ІВАНО-ФРАНКІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ НАФТИ І ГАЗУ

Проектування системи керування доступом до мережі на основі протоколу 802.1X для IoT-інфраструктури

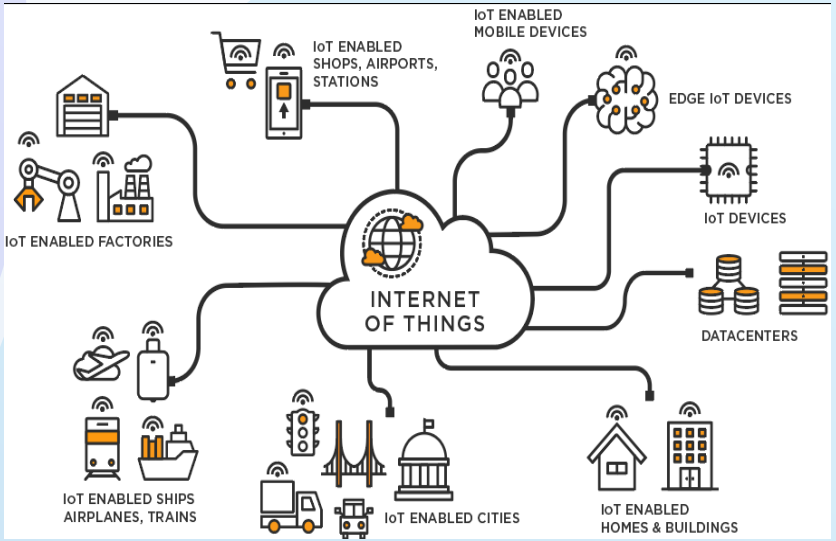
Бакалаврська робота

Виконав: ст. гр. ІСТ-22-1 Ваків В.А.
Керівник: к.т.н., доц. Заміховська О. Л.

Івано-Франківськ - 2026

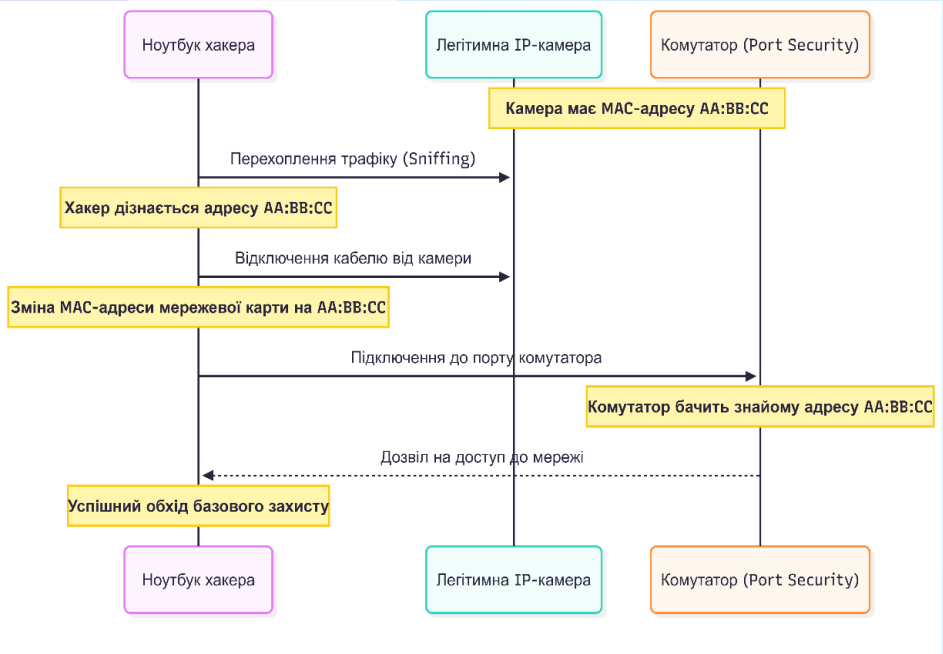
Актуальність дослідження

- **Масове розгортання IoT-пристроїв:** Стрімке впровадження IP-камер, датчиків та сенсорів у відкритих і загальнодоступних зонах.
- **Вразливість фізичного периметра:** Ризик прямого підключення хакера до внутрішньої інфраструктури через звичайний мережевий кабель пристрою.
- **Неефективність класичного захисту:** Традиційні фаєрволи та антивіруси захищають лише зовнішній периметр (від Інтернету) і безсилі проти внутрішніх атак.



