KAUNO KOLEGIJA

TECHNOLOGIJŲ FAKULTETAS
INFORMATIKOS IR MEDIJŲ TECHNOLOGIJŲ KATEDRA

Anchelikas Vitkauskas

SAUGAUS NAMŲ OFISO BELAIDŽIO TINKLO PROJEKTAS IR JO REALIZACIJA

Baigiamasis darbas

Kibernetinių sistemų ir saugos studijų programos
valstybinis kodas 6531BX024
Informatikos inžinerijos studijų krypties

Vadovas Gintaras Butkus

Kaunas, 2024

TURINYS

LENTELIŲ IR PAVEIKSLŲ SĄRAŠAS

LENTELĖS

PAVEIKSLAI

SĄVOKŲ SĄRAŠAS

Sąvoka	Aprašymas	Nuoroda į šaltinį
PoE (angl. *Power over Ethernet*)	Sistema galinti perduoti elektros energiją per ethernet tinklus	intellinetnetwork, n.d.
WPA2/3 (angl. *Wi-Fi Protected Access*)	Saugumo sertifikavimo programos, skirtos belaidžių kompiuterių tinklų apsaugai	WPA2/3, n.d.
VPN	Virtualus privatus tinklas, tai tinklas kuris apsaugo interneto ryšį ir privatumą internete.	Kaspersky, n.d.
DHCP (angl. *Dynamic Host Configuration Protocol*)	Tai kliento ir serverio protokolas, kuris automatiškai suteikia interneto protokolo (IP) prievadui jo IP adresą ir kitą susijusią konfigūracijos informaciją, pvz., potinklio kaukę ir numatytąjį šliuzą.	Microsoft, n.d.
VMPS (angl. *VLAN Management Policy Server*)	Tai būdas priskirti komutatoriaus prievadus konkretiems VLAN pagal jungiamojo įrenginio MAC adresą.	Sourceforge, n.d.
BusyBox	Sujungia daugelį mažo dydžio UNIX programų į vieną mažą vykdomąją programą	BusyBox, n.d.
Elipsinės kreivės (angl. *Elliptic Curve*)	Raktu pagrįstas duomenų šifravimo metodas. Daugiausia dėmesio skiriama viešųjų ir privačiųjų raktų poroms, skirtoms žiniatinklio srautui iššifruoti ir užšifruoti.	Avinetworks, n.d.
AES (angl. *Advanced Encryption Standard*)	Simetrinio rakto kriptografijos algoritmas neskelbtiniems duomenims apsaugoti.	Simplilearn, n.d.
Lua	Galinga, efektyvi, lengva, įterpiamų scenarijų kalba.	Lua, n.d.

SANTRAUKA

Autorius Anchelikas Vitkauskas. *Saugaus namų ofiso belaidžio tinklo projektas ir jo realizacija*. Baigiamasis darbas. Vadovas Gintaras Butkus. Kauno kolegija, Technologijų fakultetas, Informatikos ir medijų technologijų katedra. Kaunas, 2024, 50 psl.

Reikšminiai žodžiai: EAP-TLS, OpenWRT, RADIUS, SHA-256.

Baigiamajame darbe yra kuriamas saugus namų ofiso belaidžio tinklo projektas. Projektas leis naudotojams saugiai prisijungti prie belaidžio interneto tinklo naudojant išgaunamus elipsinės kreivės sertifikatus patvirtinti tapatybę. Kad įgyvendinti šį darbą bus naudojamas „UBIQUITI UniFi AC Lite“ prieigos taškas į kurį yra įrašomas *OpenWRT* su *FreeRadius* serveriu, tuomet sukuriami sertifikatai kurių pagalba vartotojai galės saugiai prisijungti prie tinklo nenaudojant jokių slaptažodžių ar prisijungimo vardų. Parodyta kaip reikėtų šį projektą susikonfigūruoti namuose, kad nustatymai būtų saugūs ir nebūtų klaidų su sertifikatų konfigūracijomis.

SUMMARY

Author Anchelikas Vitkauskas. *Wireless Network Project for Secure Home Office and Realisation.* Graduation Thesis. Supervisor Gintaras Butkus. Kauno kolegija HEI, Faculty of Technologies, Department of Informatics and Media Technologies. Kaunas, 2024, 50 pages.

Keywords: EAP-TLS, OpenWRT, RADIUS, SHA-256.

In the graduation thesis wireless network project for secure home will be created. The project will allow users to securely connect to a wireless internet network using elliptic curve certificates to authenticate themselves. To implement this work a UBIQUITI UniFi AC Lite access point will be used, which is loaded with OpenWRT and FreeRadius server, after installing OpenWRT and FreeRadius server certificates are going to be generated which will allow users to securely connect to the network without the use of any passwords or usernames. This project will give you a step by step guide on how to configure this secure wireless network without any issues and with all the correct safety settings.

ĮVADAS

Darbo aktualumas. Šiais laikais vis daugiau žmonių pradeda dirbti iš namų, o tai didina namuose naudojama interneto ir belaidžio tinklo intensyvumą. Kadangi namų tinklo vartojimo intensyvumas didėja, taip pat didėja ir kibernetinių atakų grėsmės lygis, todėl tampa vis svarbiau namuose turėti saugų belaidį tinklą.

Darbo problema. Itin dažnai namuose žmonės nesiima visų saugumo priemonių, dažnai vartotojai slaptažodžių neuždeda arba palieka numatytus, silpnus slaptažodžius ant maršrutizatoriaus ir nėra atnaujinama techninė įranga. Dėl šitų paminėtų problemų vartotojai dažnai susiduria su kibernetinėmis atakomis kur yra pavogiami slaptažodžiai, ar kiti įvairūs duomenys kurie gali būti labai svarbūs vartotojui, tokie kaip banko prisijungimo duomenys, elektroninis paštas, darbo failai ir taip toliau.

Darbo objektas. Paruošti belaidį namų ofiso tinklo projektą

Darbo tikslas – sukurti saugų belaidį tinklą namų ofise naudojantis *OpenWRT, EAP-TLS, TLS 1.3* sertifikatais ir *FreeRADIUS*.

Darbo uždaviniai:

1. Išanalizuoti šiuo metu esamas problemas su namų ofiso belaidžio tinklo saugumu;
2. Įsigilinti į *EAP-TLS, TLS 1.3, WPA3* ir kitas programines ar technines įrangas kurios bus naudojamos šiam projektui įgyvendinti;
3. Sukurti saugią namų ofiso belaidžio tinklo sistemą ir palyginti šią sistemą su kitu galimu variantu;
4. Įvertinti šios sistemos saugumą;
5. Paruošti vadovą vartotojams kaip reikėtų naudotis šia nauja sistema;
6. Apskaičiuoti projekto kainą.

Darbo rezultatai Sėkmingai parengta saugi belaidžio tinklo namų ofiso sistema. Atlikta analizė ir sukonfigūruotos sistemos. Užtikrintas projekto saugumo lygis. Yra suteikiama galimybė prijungti visus galimus įrenginius prie šios namų ofiso sistemos. Paruoštas vadovas, kad vartotojas galėtu lengvai naudotis šia saugia belaidžio tinklo sistema.

1. ANALITINĖ DALIS

1.1. Situacijos analizė

Belaidis tinklas yra kiekvieno šiuolaikinio žmogaus namuose, todėl yra svarbu, kad šis tinklas taip pat būtų ir saugus, todėl šis saugus namų ofiso belaidis tinklas padės vartotojams greitai ir lengvai apsisaugoti savo interneto tinklą.

Įrengti šį saugų namų bus naudojamos *OpenWRT, TLS* sertifikatų ir *RADIUS* programinės įrangos, taip pat pasinaudojamas „UBIQUITI UniFi AC LITE“ belaidis prieigos taškas, kad būtų galimybė paskleisti tinklą ir prie jo prisijungti.

„UBIQUITI UniFi AC LITE“ – naujoviškas prieigos taškas kuris turi daugybę funkcijų per kuriuos galima keisti įvairius nustatymus pagal jūsų norus. Šio prieigos taško gamintai teigia, kad šis prieigos taškas turi 2.4GHz ir 5GHz srauto greičius kurie yra 300MBps ir 867MBps, taip pat šis prieigos taškas palaiko *PoE* ir *Passive PoE* maitinimo metodus (Ubiquiti, n.d.). Kadangi šis modelis taip pat yra *LITE* jis yra mažesnis nei kiti panašūs modeliai ir neužima per daug vietos, todėl yra idealus prietaisas namų ofisuose.

„TP-LINK EAP225 V3“ – Populiarus prieigos taško pasirinkimas dėl jo pigios kainos ir paprastos naudotojų sąsajos, kuris turi greitą dviejų dažnių *Wi-Fi*, 2.4GHz kuris turi 450Mbps greičius ir 5GHz, kuris turi 867Mbps. EAP225 palaiko tiek 802.3af/at *PoE*, tiek pasyvųjį *PoE* maitina ir turi daugelį saugumo funkcijų, tokių kaip prieigos kontrolė, belaidis MAC adresų filtravimas, SSID priskyrimas VLAN, netikrų prieigos taškų aptikimas ir 802.1X palaikymas (tp-link, n.d.). Vartotojai gali šį prieigos tašką kontroliuoti telefonine programėle, dėl šios priežasties dauguma vartotojų renkasi šitą prieigos tašką.

„Linksys LAPAC1750“ – prieigos taškas, kuris užtikrina plačia *Wi-Fi* apimtį. Kaip ir praeiti du prieigos taškų variantai šis taip pat naudoja IEEE 802.11 interneto standartus ir gali palaikyti dviejų dažnių *Wi-Fi*, 2.4 GHz kurio greitis yra 450Mbps ir 5GHz, kurio greitis yra 1300Mbps. Taip pat turi ir daugelį saugumo funkcijų, tokius kaip kanalo izoliavimai, *RADIUS*, netikrų prieigos taškų aptikimas, SSID transliavimas, SSID priskyrimas VLAN ir Apsaugo *Wi-F*i prieiga asmeniniams ir verslo poreikiams. (Linksys, n.d.).

Prieigos taškų privalumai ir trūkumai yra palyginami 1 lentelėje. Palyginami „UBIQUITI UniFi AC LITE“, „TP-LINK EAP225 V3“ ir „Linksys LAPAC1750“ prieigos taškai, išnagrinėjami jų pagrindiniai pliusai ir minusai, yra atkreipiamas dėmesys į saugumą, valdymą, kaina ir interneto našumą.

1 lentelė. Prieigos taškų palyginimai

Prieigos taškai	Interneto našumas	Saugumas	Valdymas	Kaina
UBIQUITI UniFi AC LITE	2.4 GHz – 300MBps 5 GHz – 867MBps	*FreeRadius* integracija, WPA3	*UniFi control panel*	Ekonomiškas – 82eurų kaina
TP-LINK EAP225 V3	2.4 GHz – 450MBps 5 GHz – 867 MBps	WPA2/WPA3 šifravimas	Žiniatinklio sąsaja, *Omoda* programinė įranga	Pigus – 50 eurų kaina.
Linksys LAPAC1750	2.4 GHz – 450MBps 5 GHz – 1300 MBps	WPA2	Žiniatinklio sąsaja	Brangus – 303 eurų kaina.

Visi esantys įrenginiai gali atlikti jiems reikiamas funkcijas, tačiau buvo pasirinktas „UBIQUITI UniFi AC LITE“ dėl jo interneto našumo greičių, kurie neatsilieka nuo kitų esančių variantų. „UBIQUITI UniFi AC LITE“ taip pat turi *FreeRadius* integracija ir naudoja *WPA3* šifravimą, kas dėl saugumo yra tikrai geras ir užtikrintas pasirinkimas. Valdymas taip pat yra paprastas su *UniFi Control Panel*.

1.2. Technologijų ir technikos apžvalga

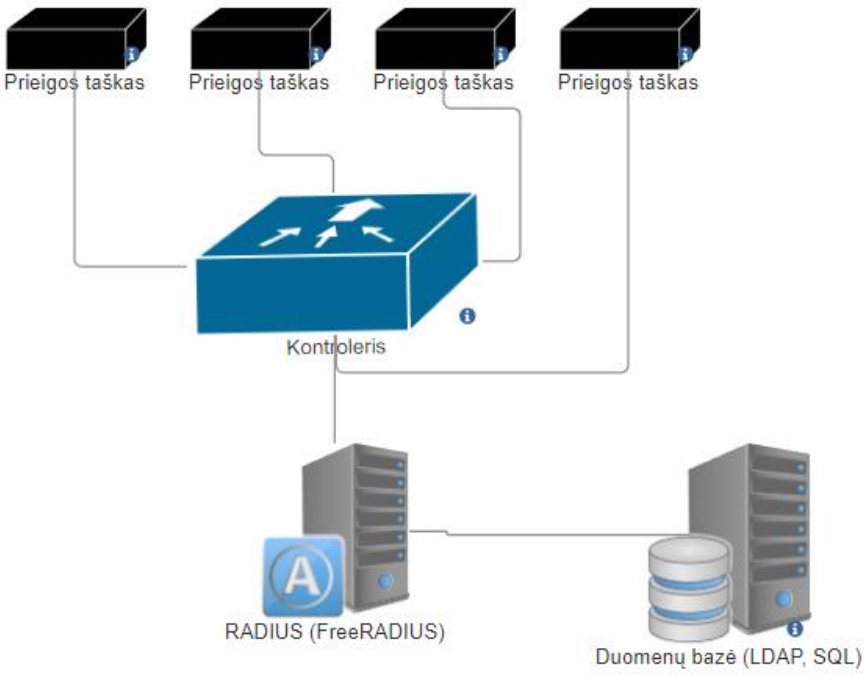
„UBIQUITI UniFi AC LITE“ – Pasirinktas populiarus prieigos taškas dėl lengvai prieinamos kainos, kompaktiškumo, našumo ir saugumo. Jis palaiko tiek *WPA2*, tiek *WPA3 Wi-Fi* saugumo protokolus, taip pat gali būti integruotas ir su *FreeRADIUS*.

Specifikacijos:

- *Wi-fi* standartai 802.11 a/b/g/n/ac
- 300MBps 2.4 GHz greitis ir 867 MBps 5 GHz greitis
- Maitinimas – *PoE*
- Maksimali prieigos taško apimti yra apie $10m^2$
- Palaiko *WPA2/WPA3*

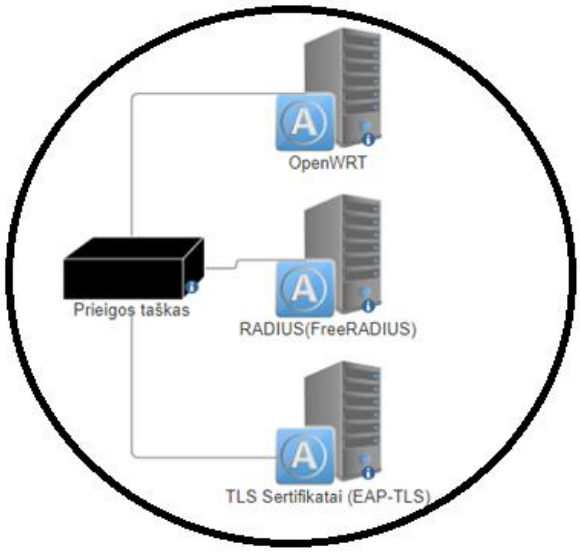
Kuriant šį belaidžio tinklo projektą buvo apsvarstyti du galimi variantai. Pirmas iš šių variantų buvo labiau išplėstinis projekto tinklas (1.1 pav.). Šis tinklo projektas naudoja daugelį prieigos taškų, kontrolerį kuriame yra prijungti ir valdomi visi prieigos taškai, atskiras *FreeRADIUS* serveris kuris tvarko tinklo vartotojų autentiškumo patvirtinimą, jei vartotojai nori prisijungti prie serverio jie yra nukreipiami į *FreeRADIUS* serverį kur jiems reikia įvesti vartotojo vardą ir slaptažodį kuris yra vartotojų duomenų bazėje, pagal šį pavyzdį galimos duomenų bazės būtų *LDAP, SQL* ar kita.

