

ІВАНО-ФРАНКІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ НАФТИ
І ГАЗУ

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

Бакалаврська робота

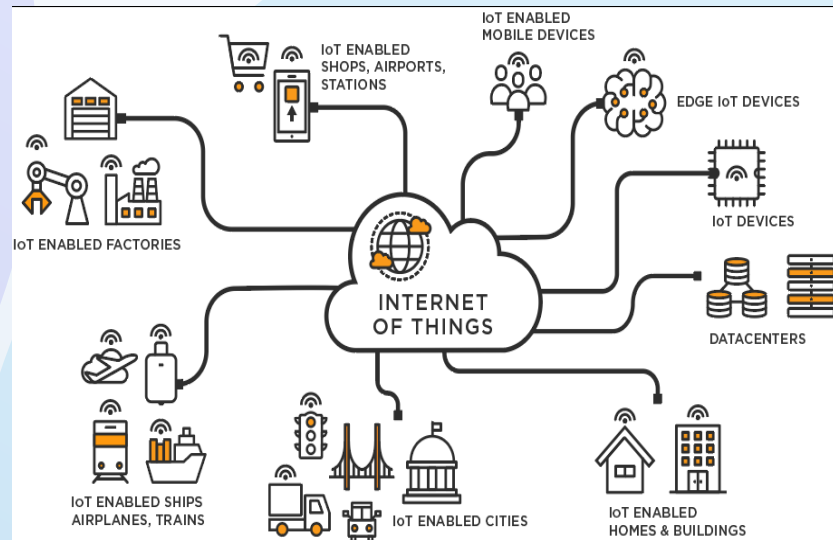
Виконав: ст. гр. ICT-22-1 Ваків В.А.

Керівник: к.т.н., доц. Заміховська О. Л.