Проблематика існуючих рішень

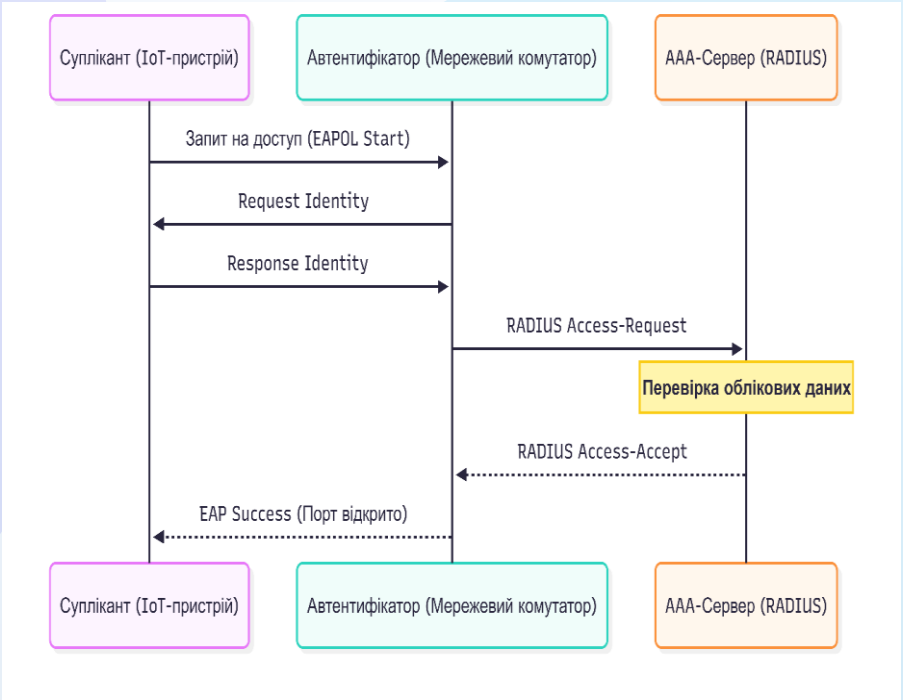
- Неефективність застарілої технології Port Security;
- Вразливість до атак MAC Spoofing (підміна апаратних адрес);
- «Headless» формат IoT-пристроїв (відсутність екранів);
- Необхідність переходу до парадигми Zero Trust.



Концепція та архітектура 802.1X

Головним об'єктом дослідження обрано стандарт IEEE 802.1X.