Šis tinklo projektas užtikrintu puikų mastelio keitimą, kad būtų galima plėstis ateityje. Taip pat užtikrina patikimą saugumą dėl daugiasluoksnio autentifikavimo proceso ir naudotojų valdymo per duomenų bazę. Norint užkirsti kelią grėsmėms ir apsaugoti aplinką, reikia saugumo strategijos. Daugiasluoksnis saugumas yra vienas iš daugelio saugumo strategijų, galinčių apsaugoti įmonės turtą, taip yra todėl, kad kiekvienas saugumo sluoksnis turi funkciją, vaidmenį ir technologiją, kuri gali aptikti grėsmes ir užkirsti joms kelią (Surantha, Wijaya, 2020.). Daugiasluoksnis saugumas yra patikimas būdas apsaugoti savo interneto tinklą, jis naudoja tokius autentifikavimus kaip *WPA2 Enterprise* su 802.1x. Daugybe organizacijų, įmonių ir universitetų naudoja *WPA-2 Enterprise* protokolą, kad galutiniai vartotojai galėtų prisijungti prie teikiamų *Wi-Fi* tinklų. Tinkamai sukonfigūravus tiek paslaugų, tiek galutinio vartotojo įrenginius, šis protokolas laikomas vienas iš saugiausiu *Wi-Fi* ryšio protokolu, be to, jis turi papildomų privalumų – kiekvienas *Wi-Fi* vartotojas turi unikalų slaptažodį. Tačiau, jei įrenginiai nėra tinkamai sukonfigūruoti, galima įvykdyti kibernetinę ataką ir pavogti naudotojų *Wi-Fi* prisijungimo duomenis. Atsižvelgdami į plačiai paplitusį išmaniųjų telefonų su *Wi-Fi* ryšiu naudojimą ir didėjantį susirūpinimą dėl naudotojų privatumo, daugiausia dėmesio skiriame *WPA2-Enterprise* pažeidžiamumo privatumo aspektams (Dagelic, Bugaric, Čagalj, 2020.). Atsižvelgus į kainą šis tinklas yra visai brangus, yra reikalingas atskiras serveris, kad galėtų naudoti *FreeRADIUS*, todėl tai yra netinkamas projektas namų ofisui, kur yra labiau pageidautinas pigesnis variantas. Taip pat šis variantas, nors ir saugus yra daug sunkesnis sukonfigūruoti, o jei projekte įvyktų klaidų ir kažkas būtų padaryta ne taip padaryta, rizika pakyla, kad į jūsų sistemą būtų galimą įsibrauti.



1.1 pav. Pirmasis tinklo pavyzdys

Antras pasirinktas pavyzdys (1.2 pav.) yra daug kompaktiškesnis ir pigesnis, nei pirmas variantas. Jis naudoja tik vieną prieigos tašką į kurio vidų yra įrašyta *OpenWRT* operacinė sistema, o tai leidžia įsirašyti papildomų saugumo funkcijų, tokių kaip *VPN* ar įsilaužimo aptikimų funkcijas. Šiame variante *FreeRADIUS* nėra atskiras serveris, o jis yra įrašytas į prieigos tašką, tai palengvina šio tinklo sąranką ir sumažina prietaisų kiekį kuriuos reikėtų kontroliuoti ir nusipirkti. Šis tinklas taip pat naudoja *EAP-TLS*, o šis metodas naudoja sertifikatus vartotojui ir serveriui patikrinti, todėl nereikia naudoti vartotojo vardo ir slaptažodžio, o tai užtikrina didesnį saugos lygį.



1.2 pav. Antrasis tinklo pavyzdys, visi šie įrenginiai yra prieigos taško viduje

2 lentelėje galima pamatyti skirtumus tarp pirmo ir antro tinklo pavyzdžių, jų kaina, saugumus ir taip toliau.

2 lentelė. Pirmo ir antro tinklo palyginimas

Tinklo privalumai	Pirmo tinklo pavyzdys	Antro tinklo pavyzdys
Tinklo didinimas	Puikus variantas didelėms įmonėms ar didesniems namų ofisams	Limituotas vienam prieigos taškui
Valdymo sunkumas	Daug sunkiau kontroliuoti dėl didesnio kiekio prietaisų	Lengva sąranka ir valdymas
Kaina	Daug brangesnis variantas dėl didelio kiekio prietaisų	Tik vienas prieigos taškas
Saugumas	Stiprus vartotojo vardo ir slaptažodžio prisijungimas	Saugus *EAP-TLS* autentifikavimas

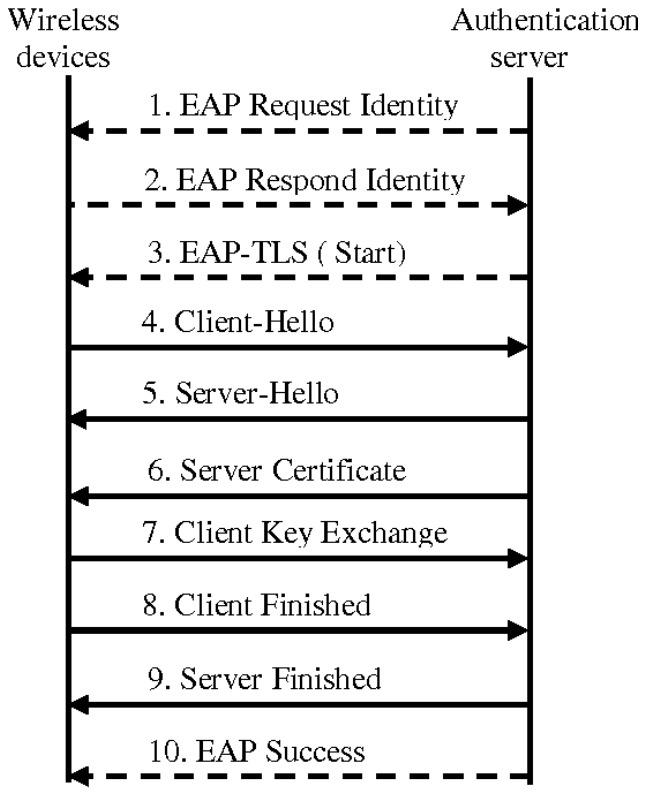
Taigi šio tinklo stipriausios dalys yra paprastumas jį pasidaryti namuose, šio viso tinklo išlaidos yra tik vienas prieigos taškas, saugumas kuris ateina su *EAP-TLS* autentifikavimo metodu, *OpenWRT* lankstumas ir integruotas *FreeRADIUS* serveris.

1.2.1. Informacinė posistemė

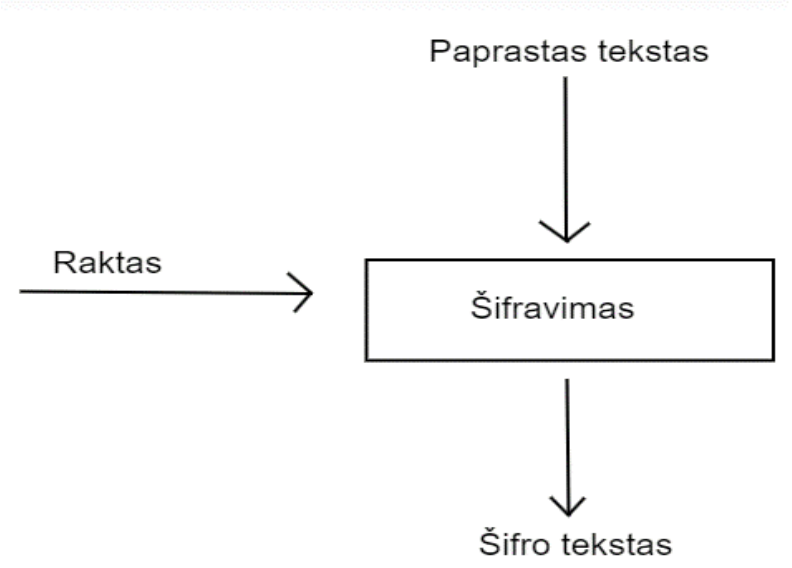
FreeRADIUS – tai, stiprus atvirojo kodo *RADIUS* serveris kuris atlieka svarbų vaidmenį saugant bevielio interneto informaciją. Jis veikia kaip serveris kuris užtikrina patikimų vartotojų prieigos kontrolę ir didina tinkle saugumą. *FreeRADIUS* yra didelio našumo ir labai konfigūruojamas kelių protokolų politikos serverių, kuris taip pat palaiko *RADIUS*, *DHCPv4* ir *VMPS* (*FreeRADIUS,* n.d.).

OpenWRT – Nemokama atvirojo kodo operacinė sistema. Ji gali būti naudojama tiek verslo lygio, tiek vartotojų lygio įrenginių. *OpenWRT* yra pagrįstas *Linux* ir buvo sukurtas tam, kad neužimtu per daug vietos ir būtu itin lengvai pritaikomas bet kokiam įrenginiui kuris neturi daug vietos, todėl puikiai tinka įrenginiams kurie turi ribotus išteklius. Kad taupytų vietą *OpenWRT* naudoja *BusyBox* aplinką, kur į *BusyBox* yra surašyta daug įprastų komandinės eilutės įrankių, todėl platintojams nereikia pateikti vykdomųjų failų, dėl to yra sumažinamas vietos poreikis ir *OpenWRT* gali suteikti beveik visą *Linux* patirtį įrenginiuose kuriuose nėra daug vietos. *OpenWRT* yra dažnai naudojamas įrenginiuose, kuriems reikia pažangios tinklo funkcijos, tai gali būti maršrutizatoriai, prieigos taškai, nes ši operacinė sistema turi daugybę funkcijų ir įrankių skirtų srautui valdyti ir optimizuoti. *OpenWRT* turi panašias funkcijas kaip ir šiuolaikinės paketais pagrįstos *Linux* distribucijos: integruotą žiniatinklio serverį su *CGI* palaikymu, *SSH* serverį ir, svarbiausia, paketų valdymo įrankį *ipkg*. Naudojant *ipkg*, naujas programas, įrankius ir branduolio tvarkykles galima pridėti ir pašalinti paleidimo metu, nereikalaujant perkrauti kompiuterio. Į būsimą maršrutizatorių *OpenWRT* įkeliama naudojant standartinį maršrutizatoriaus programinės įrangos atnaujinimo mechanizmą (Cheong, Kuinam, 2013.).

EAP-TLS – Alternatyvus prisijungimo metodas kuris nereikalauja vartotojo vardo ir slaptažodžio. *EAP-TLS* reikalauja saugumo sertifikatų abiejose belaidžio ryšio pusėse, todėl prisijungimas prie *Wi-Fi* prieigos taško yra daug saugesnis. *EAP-TLS* veiksmingai pašalina galimybę įsilaužėliams atlikti ataką tinkle (Kerner, 2017.). *TLS* perdavimo metu šie sertifikatai yra apkeičiami ir jie yra tikrinami naudojant sudėtingus matematinius sprendimus tokius kaip skaitmeninis parašas. *EAP-TLS* sukuria saugų tunelį (1.4. pav), kuriame yra naudojami stiprūs šifravimo protokolai, pavyzdžiui *AES*. *AES* yra privataus rakto kuri naudojama jau tūkstančius metų, kai ir siuntėjas, ir gavėjas naudoja tą patį raktą. Tai yra blokinis šriftas, todėl įvesties duomenys turi būti sudėti į 128 bitų ilgio blokus, o atvirojo teksto blokas užšifruojamas raktu ir gaunamas šifro blokas (1.5 pav.). Yra trijų dydžių rakto dydžiai: 128, 192 ir 256 bitų. Dažniausiai naudojamo tipo *AES* yra 128 bitų dydžio (Bowne, 2018.). Sertifikatai, kriptografija ir šifravimas padeda gerokai sustiprinti tinklo saugumą palyginant su tradiciniais autentifikavimo metodais.

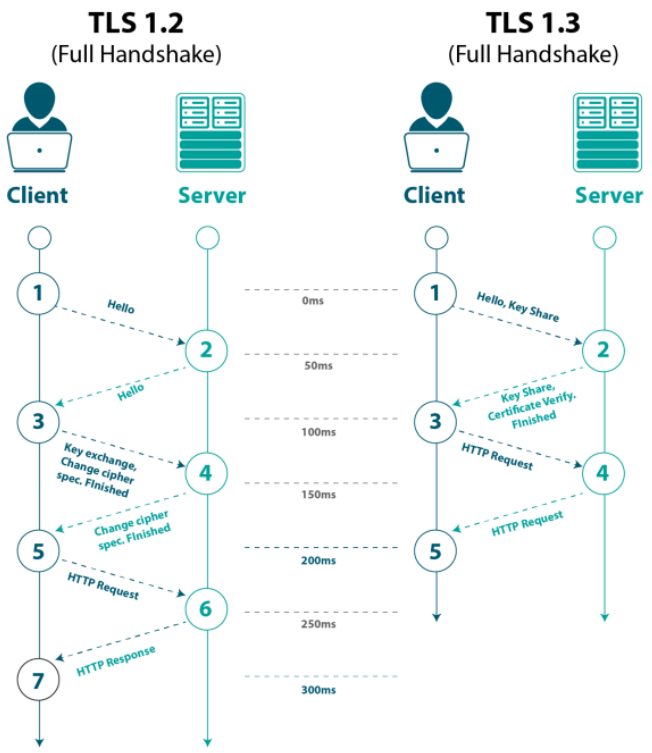


1.3 pav. *EAP-TLS* ryšio užmezgimo pavyzdys(angl. *Handshake*) (Alabdulatif, Ma, 2014)



1.4 pav. Šifro bloko pavyzdys

TLS 1.3 – naujausia ir saugiausia *TLS* protokolų integracija. Turi daug greitesnį kliento ir serverio saugaus ryšio užmezgimo protokolą palyginus su *TLS 1.2* (1.3 pav.) palyginus su senesnėmis versijomis. *TLS 1.3* taip pat turi patikimesnį saugumą kuris naudoja *Diffie-Hellman Ephemeral* algoritmą apkeisti raktus, o tai sugeneruoja skirtingus raktus po kiekvieno apsikeitimo.



1.5 pav. Saugaus ryšio užmezgimo protokolo greitis (*Patil, 2022)*

Taigi, apibendrinant, šie kriptografijos metodai ir programos buvo pasirinktos, nes jos yra vienos iš geriausių šiais laikais, dažnai naudojamos ir tinka įrenginiuose su mažai vietos.

1.2.2. Naudotojo sąsaja

Projektui bus naudojama *OpenWRT* naudotojo sąsaja su integruotu *RADIUS* serveriu, skirtu naudotojų autentiškumui patvirtinti. *OpenWRT* naudotojų sąsaja leis valdyti tinklą ir naudotojų prieigos kontrolę per paprastą ir lengvai suprantama puslapį, taip palengvinant saugaus namų ofiso tinklo administravimą.

1.3. Apibendrinimas

Šis projektas padės sukurti saugų namų ofiso tinklą integruojant *FreeRADIUS* su „UBIQUITI UniFi AC LITE“ prieigos tašku. Bus naudojami saugumo protokolas *TLS 1.3*, bei *OpenWRT*, kad būtų sustiprintas saugumas tinkle. Parodyta šio tinklo aplinkos konfigūracija ir funkcionalumas.

2. SPECIFIKACIJA

2.1. Projektuojamo objekto panaudojimas

Projektuojama objekto apibūdinimas. Kuriamas saugus namų ofiso belaidis tinklas naudojant „UBIQUITI UniFi AC LITE“ prieigos tašką į kurį yra įrašomos programos saugumui užtvirtinti.

Projektuojamo objekto paskirtis. Duoti galimybę vartotojams lengvai ir patogiai sukurti saugų namų ofiso belaidį tinklą neišleidžiant per daug pinigų ant nereikalingų prietaisų. Ši sistema leis lengvai vartotojams pridėti prietaisus prie interneto tinklo naudojant visus saugumo prietaisus, kad į šį tinklą galėtų jungtis tik patikimi vartotojai.

Projektuojamo objekto funkcija. Suprojektuotas tinklas atliks šias funkcijas:

- Leis vartotojams prisijungti naudojant *Wi-Fi*;
- Leis kontroliuoti kas gali patekti į tinklą, o kas ne;
- Bus įdiegtas *FreeRADIUS* serveris kuris leis patvirtinti naudotojų autentiškumą;
- Įdiegti *TLS* sertifikatai saugiam tinklo įrenginių ryšiui užtikrinti;
- Naudojamas *EAP-TLS* leis vartotojams prisijungti nenaudojant prisijungimo vardo ir slaptažodžio;
- Sukurta patogi naudotojo sąsaja.

2.2. Reikalavimai projektuojamo objekto posistemėms

Projektuojamo objekto posistemės reikalavimai, išdėstomi kokie prietaisai bus naudojami, kokios sisteminės įrangos reikėtų šio projekto įgyvendinimui

Reikalavimai aparatūros posistemei:

- „UBIQUITI UniFi AC LITE“ prieigos taškas.

Reikalavimai informacijos posistemei:

- *OpenWRT* operacinė sistema;
- *FreeRADIUS*;
- *TLS* sertifikatai dėl saugumo;
- *EAP-TLS* naudojama alternatyva, kad nereikėtų naudoti slaptažodžių.