Івано-Франківськ - 2026

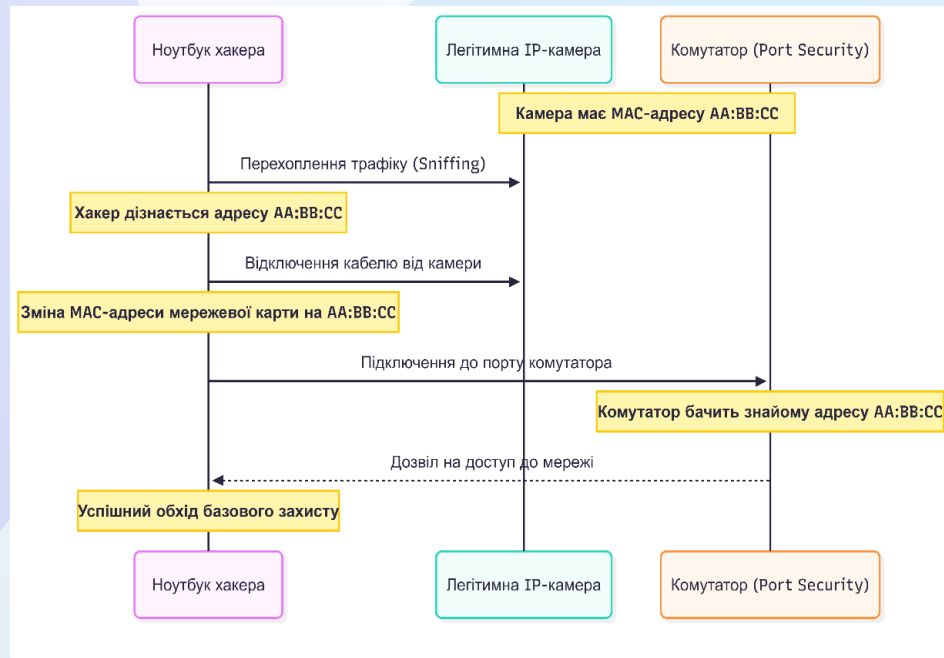
Актуальність дослідження

- **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

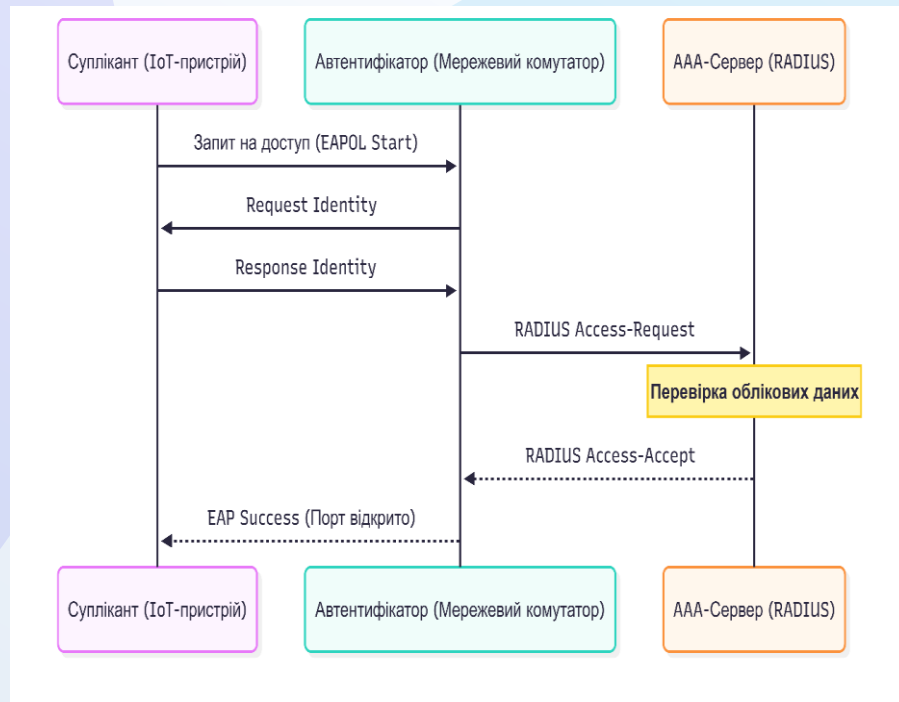
- Неефективність застарілої технології Port Security;
- Вразливість до атак MAC Spoofing (підміна апаратних адрес);
- «Headless» формат IoT-пристроїв (відсутність екранів);
- Необхідність переходу до парадигми Zero Trust.



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.

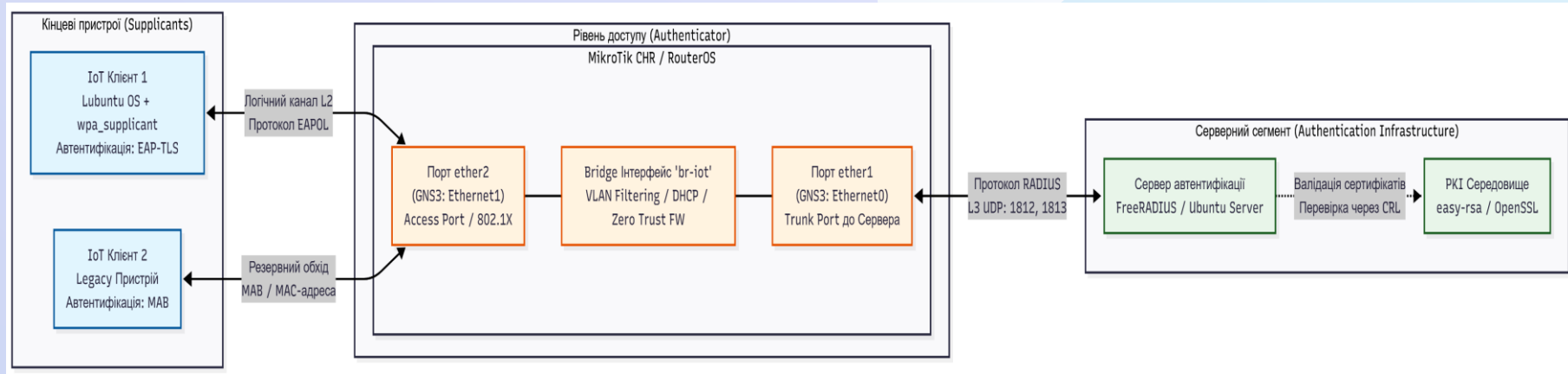


Вибір інструментарію (Open Source)

