну консоль



Рис.16.Налаштування консольного входу на R2

Перевіримо метод автентифікації ААА.

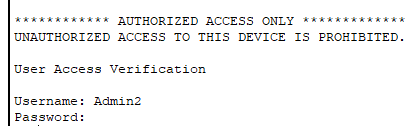


Рис.17.Перевірка автентифікації

Налаштуємо автентифікацію R3 AAA на основі сервера за допомогою RADIUS. Для цілей резервного копіювання налаштуємо локальне ім’я користувача **Admin3** і пароль **admin3pa55**.

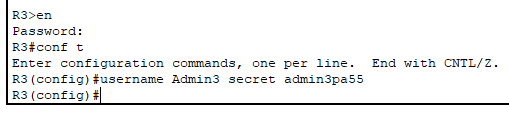


Рис.18.Налаштування локального імені і паролю для резервного копіювання

Перевіримо конфігурацію сервера RADIUS. Для цього перейдемо ЛКМ => Server-PC RADIUS => Services => AAA.

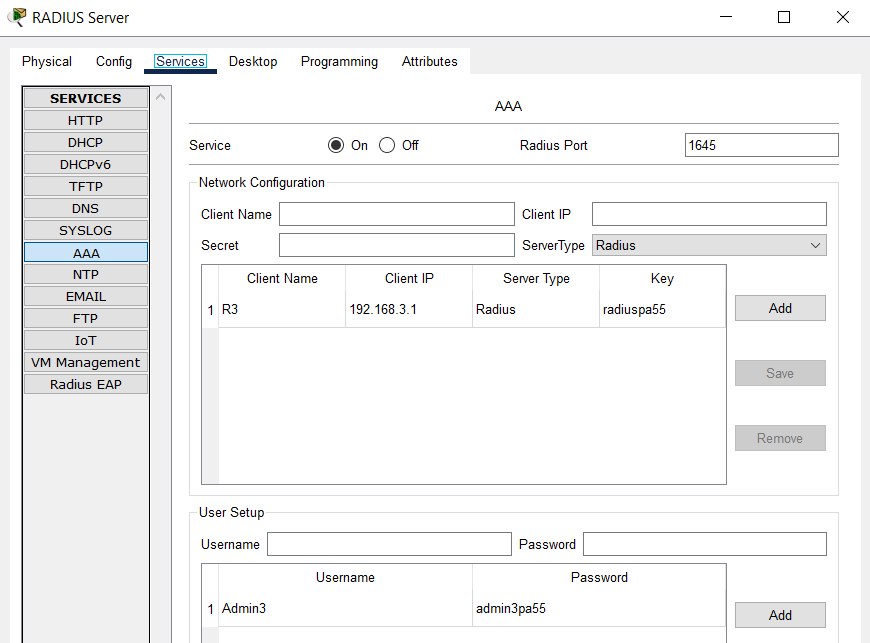


Рис.19.Перевірка конфігурації ААА сервера RADIUS

Налаштуємо IP-адресу сервера AAA RADIUS (**radius-server host 192.168.3.2**) і секретний ключ на R3(**radius-server key radiuspa55**).

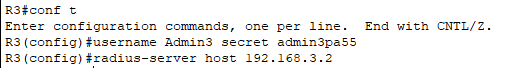
****

Рис.20.Налаштування IP-адресу сервера RADIUS і ключа на R3

Тепер потрібно на R3 AAA налаштувати всі входи для автентифікації за допомогою сервера AAA RADIUS.



Рис.21.Налаштування консольного входу на R3

А також налаштувати лінійну консоль.