Reikalavimai naudotojų sąsajai. Naudotojų sąsajai bus naudojama *OpenWRT* naudotojų sąsaja. *OpenWRT* naudotojų sąsaja yra paprastai suprantama tiek naujų vartotojų, tiek patyrusių vartotojų.

Reikalavimai saugumui. Buvo daromas projektas kur saugumas yra vienas iš svarbiausių dalykų. Kad užtikrinti saugumą yra naudojami *EAP-TLS* ir *TLS* sertifikatai. Naudojant *EAP-TLS* yra užtikrinama, kad jūsų prisijungimo duomenys nėra pavagiami ar iš duomenų bazės, ar kitais atvejais, nes slaptažodžiai, bei prisijungimo vardai nėra naudojami, o yra naudojami autentifikavimo protokolai kurie leidžia prisijungti prie tinklo naudojant skaitmeninius sertifikatus, kad būtų galima patvirtinti jūsų tapatybę tinkle.

Reikalavimai realizacijai. Tinklas turi būti saugus, nes nuo to priklauso vartotojų duomenys. Taip pat turi būti atliktos visos nurodytas funkcijas

Reikalavimai projekto dokumentacijai. Projekto dokumentacija turi būti paprasta ir lengvai suprantama, kad bet koks vartotojas pasižiūrėjęs į ją suprastu, kas kaip veikia ir kaip tai reikėtų valdyti, parengti. Dokumentacija parodys kaip reikėtų šį tinklą parengti, schemas ir detalius atitinkamus aprašymus.

3. PROJEKTINĖ DALIS

Projektinėje dalyje bus parodoma kaip buvo vykdomi projektavimo etapai, kokios yra naudojamos priemonės darbui suprojektuoti, kaip buvo vykdomas šis procesas. Šioje dalyje taip pat bus parodoma kaip buvo suprojektuoti sertifikatai, kokios yra jų specifikacijos, kokios saugumo priemonės yra naudojamos.

3.1. Aparatūros posistemė

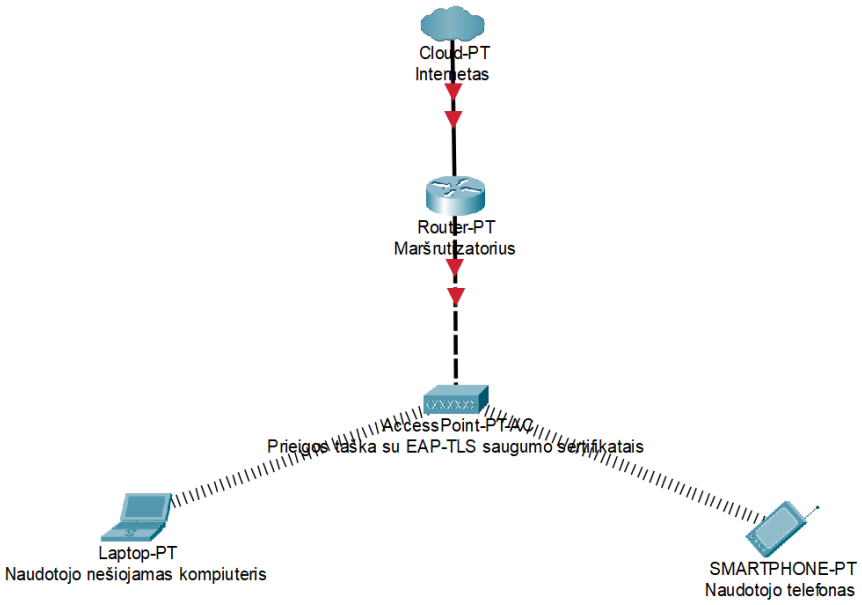
3.1.1. Projektuojamo objekto konceptuali schema ir aprašymas

Pagrindinis esamas projekto tikslas yra saugus, belaidis prisijungimas prie namų tinklo, kad šiai idėjai įgyvendinti reikia išsirinkti tinkamą programinę ir aparatinę įrangą. Šiam darbui yra pasirinktas „UBIQUITI UniFi AC LITE“ prieigos taškas, *OpenWRT* operacinė sistema ir *FreeRadius* saugumo serveris.

Naudojami komponentai konceptualiai schemai:

- Prieigos taškas - Buvo pasirinktas „UBIQUITI UniFi AC LITE“ prieigos taškas, jis yra naudojamas perduoti belaidį ryšį tarp kliento įrenginių ir laidinio tinklo. Į šį prieigos tašką bus įdiegiama *OpenWRT* operacinė sistema, kuri suteikia daugiau konfigūravimo parinkčių, nei numatytas prieigos taško programinės įrangos parinktys;
- *OpenWRT* - *OpenWRT* yra nemokama atvirojo kodo operacinė sistema skirta prietaisams kurie neturi daug vietos viduje. Ši programa leidžia lengvai ir išsamiai konfigūruoti namų tinklą. Į *OpenWRT* operacinę sistemą bus diegiamas *FreeRadius* serverio programinė įranga;
- *FreeRadius* - *FreeRadius* yra taip pat nemokama atvirojo kodo programa, kuri yra naudojama saugumo užtikrinimui. Ši programa leis naudoti *EAP-TLS* saugumo sertifikatus vartotojų patvirtinimui;
- Naudotojo įrenginiai – tai bus bet kokie galimi naudotojo įrenginiai kurie turi belaidį interneto ryšį.

Vaizduojama konceptuali schema kurioje bus pavaizduojama projekto tinklo idėja (3.1 pav.). Šioje schemoje yra vaizduojamas debesis, kuris perduoda interneto ryšį į maršrutizatorių, o maršrutizatorius yra prijungiamas prie prieigos taško, kad jo pagalba būtų skleidžiamas belaidis interneto ryšis su *EAP-TLS* sertifikatais į įvairius naudotojo įrenginius, tokius kaip nešiojamas kompiuteris ar išmanusis telefonas.



3.1 pav. Konceptuali schema

3.1.2. Darbo vietų sąsajų su specifikuotomis funkcijomis lentelė

Naudotojų patirtis šiame projekte bus palengvinta naudojant dvi pagrindines sąsajas: pirmoji iš šių sąsajų yra skirta administratoriams, o kita skirta paprastiems vartotojams. Sąsajos ir konkrečios funkcijos skirtos administratoriams ir paprastiems vartotojams aprašomos 3 lentelėje.

3 lentelė. Darbo vietų sąsajų funkcijos

Darbo vieta	Sąsaja	Funkcijos
Administratorius	Grafinė naudotojo sąsaja, šiuo atveju bus naudojamas tiek *OpenWRT*, tiek *SSH* prisijungimas naudojant bet kokią *SSH* programą	Vartotojų valdymas, *EAP-TLS* autentifikavimo konfigūravimas, *EAP-TLS* sertifikatų kūrimas, trynimas, tinklo stebėjimas, tinklo sistemų atnaujinimai, įrašomos naujos naudojamų programų versijos ir panašiai.
Vartotojas	Bevielis ryšys	Prisijungimas prie bevielio tinklo naudojant *EAP-TLS* autentifikavimo metodą.

3.1.3. Darbo vietos parinkimas ir pagrindimas

Darbo vietos parinkimui buvo žiūrima į įvairius prieigos taškus ir ką jie gali duoti. Buvo žiūrima į įvairias funkcijas, tokias ar šis prieigos taškas turi 2.4GHz ir 5GHz belaidį dažnį, 2.4GHz būtų naudojamas didesniems atstumams, o 5GHz mažesniems atstumams, kad būtų gaunamas greitesnis bevielis ryšys. Taip pat rinkantis tinkamą prieigos tašką buvo žiūrima į šio prieigos taško maksimalų duomenų perdavimo spartą, idealiausia parinktis būtų 1000 Mbit/s, nes tokio greičio

prieigos taškai dabar yra dažnai matomas dalykas ir nekainuoja per daug, kadangi tinklas vis tiek bus rengiamas namų ofisui. Rengiant namų ofiso projektą taip pat yra svarbu atsižvelgti ir į tai kokio dydžio ofisas ar jūsų namai yra, todėl atsižvelgiama į prieigos taško maksimalų atstumą patalpoje ir renkamasi prieigos tašką kuris užtikrintai galėtų pasiekti kiekvieną namų kampą. Taip pat reikia ir nepamiršti saugumo. Atsižvelgiant į saugumo algoritmus kuriuos naudoja įvairūs prieigos taškai, tinkamiausias šiuo atveju yra *WPA2* ir *WPA-Enterprise*. Buvo atsižvelgiama ir į norimus *Wi-Fi* standartus, tokį kaip 802.11ac.

Pažiūrint į visus šiuos reikalavimus ir tinkamus prieigos taško variantus teko pasirinkti „UBIQUITI UniFi AC LITE“ (3.2 pav.) prieigos tašką darbui atlikti, jis turi tiek 2.4GHz, tiek 5GHz belaidžio ryšio dažnį, platus namų ryšio pasiekiamumas, ir taip pat turi įvairius saugos algoritmus, tokius kaip *WPA2, WPA-PSK, AES, WPA-Enterprise* ir taip toliau, pilna šio prieigos taško informacija yra surašoma 4 lentelėje.

3.2 pav. „UBIQUITI UniFi AC LITE“ prieigos taško pavyzdys (Ubiquiti, n.d.)

4 lentelė. „UBIQUITI UniFi AC LITE“ specifikacijos

Specifikacijos	
2.4 GHz	Turi
5 GHz	Turi
6 GHz	Neturi
Maksimalus 2.4 GHz interneto greitis	300 Mbps
Maksimalus 5 GHz interneto greitis	867 Mbps
Maksimalus duomenų perdavimo greitis	1000 Mbps
Ethernet LAN duomenų perdavimo sparta	10, 100, 1000 Mbit/s
Maksimalus atstumas patalpoje	122 m.
Saugumas	
Turimi saugumo algoritmai	*AES, TKIP, WEP, WPA, WPA-PSK, WPA2*
Energija	
Power over Ethernet (*PoE*)	Turi
Kintamosios srovės įėjimo įtampa	24 V
Maksimalus energijos suvartojimas	6,5 W

3.2. Operacinė posistemė

Šioje dalyje atsižvelgiama į operacinę posistemę, kuri buvo pasirinkta šio darbo projektavimui.

3.2.1. Informacinė posistemės koncepcija

Projektas pagrindas – informacinė posistemė. Posistemėje yra naudojamas programos kurių pagalba yra įgyvendinamas šio tinklo tikslas sukurti *EAP-TLS* autentifikavimo procesą.

EAP-TLS sertifikatų autentifikavimo protokolas – saugus naudotojų identifikavimo patvirtinimo metodas. Jis naudoja skaitmeninius sertifikatus, kad būtų sukurtas saugus ryšys tarp naudotojo įrenginio ir autentifikavimo serverio, o tai užtikrina saugų naudotojo duomenų vientisumą ir konfidencialumą.

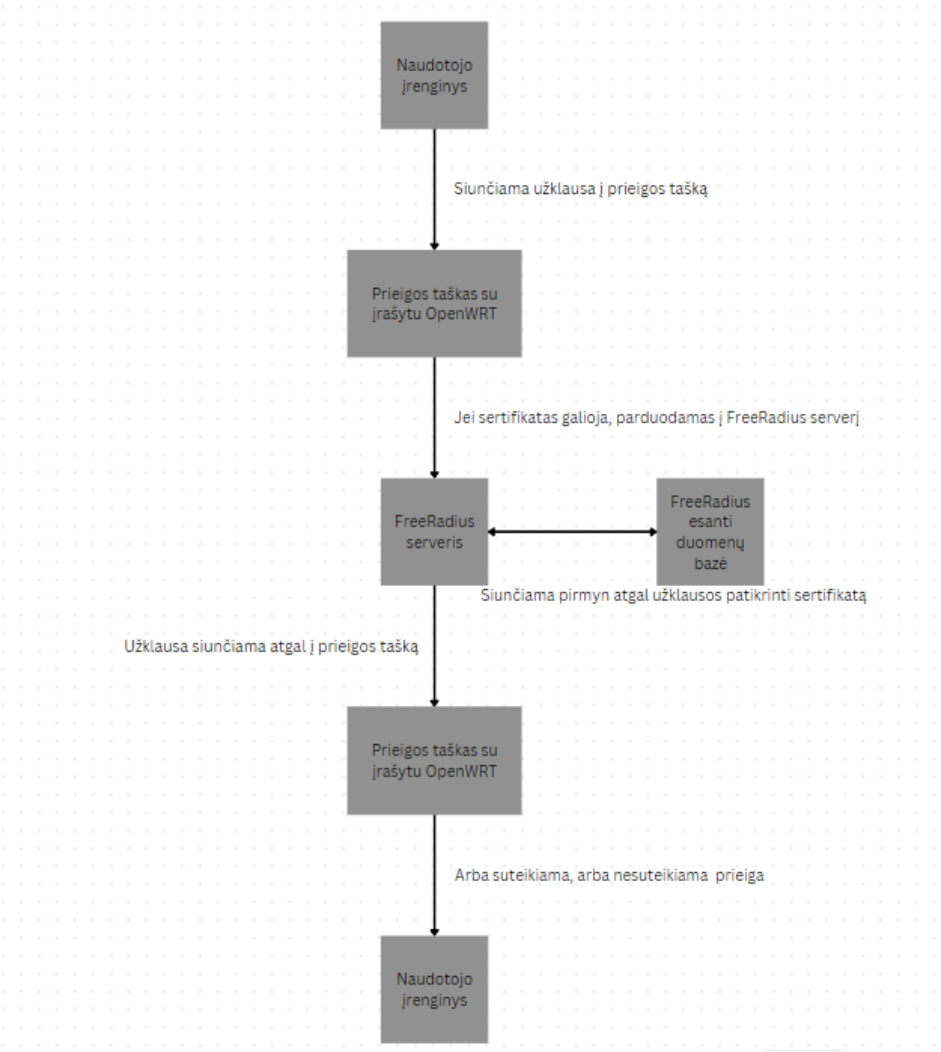
OpenWRT – veikia kaip tinklo šliužas, jis valdo maršrutizavimą, belaidį ryšį ir *EAP-TLS* autentifikavimą. Yra integruojamas su *EAP-TLS*, kad atliktų naudotojo autentiškumo patvirtinimą ir perduotų autentiškumo užklausas į *FreeRadius* serverį.

FreeRadius – tai pagrindinis serveris, kuris yra atsakingas už autentifikavimą. Jame yra saugomi naudotojų sertifikatai, *FreeRadius* pagalba yra patvirtinami ir kuriami nauji sertifikatai naudotojams.

3.2.2. Informacijos srautas

Informacijos srautas (3.3 pav.):

- Vartotojo įrenginys inicijuoja autentifikavimo procesą. Įrenginys bando prisijungti prie tinklo ir siunčia autentifikavimo užklausą į prieigos tašką su *OpenWRT*;
- Yra patikrinamas sertifikatas, užtikrindamas, kad šis sertifikatas yra autentiškas ir vis dar galioja;
- Jei sertifikatas yra galiojantis, yra perduodama užklausa *FreeRadius* serveriui;
- *FreeRadius* serveris autentifikuoja naudotoją, patikrina jo tapatybę pagal duomenų bazėje esančius duomenis ir autorizavimo politiką;
- Baigus autentifikavimo procesą yra siunčiamas signalas atgal, nurodydamas ar reikia suteikti prieigą naudotojui, ar ne.
- Baigus šiam procesui yra arba suteikiama arba nesuteikiama prieiga prie prieigos taško.