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

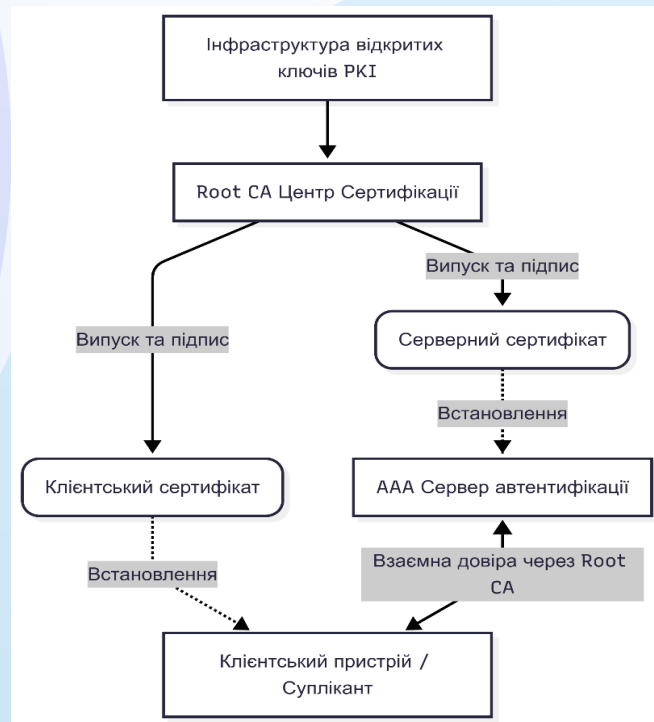


Структурно-логічна схема мережі

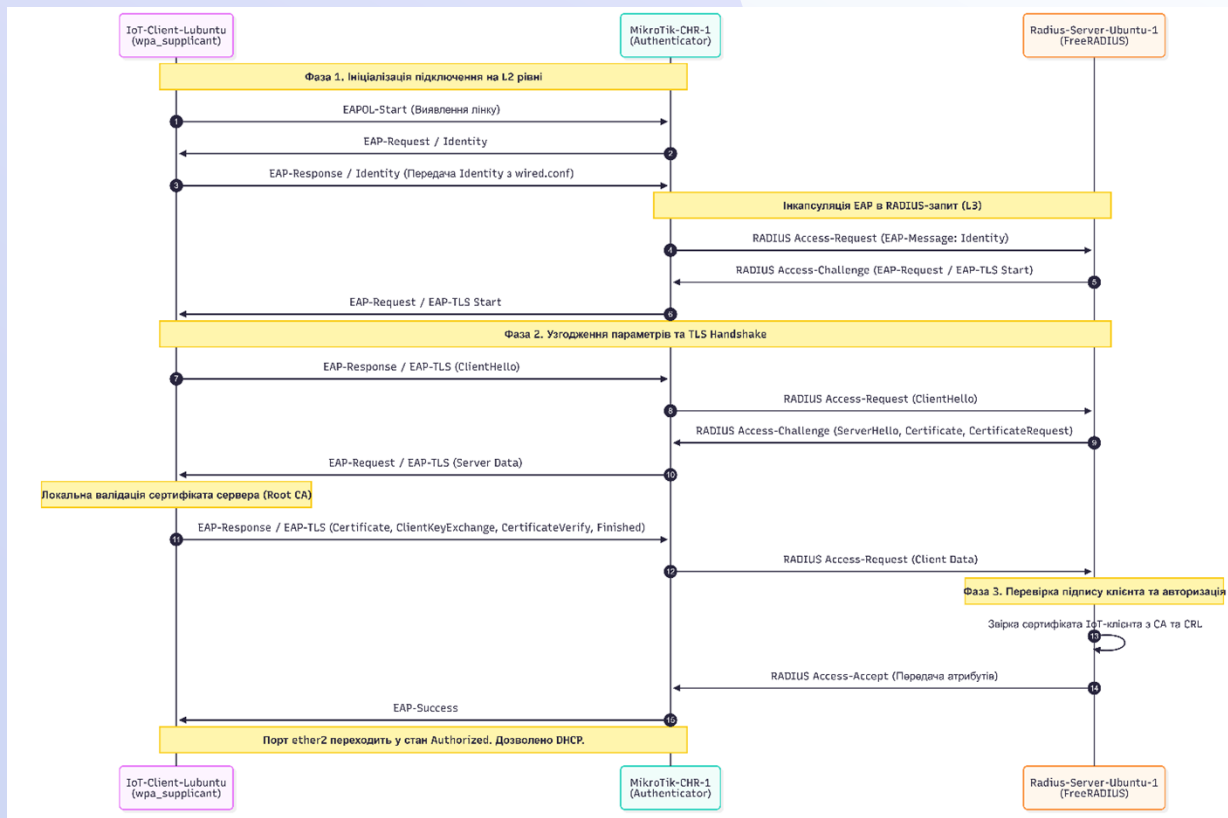


Інфраструктура відкритих ключів (PKI)

- 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.