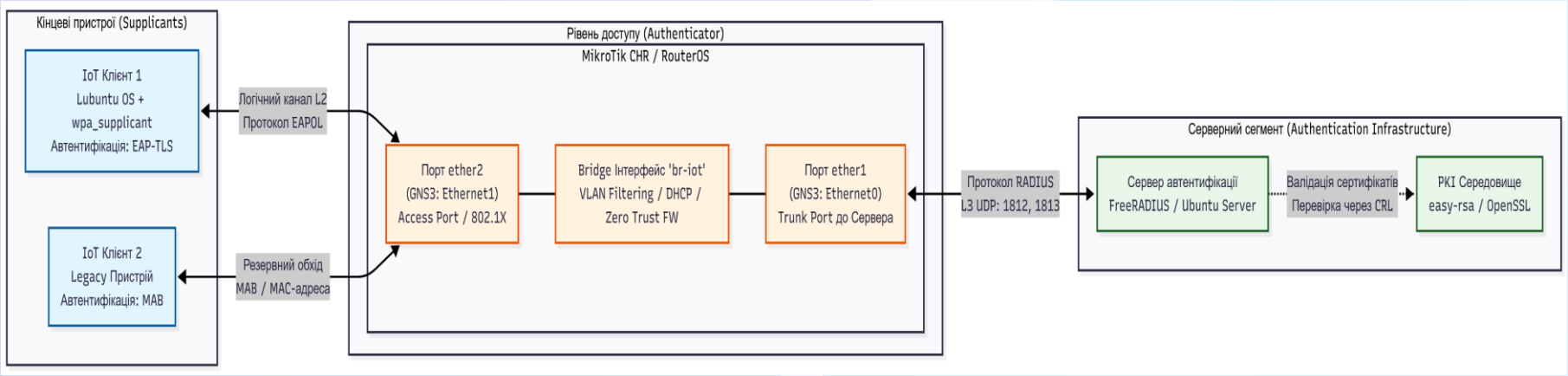
- Строгий контроль доступу на канальному рівні (L2);
- 3 компоненти: Суплікант, Автентифікатор, Сервер;
- Логічний поділ порту на контрольований та неконтрольований канали.



Вибір інструментарію (Open Source)

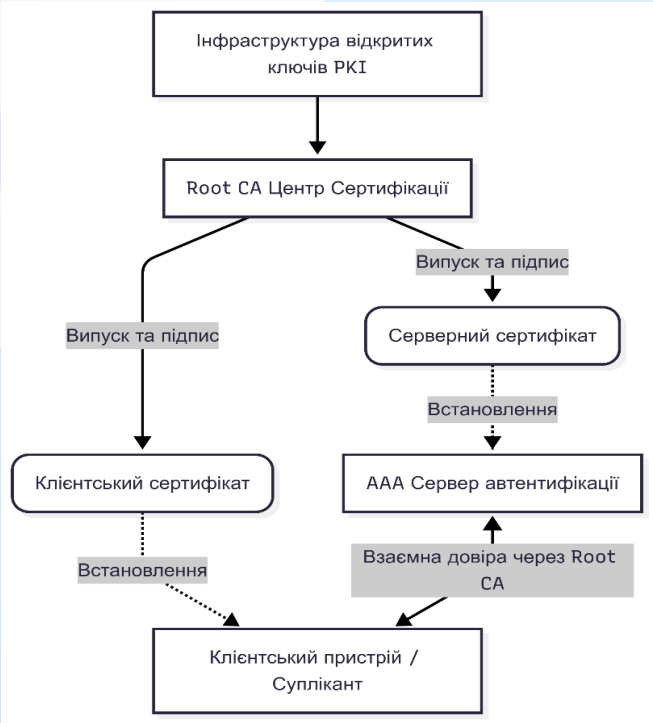
- AAA-сервер: FreeRADIUS
- Мережевий автентифікатор: MikroTik RouterOS
- Центр сертифікації (PKI): easy-rsa (Ubuntu Server)