3.3 pav. Informacijos srauto pavyzdys

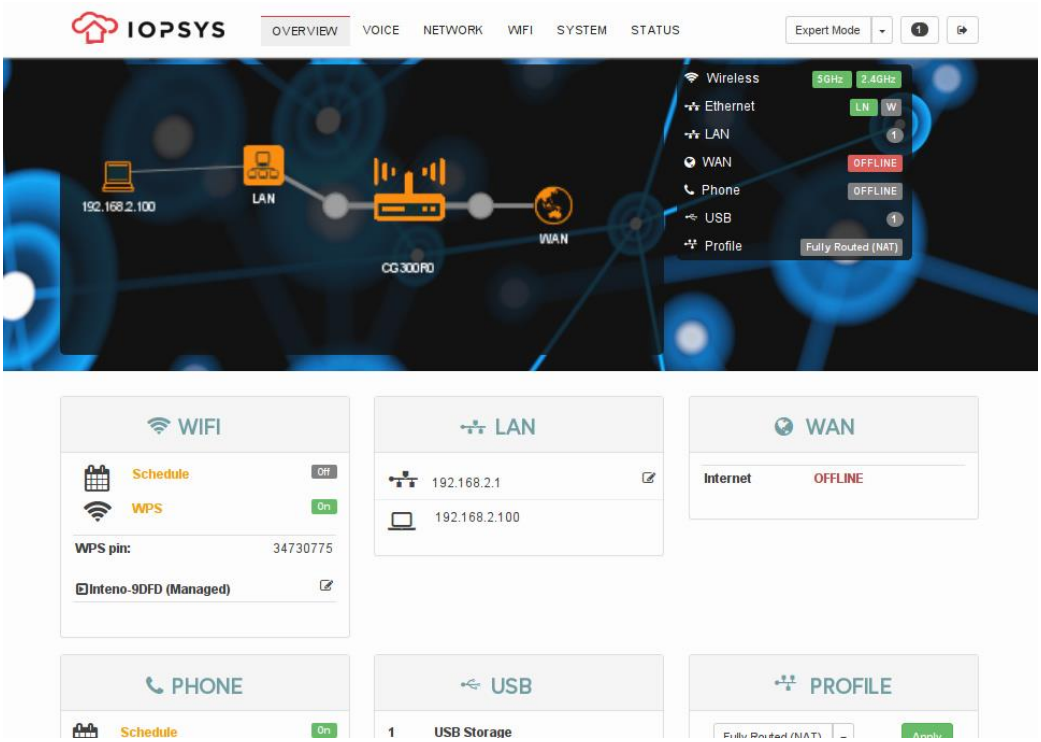
3.3. Naudotojo sąsaja

Aptariami galimi naudotojų sąsajos pasirinkimai, kurie būtų naudojami pagrindiniams šio projekto etapams atlikti, tai gali būti *FreeRadius* įrašymas ar paprasti interneto nustatymai

Grafinės naudotojų sąsajos parinkimui buvo apsvarstyti keli variantai. Buvo pažiūrima į tris skirtingus grafinės naudotojų sąsajos įrankius.

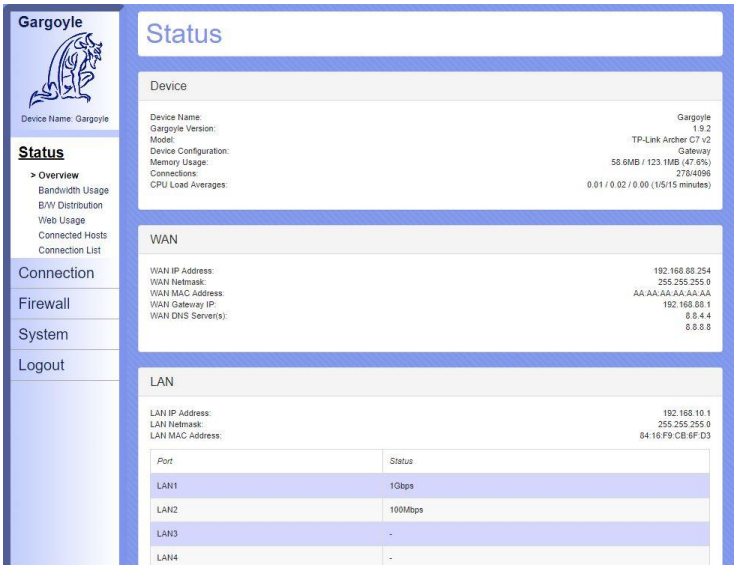
- *LuCI* – pagrindinė šio projekto priežastis buvo sukurti laisvą, švarią, plečiamą ir lengvai prižiūrimą žiniatinklio naudotojo sąsają įterptiesiems įrenginiams. Ši sąsaja išsiskiria tuo, kad nenaudoja plačiai naudojamo *Shell* kalbos, o jos vietoje naudoja *Luo* programavimo kalbą ir dėl to yra suskirstytos loginės dalys, pavyzdžiui, modeliai naudoja objektines bibliotekas ir šablonavimą. Tai užtikrina didesnį našumą, mažesni diegimo dydį, greitesnį paleidimą ir paprastą priežiūrą (LuCI, n.d.).
- *JUCI* – moderni žiniatinklio sąsaja (3.4 pav.), sukurta *OpenWRT* pagrįstiems įterptiesiems įrenginiams. Ši sąsaja yra sukurta naudojant *HTML5* ir *angular.js*, o ryšiui su įterptiniame

įrenginyje veikiančia kompaktiška ir greita *lua* operacine sąsaja palaikyti naudojami *websockets*. Galima kurti tiek tinklalapio dalį, tiek galinį serverį nepriklausomai vienas nuo kito ir naudoti juos atskirai (JUCI, n.d.).



3.4 pav. *JUCI* žiniatinklio sąsaja (JUCI, n.d.)

- *Gargoyle* (3.5 pav.) – nemokama, *OpenWRT* pagrįsta *Linux* distribucija, skirta įvairiems belaidžiams maršrutizatoriams ar įterptiesiems įrenginiams. Viena iš svarbiausių funkcijų kurią turi *Gargoyle* yra galimybė riboti ir stebėti pralaidumą bei nustatyti pralaidumo ribas konkrečiam IP adresui (Gargoyle, n.d.).



3.5 pav. *Gargoyle* žiniatinklio sąsaja(Gargoyle, n.d.)

Šios sąsajos yra palyginamos grafinių naudotojų sąsajų parinkimo 5 lentelėje, kurioje nagrinėjami pagrindiniai jų privalumai.

5 lentelė. Grafinių naudotojų sąsajų parinkimas

Funkcijos	***LuCI***	***Gargoyle***	***JUCI***
Kam pagrinde skirta šios sąsajos	*OpenWRT* konfigūracija	*OpenWRT* tinklo valdymas	*OpenWRT* konfigūracija
Kokiems naudotojas skirtas	*OpenWRT* paprastiems naudotojams	Namų vartotojams, tinklo entuziastams	Patyrusiems naudotojams
Naudojama programinė kalba	*Lua*	*HTML, CSS, JavaScript*	*JavaScript*
Resursu naudojimas	Mažas	Vidutinis	Vidutinis
Sudėtingumas	Paprastas	Vidutinis	Sunkus
Dokumentacija	Platus dokumentacijos kiekis	Vidutinis dokumentacijos kiekis	Limituotas
Integracija su *OpenWRT*	Paprasta	Reikalauja tam tikrų žinių	Paprasta

Atsižvelgus į šiuos parametrus nuspręsta naudoti *LuCI* grafinę naudotojų sąsają, dėl jos paprastumo naudotis, mažo resursų naudojimo, platus dokumentacijos kiekis taip pat leidžia paprastai susirasti reikiamą informaciją susijusia su *LuCI* grafinę sąsaja.

3.4. Sertifikatų projektavimas

Projektuojamų sertifikatų pagrindas, aprašomos saugumo priemonės naudojamos atlikti pagrindinį šio projekto tikslą – apsaugoti belaidį namų ofiso tinklą.

3.4.1. Sertifikatų kūrimo įvadas

Sertifikatų naudojimas yra esminis tinklo saugumo elementas, ypač kai yra norima sukurti saugų namų ofiso belaidį tinklą. Jie sutiekia būda autentifikuoti įrenginius, užtikrindami konfidencialumą ir vientisumą. Vietos sertifikatų išdavimo tarnyba CA įdiegimas į prieigos tašką leidžia sugeneruoti ir valdyti sertifikatus, taip padidindamas saugumo lygį.

3.4.2. Sertifikatų projektavimo etapai

Kad parengti šį saugų belaidžio tinklo projektą, reikia nuspręsti kokie parametrai bus naudojami šiam darbui įvykdyti bei kaip vyks šių sertifikatų dalijimasis:

- Rakto bitų ilgis – naudojama *secp384r1* standartinė kreivė, kuri turi 384 bitų ilgį, tai yra idealus bitų ilgis tiek saugumui, tiek našumui.
- Saugumo algoritmas – pasirinktas *SHA-256* algoritmas. Šitas *hash* algoritmas naudoja sudėtingas matematines funkcijas, kad būtų paslepiamas slaptažodis, kadangi jis taip pat yra 256 bitų ilgio yra beveik neįmanoma atkurti originalių duomenų.
- Sertifikatų galiojimo laikas – kadangi paprastiems vartotojams nėra noro pastoviai kurti naujus sertifikatus kai jų galiojimo laikas pasibaigia, yra sukuriamas sertifikatas 3650 dienų pridedant prie komandos „-days 3650“, kas yra beveik 10 metų.
- Išdavimo politika – galimybė išduoti sertifikatus serveriams, šie sertifikatai naudojami prietaisams jūsų tinkle, tai gali būti prieigos taškai, ar maršrutizatoriai, kad būtų pajungtas saugus bendravimas su klientais naudojant *EAP-TLS* autentifikavimą. Taip pat egzistuos ir galimybė gauti klientų sertifikatus, juos galės dalinti individualiems vartotojams dėl autentifikavimo priežasčių.
- Užtikrinti saugų prisijungimo ryšį bus naudojami saugaus šifro sąrašas. Šiame sąraše yra paminėti saugūs prisijungimo šifrai tokie kaip *ECDHE-ECDSA-AES256-GCM-SHA384* ir kiti saugūs rinkiniai.
- Kad tinklas būtų dar saugesnis, bus pakeičiamas numatytasis *EAP* tipas iš *MD5*, kuris jau yra pasenęs ir naudoja vartotojo vardą, bei slaptažodį vartotojų autentifikavimui į *TLS* autentifikavimo metodą, kuris yra vadinamas auksiniu standartu šiais laikais, dėl jo saugaus ir greito autentifikavimo, nėra prisijungimo slaptažodžiu ir taip toliau. 3.6 paveiksle yra palyginami dažniausiai naudojami *EAP* protokolai, kur galima pamatyti skirtumus tarp pasenusių *EAP* protokolų ir *EAP-TLS*.

WPA2 & WPA3 Enterprise Common Protocols	Level of Encryption	Authentication Speed	Directory Support	Credentials
EAP-TLS	Public-Private Key Cryptography	Fast - 12 Steps	Universal	Passwordless
PEAP-MSCHAPv2	Bad Encryption (MD4, Compromised since 1995)	Slow - 22 Steps	Active Directory	Passwords
EAP-TTLS/PAP	No Credential Encryption	Slowest - 25 Steps	Non-AD LDAP Servers	Passwords

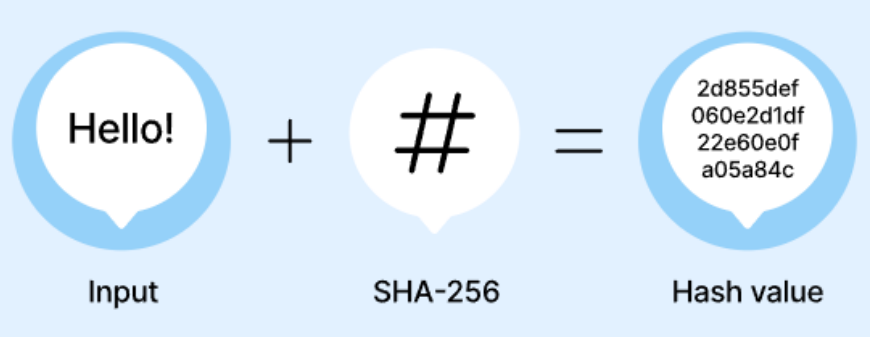
3.6 pav. *EAP* protokolų palyginimas (securew2, n.d.)

Secp384r1 – 384 bitų ilgio elipsinė kreivė, kuri naudojama rakto sukūrimo procesui. *Secp384r1*, dar dažnai yra vadinamas P-384. Šios kreivės paprastoji eilė yra apytiksliai 394×10113. P-384 yra nusakoma lygtimi $y^2 = x^3 - 3x + b$, kur ‚b' nusako tam tikrą 384 bitų skaičių. Rakto bitų ilgis yra lygus kreivės eilės ilgiui, kuris taip pat yra 384 bitai. Pažiūrėjus į 3.7 paveikslą yra galima pamatyti kiek pasikeitė skirtingos *NIST* kreivių versijos, taip pat galima pamatyti, kad kreivės eilės ilgis yra dvigubai ilgesnis nei senoje P-192 versijoje. Ši elipsinė kreivė yra rekomenduojama *NSA* (angl. *National Security Agency*), todėl yra vienas iš saugiausių pasirinkimų šiam projektui.

Name	*b*
NIST P-192	2455155546008943817740293915197451784769108058161191238065
NIST P-224	18958286285566608000408668544493926415504680968679321075787234672564
NIST P-256	41058363725152142129326129780047268409114441015993725554835256314039467401291
NIST P-384	27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575

3.7 pav. Kreivių dydžių palyginimas (Ivo Kubjas, 2015)

SHA-256 – Naudojamas duomenų vientisumui tikrinti naudojant saugaus šifravimo algoritmą. Šis algoritmas naudojant *hash* funkcija paverčia paprastą tekstą į užšifruotą tekstą (3.8 pav.).

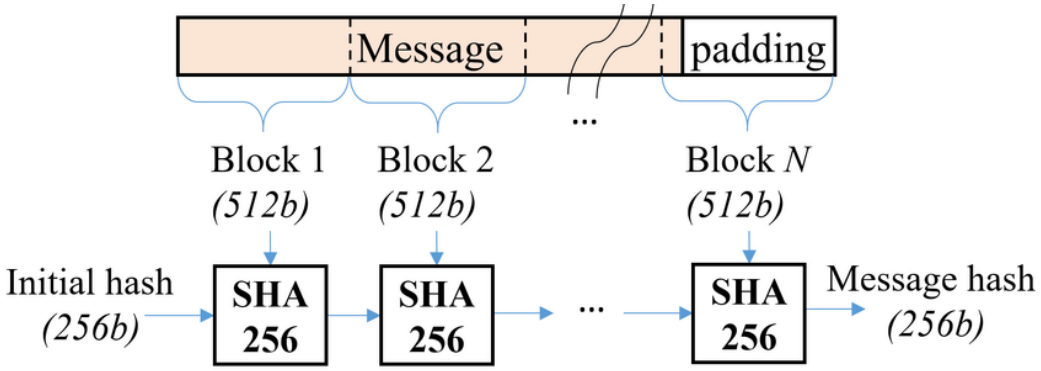


3.8 pav. SHA-256 *Hash* funkcijos pavyzdys (NordVPN, n.d.)

SHA-256 algoritmas veikia taip:

- *SHA-256* pasiimi parašytą žinute, tekstą, slaptažodį;
- Algoritmas šį tekstą apdoroja keliais raundais, kuriuose yra atliekamos sudėtingos matematinės funkcijos (3.9 pav.);
- Duomenims yra taikomos bitų loginės operacijos, pavyzdžiui *AND, OR, XOR*;
- Modulinė aritmetika ir sąlyginiai teiginiai toliau transformuoja tekstą;
- Kas kart yra didinami poslinkiai, bei pridėtinės konstantos;

- Šių operacijų poveikis sukuria unikalią *hash* vertę, kurios ilgis visada yra 256 bitai (3.10 pav.);
- Net ir mažas pakeitimas tekste gali visiškai pakeisti *hash* vertę, dėl vadinamo *avalanche effect*.;
- Šis dizainas užtikrina, kad beveik nėra galimybės, kad du failai galėtų turėti tą pačia *hash* vertę. Šansas, kad tai atsitiktų yra 1 iš 2^256;
- Kadangi algoritmas yra vienakryptė funkcija, yra beveik neįmanoma išgauti pradinę *hash* vertę.

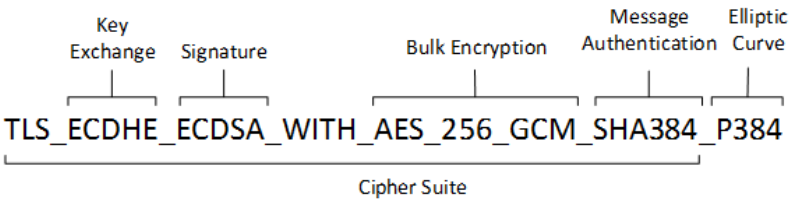


3.9 pav. *SHA-256* su visais daromai priedais šifravimui atlikti pavyzdys (T. Tran, P. Luan, 2021)

INPUT DATA	HASH OUTPUT (SHA-256)
My name is Toby	cacb5418163039b016be9746818a2926f68fd1e4bad1b04f6791f6aabb5e8c52
My name is Tony	9cd2444dc56929bdb97123add1f007643effa88bf1ed061eee1eead4e15ac7f9
My name is Toby and this is my project	9abbaa0c54fcd028ac51bede2608d06e8d3a026784e34adfac14fadd143d212c

3.10 pav. Pavyzdys naudojant panašius tekstus ir gaunant skirtingus atsakymus (Toby Chitty, 2020)

Šifrų rinkinio sąrašas – sukuriama eilutė, kurioje yra surašomas šifrų rinkinių sąrašas. Kiekvienas iš šių paminėtų šifrų siūlo tam tikrą keitimosi raktais, šifravimo ir pranešimo autentiškumo patvirtinimo algoritmų derinį (3.11 pav.). Pasiimant kaip pavyzdį *ECDHE-ECDSA-AES256-GCM-SHA384* šifrų rinkinį, čia *ECDHE* yra naudojamas raktų keitimui, *ECDSA* yra skaitmeninio parašo algoritmas kuris dažnai naudojamas elipsinės kreivės kriptografijose, *AES256* reikalingas šifravimui, *GCM* užtikrina konfidencialumą ir autentiškumą ir *SHA384* užtikrina duomenų vientisumą. Čia yra vienas iš daugumos šifrų rinkinių. Rinkiniai skirti tam, kad kai užmezgamas ryšys su klientu, būtų nustatytas abipusis stipriausias šifrų rinkinys, todėl yra paminama didelis kiekis įvairių šifro rinkinių. Taip pat yra užrašytas ir sąrašas šifrų, su kuriais serveris neužmegs ryšio, keletas iš jų būtų *MD5, 3DES, EXP*.