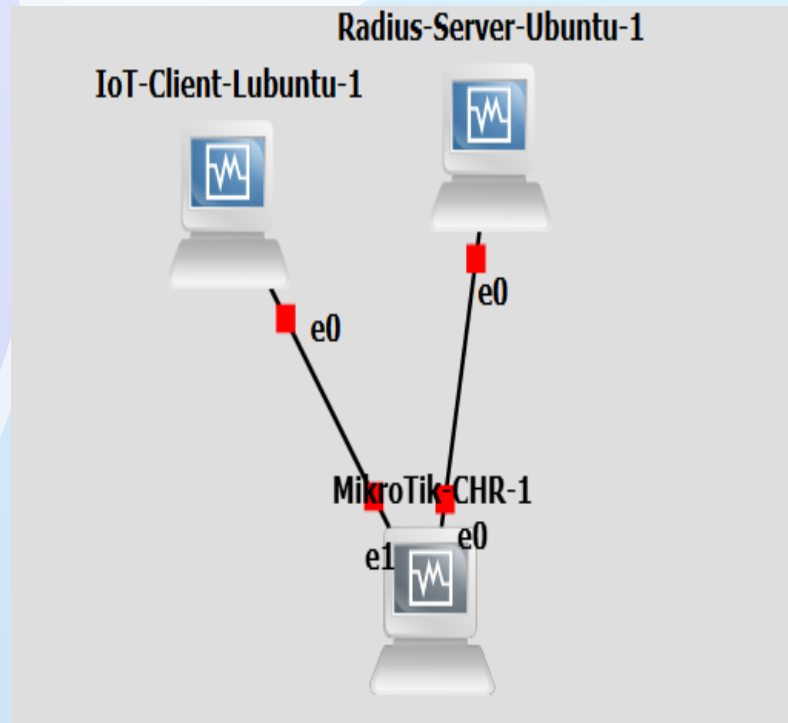
ПОЛІТИКА 2 (Застаріле обладнання):

- 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).

```
lotadmin@lotadmin-virtualbox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN gr
oup default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel s
tate UP group default qlen 1000
    link/ether 08:00:27:6e:93:ce brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.100/24 brd 192.168.20.255 scope global dynamic nop
refixroute enp0s3
        valid_lft 1776sec preferred_lft 1776sec
    inet6 fe80::6be3:eb48:c682:de84/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
lotadmin@lotadmin-virtualbox:~$ ping 192.168.10.10 -c 4
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.

--- 192.168.10.10 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3095ms
```

No.	Time	Source	Destination	Protocol	Length	Info
29	29.274810	192.168.10.1	192.168.10.10	RADIUS	202	Response, Identity
30	29.276476	192.168.10.10	192.168.10.1	RADIUS	110	Request, TLS EAP (EAP-TLS)
31	29.286531	192.168.10.1	192.168.10.10	RADIUS	395	Client Hello
32	29.289290	192.168.10.10	192.168.10.1	RADIUS	1122	Request, TLS EAP (EAP-TLS)
33	29.293688	192.168.10.1	192.168.10.10	RADIUS	211	Response, TLS EAP (EAP-TLS)
34	29.294659	192.168.10.10	192.168.10.1	RADIUS	1122	Request, TLS EAP (EAP-TLS)
35	29.299344	192.168.10.1	192.168.10.10	RADIUS	211	Response, TLS EAP (EAP-TLS)
36	29.300378	192.168.10.10	192.168.10.1	RADIUS	384	Continuation Data
38	29.312693	192.168.10.1	192.168.10.10	RADIUS	143	Response, TLS EAP (EAP-TLS)
39	29.314397	192.168.10.10	192.168.10.1	RADIUS	122	Request, TLS EAP (EAP-TLS)
40	29.323992	192.168.10.1	192.168.10.10	RADIUS	919	Ignored Unknown Record
41	29.326243	192.168.10.10	192.168.10.1	RADIUS	177	Change Cipher Spec, Encrypted Handshake Message
42	29.332533	192.168.10.1	192.168.10.10	RADIUS	211	Response, TLS EAP (EAP-TLS)
43	29.334062	192.168.10.10	192.168.10.1	RADIUS	303	Success

Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.10.1		0000	08 00 27 81 2c
User Datagram Protocol, Src Port: 1812, Dst Port: 57532		0010	01 21 da ba 00
RADIUS Protocol		0020	0a 01 07 14 e0
Code: Access-Accept (2)		0030	f2 89 46 ad 98
Packet identifier: 0x11 (17)		0040	f9 fb 73 9e 15
Length: 261		0050	40 06 00 00 00
Authenticator: d70cf28946ad989934eac4cd1fbf0e53		0060	1a 3a 00 00 01
[This is a response to a request in frame 42]		0070	7f d7 35 55 c5
[Time from request: 1.529000 milliseconds]		0080	32 83 df 02 fe
Attribute Value Pairs		0090	f2 7f b4 01 76
AVP: t=Message-Authenticator(80) l=18 val=f9fb739e151b766888de1df530c6af58		00a0	10 34 99 c0 1c
AVP: t=Tunnel-Type(64) l=6 Tag=0x00 val=VLAN(13)		00b0	a2 a8 2b f2 c7
AVP: t=Tunnel-Medium-Type(65) l=6 Tag=0x00 val=IEEE-802(6)		00c0	55 2c 3e f1 17
AVP: t=Tunnel-Private-Group-Id(81) l=4 val=20		00d0	d9 85 e3 a8 4f
AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)		00e0	63 6c 69 65 6e
AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)		00f0	51 3c 65 71 64
AVP: t=EAP-Message(79) l=6 Last Segment[1]		0100	35 dd ed 54 0a
AVP: t=User-Name(1) l=12 val=iot-client		0110	67 bd 17 48 c7
AVP: t=Framed-MTU(12) l=6 val=994		0120	14 6d 53 44 53
AVP: t=EAP-Key-Name(102) l=67 val=Bda3513c6571e45aa98364cf863a21b11a35dde4540cf6a2a0753c18499e			

Тест 2: Резервний режим MAV

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

radius					
No.	Time	Source	Destination	Protocol	Length Info
282	282.813197	192.168.10.1	192.168.10.10	RADIUS	395 Client Hello
283	282.816082	192.168.10.10	192.168.10.1	RADIUS	1122 Request, TLS EAP (EAP-TLS)
284	282.820105	192.168.10.1	192.168.10.10	RADIUS	211 Response, TLS EAP (EAP-TLS)
285	282.821522	192.168.10.10	192.168.10.1	RADIUS	1122 Request, TLS EAP (EAP-TLS)
286	282.824508	192.168.10.1	192.168.10.10	RADIUS	211 Response, TLS EAP (EAP-TLS)
287	282.825764	192.168.10.10	192.168.10.1	RADIUS	384 Continuation Data
289	282.832174	192.168.10.1	192.168.10.10	RADIUS	143 Response, TLS EAP (EAP-TLS)
290	282.833781	192.168.10.10	192.168.10.1	RADIUS	122 Request, TLS EAP (EAP-TLS)
291	282.837150	192.168.10.1	192.168.10.10	RADIUS	919 Ignored Unknown Record
292	282.839398	192.168.10.10	192.168.10.1	RADIUS	177 Change Cipher Spec, Encrypted Handshake Message
293	282.845884	192.168.10.1	192.168.10.10	RADIUS	211 Response, TLS EAP (EAP-TLS)
294	282.847460	192.168.10.10	192.168.10.1	RADIUS	303 Success
295	282.854822	192.168.10.1	192.168.10.10	RADIUS	170 Accounting-Request id=75
296	282.856540	192.168.10.10	192.168.10.1	RADIUS	62 Accounting-Response id=75
840	891.363236	192.168.10.1	192.168.10.10	RADIUS	218 Accounting-Request id=76
841	891.383133	192.168.10.10	192.168.10.1	RADIUS	62 Accounting-Response id=76
980	1039.542668	192.168.10.1	192.168.10.10	RADIUS	226 Access-Request id=77
981	1039.553022	192.168.10.10	192.168.10.1	RADIUS	96 Access-Accept id=77
982	1039.562768	192.168.10.1	192.168.10.10	RADIUS	177 Accounting-Request id=78