Структурно-логічна схема мережі

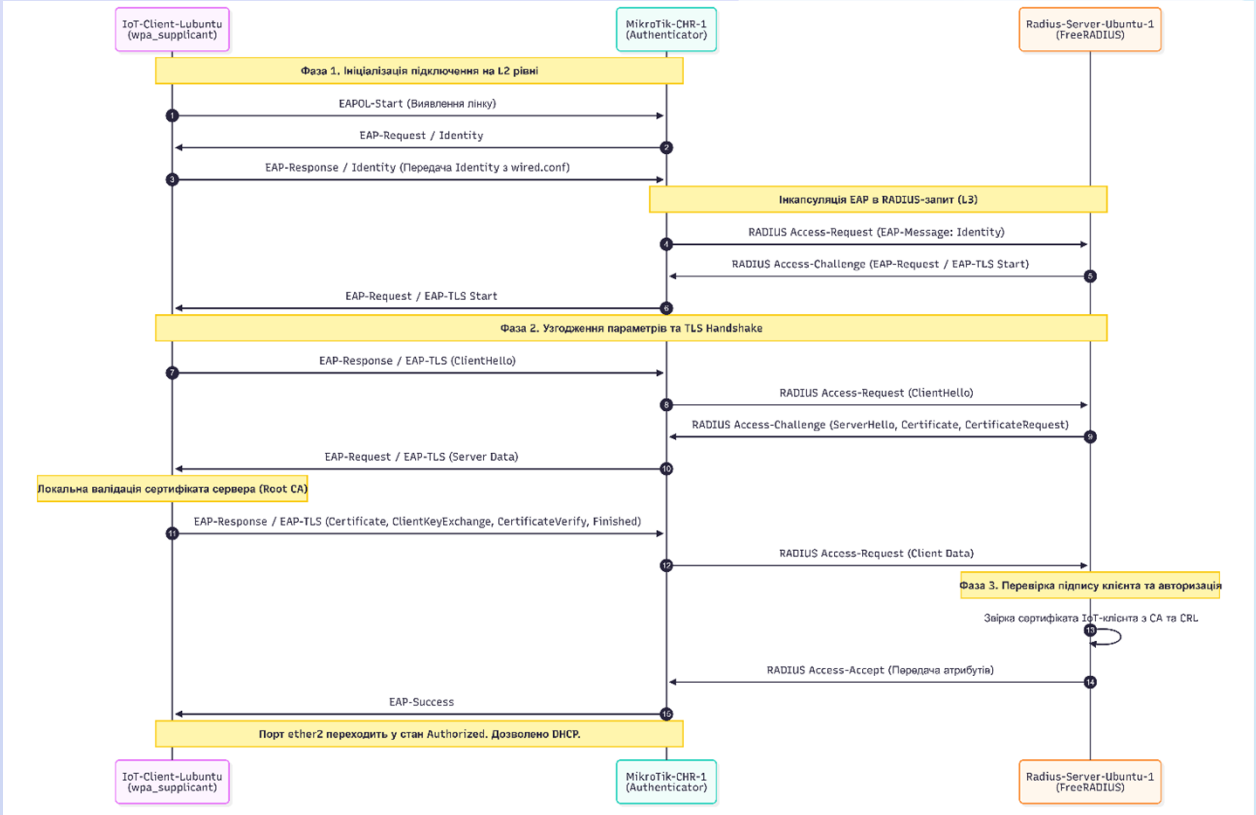


Інфраструктура відкритих ключів (PKI)

- Повна відмова від традиційних паролів для автономного обладнання;
- Генерація цифрових сертифікатів стандарту X.509;
- Еліптична криптографія у форматі «nopass»;
- Здатність до автономного відновлення зв'язку.



Механізм автентифікації EAP-TLS



Політики доступу: Мікросегментація та MAB

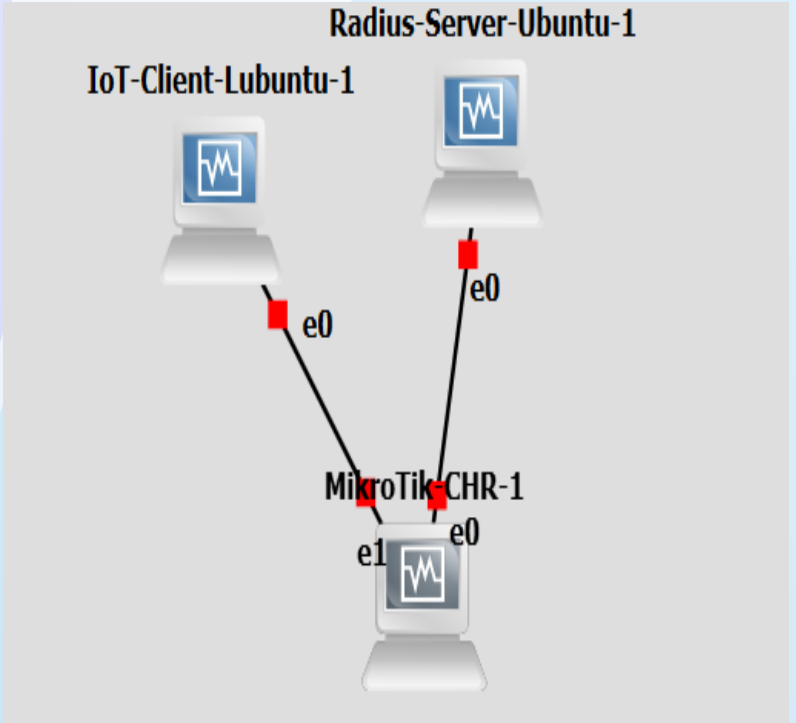
ПОЛІТИКА 1 (Легітимні пристрої):
• Динамічна мікросегментація після перевірки сертифіката;
• Призначення ізольованого VLAN 20.
ПОЛІТИКА 2 (Застаріле обладнання):
• Резервний гібридний режим MAB;
• Примусова ізоляція у карантинному VLAN 30.

```
"iot-client"
        Tunnel-Type = VLAN,
        Tunnel-Medium-Type = IEEE-802,
        Tunnel-Private-Group-Id = "20"

"00:11:22:33:44:55" Cleartext-Password := "00:11:22:33:44:55"
        Tunnel-Type = VLAN,
        Tunnel-Medium-Type = IEEE-802,
        Tunnel-Private-Group-Id = "30"
```

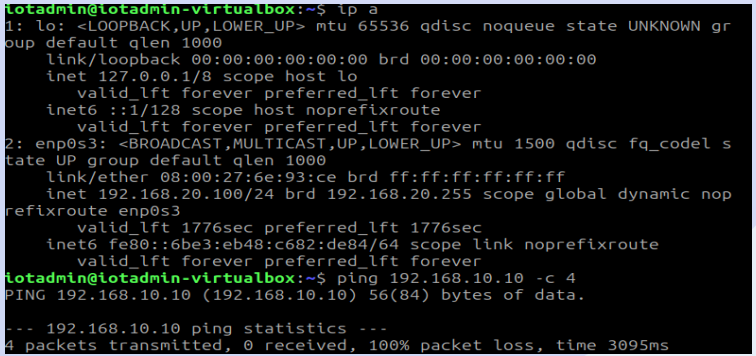
Топологія тестового стенда

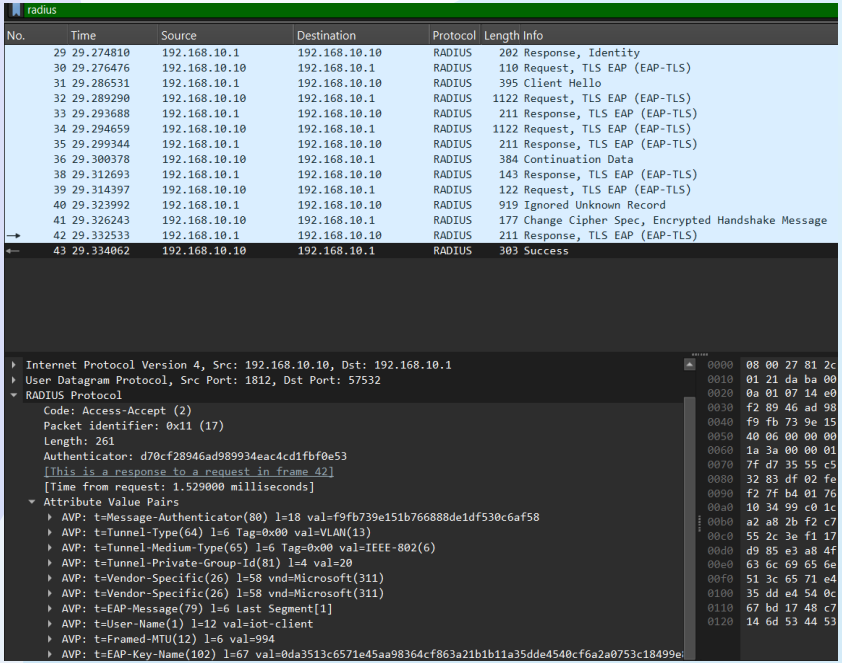
- Середовище глибокої мережевої симуляції: GNS3;
- Ресурси IoT-супліканта: 1 vCPU, 512 MB RAM;
- Інспекція пакетів (DPI): Аналізатор Wireshark.



Тест 1: Штатна робота EAP-TLS

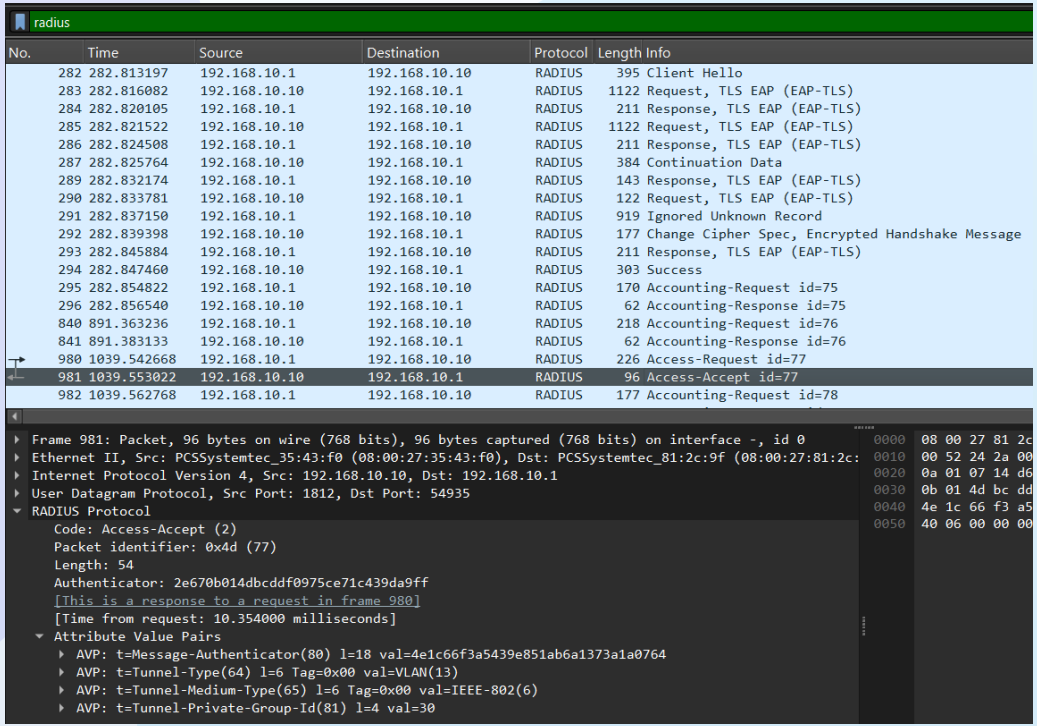
- Успішне криптографічне рукостискання (TLS Handshake);
- Отримання пакета Access-Accept;
- Динамічне призначення VLAN 20;
- Блокування ICMP-запитів до сервера (Zero Trust).





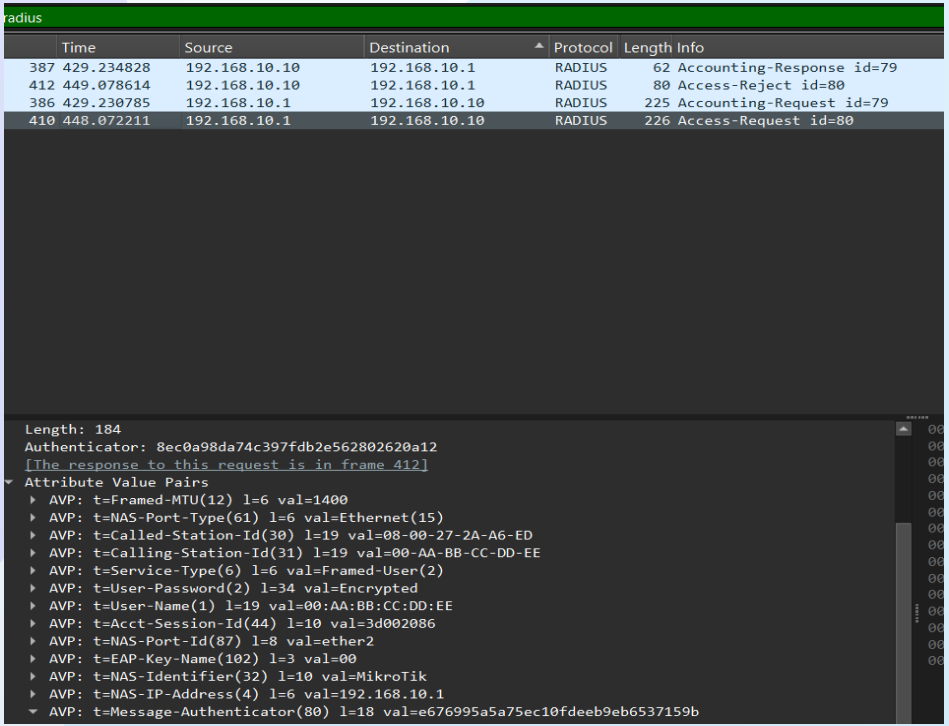
Тест 2: Резервний режим MAB

- 6-секундний таймаут очікування EAP-відповіді;
- Авторизація за апаратною MAC-адресою;
- Примусова ізоляція вузла (Tunnel-Private-Group-Id = 30).



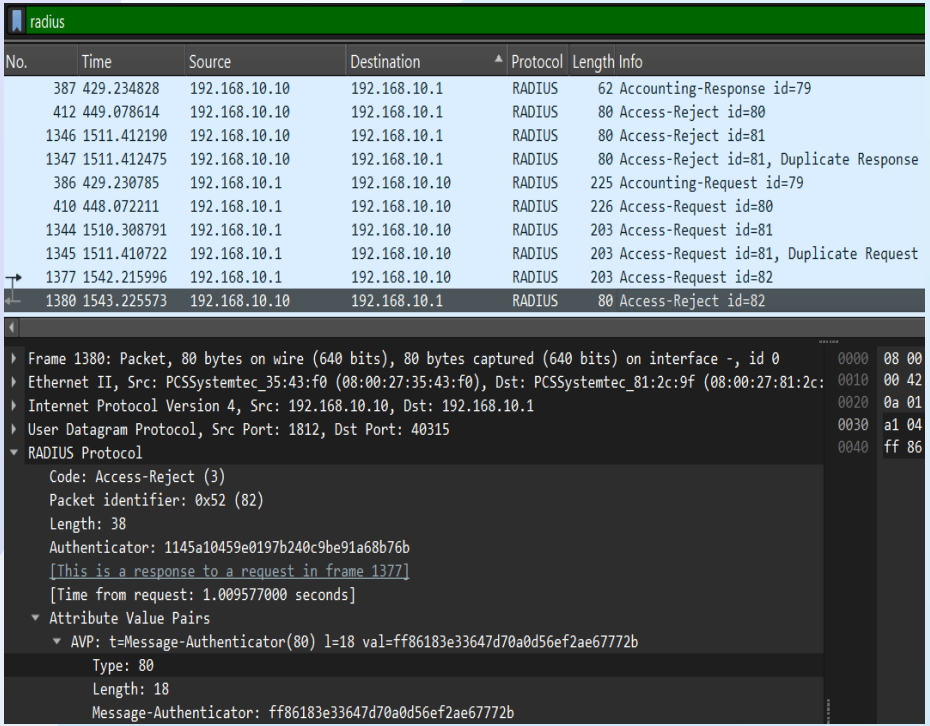
Тест 3: Захист від MAC Spoofing

- Підміна апаратної адреси клієнта на неавторизовану;
- Відсутність адреси у файлі конфігурації users;
- Миттєва генерація повідомлення Access-Reject;
- Надійне апаратне блокування порту периметра.



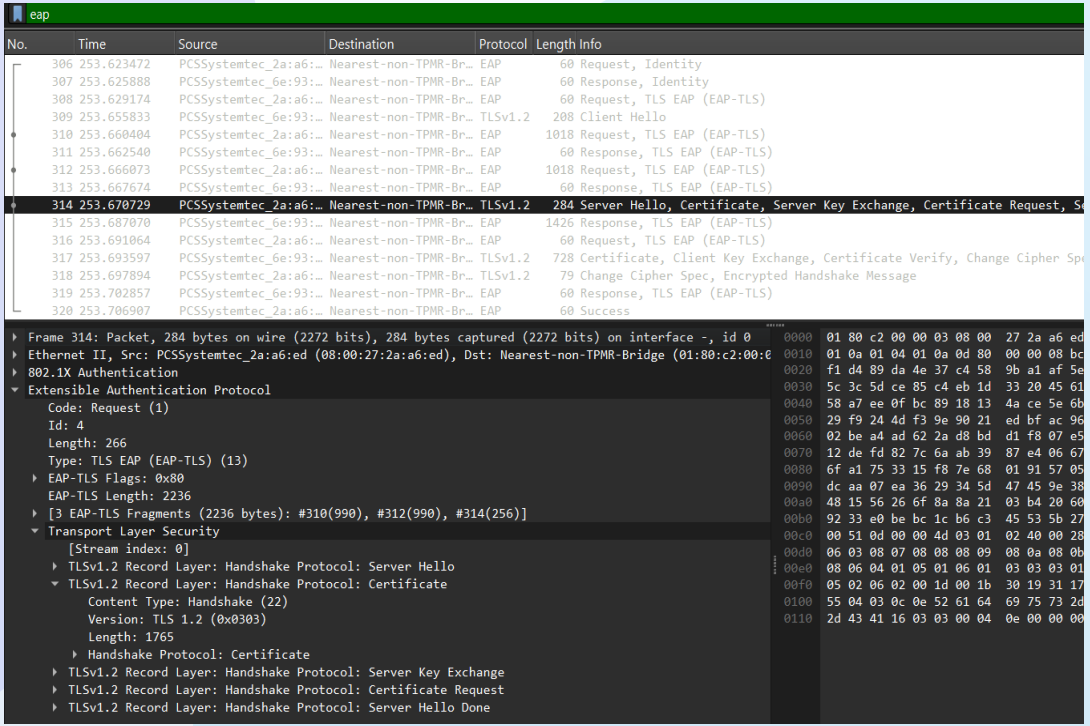
Тест 4: Відкликання сертифікатів (CRL)

- Імітація фізичної крадіжки легітимного пристрою;
- Анулювання мандата та оновлення файлу crl.pem;
- Виявлення компрометації модулем EAP;
- Перехід порту у стан Unauthorized.



Аналіз операційної ефективності

- Тривалість повної перевірки (TLS Handshake): ~83 мілісекунди;
- Максимальне навантаження на канал: 1122 байти;
- Відсутність перевантажень комутаційного обладнання;
- Повна придатність для індустріальних IoT-мереж.



ВИСНОВКИ

1. Перехід до Zero Trust: Успішно спроєктовано систему контролюдоступу на базі IEEE 802.1X та EAP-TLS, що усуває вразливості "headless" IoT-пристроїв.
2. Динамічна мікросегментація: Реалізовано автоматичний розподіл пристроїв по ізольованих VLAN та налаштовано механізм MAB для застарілого обладнання.
3. Економічна ефективність: Архітектуру побудовано виключно на базі відкритого ПЗ (FreeRADIUS, MikroTik, easy-rsa), що мінімізує витрати на впровадження.
4. Апробація: Працездатність підтверджено у середовищі GNS3. Результати опубліковано на Міжнародній конференції «Synergy of Knowledge»

Дякую за увагу!