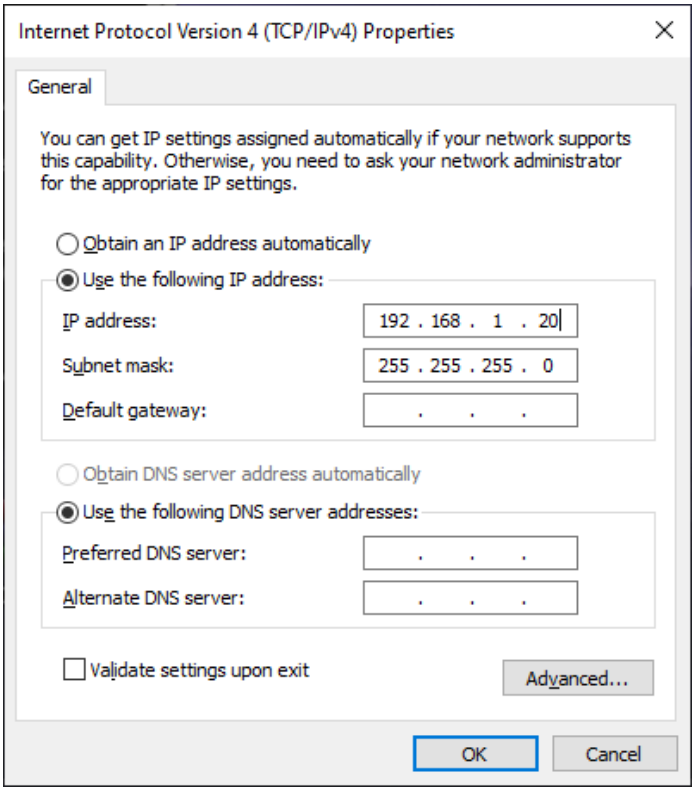
3.11 pav. Pavyzdys kaip veikia šifravimo rinkinys (Cody Richardson, 2021)

Taigi, šiam sertifikatų projektavimui buvo pasirinktas *secp384r1* 384 bitų elipsinė kreivė, kuri bus naudojama saugiam raktų kūrimui, taip pat renkamasi *SHA-256*, kad būtų užtikrintas duomenų vientisumas naudojant saugaus šifravimo metodą. Galiojimo laikas pasirinktas 3650 dienos, kad nebūtų problemų su kasdieniniu sertifikatų naujinimu. Taip pat užtikrinti ryšį yra naudojami įvairūs saugūs šifro rinkiniai, kad būtų parenkamas tinkamiausias šifras pagal jūsų prietaisą. Galimybė išduoti sertifikatus tiek serveriams, tiek paprastiems vartotojams naudojant komandas.

4. EKSPERIMENTINĖ DALIS

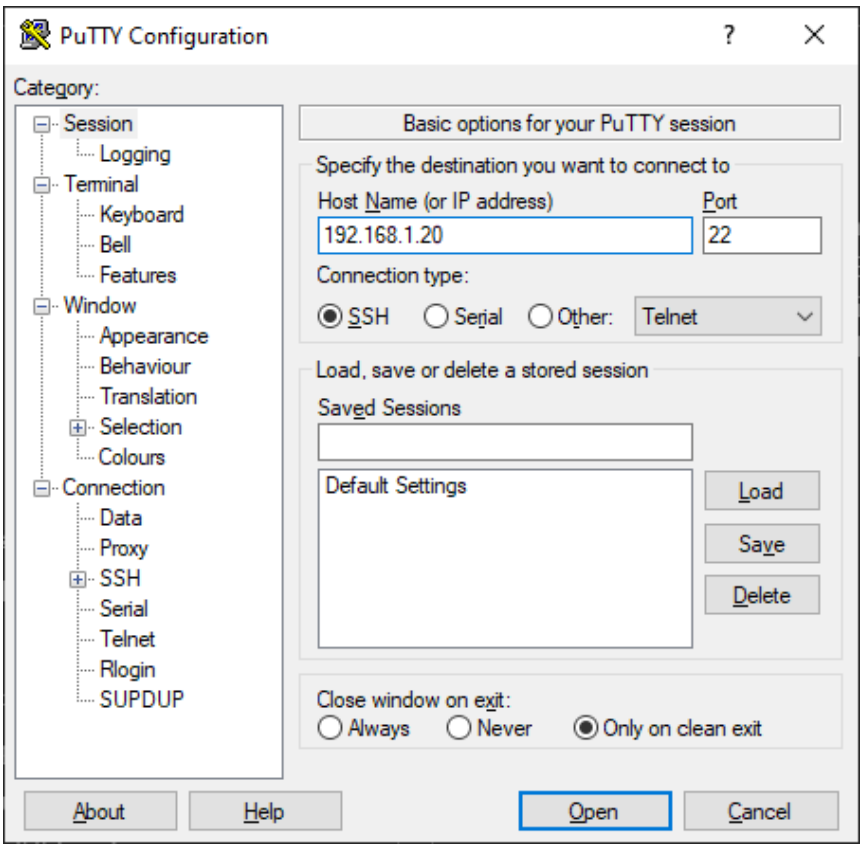
4.1. *OpenWRT* įrašymas į prieigos tašką

Viso darbo pagrindas yra *OpenWRT*, todėl norint pradėti darbą reikėtų įsirašyti *OpenWRT* į prieigos tašką. Pradedant reikėtų pasiimti *Gigabit PoE* montavimo laikiklį kuris turi *PoE* ir *LAN* jungtis. Prijungti *PoE* į prieigos tašką su interneto kabeliu, o *LAN* jungti įkišti į kompiuterį naudojant interneto kabelį. Pradedant darbą reikia sukonfigūruoti kompiuterio statinį IP adresą per valdymo skydą paspaudžiant ant tinklas ir internetas, ir galiausiai paspaudžiant ant tinklo ir bendrinimo centras. Paspaudus ant prijungto interneto laido apačioje lauko bus savybės mygtukas kur paspaudus reikės pasirinkti *Internet Protocol Version 4 (TCP/IPv4)* ir vėl paspausti savybės, atsidarius naujam laukui reikia įvesti reikiamą tinklo IP adresą, negalima naudoti tokių IP adresų kaip 192.168.1.20 ar 192.168.1.1, o geriausia naudoti 192.168.1.10 ir tinklo kaukę 255.255.255.0 (4.1 pav.).



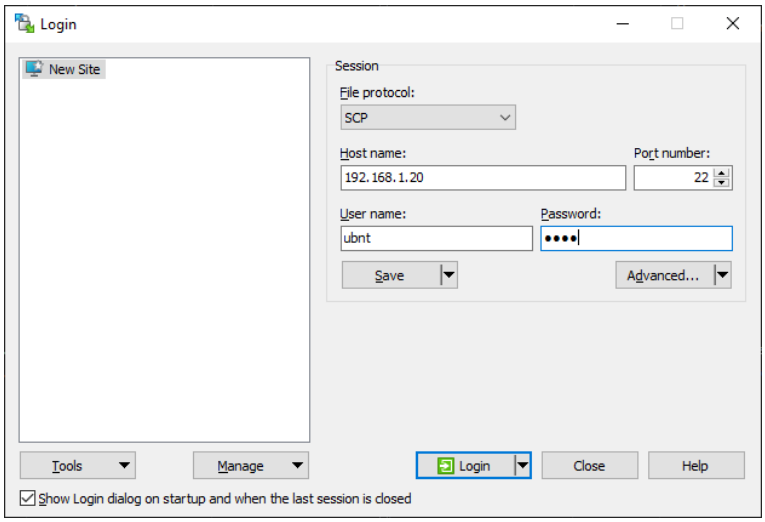
4.1 pav. IP adreso nustatymai

Pakeitus IP adresą galima pradėti prisijungimą prie prieigos taško. Prisijungimui galima naudoti bet kokį *SSH* klientą su komandinėmis eilutėmis, *KiTTY*, *Xshell* ir taip toliau. Šiam darbui bus naudojamas *PuTTY* programa prisijungti prie prieigos taško. Atsidarius *PuTTY* į *Host Name (or IP address)* reikia įvesti 192.168.1.20 IP adresą (4.2 pav.), o kituose vietose palikti numatytus nurodymus ir spausti Atidaryti (angl. *Open*).



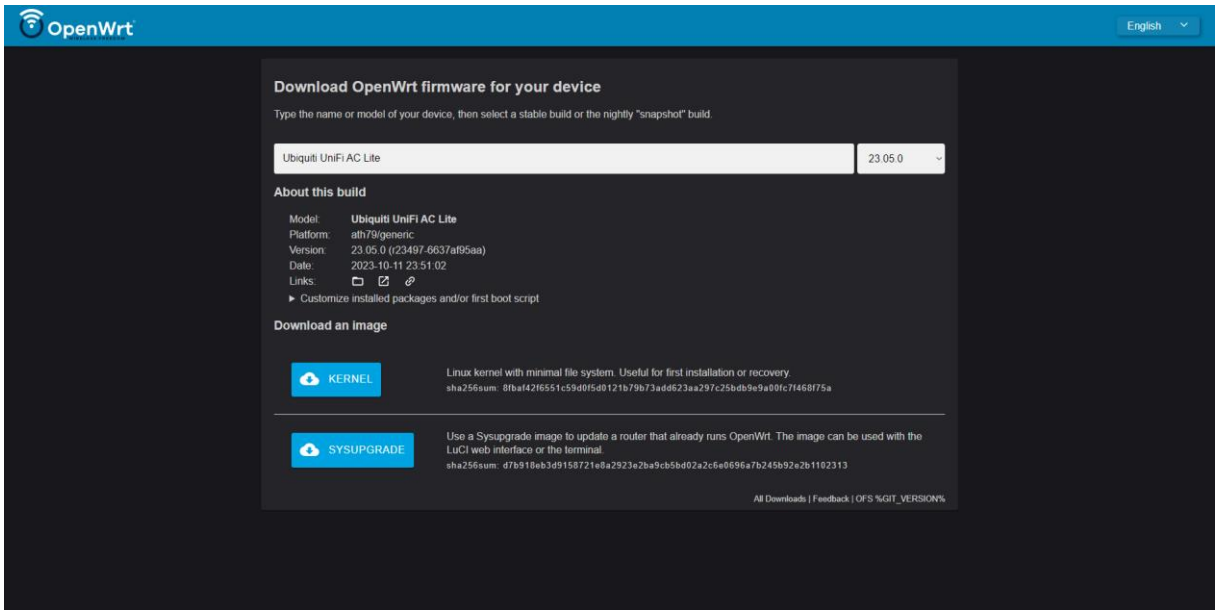
4.2 pav. *PuTTY* konfigūracija

Prisijungus į *PuTTY* reikia įvesti prieigos taško prisijungimo vardą ir slaptažodį, numatyti „UBIQUITI UniFi AC Lite“ prisijungimo duomenys yra *ubnt* tiek slaptažodžiui, tiek prisijungimo vardui, o baigus prisijungimą bus galima matyti numatyti *Ubiquiti* produktų langą. Sekančiai daliai taip pat yra parsisiunčiamas *WinSCP* failų valdymų klientas, kad į jį prisijungti reikia įvesti į *Host Name* 192.168.1.20 IP adresą, pasirinkti failų protokolą (angl. *File Protocol*) SCP ir įvesti Prisijungimo vardą ir slaptažodį kurie yra „ubnt“ (4.3 pav.).

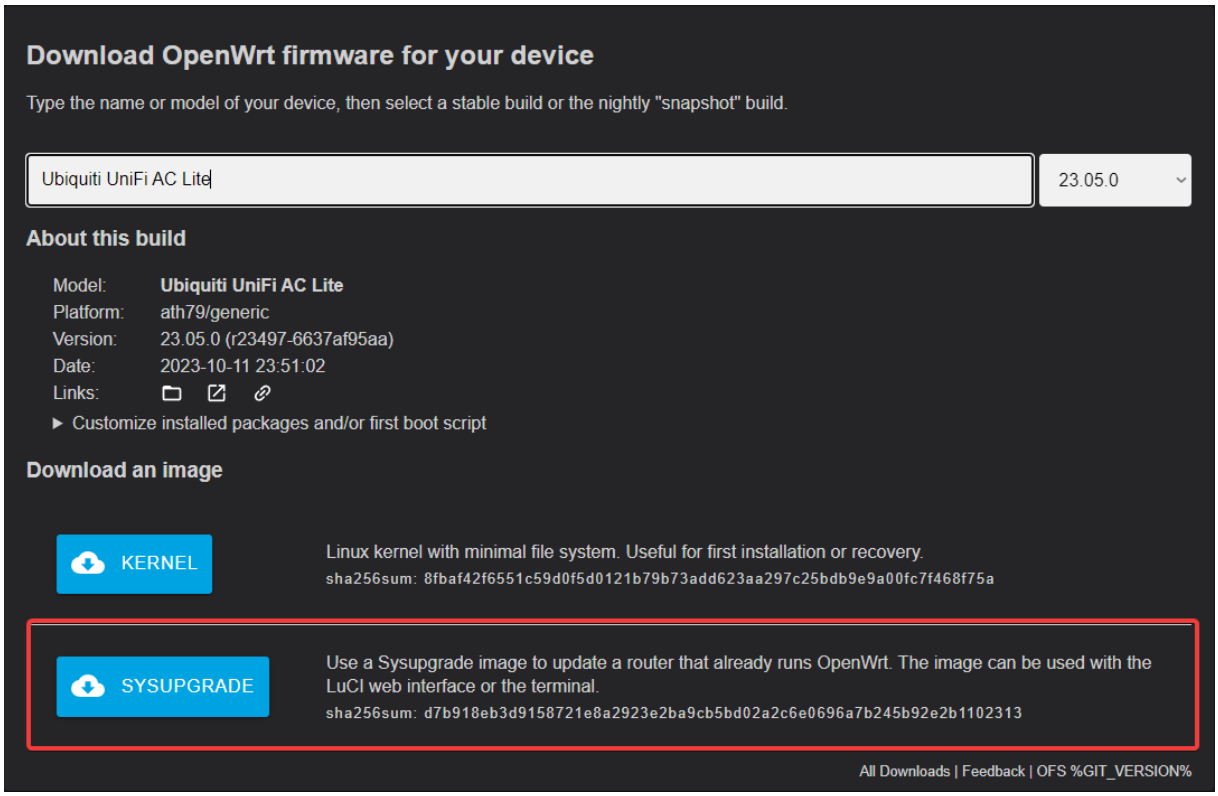


4.3 pav. *WinSCP* prisijungimas prie prieigos taško

Atlikus prisijungimus į prieigos tašką dabar reikėtų parsisiųsti tinkamą *OpenWRT* versija pagal jūsų pasirinktą prieigos tašką (4.4 pav.). Kadangi šiame darbe yra naudojamas „UBIQUITI AC LITE“ prieigos taškas į paieškos langą įrašome „Ubiquiti UniFi AC LITE“ ir parsisiunčiame *Sysupgrade OpenWRT* versiją (4.5. pav.).



4.4 pav. *OpenWRT* programinės įrangos langas kur reikia parsisiųsti reikalingą *OpenWRT* versiją (OpenWRT, n.d.)



4.5 pav. „UBIQUITI UniFi AC LITE“ *Sysupgrade* parsisiuntimo langas(OpenWRT, n.d.)