▶ Frame 981: Packet, 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface -, id 0	0000	08 00 27 81 2c
▶ Ethernet II, Src: PCSSystemtec_35:43:f0 (08:00:27:35:43:f0), Dst: PCSSystemtec_81:2c:9f (08:00:27:81:2c:9f)	0010	00 52 24 2a 00
▶ Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.10.1	0020	0a 01 07 14 d6
▶ User Datagram Protocol, Src Port: 1812, Dst Port: 54935	0030	0b 01 4d bc dd
▼ RADIUS Protocol	0040	4e 1c 66 f3 a5
Code: Access-Accept (2)	0050	40 06 00 00 00
Packet identifier: 0x4d (77)		
Length: 54		
Authenticator: 2e670b014dbcdff0975ce71c439da9ff		
[This is a response to a request in frame 980]		
[Time from request: 10.354000 milliseconds]		
▼ Attribute Value Pairs		
▶ AVP: t=Message-Authenticator(80) l=18 val=4e1c66f3a5439e851ab6a1373a1a0764		
▶ AVP: t=Tunnel-Type(64) l=6 Tag=0x00 val=VLAN(13)		
▶ AVP: t=Tunnel-Medium-Type(65) l=6 Tag=0x00 val=IEEE-802(6)		
▶ AVP: t=Tunnel-Private-Group-Id(81) l=4 val=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.

radius					
Time	Source	Destination	Protocol	Length	Info
387.429.234828	192.168.10.10	192.168.10.1	RADIUS	62	Accounting-Response id=79
412.449.078614	192.168.10.10	192.168.10.1	RADIUS	80	Access-Reject id=80
386.429.230785	192.168.10.1	192.168.10.10	RADIUS	225	Accounting-Request id=79
410.448.072211	192.168.10.1	192.168.10.10	RADIUS	226	Access-Request id=80

Length: 184	
Authenticator: 8ec0a98da74c397fdb2e562802620a12	
[The response to this request is in frame 412]	
Attribute Value Pairs	
AVP: t=Framed-MTU(12)	l=6 val=1400
AVP: t=NAS-Port-Type(61)	l=6 val=Ethernet(15)
AVP: t=Called-Station-Id(30)	l=19 val=08-00-27-2A-A6-ED
AVP: t=Calling-Station-Id(31)	l=19 val=00-AA-BB-CC-DD-EE
AVP: t=Service-Type(6)	l=6 val=Framed-User(2)
AVP: t=User-Password(2)	l=34 val=Encrypted
AVP: t=User-Name(1)	l=19 val=00-AA-BB-CC-DD-EE
AVP: t=Acct-Session-Id(44)	l=10 val=3d002086
AVP: t=NAS-Port-Id(87)	l=8 val=ether2
AVP: t=EAP-Key-Name(102)	l=3 val=00
AVP: t=NAS-Identifier(32)	l=10 val=MikroTik
AVP: t=NAS-IP-Address(4)	l=6 val=192.168.10.1
AVP: t=Message-Authenticator(80)	l=18 val=e676995a5a75ec10fdeeb9eb6537159b

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.

radius					
No.	Time	Source	Destination	Protocol	Length Info
387	429.234828	192.168.10.10	192.168.10.1	RADIUS	62 Accounting-Response id=79
412	449.078614	192.168.10.10	192.168.10.1	RADIUS	80 Access-Reject id=80
1346	1511.412190	192.168.10.10	192.168.10.1	RADIUS	80 Access-Reject id=81
1347	1511.412475	192.168.10.10	192.168.10.1	RADIUS	80 Access-Reject id=81, Duplicate Response
386	429.230785	192.168.10.1	192.168.10.10	RADIUS	225 Accounting-Request id=79
410	448.072211	192.168.10.1	192.168.10.10	RADIUS	226 Access-Request id=80
1344	1510.308791	192.168.10.1	192.168.10.10	RADIUS	203 Access-Request id=81
1345	1511.410722	192.168.10.1	192.168.10.10	RADIUS	203 Access-Request id=81, Duplicate Request
1377	1542.215996	192.168.10.1	192.168.10.10	RADIUS	203 Access-Request id=82
1380	1543.225573	192.168.10.10	192.168.10.1	RADIUS	80 Access-Reject id=82