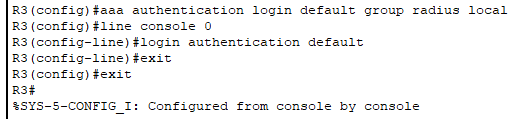


Рис.22.Налаштування лінійної консолі

Перевірка методу автентифікації ААА

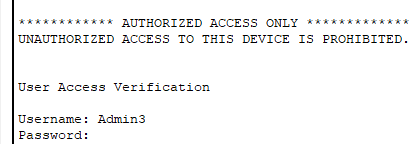
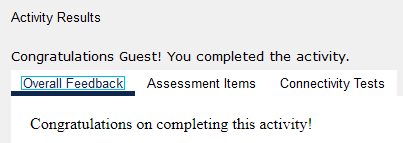
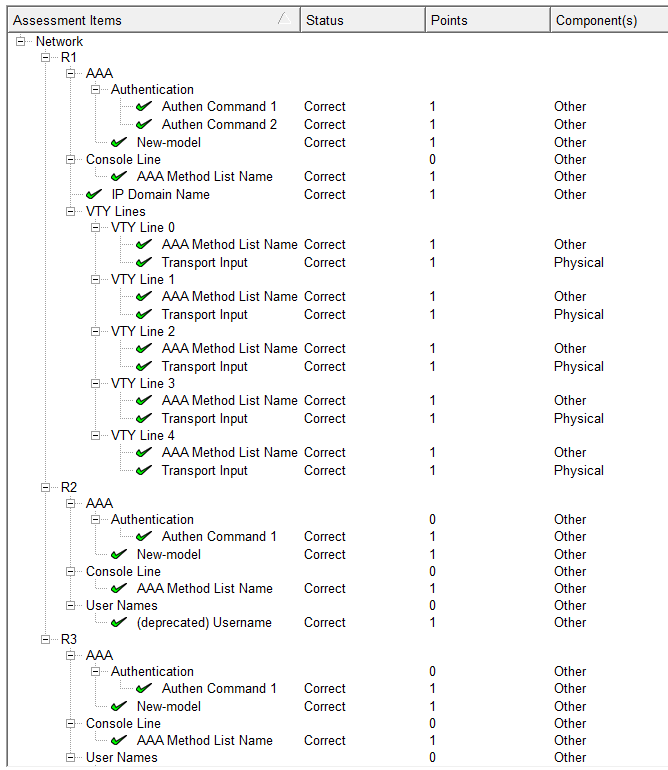


Рис.23.Перевірка атентрифікації на R3

Перевіримо результати. Має бути не менше 80%.

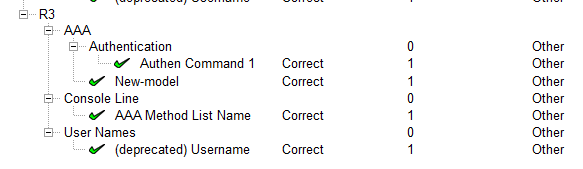
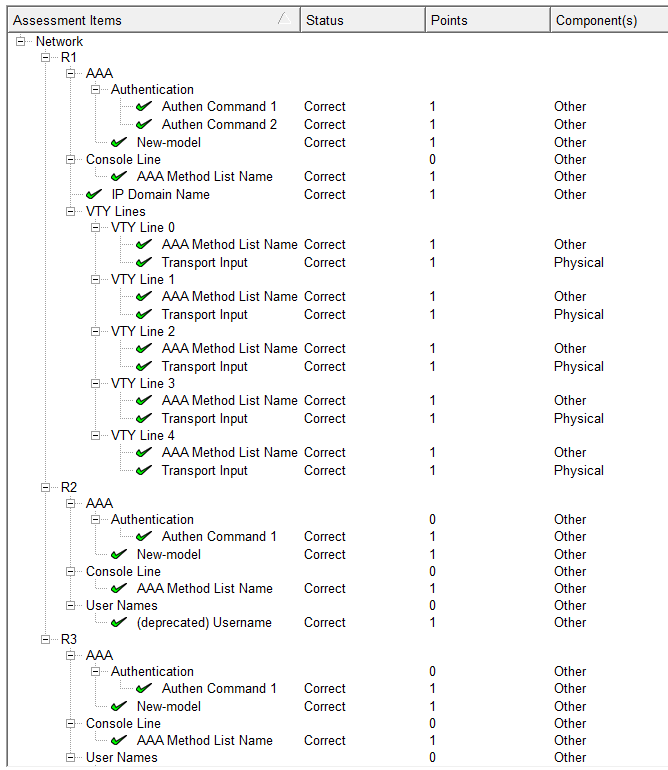


Рис.24.Перевірка результатів роботи

**Висновок:**

У результаті виконання лабораторної роботи отримано перші навички роботи з Cisco Packet Tracer. Виконано налаштування системи AAA на маршутизаторах та серверах Cisco, що дозволило краще зрозумыти принципи функціонування та застосування.