Naudojant *WinSCP* reikia paspausti „...“ du kartus ir nueiti į pagrindinį prieigos taško failų puslapį kur bus galima matyti „*tmp*“. Paspausti ant „*tmp*“ ir įkelti “*sysupgrade*” failą į jo vidų naudojant *WinSCP*. Įkėlus *sysupgrade* failą reikia atsidaryti *PuTTY* ir įvesti “echo “5edfacbf” > /proc/ubnthal/.uf” komandą, ši komanda atrakina *mtd* particijas, o tai reiškia, kad yra išjungiama tam tikrų skirsnių apsaugą, kad būtų galimą įrašyti naują įrangą. Kad patikrinti ar praeita komanda pavyko galima įvesti komandą “cat /proc/mtd”, jei ši komanda rodo (4.6 pav.) esančias particijas reiškia, kad skirsnių apsauga buvo išjungta sėkmingai.

```
BZ.v6.5.28# cat /proc/mtd
dev:    size   erasesize  name
mtd0: 00060000 00010000 "u-boot"
mtd1: 00010000 00010000 "u-boot-env"
mtd2: 00790000 00010000 "kernel0"
mtd3: 00790000 00010000 "kernel1"
mtd4: 00020000 00010000 "bs"
mtd5: 00040000 00010000 "cfg"
mtd6: 00010000 00010000 "EEPROM"
```

4.6 pav. Išjungtų skirsnių apsaugos patikrinimo pavyzdys

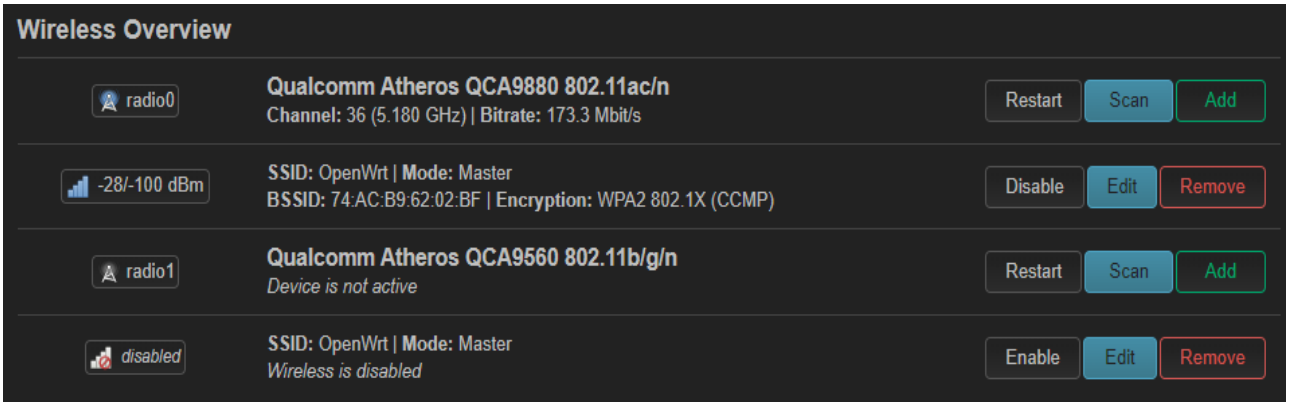
Sekantis žingsnis būtų įrašyti *OpenWRT* į *kernel0* ir *kerne1*. *PuTTY* platformoje reikia įvesti „dd if=/tmp/openwrt-23.05.0-ath79-generic-ubnt_unifiac-pro-squashfs-sysupgrade.bin of=/dev/mtdblock2” komandą ir palaukti keletą minučių kol *OpenWRT* įsirašys į *kernel0*. Kai *OpenWRT* baigs rašytis į *kernel0* reikia jį taip pat įrašyti ir į *kernel1* naudojant komandą „dd if=/tmp/openwrt-23.05.0-ath79-generic-ubnt_unifiac-pro-squashfs-sysupgrade.bin of=/dev/mtdblock3“, kaip ir su *kernel0* reikia palaukti porą minučių kol tai sėkmingai įsirašys. Jei tai sėkmingai įsirašė po abiejų komandų turi matytis „*12544+1 records in ir 12544+1 records out*“ eilutės. Alternatyviai, jei yra susiduriama su problemomis galima ištrinti *kernel0* naudojant komanda „dd if=/dev/zero of=/dev/mtdblock3”. Baigus šią dalį reikėtų nustatyti, kad *OpenWRT* krautųsi iš *kernel0* naudojant komandą „dd if=/dev/zero bs=1 count=1 of=/dev/mtdblock4”, baigus šiai komandai reikėtų perkrauti *OpenWRT* su komanda „*reboot*“. Dabar prieigos taškas turėtų pradėti mirksėti balta spalva, reikia palaukti iki kol ji bus stabili mėlyna spalva ir tuomet *OpenWRT* bus sėkmingai užkrautas.

4.2. *OpenWRT* nustatymas vartojimui

Kai prieigos taškas šviečia mėlyna spalva reikėtų atsidaryti naršyklę ir įvesti IP adresą „192.168.1.1“, tai turėtų atidaryti *OpenWRT* naudotojų sąsają. Reikia prisijungti, kadangi slaptažodžio numatyti nustatymai neturi, tiesiog reikia paspausti prisijungti (angl. *Login*) mygtuką. Prisijungus reikia naviguoti į tinklo nustatymus ir paspausti belaidis (angl. *Wireless*) (4.7 pav.).

4.7 pav. Belaidžio tinklo nustatymai

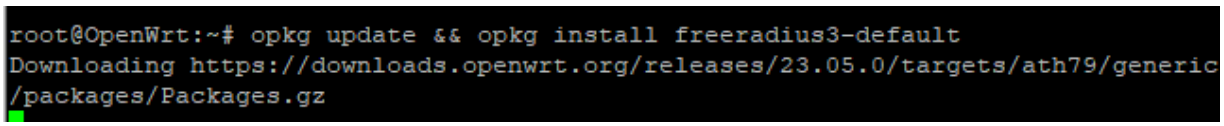
Nuėjus į bevielio interneto nustatymus bus galima matyti 4 laukus, pirmam prijungimui reikėtų paspausti įjungti ant “SSID: OpenWRT | Mode: Master” eilutės ir tuomet ant trečios eilutės paspausti skenuoti mygtuką ir prijungti šį prieigos tašką prie namų interneto (4.8 pav.).



4.8 pav. Belaidžio tinklo nustatymo vidus

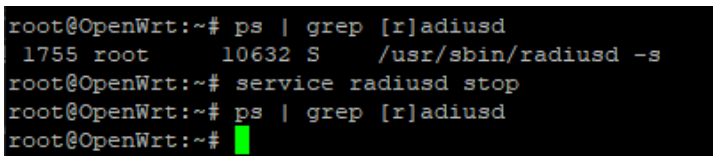
4.3. *FreeRadius* įrašymas į *OpenWRT*

Prisijungus prie prieigos taško naudojant *PuTTY* su interneto prieiga dabar galima pradėti įrašinėti *FreeRadius*. Pirmiausia reikėtų įvesti komandą „opkg update && opkg install freeradius3-default“. Ši komanda atnaujins *OpenWRT* paketus ir įrašys *FreeRadius* paketą į prieigos taško vidų. Taip pat galima įrašyti *FreeRadius* 3 testavimo ir monitoriavimo įrankius pasinaudojant komanda „opkg install freeradius3-utils” (4.9 pav.).



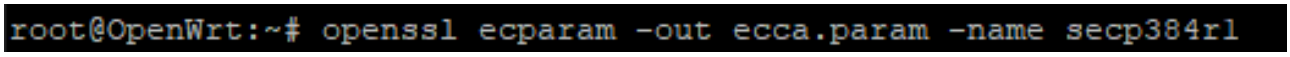
4.9 pav. *FreeRadius* įrašymas į *OpenWRT*

Kai *FreeRadius* 3 baigs diegtis yra galimybė pažiūrėti ar jis šiuo metu veikia pasinaudojant komanda „ps | grep [r]adiusd“, jei po komandos yra matoma kokia nors išvestis, *FreeRadius* reikėtų sustabdyti su komanda “/etc/init.d/radiusd stop” arba komanda “server radiusd stop” (4.10 pav.).

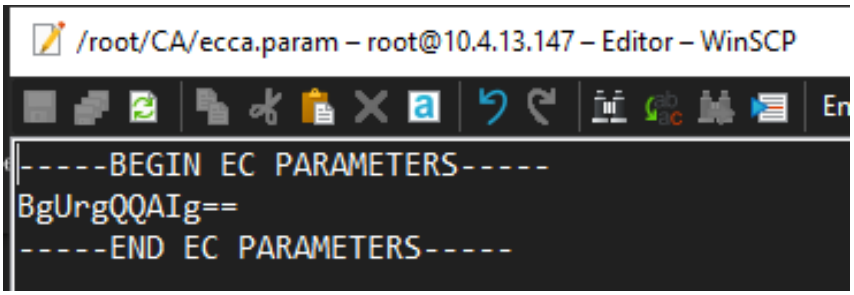


4.10 pav. *FreeRadius* patikrinimo ar yra pajungtas ir kaip sustabdyti pavyzdys

Dabar galima pradėti nustatinėti *EAP-TLS* ir sertifikatų įrašymą. Pirmiausia reikėtų įsirašyti „opkg install openssl-util libopenssl“, tuomet į komandinę eilutę įrašyti „cd /root/CA“, ši komanda nukels jus į root/CA katalogą. Baigus įrašymui reikia įvesti komandą ir nuėjus į reikiamą katalogą „openssl ecparam -out ecca.param -name secp384r1” (4.11 pav.), ši komanda sukurs elipsinės kreivės parametrus (4.12 pav.).



4.11 pav. Elipsinių kreivių parametrų komanda



4.12 pav. Sukurtos elipsinės kreivės failo pavyzdys

Tuomet reikėtų sukurti vartotojo elipsinės kreivės raktų porą naudojant komandą „openssl req -nodes -newkey ec:ecca.param -days 3650 -x509 -sha256 -keyout ecca.key -out ecca.crt“ (4.13 pav.), ši komanda sukurs du failus, vienas iš jų bus „ecca.key“, kur bus saugomas privatus raktas ir „ecca.crt“, kur bus saugomas viešasis raktas. Taip pat reikėtų sukurti ir serverio elipsinės kreivės raktų porą naudojant komandą „openssl rq -nodes -newkey ec:ecca.crt -days 3650 -sha256 -keyout serverec.key -out serverec.csr“ (4.14 pav.).

```
root@OpenWrt:~/CA# openssl req -nodes -newkey ec:ecca.param -days 3650 -x509 -sh
a256 -keyout ecca.key -out ecca.crt
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:LT
State or Province Name (full name) [Some-State]:Kaunas
Locality Name (eg, city) []:Kaunas
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Kauno Kolegija
Organizational Unit Name (eg, section) []:.
Common Name (e.g. server FQDN or YOUR name) []:Anchelikas
Email Address []:anchelikas@gmail.com
```

4.13 pav. Vartotojų elipsinės kreivės raktų sukūrimas

```
root@OpenWrt:~/CA# openssl req -nodes -newkey ec:ecca.crt -days 3650 -sha256 -keyout serverec.key -out serverec.csr
Ignoring -days without -x509; not generating a certificate
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:LT
State or Province Name (full name) [Some-State]:Kauno
Locality Name (eg, city) []:Kaunas
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Kauno Kolegija
Organizational Unit Name (eg, section) []:.
Common Name (e.g. server FQDN or YOUR name) []:Anchelikas
Email Address []:anchelikas@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Slaptazodis
An optional company name []:
```

4.14 pav. Serverio elipsinės kreivės raktų sukūrimas

Tuomet norėdami naudoti *OpenSSL Demo CA*, reikia sukurti jai skirtą katalogo architektūrą ir inicializuoti pirmojo pasirašyto sertifikato serijos numerį į 01, tai galima padaryti naudojant komandas “mkdir ./demoCA/”, “mkdir ./demoCA/newcerts“, „touch ./demoCA/index.txt“, „echo 01 > ./demoCA/serial” (4.15 pav.).

```
$ mkdir ./demoCA/
$ mkdir ./demoCA/newcerts
$ touch ./demoCA/index.txt
$ echo 01 > ./demoCA/serial
```

4.15 pav. Direktorijos sukūrimas

Tuomet naudojant komandinę eilutę reikia pasirašyti serverio raktą naudojant šakninį CA raktą, tai galima padaryti naudojant komandą „openssl ca -extension v3_ca -days 3650 -out serverec.crt -in serverec.csr -cert ecca.crt -keyfile ecca.key“ (4.16 pav.).

```
root@OpenWrt:~/CA# openssl req -nodes -newkey ec:ecca.crt -days 3650 -sha256 -keyout serverec.key -out serverec.csropenssl ca -extensions v3_
ca -days 3650 -out serverec.crt -in serverec.csr -cert ecca.crt -keyfile ecca.key
req: Use -help for summary.
root@OpenWrt:~/CA# openssl ca -extensions v3_ca -days 3650 -out serverec.crt -in serverec.csr -cert ecca.crt -keyfile ecca.key
Using configuration from /etc/ssl/openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 3 (0x3)
        Validity
            Not Before: May 11 16:43:13 2024 GMT
            Not After : May  9 16:43:13 2034 GMT
        Subject:
            countryName               = LT
            stateOrProvinceName       = Kauno
            organizationName          = Kauno Kolegija
            commonName                = Anchelikas
            emailAddress              = anchelikas@gmail.com
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                FF:26:6C:59:E7:E9:2B:FA:90:F1:53:7C:A7:46:0C:5C:02:B4:DA:D7
            X509v3 Authority Key Identifier:
                49:41:13:8D:E4:E6:94:2E:F7:F0:2C:5B:57:6F:4D:56:DC:4B:9A:D0
            X509v3 Basic Constraints: critical
                CA:TRUE
Certificate is to be certified until May  9 16:43:13 2034 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database updated
```

4.16 pav. Pasirašyto rakto pavyzdys

Sertifikatų kūrimas yra baigtas, tačiau jeigu yra norima šį sertifikatą įsikeli į telefoną reikia įvesti dar vieną komandą kuri sukurs P12 formato failą kurį reikės įsikelti į telefoną „openssl pkcs12 -export -in CLIENT.crt -inkey CLIENT.key -out CLIENT.p12 -certfile ecca.crt -passout pass:*slaptažodis*“ (4.17 pav.).

```
root@OpenWrt:~/CA# openssl ca -extensions v3_ca -days 3650 -out CLIENT.crt -in CLIENT.csr -cert ecca.crt -keyfile ecca.key
Using configuration from /etc/ssl/openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4 (0x4)
        Validity
            Not Before: May 11 17:00:16 2024 GMT
            Not After : May  9 17:00:16 2034 GMT
        Subject:
            countryName               = LT
            stateOrProvinceName       = Kauno
            organizationName          = Kauno Kolegija
            commonName                = Vienas
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                76:EB:F8:F9:E9:A5:42:C7:73:FF:A7:1B:2E:3B:6B:F7:DC:13:81:0B
            X509v3 Authority Key Identifier:
                49:41:13:8D:E4:E6:94:2E:F7:F0:2C:5B:57:6F:4D:56:DC:4B:9A:D0
            X509v3 Basic Constraints: critical
                CA:TRUE
Certificate is to be certified until May  9 17:00:16 2034 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database updated
```

4.17 pav. Telefonui skirtas P12 formato sertifikato failo kūrimas

Baigus šią dalį reikėtų nueiti į */etc/freeradius3/mods-enabled/eap* ir užkomentuoti „default_eap_type = md5" eilutę ir apačioje pridėti naują eilutę „default_eap_type = tls", padarius tai, tame pačiame faile taip pat reikia surasti „cipher_list" eilutę, ją užkomentuoti ir apačioje pridėti „cipher_list = "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA256:ECDHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS;"" šifrą.