Frame 1380: Packet, 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface -, id 0	0000	08 00
Ethernet II, Src: PCSSystemtec_35:43:f0 (08:00:27:35:43:f0), Dst: PCSSystemtec_81:2c:9f (08:00:27:81:2c:9f)	0010	00 42
Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.10.1	0020	0a 01
User Datagram Protocol, Src Port: 1812, Dst Port: 40315	0030	a1 04
RADIUS Protocol	0040	ff 86
Code: Access-Reject (3)		
Packet identifier: 0x52 (82)		
Length: 38		
Authenticator: 1145a10459e0197b240c9be91a68b76b		
[This is a response to a request in frame 1377]		
[Time from request: 1.009577000 seconds]		
Attribute Value Pairs		
AVP: t=Message-Authenticator(80) l=18 val=ff86183e33647d70a0d56ef2ae67772b		
Type: 80		
Length: 18		
Message-Authenticator: ff86183e33647d70a0d56ef2ae67772b		

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.

No.	Time	Source	Destination	Protocol	Length	Info
306	253.623472	PCSSystemtec_2a:a6:...	Nearest-non-TPMR-Br...	EAP	60	Request, Identity
307	253.625888	PCSSystemtec_6e:93:...	Nearest-non-TPMR-Br...	EAP	60	Response, Identity
308	253.629174	PCSSystemtec_2a:a6:...	Nearest-non-TPMR-Br...	EAP	60	Request, TLS EAP (EAP-TLS)
309	253.655833	PCSSystemtec_6e:93:...	Nearest-non-TPMR-Br...	TLV1.2	208	Client Hello
310	253.660404	PCSSystemtec_2a:a6:...	Nearest-non-TPMR-Br...	EAP	1018	Request, TLS EAP (EAP-TLS)
311	253.662540	PCSSystemtec_6e:93:...	Nearest-non-TPMR-Br...	EAP	60	Response, TLS EAP (EAP-TLS)
312	253.666073	PCSSystemtec_2a:a6:...	Nearest-non-TPMR-Br...	EAP	1018	Request, TLS EAP (EAP-TLS)
313	253.667674	PCSSystemtec_6e:93:...	Nearest-non-TPMR-Br...	EAP	60	Response, TLS EAP (EAP-TLS)
314	253.670729	PCSSystemtec_2a:a6:...	Nearest-non-TPMR-Br...	TLV1.2	284	Server Hello, Certificate, Server Key Exchange, Certificate Request, S...
315	253.687070	PCSSystemtec_6e:93:...	Nearest-non-TPMR-Br...	EAP	1426	Response, TLS EAP (EAP-TLS)
316	253.691064	PCSSystemtec_2a:a6:...	Nearest-non-TPMR-Br...	EAP	60	Request, TLS EAP (EAP-TLS)
317	253.693597	PCSSystemtec_6e:93:...	Nearest-non-TPMR-Br...	TLV1.2	728	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Sp...
318	253.697894	PCSSystemtec_2a:a6:...	Nearest-non-TPMR-Br...	TLV1.2	79	Change Cipher Spec, Encrypted Handshake Message
319	253.702857	PCSSystemtec_6e:93:...	Nearest-non-TPMR-Br...	EAP	60	Response, TLS EAP (EAP-TLS)
320	253.706987	PCSSystemtec_2a:a6:...	Nearest-non-TPMR-Br...	EAP	60	Success
Frame 314: Packet, 284 bytes on wire (2272 bits), 284 bytes captured (2272 bits) on interface -, id 0 Ethernet II, Src: PCSSystemtec_2a:a6:ed (08:00:27:2a:a6:ed), Dst: Nearest-non-TPMR-Bridge (01:80:c2:00:00:00) 802.1X Authentication Extensible Authentication Protocol Code: Request (1) Id: 4 Length: 266 Type: TLS EAP (EAP-TLS) (13) EAP-TLS Flags: 0x80 EAP-TLS Length: 2236 [3 EAP-TLS Fragments (2236 bytes): #310(990), #312(990), #314(256)] Transport Layer Security [Stream index: 0] TLV1.2 Record Layer: Handshake Protocol: Server Hello TLV1.2 Record Layer: Handshake Protocol: Certificate Content Type: Handshake (22) Version: TLS 1.2 (0x0303) Length: 1765 Handshake Protocol: Certificate TLV1.2 Record Layer: Handshake Protocol: Server Key Exchange TLV1.2 Record Layer: Handshake Protocol: Certificate Request TLV1.2 Record Layer: Handshake Protocol: Server Hello Done						

ВИСНОВКИ

1. Перехід до Zero Trust: Успішно спроєктовано систему контролю доступу 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!