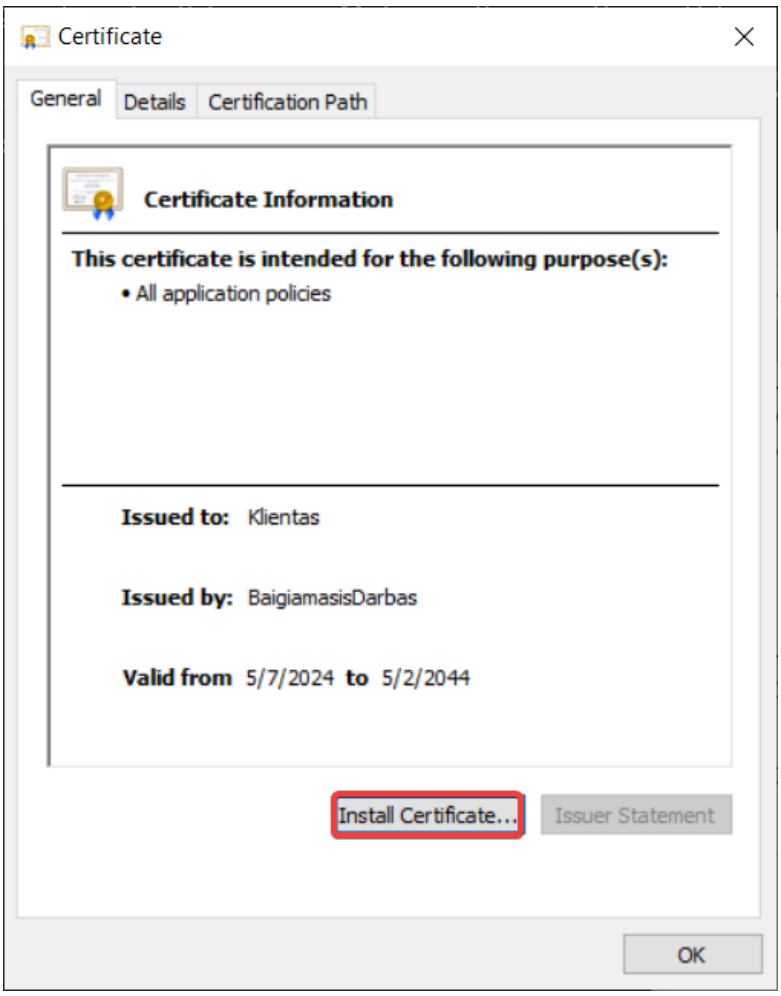
Atlikus visa tai į komandinę eilutę reikia įvesti „radiusd -XX", kad paleisti *radiusd,* jei viskas pasijungė tvarkingai turėtų rodyti „*Info: Ready to process requests*" (4.18 pav.).

```
Sat May 11 17:18:50 2024 : Debug: Listening on auth address * port 1812 bound to server default
Sat May 11 17:18:50 2024 : Debug: Opened new proxy socket 'proxy address * port 60359'
Sat May 11 17:18:50 2024 : Debug: Listening on proxy address * port 60359
Sat May 11 17:18:50 2024 : Info: Ready to process requests
```

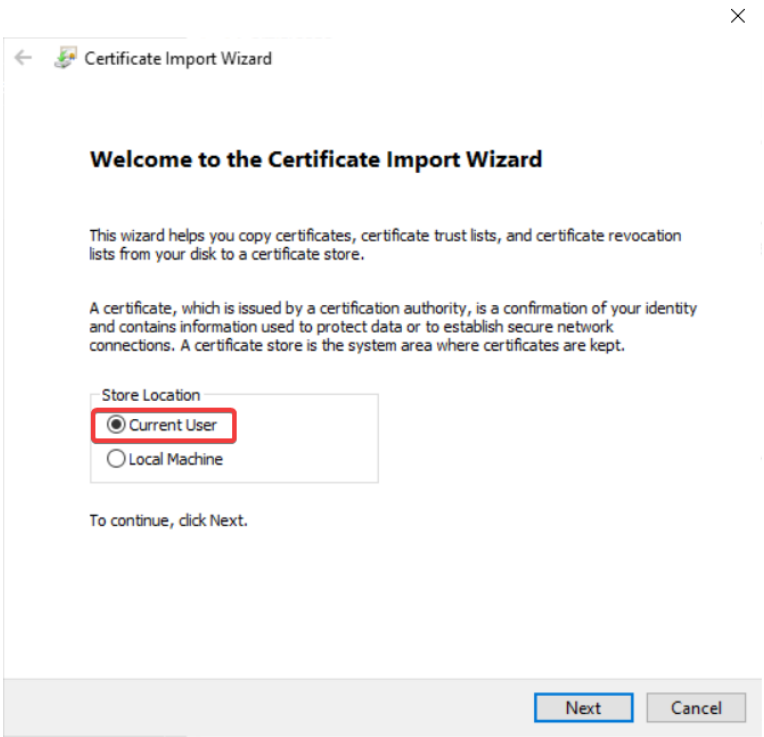
4.18 pav. *Radiusd* -XX pajungimo pavyzdys

4.4. Sertifikatų įkėlimas ir įrašymas

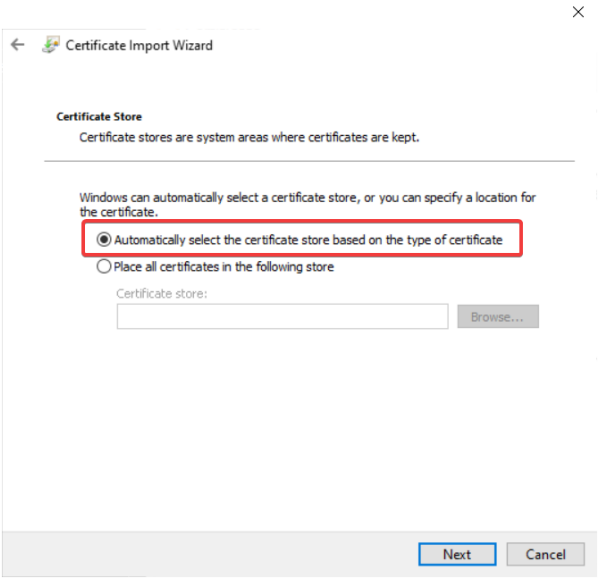
Baigus *FreeRadius* nustatymus ir sukūrus raktus reikėtų juos taip pat ir įsirašyti į kompiuterį ar kitą prietaisą. Tai padaryti reikia per *WinSCP* ar kitą pasirinktą programa nueiti į „/root/CA", susirasti tinkamą .crt failą, šiuo atveju „Klientas.crt" ir jį išsikelti į kompiuterį. Baigus išsikelti šį failą reikia ant jo paspausti du kartus iki kol jis pasijungs. Pasijungus reikėtų paspausti įrašyti sertifikatą mygtuką (angl. *Install Certificate*) (4.19 pav.), kitoje skiltyje yra pasirinkimas tarp dabartinio naudotojo ir vietinės mašinos, šį kartą renkamės dabartinį naudotoją (4.20 pav.). Kitame vedlio lange renkamės „Automatiškai parinkti sertifikatą pagal sertifikato tipą" (4.21 pav.). Paskutiniame lange dar galima pasižiūrėti visą informaciją kurią pasirinkote, jei viskas tinka, reikia spausti baigti ir sertifikatas bus įrašytas (4.22 pav.) . Baigus sertifikato įsirašymui reikėtų prisijungti prie prieigos taško (4.23 pav.), kad tai padaryti reikia paspausti ant *Wi-Fi*, pasirinkti prieigos tašką ir paspaudus ant jo pasirinkti jungtis naudojant sertifikatą (angl. *Connect using a certificate*).



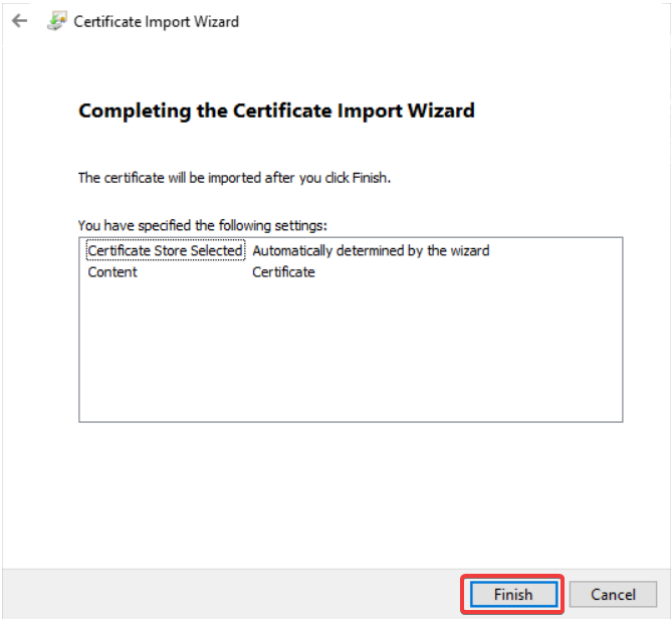
4.19 pav. Sertifikato įrašymo pavyzdys



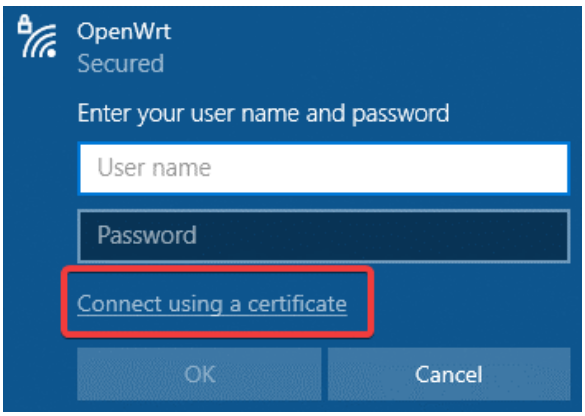
4.20 pav. Pasirinkimas tarp dabartinio naudotojo ir vietinės mašinos



4.21 pav. Sertifikato pasirinkimas kur jį patalpinti

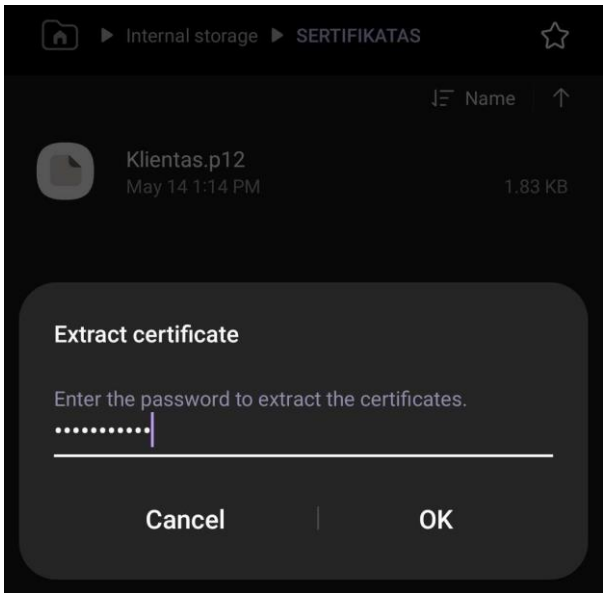


4.22 pav. Vedlio paskutinis laukas

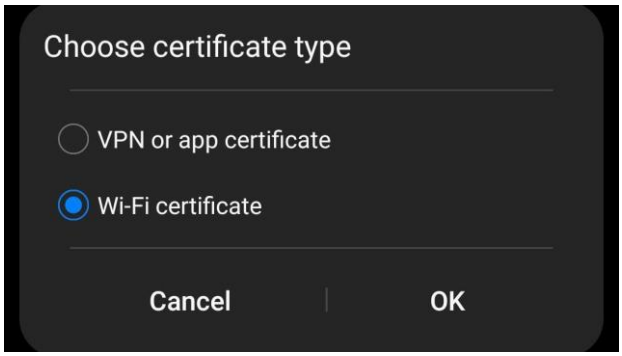


4.23 pav. Prisijungimas prie *OpenWRT* naudojant sertifikatą

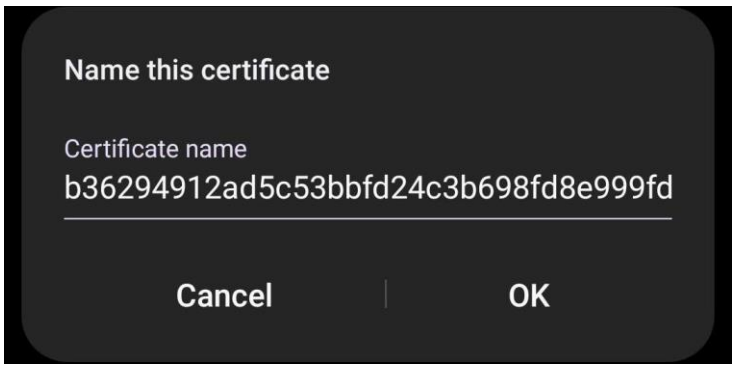
Sertifikato įrašymas į *Android* sistemą yra panašus kaip ir kompiuterio, tik šį kartą reikia išsikelti .p12 failą į telefoną, ir vedlio pagalbą jį įsirašyti. Pradedant vedlį reikia įvesti slaptažodį (4.24 pav.), slaptažodis yra gaunamas naudojant komandą gauti .p12 failą, „-passout pass:“ dalyje. Po slaptažodžio atsiras skiltis, kur reikia pasirinkti kokio tipo sertifikatą norite naudoti, šiuo atveju yra spaudžiamas *Wi-Fi* sertifikatas (4.25 pav.). Baigus sertifikato tipo pasirinkimą yra duodama galimybė pavadinti šį sertifikatą, kad būtų lengviau atpažinti (4.26 pav.). Kai paspausti „gerai“ sertifikato pasirinkimo skiltyje, sertifikatas jau turėtų būtį įrašytas. Kad patikrinti ar sertifikatas tikrai įsirašė galima nueiti į nustatymus ir surasti „Naudotojo sertifikatai“ skiltį kur ant jos paspaudus išmetu visus sertifikatus kurie yra jūsų telefone. Paspaudus ant naujai įrašyto sertifikato galima pamatyti sertifikato informaciją (4.27 pav.). Dabar prisijungiant reikėtų eiti į *Wi-Fi* nustatymus ir susirasti *OpenWRT* prieigos tašką (4.28 pav.), paspausti ant jo, viršuje yra *EAP* metodas (angl. *EAP method*) mygtukas kurį reikią paspausti ir pasirinkti *TLS*, tuomet ant CA sertifikatas ir naudotojų sertifikatas pasirinkti įrašytą sertifikatą (4.29 pav.) ir paspausti jungtis, po kelių sekundžių bus prisijungta prie *Wi-Fi* (4.30 pav.).



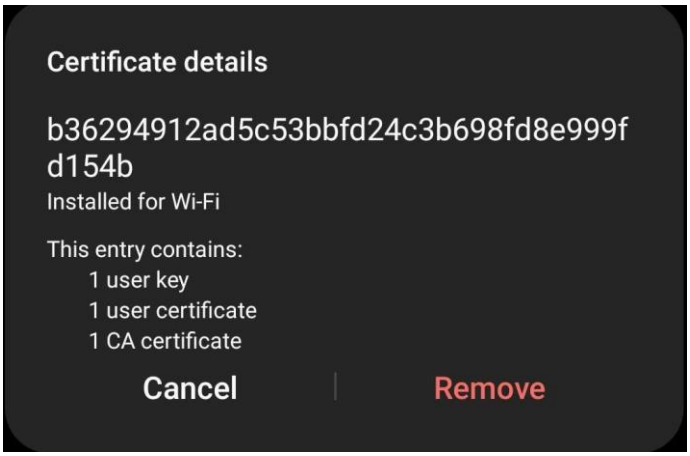
4.24 pav. Slaptažodžio įvedimas sertifikatui įrašyti



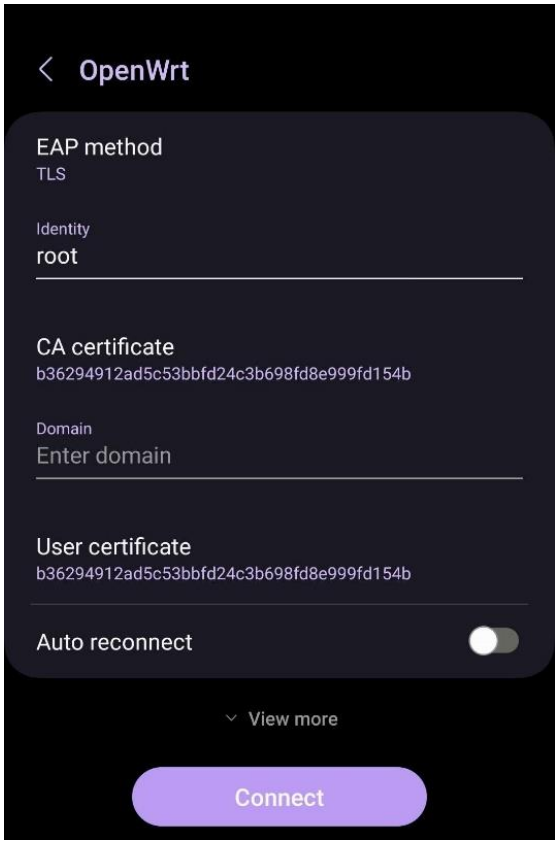
4.25 pav. Sertifikato tipo pasirinkimas



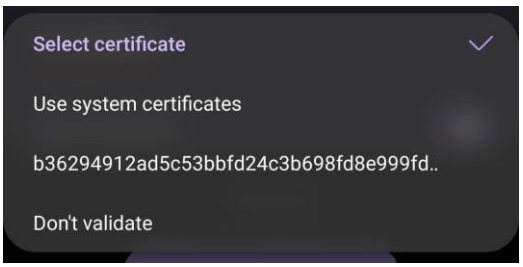
4.26 pav. Sertifikato pavadinimas



4.27 pav. Įrašyto sertifikato informacinis langas



4.28 pav. Prisijungimo laukas



4.29 pav. Sertifikatų pasirinkimas

4.30 pav. Laukas kuris matomas prisijungus prie prieigos taško

Taigi, baigus prisijungti prie prieigos taško naudojant telefonu ar nešiojamu kompiuteriu dabar galima naudotis saugiu belaidžiu interneto tinklu jūsų namų ofise.

5. EKONOMINĖ DALIS

5.1. Įrangos pirkimas ir nuoma

6 lentelėje nurodyta techninė įranga, kiekis ir kokia yra siūloma pirkimo kaina.

6 lentelė. Perkama techninė įranga

Nr.	Pavadinimas ir techninės charakteristikos	Mato vnt.	Kiekis	Kaina, Eur	Suma, Eur
1.	„UBIQUITI UniFi AC LITE“ prieigos taškas	Vnt.	1	82,00	82,00
2.	*Digitus* | *Patch Cord* | DK-1512-030 interneto kabelis	Vnt.	2	3,68	7,36
3.	*OpenWRT* operacinė sistema	Vnt.	1	0,00	0,00
4.	*FreeRadius*	Vnt.	1	0,00	0,00
				Iš viso, Eur:	89,36
				PVM, 21%	18,77
				Bendra suma, Eur:	108,13

7 lentelėje surašyti įrangos nuomos planai, nurodytos sumos, kurias reikia sumokėti kiekvieną mėnesį, nes nėra galimybės nusipirkti.

7 lentelė. Nuomojami planai

Nr.	Įrangos pavadinimas	Tiekėjo pavadinimas	Kaina, Eur/mėn.	Kiekis, mėn.	Suma, Eur
1.	1 GB/S, 2,5DBI interneto planas	Besmegeniai.lt	8,97	12	107,64
				Iš viso, Eur:	107,64
				PVM, 21%	22,60
				Bendra suma, Eur:	130,24

5.2. Įrangos nusidėvėjimas

8 lentelėje pateikiama įranga, programos, kurių nereikėjo nusipirkti tačiau buvo reikalingos įgyvendinti šį projektą ir jo realizaciją, nurodytas jos nusidėvėjimo normatyvas ir galimos išlaidos jai.

8 lentelė. Įrangos ir programų nusidėvėjimas

Pavadinimas	1 mėn. vertė, Eur	Nusidėvėjimo normatyvas metais	Mėn. kiekis, vnt.	Iš viso, Eur
Ilgalaikis turtas				
Nešiojamas kompiuteris Lenovo IdeaPad Gaming 3	14,58	4	3	43,74
Pelė Glorious Model o-	1,25	3	3	3,75
Monitorius HP X24ih	2,04	7	3	6,12
Klaviatūra GK630K	1,27	3	3	3,81
Programinė įranga				
Windows 11 Operacinė sistema	1,04	10	3	3,12
			Iš viso, Eur:	60,54
			PVM, 21%	12,71
			Bendra suma, Eur:	73,25

5.3. Darbo užmokesčio skaičiavimas

9 lentelėje yra pateikiami darbai ir jų trukmės, projekto metu įvykdyti darbai, bei kiek kiekvienas iš šių darbų užtruko laiko atlikti.

9 lentelė. Projekto trukmė

Darbai	Dirbta valandų
Situacijos analizė	32
Įrangos įsigijimas/sujungimas	32
Projektavimas	32
Programinės įrangos kūrimas, bei konfigūravimas	90
Projekto testavimas	10
Iš viso:	196

Apskaičiuoti darbo užmokestį bus naudojamas vidutinis IT saugumo specialisto atlyginimas kuris yra 2014 eurų naudojantis 2023 metų duomenimis.

Valandinio įkainio apskaičiavimas

- Bruto mėnesinis atlyginimas (neatskaičiavus mokesčių) Eur / 21 darbo diena (dirbamų dienų per mėnesį vidurkis) / 8 darbo valandos = valandinis įkainis, Eur;
- Valandinis atlyginimas = 2014 / 21 darbo d. / 8 val. = 11,99 Eur.
- Bruto atlyginimas, įvertinus kiek laiko užtruko atlikti projektą;
  Valandinis įkainis, Eur X projekto atlikimo trukmė, val. = projekto įgyvendinimo rengėjo atlyginimo sąnaudos, Eur.
  Bruto atlyginimas = 11,99 Eur * 196 val. = 2350,04 Eur.

5.4. Įdiegto projekto palaikymo sąnaudos

10 lentelėje yra pateikiamos projekto palaikymo įrangos, už kurias reikėtų mokėti kiekvieną mėnesį, kad projektas veiktų.

10 lentelė. Projekto palaikymo kainos lentelė

Įrangos pavadinimas	Tiekėjo pavadinimas	Kaina, Eur/mėn.	Kiekis, mėn	Suma, Eur
1 GB/S, 2,5DBI interneto planas	Besmegeniai.lt	8,97	12	107,64
			Iš viso, Eur:	107,64
			PVM, 21%	22,60
			Bendra suma, Eur:	130,24

5.5. Projekto sąmata

11 lentelėje yra nurodoma projekto sąmata, yra skaičiuojama viso projekto kaina ir pridedamas administracinis sąnaudos mokestis kuris yra 10%.

11 lentelė. Projekto sąmata

Nr.	Pavadinimas	Suma, Eur
1.	Programinės ir techninės įrangos pirkimas	108,13
2.	Planų nuoma	130,24
3.	Įrangos nusidėvėjimas	73,25
4.	Darbo užmokestis	2350,04
5.	Projekto palaikymo sąnaudos	130,24
	Iš viso:	2791,9
6.	Administracinės sąnaudos (10%)	279,19
	Iš viso:	3071,09

5.6. Ekonominės naudos nustatymas

Kadangi bus užtikrinamas internetinis saugumas bus naudojami skaičiavimai naudojantis NKSC esančia „Rizikos analizės vadovas“ knyga.

Naudojamas pažeidžiamumo veiksnys (PV), kad būtų paskaičiuotas tikėtinas vienkartinis nuostolis (TVN). Kadangi šis tinklas yra skirtas namų ofisui, tai turto vertė nebus labai didelė, todėl pasirinkau 3000 Eur vidutinį eurų skaičių ir PV pasirinktas 5%. Taigi TVN yra skaičiuojamas naudojant formulę „turto vertė (Eur) * Pažeidžiamumo veiksnys (PV) = TVN.

- 3000 EUR * 5% = 150 Eur.

Toliau yra skaičiuojamas metinis dažnumo rodiklis (MDR), tai skaičius, kuris išreiškia apskaičiuotą grėsmės iškilimo dažnumą per metus. Čia ir vėl reikėtų įvertinti, kad tai visgi yra namų

ofiso projektas, todėl pasirinkta tikimybė, kad 5 įsilaužėliai 6 kartus per metus mėgins įsilaužti į tinklą yra didelė, tad MDR yra gaunamas 30.

Tikėtinas metinis nuostolis (TMN), tai yra piniginė išraiška, apskaičiuojama pagal formulę „tikėtinas vienkartinis nuostolis (TVN) * metinis dažnumo rodiklis (MDR) = TMN“.

- 150 * 30 = 4500 Eur.

Apsaugant tinklą nuo tokių įsilaužimų MDR praktiškai krenta į 0 arba 1 įsilaužimus, todėl TMN taip pat tampa 0 Eur.

Kad apskaičiuoti atsipirkimo laikotarpį reikia sužinoti ir TMN kai sistema jau yra apsaugoti, taigi TMN skaičius tampa arba 0 Eur, arba 150 Eur.

Naudojama formulė apskaičiuoti atsipirkimo laikotarpį:

„TMN (prieš ir po sistemos įdiegimo)/projekto kaina = atsipirkimo laikotarpis“

- Atsipirkimo laikotarpis kai nėra įdiegta saugaus namų ofiso sistema: 4500/3071,09 = 1,47 metai.
- Atsipirkimo laikotarpis kai sistema yra įdiegta su minimaliu nuostoliu 150/3071,09 = 0,049 metai.

Taigi pasižiūrėjus į šiuos du variantus tampa akivaizdu, kad turint saugia namų ofiso sistemą yra daug saugiau ir geriau.

IŠVADOS

1. Buvo išanalizuotos šiuo metu esamos saugaus namų ofiso belaidžio tinklo sistemos. Buvo apžiūrėta kita galima belaidžio tinklo sistema, tačiau dėl jos dydžio ir sunkumo padaryti jį nebuvo pasirinkta. Dėl to buvo rinktasi daug pigesnis ir lengviau paruošiamas namų belaidis tinklas, kur yra naudojamas tik vienas prieigos taškas į kurį įrašomos programos, kurios padeda apsaugoti namų belaidį tinklą. Dėl šio tinklo mažesnio mastelio jį yra lengviau valdyti nei mėginant daryti didesnio masto tinklo projektą, kur paprastiems vartotojams jis galėtų būti netinkamas.
2. Buvo įsigilinta į įvairias programas, bei saugumo sertifikatus kurie buvo naudingi paruošiant šį projektą. Buvo atsižvelgta į *EAP-TLS* autentifikavimą, ir atsižvelgiama į kitus galimus variantus, tokius kaip *EAP-TTLS, PEAP-TLS*. Įsigilinta į *OpenWRT* ir *FreeRadius* programinę įrangą, jos įvairius konfigūravimo nustatymus.
3. Sukurtas projektas, kurį įgyvendinus jis turėtų atrodyti, kokias funkcijas turėtų atlikti, ir kokią naudą duotų.
4. Buvo įvertintas sistemos saugumas atsižvelgus į dabar esančius autentifikavimo metodus ir naudojant *EAP-TLS*. Šiuo metu *EAP-TLS* yra auksinis autentifikavimų standartas, nors šio standarto nenaudoja didelė dalis žmonių.
5. Sukurtas naudotojų vadovas, kur yra išdėstomas kelias kaip reikėtų pasidaryti šį projektą savo namuose. Paaiškinama ką daro kiekviena parodyta komandinė eilutė ar kur reikia eiti grafinėje vartotojų sąsajoje. Taip pat parodytos komandos kurių pagalba galima pažiūrėti ar tinklas pasijungia tvarkingai, o jei ne, šios komandos parodo kur gali būti problemos.
6. Apskaičiuotos projekto įvykdymo išlaidos, šios išlaidos yra 3071,09 EUR, o kad įvykdyti šį projektą buvo praleistos 196 valandos. Palyginamas atsipirkimo laikotarpis prieš įrengiant sistemą ir po sistemos įrengimo. Galima pamatyti, kad skirtumas prieš įrengimo ir po įrengimo yra gana didelis, pasikeičia nuo 1,47 metų iki vos 0,049 metų.

LITERATŪRA IR KITI INFORMACIJOS ŠALTINIAI

1. A. Dagelić, M. Bugarić, M. Čagalj (2020.). On WPA2-Enterprise Privacy in High Education and Science https://www.hindawi.com/journals/scn/2020/3731529/
2. Abdullah Alabdulatif, Xiaogi Ma (2014.). Analysing the EAP-TLS handshake and the 4-way handshake of the 802.11i standard https://www.semanticscholar.org/paper/Analysing-the-EAP-TLS-handshake-and-the-4-way-of-Alabdulatif-Ma/21013f6886c014f92c5b272c29f2924d53ec9df6
3. BusyBox https://busybox.net/about.html
4. Cody Richardson (2021). Secure Cipher Suites and TLS https:// blog. Codyrichardson .io /2021/07/secure-cipher-suites-and-tls-in-2021.html
5. Dynamic Host Configuration Protocol (DHCP) https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top
6. EAP-TLS vs. PEAP-MSCHAPv2: Which Authentication Protocol is Superior https://www .securew2.com/blog/eap-tls-vs-peap-mschapv2-which-authentication-protocol-is-superior
7. Elliptic Curve Cryptography Definition https://avinetworks.com/glossary/elliptic-curve-cryptography/
8. FreeRADIUS (n.d.). FreeRADIUS dokumentacija https://github.com/FreeRADIUS/ freeradius-server/tree/v3.2.x/doc/
9. Gargoyle Router https://www.gargoyle-router.com
10. Gautama Wijaya, Nico Surantha (2020.). Mutli-layered Security Design and Evaluation for Cloud-based Web Application: Case Study of Human Resource Management System https://www.researchgate.net/publication/347151915_Multi-layered_Security_Design_and_Evaluatio n_for_Cloud-based_Web_Application_Case_Study_of_Human_Resource_Management_System
11. Ivo Kubjas (2015) Modern elliptic curve cryptography https://www.semanticscholar.org /paper/Modern-elliptic-curve-cryptography-Kubjas/ab9cdcfa6fd1351f4e66_8535bc48ea51_b942ebe0#related-papers
12. JUCI Webgui for Embedded Routers https://github.com/mkschreder/juci
13. Kerner S. (2017). EAP-TLS Detailed as WiFi Security Best Practice at SecTor. https://web.p.ebscohost.com/ehost/detail/detail?vid=8&sid=d03d0c25-3f99-45ac-9bd42743bf6a7f9a%40redis&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=126265026&db=asn
14. Kerner Sean Michael (2018). TLS 1.3 Encryption Standard Moves Forward, Improving Internet Securityhttps://web.p.ebscohost.com/ehost/detail/detail?vid=17&sid=28d5f362-987c-4017-a252-972004d5d16d%40redis&bdata=JnNpdGU9ZWhvc3Qt bGl2ZQ%3d% 3d#db=e000xw w&AN=1841869

15. Kim Cheong, Kim Kuinam Implementation of a cost-effective home lightning control system on embedded Linux with OpenWrt. https://web.p.ebscohost.com/e host/detail/detail ?vid=4&sid=8bac3ed4-c586-4de8-8c2b-e5cb4b8b2bdc%40redis&bdata=JnNpdGU9 ZW hvc3QtbGl2ZQ%3d%3d#AN=94449962&db=asn
16. Krupa Patil (2022.). Why Is TLS 1.3 Better And Safer Than TLS 1.2? https://www.appviewx.com/blogs/why-is-tls-1-3-better-and-safer-than-tls-1-2/
17. Linksys (n.d.). Linksys LAPAC1750 Technical Specifications https://www.linksys.com/lapac1750-business-ac1750-dual-band-access-point/LAPAC1750.html
18. Lua programming language https://www.lua.org/about.html
19. LuCI https://github.com/openwrt/luci/wiki/
20. OpenVMPShttps://sourceforge.net/projects/vmps/
21. OpenWRT firmware selector https://firmware-selector.openwrt.org/?version=23.05.0& target=ath79%2Fgeneric&id=ubnt_unifiac-lite
22. Power over Ethernet https://intellinetnetwork.eu/pages/power-over-ethernet
23. Samuel Bowne (2018). Hands-On Cryptography with Python : Leverage the Power of Python to Encrypt and Decrypt Data https://web.p.ebscohost.com/ehost/detail/detail?vid=17 &sid= 28d5f362-987c-4017-a252-972004d5d16d%40redis&bdata=JnNpdGU9ZWhvc3QtbG l2ZQ%3d%3d#db=e000xww&AN=1841869
24. TLS Cipher Suites in Windows 10 V1709 https://eddiejackson.net/wp/?p=17213
25. Tobby Chitty (2020). The Mathematics of Bitcoin – SHA-256 https://medium.com/swlh/the-mathematics-of-bitcoin-74ebf6cefbb0
26. Tp-link (n.d.). TP-LINK EAP225 V3 Technical Specifications https://www.tp-link.com /us/business-networking/ceiling-mount-access-point/eap225/
27. Tran Thi Hong, Hoai Luan Pham (2021). A High-Performance Multimem SHA-256 Accelerator for Society 5.0 https://www.researchgate.net/publication/349744176_A_High-Performance_Multimem_SHA-256_Accelerator_for_Society_50
28. Ubiquiti (n.d.). Ubiquiti UniFi AC LITE Technical Specifications https://techspecs.ui.com/unifi/wifi/uap-ac-lite
29. What is the SHA-256 algorithm, and how does it work? https://nordvpn.com/lt/blog/sha-256/
30. What is VPN? How It Works, Type https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn
31. What is WPA3 vs. WPA2? https://www.portnox.com/cybersecurity-101/wpa3/
32. What is AES Encryption and How does it Work?https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption