Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: *Маршрутизатор пакетів комп'ютерної мережі на основі Raspberry PI та Open WRT*

Виконав: студент *IV* курсу, групи *CI-42*
спеціальності *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

	(підпис)	*Яшнюк О.І.* (прізвище та ініціали)
Керівник	(підпис)	*Яцишин В.В.* (прізвище та ініціали)
Нормоконтроль	(підпис)	*Тиш Є.В.* (прізвище та ініціали)
Завідувач кафедри	(підпис)	*Осухівська Г.М.* (прізвище та ініціали)
Рецензент	(підпис)	*Карпінський М.П.* (прізвище та ініціали)

Тернопіль
2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет *комп'ютерно-інформаційних систем і програмної інженерії*
(повна назва факультету)

Кафедра *комп'ютерних систем та мереж*
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ *Осухівська Г.М.*
(підпис) (прізвище та ініціали)
« ___ » _____ 2024 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *бакалавр*
(назва освітнього ступеня)

за спеціальністю *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

студенту *Яшнюку Олександру Ігоровичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Маршрутизатор пакетів комп'ютерної мережі на основі Raspberry PI та Open WRT*

Керівник роботи *Яцишин Василь Володимирович, к.т.н., доцент*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « *24* » *квітня* 2024 року № *4.7-408*

2. Термін подання студентом завершеної роботи *24.06.2024 р.*

3. Вихідні дані до роботи *Характеристики Raspberry PI, особливості прошивки Open WRT, типи і функції маршрутизаторів, принципи функціонування комп'ютерної мережі*

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Аналіз типів комп'ютерних мереж та ролі маршрутизаторів 2. Проектування та налаштування маршрутизатора на Raspberry PI 4 з Open WRT 3. Налаштування служб і сервісів маршрутизатора на базі Raspberry PI 4. Безпека життєдіяльності, основи охорони праці. Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. *Види і характеристика комп'ютерних мереж.*
2. *Типова організація VPN-мережі.*
3. *Структурна схема типового маршрутизатора*
4. *Інфраструктура мережі на основі Raspberry PI та Open WRT.*

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	*Пилипець М.І., д.т.н., проф. каф. МТ*		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	*Розробка і затвердження технічного завдання*	*24.04-28.04.2024*	
2.	*Аналіз технічного завдання*	*28.04-02.05.2024*	
3.	*Аналіз типів комп'ютерних мереж та ролі маршрутизаторів*	*02.05-05.05.2024*	
4.	*Проектування та налаштування маршрутизатора на Raspberry PI 4 з Open WRT*	*05.05-10.05.2024*	
5.	*Налаштування служб і сервісів маршрутизатора на базі Raspberry PI*	*10.05-25.05.2024*	
6.	*Розробка інструкцій щодо використання маршрутизатора*	*25.05-29.05.2024*	
7.	*Безпека життєдіяльності, основи охорони праці*	*01.06-05.06.2024*	
8.	*Оформлення кваліфікаційної роботи*	*05.06-12.06.2024*	
9.	*Попередній захист кваліфікаційної роботи*	*12.06-17.06.2024*	
10.	*Захист кваліфікаційної роботи*	*24.06-27.06.2024*	

Студент _____ *Яшнюк Олександр Ігорович*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Яцишин Василь Володимирович*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Маршрутизатор пакетів комп’ютерної мережі на основі Raspberry PI та Open WRT // Кваліфікаційна робота на здобуття освітнього ступеня бакалавр // Яшнюк Олександр Ігорович // ТНТУ, спеціальність 123 «Комп’ютерна інженерія»// Тернопіль, 2024 // с.– 87 , рис. – 48 , табл. – 4, аркушів А1 – 4, бібліогр. – 22.

Ключові слова: маршрутизатор, мережа, мікроконтролер, Raspberry PI, Open WRT.

У кваліфікаційній роботі розроблено проект маршрутизатора комп’ютерної мережі з використанням мінікомп’ютера Rapsberry PI 4 та прошивки Open WRT версії bcm2711.

У проекті передбачено: швидкість передачі даних на рівні 1 Гб/с; створено дві віртуальні локальні мережі; імплементовано сервіс блокування реклами; налаштовано доступ до медіа сервера; організовано торент-клієнт.

Усі перелічені служби і сервіси працюють у Docker-контейнерах, тобто ізольовано від інших мереж.

У роботі представлено базове налаштування Open WRT для Raspberry PI 4, визначено зони FireWall для різних віртуальних мереж і служб, що дало можливість підвищити рівень безпеки та якість надання послуг кінцевому користувачу у порівнянні з типовими маршрутизаторами серійного виробництва.

ABSTRACT

A computer network router based on Raspberry PI and Open WRT// Bachelor's thesis // Yashniuk Oleksandr // TNTU, speciality 123 «Computer engineering»// Ternopil, 2024 // p.– 87, fig. – 48 , tab. – 4, posters A1 – 4, ref. – 22.

Keywords: router, network, microcontroller, Rapberry PI, Open WRT.

In the qualifying work, a computer network router project was developed using a Rapsberry PI 4 minicomputer and Open WRT firmware version bcm2711.

The project provides for: data transfer speed at the level of 1 Gb/s; two virtual local networks were created; an ad blocking service has been implemented; access to the media server is configured; torrent client is organized.

All the listed services and services work in Docker containers, that is, isolated from other networks. The paper presents the basic configuration of Open WRT for Raspberry PI 4, defined FireWall zones for various virtual networks and services, which made it possible to increase the level of security and quality of service provision to the end user in comparison with typical mass-produced routers.

ЗМІСТ

ВСТУП

Стрімкий розвиток комп'ютерних технологій вимагає повсякчасного впровадження комунікаційної інфраструктури, що забезпечує швидкий обмін даними, сприяє їх доставці до місця зберігання та дозволяє трансляцію медіа в режимі реального часу. При побудові мереж передачі даних використовуються пристрої комутації, маршрутизації, точки доступу та інші без яких неможлива передача даних на великі відстані. Сьогодні будь-яке підприємство чи організація як мінімум використовує локальну обчислювальну мережу з доступом до мережі Інтернет. Окрім цього в домашніх умовах використовується, як мінімум один маршрутизатор, що забезпечує доступ до глобальної мережі.

Такі параметри як пропускна здатність, швидкість, безпека та надійність залежать від пристроїв комутації та маршрутизації.

Найчастіше інтернет-провайдер, окрім послуг Інтернету, зазвичай надає маршрутизатор. Він «сертифікований» для мережі Інтернет-провайдера та забезпечує дротове та бездротове підключення для всіх пристроїв у домі. У більшості випадків люди не намагаються замінити цей маршрутизатор, оскільки це підвищує вартість і ускладнює налаштування мережі. Але, коли справа стосується домашньої мережі чи мережі підприємства важливим є забезпечення показників безпечності та продуктивності.

Доволі часто можна спостерігати ситуацію, коли сертифіковані маршрутизатори містять невиправлені вразливості, UPnP увімкнено за замовчуванням, неможливість виконати розділення гостьових і локальних клієнтів тощо.

Сконфігурувати апаратне забезпечення комп'ютерної мережі користувачу без досвіду досить складно, особливо, коли це маршрутизатор. У цьому випадку краще використовувати точку доступу за правильним брандмауером маршрутизатора, ніж універсальний пристрій, який не може правильно виконувати одну з цих речей.

Інтегроване у маршрутизатор програмне забезпечення не дає змоги налаштувати WireGuard чи OpenVPN, а також забезпечити налаштування правильного доступу до правил брандмауера або MultiWAN. Все що забезпечують сучасні відносно недорогі маршрутизатори – це можливість перемикати DNS-сервер і налаштовувати діапазони DHCP.

Альтернативою застосуванню стандартних маршрутизаторів є створення власного маршрутизатора на базі Raspberry PI, що дозволить забезпечувати швидкість передачі даних на рівні 1 Гб/с з прошивкою від Open WRT. Отже, метою кваліфікаційної роботи є розробка проекту маршрутизатора на базі Raspberry PI з використанням Open WRT та налаштуванням сервісів безпеки, віддаленого доступу, блокуванням реклами та служби торентів.

РОЗДІЛ 1 АНАЛІЗ ТИПІВ КОМП'ЮТЕРНИХ МЕРЕЖА ТА РОЛІ МАРШРУТИЗАТОРІВ

1.1 Аналіз типів і характеристик комп'ютерних мереж

Під комп'ютерною мережею прийнято розуміти кластер комп'ютерів, які спільно використовуються канал зв'язку та ресурси робочих станцій і серверів, які формують вузли мережі [1].

Комп'ютерні мережі забезпечують:

– можливість комунікації із застосуванням сервісів електронної пошти, відеообміну, обміну різними типами повідомлень тощо;

– спільне використання пристроїв, таких як принтери, сканери та інша периферія;

– обмін файлами;

– спільне використання програмного забезпечення та операційних програм у віддалених системах;

– можливість користувачів мережі легко отримувати доступ до інформації та підтримувати її.

Загалом виділяють п'ять типів комп'ютерних мереж:

– персональна мережа (PAN);

– локальна обчислювальна мережа (LAN);

– мережа рівня організацій (містечка) (CAN);

– мережа рівня міста (MAN);

– глобальна мережа (WAN);

На рис. 1.1 показано найбільш використовувані типи комп'ютерних мереж.

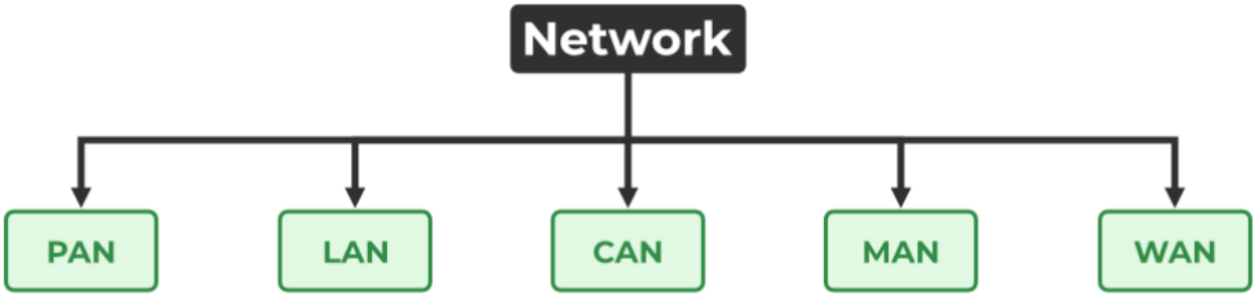

Рисунок 1.1 – Типи комп’ютерних мереж

Персональні комп’ютерні мережі відносяться до найпростішого типу комп’ютерних мереж. Ця мережа обмежується однією особою, тобто комунікацією між комп’ютерними пристроями зосереджено лише у робочому просторі окремої людини.

PAN має розмір від 1 до 100 метрів від людини до пристрою, що забезпечує зв’язок. Його швидкість передачі дуже висока з дуже простим обслуговуванням і дуже низькою ціною. Тут використовуються технології Bluetooth, IrDA та Zigbee. Прикладами PAN є USB, комп’ютер, телефон, планшет, принтер, КПК тощо. На рис. 1.2 показано приклад мережі, яка відноситься до персонального типу.

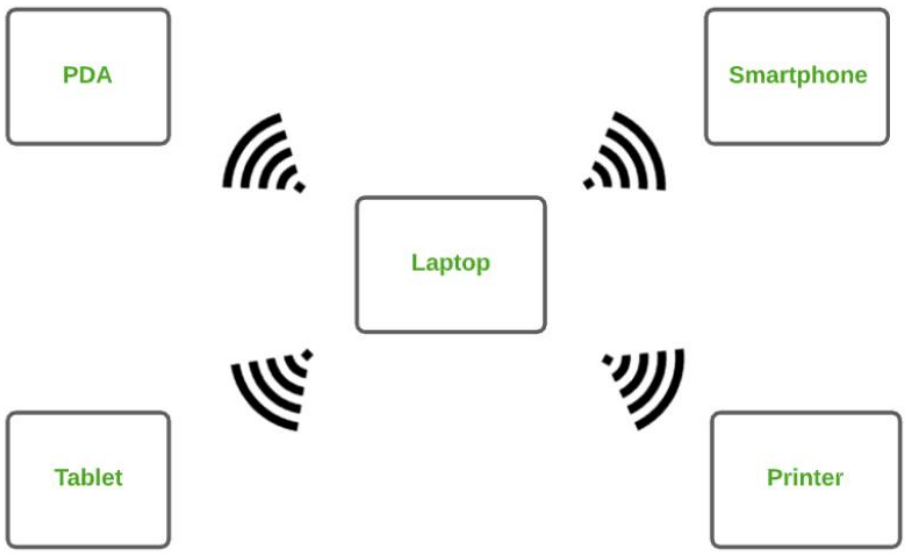

Рисунок 1.2 – Приклад мережі PAN

Локальна мережа (LAN) є найбільш часто використовуваною мережею. Локальна мережа – це тип комп’ютерної мережі, яка об’єднує комп’ютери через загальний канал зв’язку, що покриває обмежену зону, тобто є локальним.

Локальна мережа охоплює два або більше комп’ютерів, з’єднаних через сервер. Дві важливі технології, задіяні в цій мережі – це Ethernet і Wi-Fi. Дана комп’ютерна мережа може покривати площу на відстані до 2 км, швидкість передачі дуже висока. При цьому її легко обслуговувати, а вартість мережі є невисокою. Прикладами локальної мережі є домашня мережа, мережа у школі, бібліотеці, лабораторії, коледжі, офісі тощо. На рис. 1.3 показано приклад організації локальної комп’ютерної мережі.

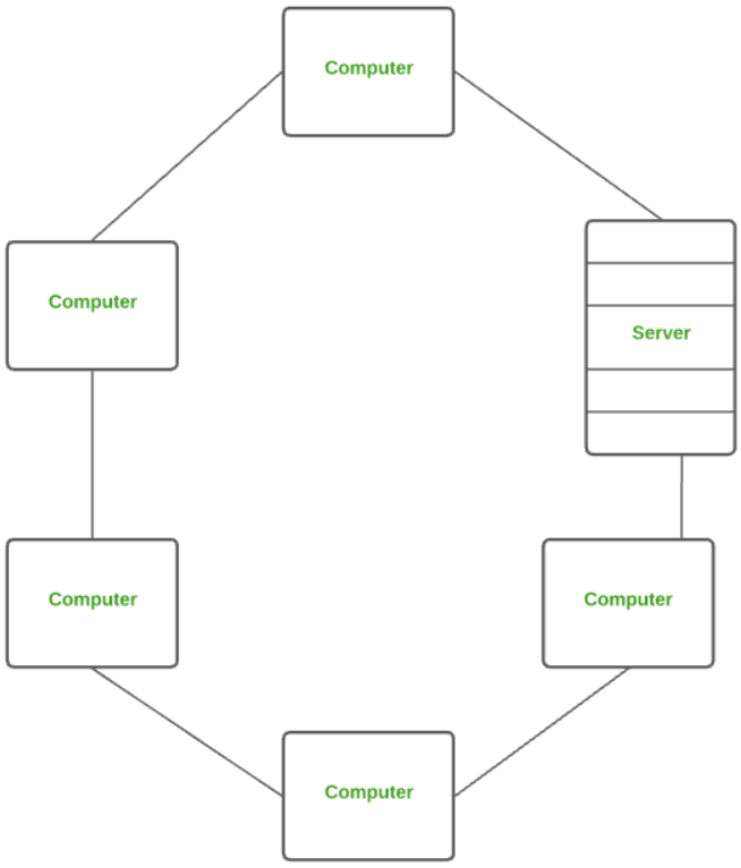

Рисунок 1.3 – Приклад локальної комп’ютерної мережі

Мережа типу CAN більша за розмірами від LAN, але менша за MAN. Це тип комп’ютерної мережі, яка зазвичай використовується в таких місцях, як школа чи коледж. Ця мережа охоплює обмежену географічну територію, тобто

поширюється на кілька будівель у межах кампусу. В основному вона використовує технологію Ethernet із радіусом дії від 1 км до 5 км. Швидкість передачі даних дуже висока з помірними витратами на обслуговування. Прикладами CAN є мережі, які охоплюють школи, коледжі, офісні будівлі. Приклад типу мережі CAN проілюстровано на рис. 1.4.

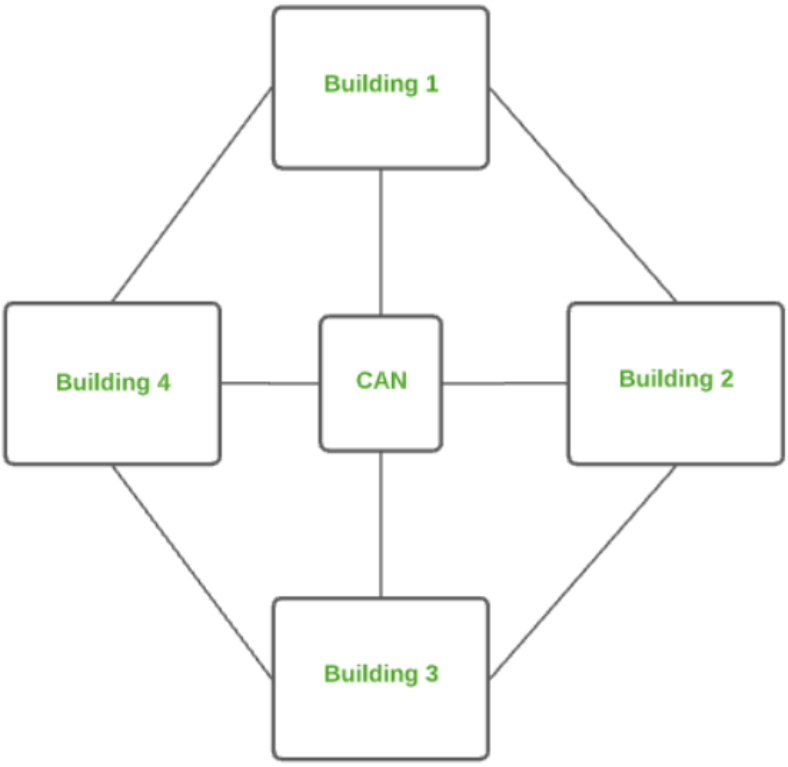

Рисунок 1.4 – Приклад організації мережі типу CAN

Тип мережі MAN більший за LAN, але менший за WAN. Комп'ютерна мережа розміру «метрополії» з'єднує комп'ютери на деякій відстані за допомогою спільного каналу зв'язку у місті, селищі чи окремій територіальній зоні. Ця мережа в основному використовує технології FDDI, CDDI та ATM із радіусом дії від 5 до 50 км. При такій організації мережі швидкість передачі даних є середньою. Цю мережу складно обслуговувати, і відповідно це пов'язано з високою вартістю. Прикладами MAN є мережеві зв'язки у великих містах, окремому великому масиві, великій території в кількох будівлях тощо. На рис. 1.5 показано приклад MAN мережі.

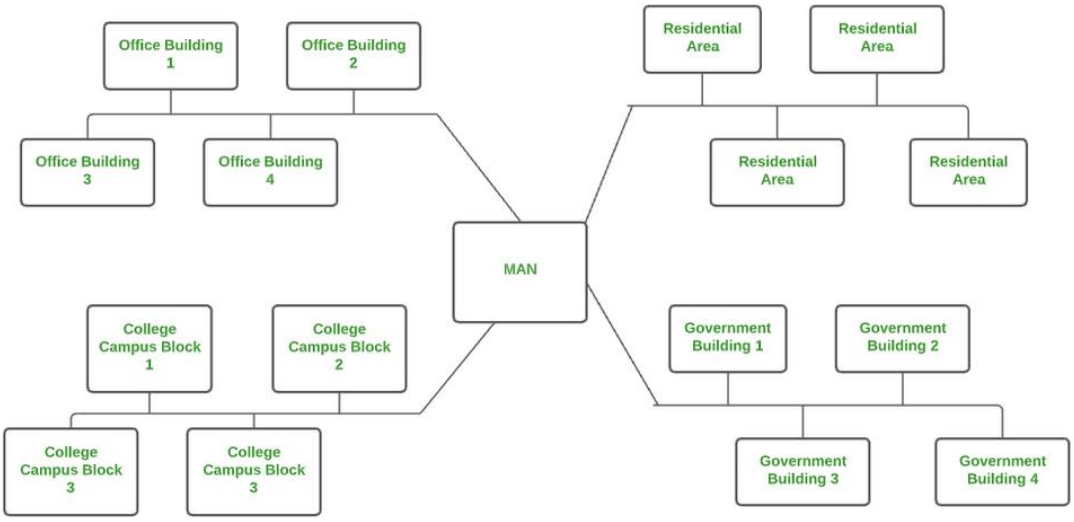

Рисунок 1.5 – Комп’ютерна мережа типу MAN

WAN є різновидом комп’ютерної мережі, що з’єднує комп’ютери на великій географічній відстані через спільний канал зв’язку. Мережа не обмежена одним місцем, а поширюється на багато місць. WAN також можна визначити як групу локальних мереж, які спілкуються одна з одною на відстані понад 50 км і може використовувати технологію виділеної лінії та комутованого доступу. Швидкість передачі даних при цьому дуже низька з дуже високими витрати на обслуговування. Найпоширенішим прикладом WAN є Інтернет. Приклад мережі типу WAN наведено на рис. 1.6.

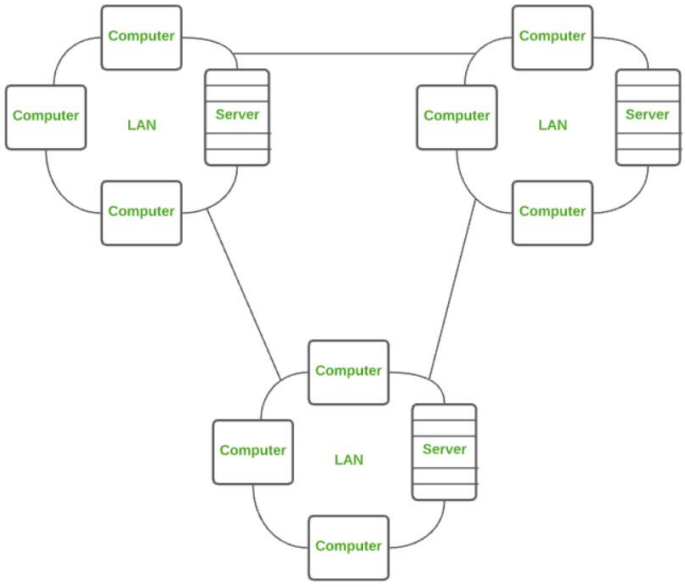

Рисунок 1.6 – Приклад організації WAN мережі

Порівняльна характеристика різних типів комп'ютерних мереж представлена у табл. 1.1.

Таблиця 1.1 – Порівняльна характеристика різних типів мереж

Параметри	PAN	LAN	CAN	MAN	WAN
Назва	Personal Area Network	Local Area Network	Campus Area Network	Metropolitan Area Network	Wide Area Network
Технологія	Bluetooth, IrDA, Zigbee	Ethernet, Wifi	Ethernet	FDDI, CDDi, ATM	Leased Line, Dial-Up
Розмір	1-100 м	До 2км	1 – 5 км	5-50 км	Понад 50 км
Швидкість передачі	Дуже висока	Дуже висока	Висока	Середня	Низька
Власник	Приватна	Приватна	Приватна	Приватна/ публічна	Приватна/ публічна
Обслуговування	Дуже просто	Просто	Середньо	Складно	Дуже складно
Вартість	Дуже низька	Низька	Середня	Висока	Дуже висока

Серед інших типів комп'ютерних мереж варто виділити насиупні:

– бездротова локальна мережа (WLAN);
– мережа зберігання даних (SAN);
– системна мережа (SAN);

– пасивна оптична локальна мережа (POLAN);
– корпоративна приватна мережа (EPN);
– віртуальна приватна мережа (VPN);
– домашня мережа (HAN).

Бездротова локальна мережа є таким видом комп’ютерної мережі, що працює як локальна мережа, але використовує бездротову мережеву технологію, наприклад, Wi-Fi. Ця мережа не дозволяє пристроям комунікувати через фізичні кабелі, як у локальній мережі, але дозволяє пристроям спілкуватися без проводів. На рис. 1.7 показано приклад організації мережі на основі WiFi технології.

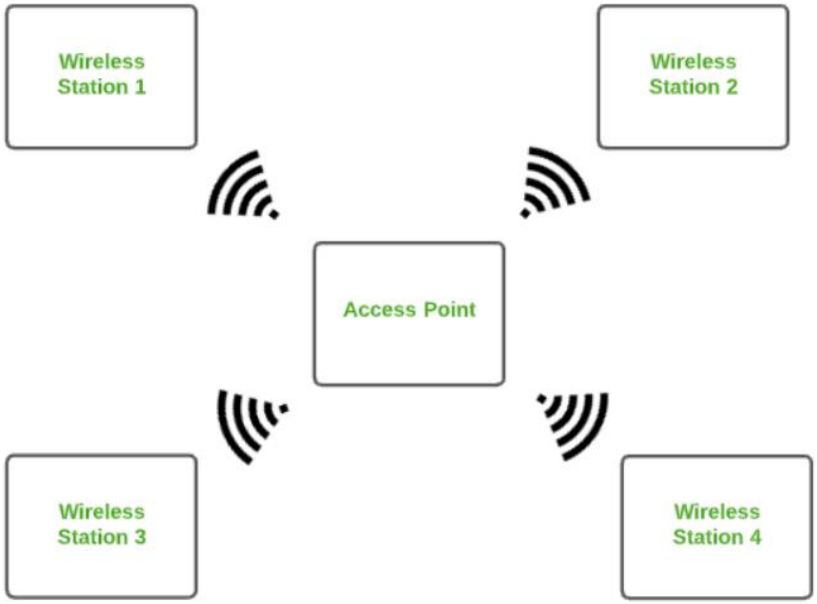

Рисунок 1.7 – Приклад організації комп’ютерної мережі на основі WiFi

Мережа зберігання даних – це тип високошвидкісної комп’ютерної мережі, яка з’єднує групи пристроїв зберігання даних із кількома серверами. Ця мережа не залежить від LAN або WAN. Натомість SAN переміщує ресурси зберігання з мережі до своєї потужної мережі. SAN забезпечує доступ до сховища даних на рівні блоків. Прикладами цього типу мережі є мережа дисків, до яких має доступ мережа серверів. На рис. 1.8 показано приклад організації мережі зберігання даних.

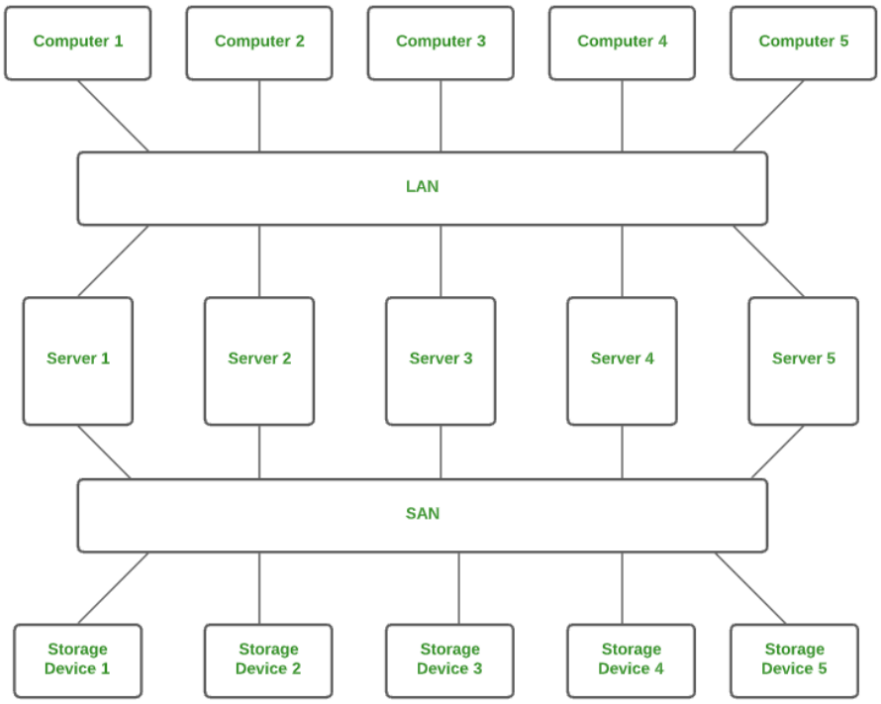

Рисунок 1.8 – Приклад мережі SAN

Системна мережа – це тип комп'ютерної мережі, яка об'єднує кластер високопродуктивних комп'ютерів. Це орієнтована на підключення мережа з високою пропускною здатністю. Системну мережу можна розглядати як тип локальної мережі, яка обробляє великі обсяги інформації у великих запитах. Ця мережа корисна для обробки програм, які потребують високої продуктивності мережі. Для приклад Microsoft SQL Server використовує системну мережу через адаптер віртуального інтерфейсу. На рис. 1.9 показано приклад системної мережі.

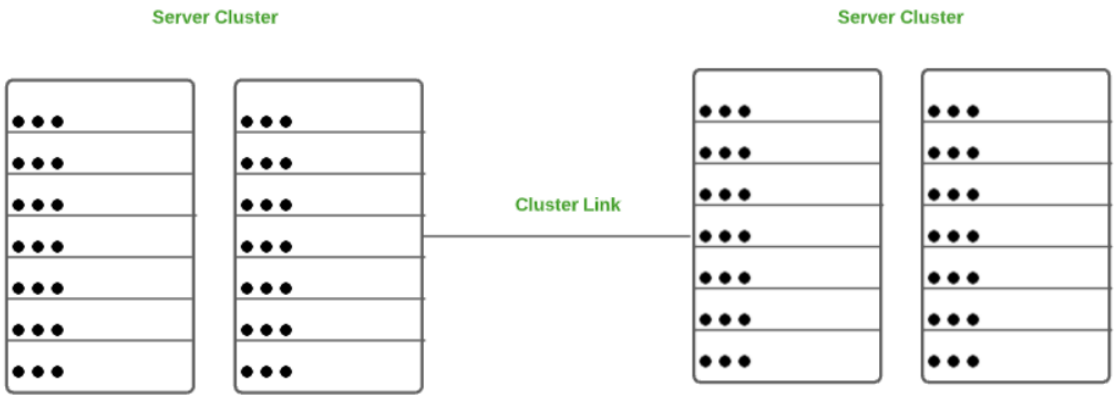

Рисунок 1.9 – Організація системної мережі

POLAN – це тип комп’ютерної мережі, яка є альтернативою локальній мережі. POLAN використовує оптичні розгалужувачі для поділу оптичного сигналу з однієї нитеи одномодового оптичного волокна на кілька сигналів для розподілу між користувачами та пристроями. Коротше кажучи, POLAN – це архітектура локальної мережі «точка-мультиточка», яка показана на рис. 1.10.

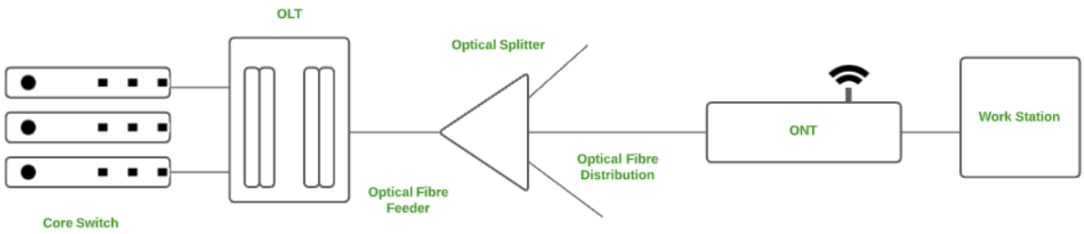

Рисунок 1.10 – Тип мережі POLAN

EPN – це тип комп’ютерної мережі, який переважно використовується компаніями, яким потрібне безпечне з’єднання в різних місцях для спільного використання комп’ютерних ресурсів (рис. 1.11).

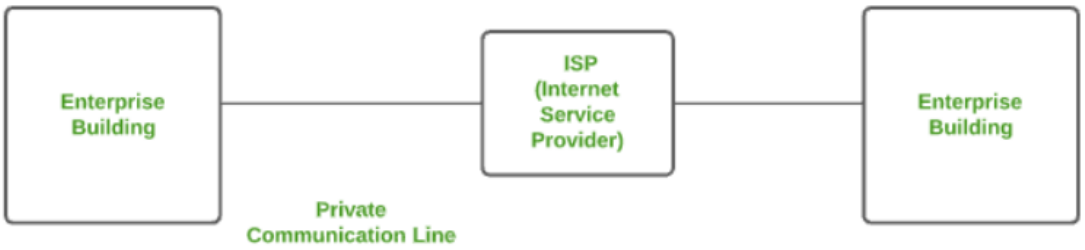

Рисунок 1.11 – Тип мережі EPN

VPN представляє собою тип комп’ютерної мережі, що дає змогу розширювати приватну мережу через Інтернет і надає сервіси для користувача щодо надсилання й одержання даних так, ніби він дійсно під’єднаний до мережі, хоча це може бути це не так.

Через віртуальне з’єднання «точка-точка» користувачі можуть віддалено отримувати доступ до приватної мережі. VPN захищає від зловмисних джерел

загроз, працюючи як середовище, яке забезпечує захищене мережеве з’єднання (рис. 1.12).

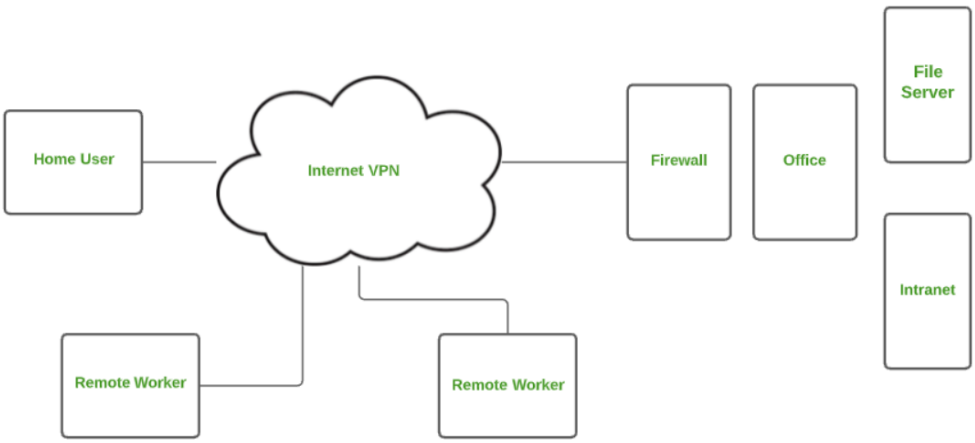

Рисунок 1.13 – Типова організація мережі VPN

У багатьох приватних будинках може бути більше, ніж один комп’ютер. Для з’єднання між цими комп’ютерами та іншими периферійними пристроями необхідно створити мережу, подібну до локальної мережі (LAN). Такий тип мережі, який дозволяє користувачеві з’єднувати кілька комп’ютерів та інших цифрових пристроїв удома, називається домашньою мережею (HAN).

HAN забезпечує спільний доступ до ресурсів, файлів і програм у мережі. Він підтримує як дротовий, так і бездротовий зв'язок. Приклад організації домашньої мережі показано на рис. 1.14.

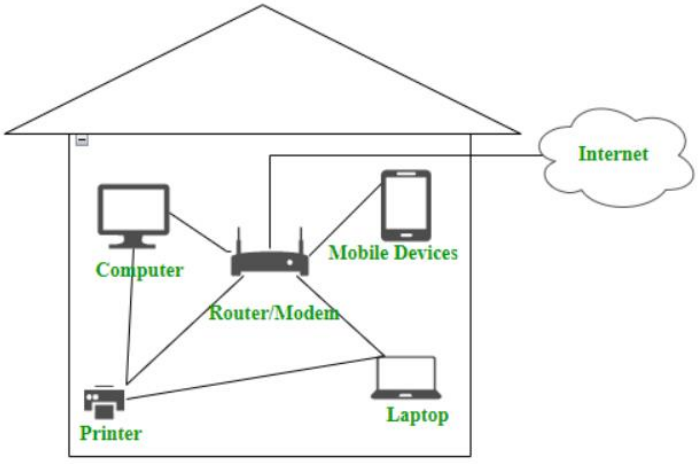

Рисунок 1.14 – Тип мережі HAN

1.2 Аналіз мережевих пристроїв та їх характеристик

Мережеві пристрої – це фізичні пристрої, які дозволяють обладнанню в комп'ютерній мережі обмінюватися даними та взаємодіяти одне з одним [1]. До мережевих пристроїв, які можуть використовуватися в комп'ютерній мережі належать:

- ретранслятор;
- концентратор;
- міст;
- комутатор;
- шлюз;
- маршрутизатор;
- мережева карта.

Маршрутизатор представляє собою мережевий пристрій, що забезпечує пересилання пакетів даних між комп'ютерними мережами. За допомогою маршрутизатора можна з'єднати одну або кілька мереж або підмереж з комутацією пакетів. Надсилаючи пакети даних на призначені IP-адреси, він керує трафіком між різними мережами та дає можливість декільком пристроям спільно використовувати Інтернет-з'єднання.

Припустимо, що користувач хоче виконати пошук за допомогою пошукового двигуна Google. Для цього у своєму веб-браузері він вводить відповідну адресу для доступу до сторінки пошуку. Запит користувача в цьому випадку є не що іншим, як потоком пакетів, які не просто відразу надходять на сервер Google, вони проходять через серію мережевих пристроїв, зокрема маршрутизатор. Роутер приймає ці пакети та пересилає за правильним маршрутом, і, отже, вони досягають сервера призначення.

Маршрутизатор має кілька інтерфейсів, за допомогою яких він може підключатися до кількох хост-систем. Маршрутизатори – це пристрої, які працюють на мережевому рівні моделі OSI, це найпоширеніші пристрої, що використовуються в мережі.

Маршрутизатор визначає майбутній шлях пакета, перевіряючи IP-адресу призначення в заголовку та порівнюючи її з базою даних маршрутизації. У списку таблиць маршрутизації описано, як надсилати дані в певне розташування мережі. Вони використовують набір правил для визначення найбільш ефективного способу передачі даних на вказану IP-адресу.

Щоб забезпечити зв'язок між іншими пристроями та Інтернетом, маршрутизатори використовують модем, наприклад кабельний, оптоволоконний або DSL.

Більшість маршрутизаторів мають багато портів, які можуть підключати до Інтернету різні пристрої одночасно. Щоб вирішити, куди доставляти дані та звідки надходить трафік, потрібні таблиці маршрутизації.

Таблиця маршрутизації в першу чергу визначає шлях маршрутизатора за замовчуванням. У результаті він може не визначити оптимальний шлях для пересилання даних для певного пакету. Наприклад, офісний маршрутизатор спрямовує всі мережі до свого інтернет-провайдера через єдиний канал за замовчуванням.

Статичні та динамічні таблиці в маршрутизаторі бувають двох різновидів. Динамічні таблиці маршрутизації автоматично оновлюються динамічними маршрутизаторами на основі мережевої активності, тоді як статичні таблиці маршрутизації налаштовуються вручну.

Типи маршрутизаторів.

Існує кілька типів маршрутизаторів.

Широкосмугові маршрутизатори – це один із важливих типів маршрутизаторів. Він використовується для виконання різних типів задач:

– для підключення комп'ютерів
– для доступу до мережі Інтернет.

Безпровідні маршрутизатори – використовуються для створення бездротового сигналу в офісі чи вдома.

Маршрутизатори без безпровідної технології передачі даних –дротовий маршрутизатор використовується для підключення кількох пристроїв за

допомогою кабелю Ethernet. Він приймає дані передачі від модему та розподіляє їх у подальшу мережу, він широко використовується в школах і невеликих офісах.

На рис. 1.15 показано приклад застосування пристроїв маршрутизації у типовій комп'ютерній мережі підприємства.

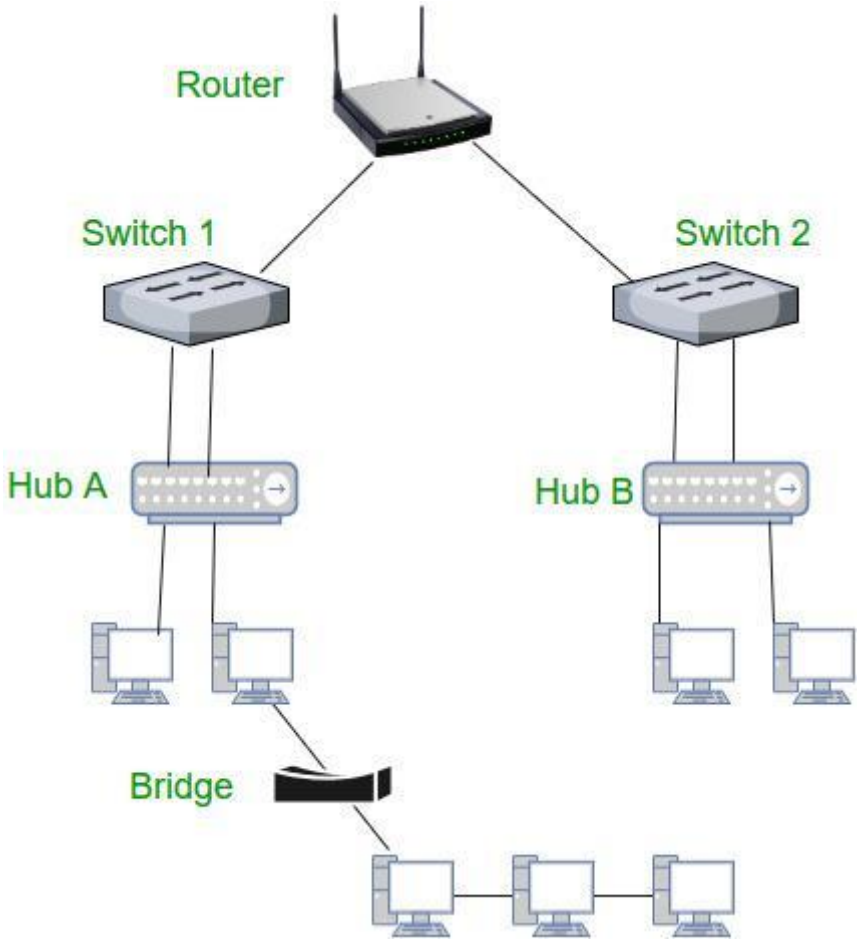

Рисунок 1.15 – Мережеві пристрої типової офісної комп'ютерної мережі

Кінцеві маршрутизатори – розташовуються на краях мережі, зазвичай підключеної до Інтернет-провайдера, і розподіляють пакети між мультипакетами.

Основні маршрутизатори – розподіляють пакети в одній мережі. Основне завдання - це передача великих даних.

Віртуальний маршрутизатор – реалізується за допомогою програмного забезпечення на віртуальній машині, вони більш гнучкі та масштабовані.

Портативні маршрутизатори – використовуються для створення приватного Wi-Fi і, отже, призначені для легкого перенесення.

Перевагами застосування комп’ютерних мереж є те, що :

– файли зберігаються в базі даних центрального сховища, яка допомагає легко отримати доступ і доступна кожному;

– одне з’єднання можна спрямувати для з’єднання кількох комп’ютерних пристроїв;

– файли та дані можна легко обмінювати між кількома пристроями, що полегшує спілкування між організацією;

– комп’ютерна мережа забезпечує додаткову безпеку та захист інформації в системі;

Недоліки комп'ютерної мережі:

– віруси та зловмисне програмне забезпечення можуть пошкодити всі вузли мережі;

– висока вартість налаштування – початкове налаштування комп’ютерної мережі є дорогим, оскільки воно складається з великої кількості проводів і кабелів разом із пристроєм;

– втрата інформації – у разі системного збою це може призвести до втрати деяких даних;

– управління мережею є певною мірою складним для звичайного користувача, воно вимагає навчання для правильного використання.

РОЗДІЛ 2 ПРОЕКТУВАННЯ ТА НАЛАШТУВАННЯ МАРШРУТИЗАТОРА НА RASPBERRY PI 4 З OPEN WRT

2.1 Функції маршрутизаторів у комп'ютерної мережі

Роутер виконує наступні основні функції:

Пересилання пакетів – маршрутизатор отримує пакети зі своїх вхідних портів, перевіряє їх заголовок, виконує деякі основні функції, наприклад, перевірку контрольної суми, а потім переглядає таблицю маршрутизації, щоб знайти відповідний вихідний порт для пересилання пакетів, і надсилає пакети на нього.

Маршрутизація – це процес, на основі якого маршрутизатор визначає найкращий шлях для досягнення пакетом місця призначення. Він підтримує таблицю маршрутизації, створену за допомогою різних алгоритмів лише маршрутизатором.

Трансляція мережевих адрес – маршрутизатори використовують NAT для трансляції між різними діапазонами IP-адрес. Це дозволяє пристроям у приватній мережі отримувати доступ до Інтернету за допомогою єдиної публічної IP-адреси.

Безпека – маршрутизатори можуть бути налаштовані з брандмауерам та іншими функціями безпеки для захисту мережі від несанкціонованого доступу, зловмисних програм та інших загроз.

Якість обслуговування (QoS) – маршрутизатори можуть визначати пріоритети мережевого трафіку на основі типу даних, що передаються. Це гарантує, що критично важливе ПЗ і відповідні служби одержать необхідну пропускну здатність і на них не впливає трафік з нижчим пріоритетом.

Підключення до віртуальної приватної мережі (VPN) – маршрутизатори можна налаштувати так, щоб віддалені користувачі могли безпечно підключатися до мережі за допомогою VPN.

Керування смугою пропускання – маршрутизатори можна використовувати для керування смугою пропускання мережі, контролюючи обсяг даних, які дозволено передавати через мережу. Це може запобігти перевантаженню мережі та гарантувати, що критичні програми та служби отримають достатню пропускну здатність.

Моніторинг і діагностика – маршрутизатори можна налаштувати для моніторингу мережевого трафіку та надання діагностичної інформації у разі збоїв у мережі чи інших проблем. Це дозволяє адміністраторам мережі швидко виявляти та вирішувати проблеми.

2.2 Архітектура маршрутизатора

Типовий маршрутизатор складається з таких компонентів:

Вхідний порт – це інтерфейс, за допомогою якого пакети надходять до маршрутизатора. Він виконує кілька ключових функцій, зокрема, завершення фізичного з’єднання на маршрутизаторі, це робиться крайньою лівою частиною на діаграмі (рис. 2.1), а середня частина виконує роботу взаємодіючи з канальним рівнем, як декапсуляція, в останній частині вхідного порту шукається таблиця пересилання та використовується для визначення відповідного вихідного порту на основі адреси призначення.

Комутаційна структура – це серце маршрутизатора, воно з’єднує вхідні порти з вихідними портами. Це свого роду мережа всередині мережевого пристрою. Комутаційна структура може бути реалізована декількома способами.

Перемикання через пам'ять – у цьому випадку є процесор, який копіює пакет із вхідних портів і надсилає його на відповідний вихідний порт. Він працює як традиційний центральний процесор із портами введення та виведення, які діють як пристрої введення та виведення.

Перемикання через шину – у цій реалізації є шина, яка з'єднує всі вхідні порти з усіма вихідними портами. Отримавши пакет і визначивши, до якого вихідного порту його потрібно доставити, вхідний порт поміщає в пакет певний маркер і передає його на шину. Усі вихідні порти можуть бачити пакети, але вони будуть доставлені до вихідного порту, токен якого було вставлено, маркер потім видаляється цим вихідним портом і пакет пересилається.

Комутація через мережу взаємозв'язку – це більш складна мережа, тут замість однієї шини використовується шина 2N для з'єднання n вхідних портів з n вихідними портами.

Вихідний порт – це сегмент, з якого пакети передаються з маршрутизатора. Вихідний порт переглядає свої буфери черги (коли кілька пакетів потрібно передати через той самий вихідний порт, формуються буфери черги) і приймаються пакети, виконуються функції канального рівня і, нарешті, передаються пакети вихідному каналу.

Процесор маршрутизації – виконує протоколи маршрутизації та працює як традиційний процесор. Він використовує різні алгоритми маршрутизації, наприклад: алгоритм стану зв'язку, алгоритм вектора відстані тощо. Це робиться з метою підготовки таблиці пересилання, яка переглядається для визначення маршруту та вихідного порту.

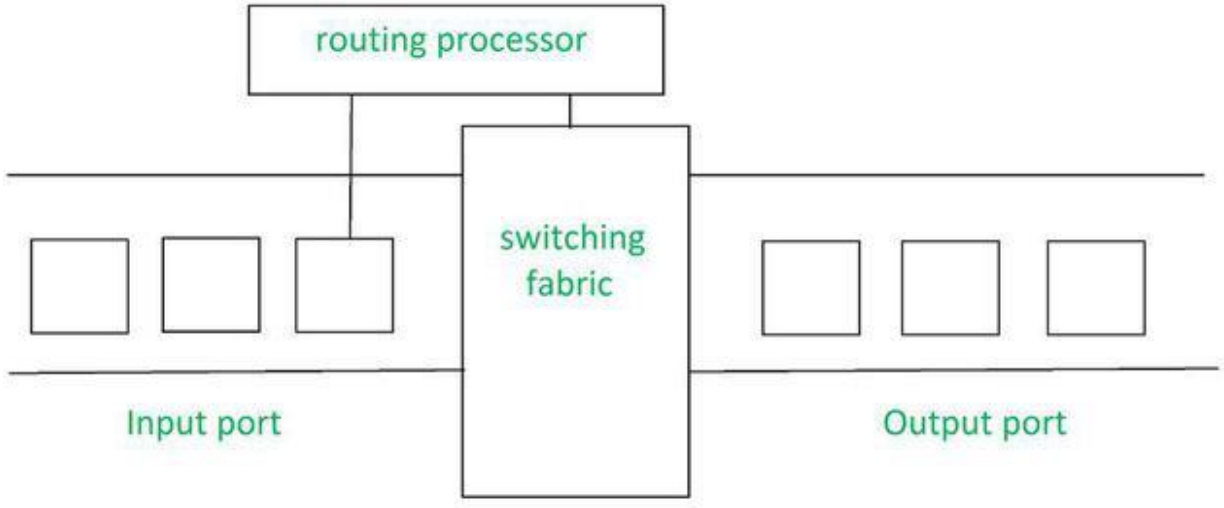

Рисунок 2.1 – Концептуальна архітектура маршрутизатора

Проблеми безпеки в маршрутизаторі.

Існує кілька проблем, з якими стикаються користувачі маршрутизаторів, через які ззовні може здійснюватися несанкціонований доступ. Серед важливих проблем безпеки в маршрутизаторі можна виділити наступні:

1. Використання вразливостей.

Прошивка автоматично встановлюється на всіх апаратних маршрутизаторах, щоб забезпечити працездатність маршрутизатора. Як і будь-яка інша програма, прошивка маршрутизатора часто має недоліки, які хакери можуть використати проти пристрою. Виробники маршрутизаторів, зазвичай, випускають оновлення, щоб виправити ці недоліки. Як наслідок, мікропрограму маршрутизатора необхідно оновлювати часто. Зловмисники мають можливість відстежувати трафік на невиправлених маршрутизаторах і використовувати їх як частину ботнету.

2. DDoS-атаки.

Розподілені атаки типу «відмова в обслуговуванні» (DDoS) на мережеву інфраструктуру часто спрямовані на великі та малі організації. Збої в мережі можуть бути спричинені DDoS-атаками на мережевому рівні, які здатні перевантажити маршрутизатори або вивести їх з ладу. Використання Cloudflare Magic Transit є одним із способів захисту мереж і маршрутизаторів від DDoS-атак такого характеру.

3. Облікові дані адміністратора.

Для виконання завдань адміністрування до кожного маршрутизатора входить набір облікових даних адміністратора. Значення за замовчуванням для цих облікових даних:

– «admin» - для імені користувача
– «admin» - для пароля.

Ім’я користувача і пароль потрібно негайно змінити на більш надійні, оскільки, якщо цього не зробити, зловмисники можуть використовувати їх для віддаленого захоплення маршрутизатора. Вони знають типові значення за замовчуванням для цих облікових даних.

2.3 Переваги та недоліки маршрутизаторів

До переваг використання роутера належать:

– простота підключення;
– забезпечення безпеки;
– використання NAT;
– динамічна маршрутизація4
– фільтрація пакетів.

Просте підключення – спільний доступ до одного мережевого підключення між багатьма машинами є головною перевагою маршрутизатора. Це дозволяє багатьом користувачам підключатися до Інтернету, підвищуючи загальну продуктивність праці. Крім того, маршрутизатори мають з'єднання між різними носіями та мережевими конструкціями.

Безпека – безсумнівно, встановлення маршрутизатора є першим кроком у захисті підключення до мережі. Оскільки використання модему для прямого підключення до Інтернету наражає комп'ютер на низку ризиків безпеки. Щоб середовище було певною мірою безпечним, маршрутизатори можна використовувати як посередника між двома мережами. Хоча це не заміна брандмауеру чи антивірусу.

Використання NAT – маршрутизатори використовують трансляцію мережевих адрес (NAT), щоб зіставити кілька приватних IP-адрес в одну публічну IP-адресу. Це забезпечує краще підключення до Інтернету та потік інформації між усіма пристроями, підключеними до мережі.

Підтримка динамічної маршрутизації: маршрутизатор використовує стратегії динамічної маршрутизації, щоб забезпечити мережеву комунікацію. Оптимальний шлях роботи в Інтернеті вибирається за допомогою динамічної маршрутизації. Крім того, це створює колізії та широкомовні домени. Загалом це може зменшити мережевий трафік.

Фільтрування пакетів: перемикання між пакетами та фільтрація пакетів є ще двома службами маршрутизатора. Набір правил фільтрації використовується

маршрутизаторами для фільтрації мережі, тобто виявляються пакети, які дозволені у мережі і відповідно заборонені.

Серед недоліків маршрутизаторів можна вказати наступні:

– недостатня швидкість функціонування;
– висока вартість;
– складність та необхідність конфігурації;
– необхідність оновлення конфігурації;
– можливі проблеми забезпечення якості передачі даних
– дефіцит пропускної здатності;

Маршрутизатори є повільними пристроями, які аналізують кілька рівнів інформації, від фізичного до мережевого, що уповільнює з'єднання. З такою ж проблемою можна зіткнутися, коли до цих мережевих пристроїв підключено кілька пристроїв, що спричиняє «очікування з'єднання».

Висока вартість – маршрутизатори дорожчі, ніж деякі інші інструменти для системного адміністрування. Це включає в себе безпеку, розширення та координаційний центр. Як наслідок, маршрутизатори, зазвичай, не є найкращим варіантом вирішення проблем.

Необхідність конфігурації – маршрутизатор має бути належним чином налаштований для забезпечення надійності роботи. Загалом, чим складніше передбачуване використання, тим більше налаштування конфігурацій потрібно. При цьому може знадобитися професійне встановлення, яке може збільшити витрати на придбання маршрутизатора.

Проблеми з якістю – часові переходи не завжди точні. Незважаючи на це, деякі сучасні пристрої використовують діапазон 2,4 ГГц, який часто деактивується. Такі розділення часто можливі для тих, хто живе в багатоквартирних будинках.

Дефіцит пропускної здатності – методи динамічної маршрутизації, які використовуються маршрутизаторами для підтримки з'єднань, як правило, спричиняють накладні витрати на мережу, споживаючи значну пропускну здатність. Це призводить до дефіциту пропускної здатності, що значно сповільнює інтернет-з'єднання між підключеними пристроями.

Існує кілька застосувань маршрутизаторів, оскільки в даний час вони широко використовуються в більшості мережевих комунікацій для кращого зв’язку.

Апаратне обладнання, таке як сервери BSC, MGW, IN, SGSN та інших віддалених мереж, підключається до них через маршрутизатори. Роутер використовується як при дротовому, так і при бездротовому зв’язку, оскільки підтримує високу швидкість передачі даних завдяки використанню з’єднань STM для підключення.

Маршрутизатори часто використовуються постачальниками послуг Інтернету для передачі даних, таких як аудіо, відео, зображення та електронна пошта, з одного місця в інше. Крім того, вони можуть передавати дані глобально, використовуючи IP-адресу призначення.

Маршрутизатори забезпечують контроль доступу, тобто їх можна налаштувати так, щоб одні користувачі мали доступ до всіх даних, а інші – лише до їх частини.

Маршрутизатор може розпізнавати інші роутери в мережі та динамічно вирішувати, куди доставляти всі мережеві повідомлення через протокол маршрутизації. Існує кілька протоколів, деякі з яких наведено нижче.

Open Shortest Path First: коли пакети подорожують кількома мережами, він використовується для визначення оптимального шляху, яким вони повинні пройти, щоб прибути до місця призначення.

Протокол Border Gateway Protocol (BGP): полегшує обмін інформацією між периферійними маршрутизаторами для контролю маршрутизації пакетів Інтернету. Для маршрутизаторів він забезпечує стабільність мережі. Він може легко переключитися на інше мережеве підключення для передачі пакетів.

Протокол внутрішньої маршрутизації шлюзу (IGRP) – описує протокол для обміну даними маршрутизації між шлюзами в окремих мережах. Інформацію про маршрутизацію потім можуть використовувати інші мережеві протоколи, щоб вирішити, як маршрутизувати пакети даних.

Enhanced Interior Gateway Routing Protocol (EIGRP) – протокол, який вимагає від маршрутизатора керувати маршрутами своїх сусідів, якщо він не

може знайти шлях до пункту призначення в таблицях маршрутизації. Потім сусіди пересилають запит іншим сусідам, доки маршрутизатор не знайде шлях.

Протокол зовнішнього шлюзу (EGP) – часто використовується для передачі даних таблиці маршрутизації між хостами Інтернету

2.4 Технічні характеристики Raspberry PI, як маршрутизатора

У кваліфікаційній роботі запропоновано реалізувати маршрутизатор на базі Raspberry PI 4, що працює через Power over Ethernet з використанням прошивки OpenWRT. На рис. 2.2 показано структуру, яку необхідно реалізувати із використанням Raspberry PI 4.

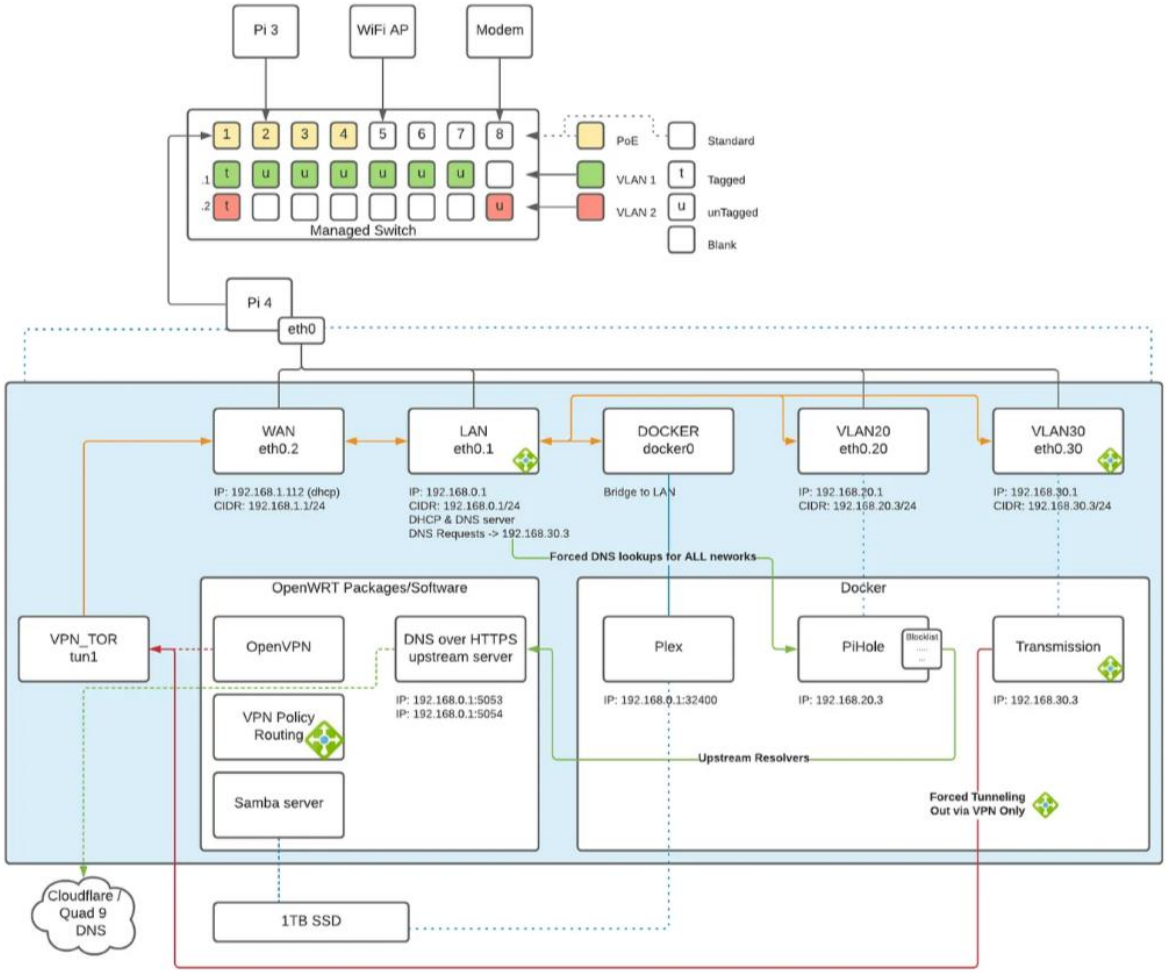

Рисунок 2.2 – Інфраструктура на основі маршрутизатора Raspberry PI 4

Як видно з рис. 2.2, при організації маршрутизатора необхідно забезпечити:

– використання єдиного гігабітного порту локальної мережі Ethernet для керування/маршрутизації трафіку;

– підключення до керованого гігабітного комутатора;

– запуск Docker у мережах OpenWRT VLAN;

– сервер Plex із підключеним диском SSD;

– блокування реклами з використанням PiHole;

– вихідні сервери DNS через HTTPS, налаштовані для PiHole.

Апаратні пристрої, які входять в інфраструктуру включають:

– Raspberry PI 4 – маршрутизатор з PoE і прошивкою Open WRT, який підключається до першого PoE керованого комутатора;

– Raspberry PI 3 – мімкомп'ютер, який підключений до третього PoE порта керованого комутатора;

– NetGear GS108PE – 8-ми портовий керований комутатор;

– TL-WA1201 – точка доступу від TP-Link, яка підключається до 5-го порта комутатора, що не є PoE портом;

– Модем – підключається як резервний пристрій доступу до мережі Internet через порт 8.

При розробці такої інфраструктури передбачено налаштування двох VLAN:

– VLAN1 – призначається на порти 1-7 керованого комутатора;

– VLAN2 – призначено на порт 1 і 8 керованого комутатора.

Окрім цього, необхідно забезпечити авторизований доступ до медіа файлів, які зберігаються на SD-карті, що вставлена у маршрутизатор на базі Raspberry PI 4.

Програмне забезпечення для блокування реклами PiHole, медіасервер Plex та торент-клієнт Transmission у вигляді Docker-контейнерів необхідно також розгорнути для функціонування на маршрутизаторі.

Для реалізації визначених задач необхідно провести аналіз технічних характеристик Raspberry PI 4.

2.5 Особливості і характеристики Raspberry PI 4

Raspberry Pi 4 належить до відносно нової лінійки мінікомп’ютерів Raspberry Pi і характеризується підвищеною швидкістю роботи процесора, поліпшеною продуктивністю модуля мультимедіа, збільшеним об’ємом і продуктивністю оперативної пам'яті та оновленим мережевим модулем.

До ключових характеристик RPI 4 Model B як пристрою маршрутизації пакетів у комп’ютерній мережі відноситься:

– 64-розрядний з чотирма ядрами процесор високої продуктивності;

– 4 Гб оперативної пам'яті,

– модуль безпровідної передачі даних з підтримкою двохдіапазонів роботи 2,4 і 5,0 ГГц

– наявність Gigabit Ethernet,

– наявність портів USB 3.0 (3 шт.) і PoE.

На рис. 2.3 показано зовнішній вигляд Raspberry PI 4.

Рисунок 2.3 – Raspberry PI 4

Оскільки, модель мінікомп’ютера, яка показана на рис. 2.3, володіє доволі потужними технічними характеристиками та здатна виконувати багато різноманітних функцій, то доцільним є встановлення зовнішнього охолодження PoE HAT.

Зовнішній вигляді майбутнього маршрутизатора на базі RPI 4 із встановленою системою повітряного охолодження показано на рис. 2.4.

Рисунок 2.4 – Маршрутизатор на базі Raspberry PI 4

Наступні дії, які необхідно виконати для застосування Raspberry PI як маршрутизатора полягають у проведенні інсталяції та базових налаштувань Open WRT.

2.6 Встановлення OpenWRT на Raspberry PI 4

Перед тим, як перейти до безпосереднього встановлення прошивки Open WRT на Raspberry PI потрібно з офіційного сайту завантажити підтримувану версію ядра маршрутизатора. У роботі пропонуєтсься скористаися версією bcm2711, як показано на рис. 2.5.

Image for your Device	sha256sum	File Size	Date
rpi-4-ext4-factory.img.gz	29bd00edf60f1b99a1b4a955eb352595fdd1ffe0c1239e92ab2c2512aafe38ad	14026.1 KB	Sun Feb 21 11:49:18 2021
rpi-4-ext4-sysupgrade.img.gz	764b6ed4fb092bb26252567a19084be6a4e36843303332e165f57daa0c8bc2e7	14026.4 KB	Sun Feb 21 11:49:18 2021
rpi-4-squashfs-factory.img.gz	ded4dea88c02fd4f1957eda9f700e89a23f1412e81ed434e1ef1e83620f441de	12675.8 KB	Sun Feb 21 11:49:17 2021
rpi-4-squashfs-sysupgrade.img.gz	95221e403e34e9c1b90fa73e14780447756e65a602818f2e6bfb467f7e965da9	12676.2 KB	Sun Feb 21 11:49:17 2021

Рисунок 2.5 – Завантаження прошивки bcm2711

Після того, як потрібний образ Open WRT завантажено на персональний комп'ютер необхідно за допомогою програми Raspberry Pi Imager або balenaEtcher виконати його запис на SD-карту. Процедура запису образу є доволі простою і тому не потребує особливої уваги та опису.

Враховуючи те, що файлова система не розширюється автоматично, тому використано утиліту GParted на Linux Mint, щоб розширити її (рис. 2.6).

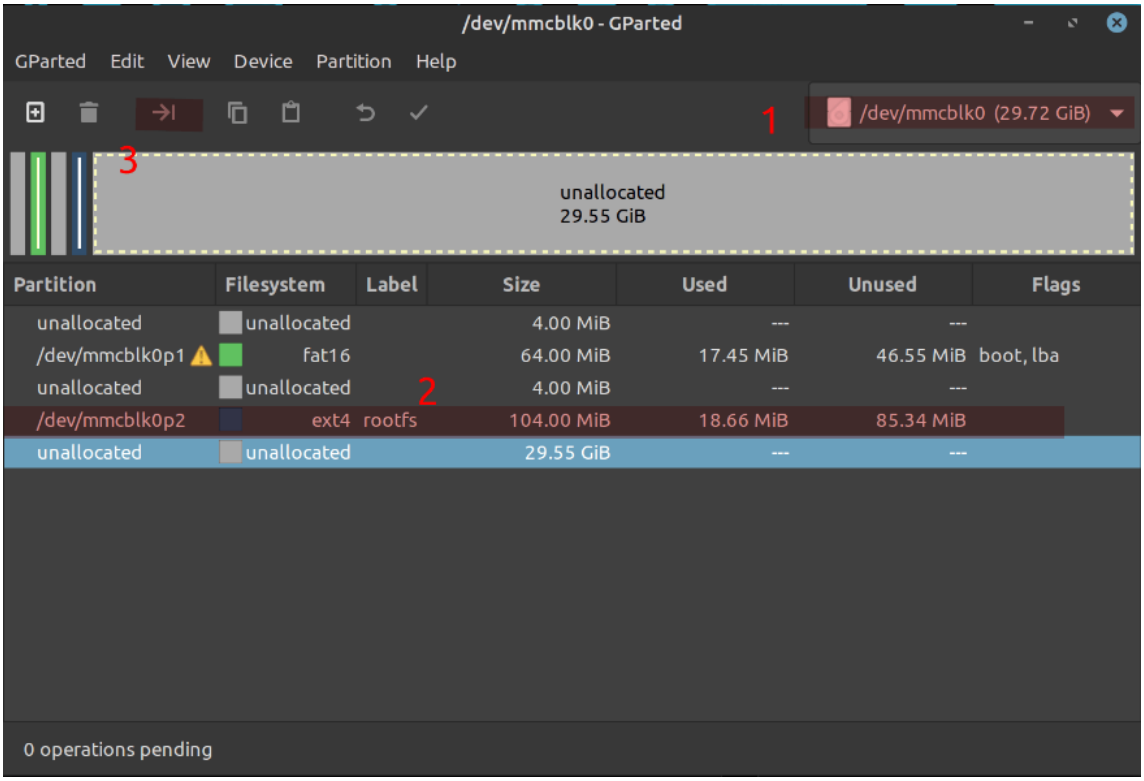

Рисунок 2.6 – Головне вікно утиліти для розширення файлової системи

GParted – це безкоштовний менеджер розділів, який дозволяє змінювати розмір, копіювати та переміщувати розділи без втрати даних. Найкращий спосіб отримати доступ до всіх функцій програми GParted – це використати завантажувальний образ GParted Live. GParted Live дозволяє використовувати GParted у GNU/Linux, а також в інших операційних системах, таких як Windows або Mac OS X.

Для того, щоб збільшити розмір диску під файлову систему необхідно повзунок, який показано на рис. 2.7 перетягнути у крайнє праве положення.

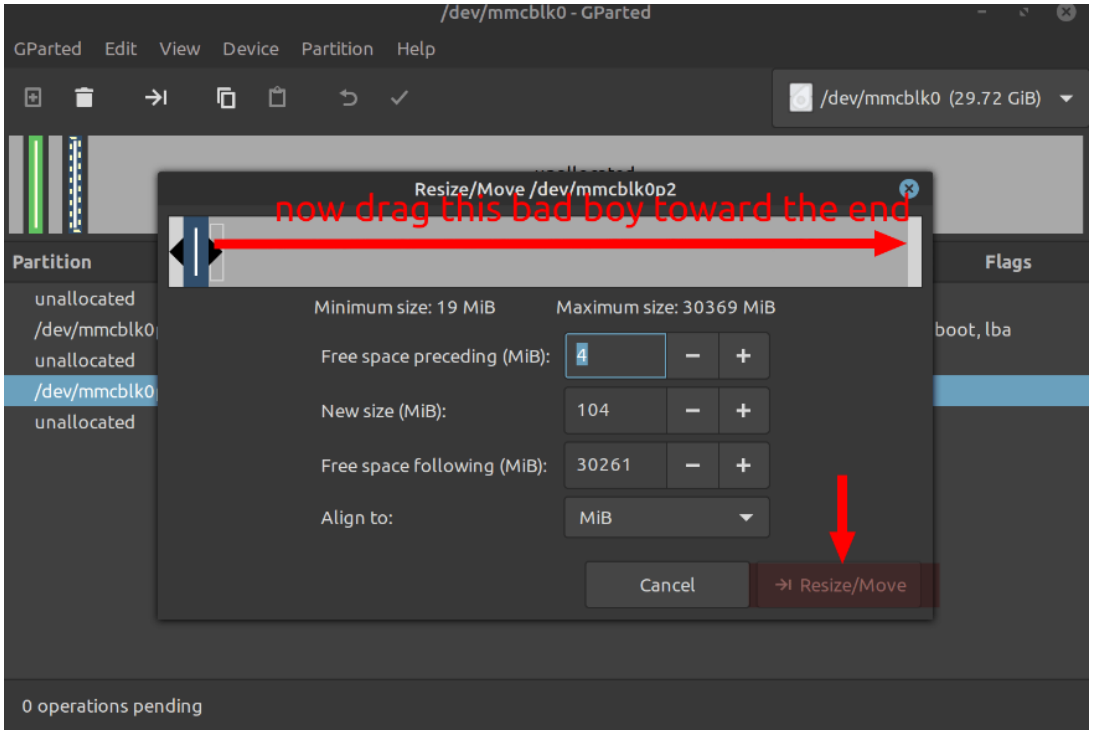

Рисунок 2.7 – Збільшення розміру під файлову систему

Після того, як виділено необхідний розмір під образ Open WRT необхідно зберегти усі внесені до цього зміни, як показано на рис. 2.8.

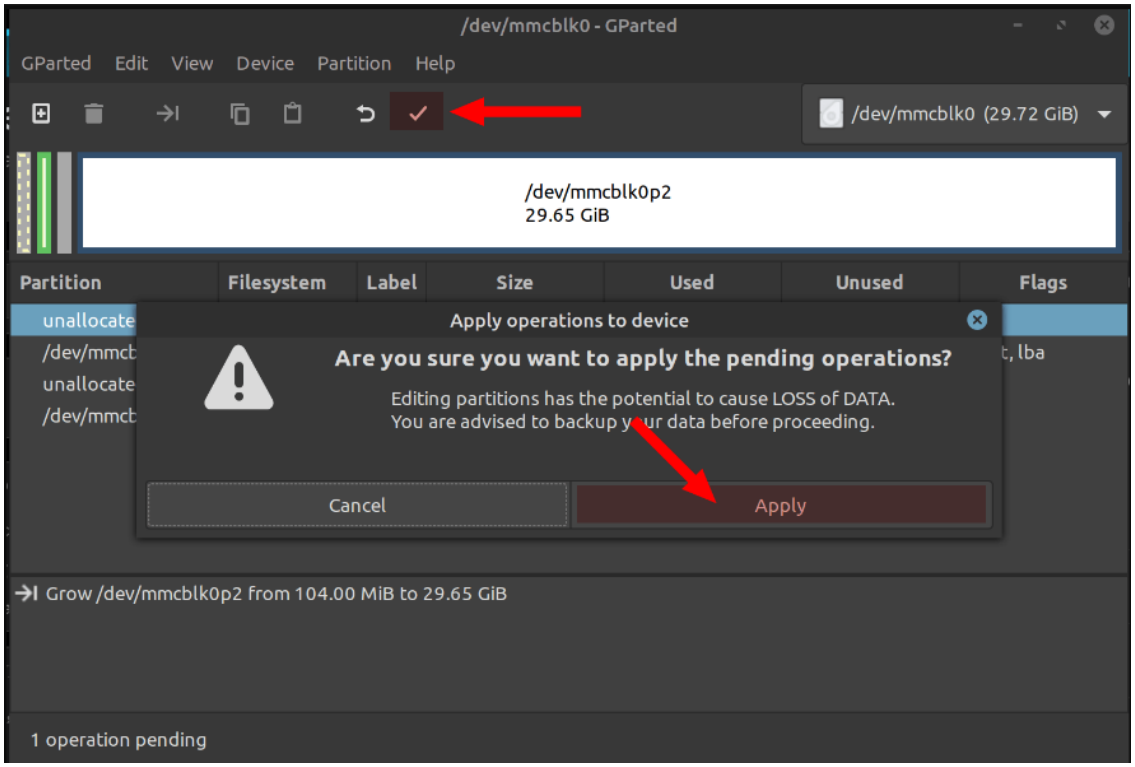

Рисунок 2.8 – Збереження і застосування внесених змін щодо розміру файлової системи

Після проведених процедур, SD-карту потрібно вставити у відповідний порт Pi4 і налаштовувати базові параметри OpenWRT.

При увімкненні Raspberry PI 4 за замовчуванням використовується IP-адреса 192.168.1.1. Для підключення до мінікомп'ютера можна скористатися зовнішнім обчислювальним пристроєм для підключення до його вбудованої мережної карти.

Наступний крок полягає у призначенні статичної IP-адреси в діапазоні 192.168.1.0/24, наприклад 192.168. 1.10 з маскою мережі 255.255.255.0. Для доступу до Raspberry PI через SSH використовується команда:

«ssh root@192.168.1.1» із порожнім паролем.

Якщо використовується Windows 10, то для підключення через SSH, можна застосовувати PowerShell, який тепер підтримує це нативно і не потрібно використовувати Putty/Kitty.

```
ip a

# Sample command output:
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group 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
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master br-lan state UP group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 ff:ff:ff:ff:ff:ff
5: br-lan: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/24 brd 192.168.1.255 scope global br-lan
       valid_lft forever preferred_lft forever
    inet6 fe80::dea6:32ff:feac:78c9/64 scope link
       valid_lft forever preferred_lft forever
6: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
```

Рисунок 2.9 – Результат успішного налаштування IP-адреси RPI 4

Згідно, схеми інфраструктури, яка показана на рис. 2.2 потрібно забезпечити створення двох VLAN. У наступному пункті даного розділу проводиться базове налаштування VLAN.

2.7 Налаштування VLAN

Найпростіший спосіб налаштувати інтерфейси VLAN з мітками – це редагування файлу /etc/config/network. Вносити у нього зміни можна через сеанс SSH на Raspberry Pi або вставивши SD-карту в комп'ютер. На рис. 2.10 показано які повинні бути налаштування конфігураційного файлу.

```
config interface 'loopback'
        option ifname 'lo'
        option proto 'static'
        option ipaddr '127.0.0.1'
        option netmask '255.0.0.0'

config interface 'lan'
        option ifname 'eth0.1'
        option proto 'static'
        option netmask '255.255.255.0'
        option ipaddr '192.168.0.1'

config interface 'wan'
        option ifname 'eth0.2'
        option proto 'dhcp'
```

Рисунок 2.10 – Файл конфігурації VLAN

Як видно з рис. 2.10, створюються два віртуальні інтерфейси: «lan» (з тегом VLAN 1) і «wan» (з тегом VLAN 2).

Очевидно, що у конкретних випадках потрібно буде відредагувати IP-адресу інтерфейсу «LAN» відповідно до параметрів локальної мережі.

На даному етапі можна підключити Raspberry Pi до порту 5 комутатора, підключити до комутатора решту пристроїв локальної мережі через порт 1, 2 або 3, підключити модем до порту 4 і мережева частина конфігурації буде завершена.

При існуючій локальній комп’ютерній мережі можливо доведеться переналаштувати інтерфейс «Wan» для використання «pppoe» або іншого протоколу, залежно від того, яке підключення використовується інтернет-провайдером. Завершення конфігарції VLANів можна за допомогою веб-інтерфейсу OpenWRT.

2.8 Налаштування керованого комутатора 3 рівня

В якості керованого комутатора застосовується NetGear GS108PE. Його налаштування, як було зазначено раніше повинні відповідати схемі, яка показана на рис. 2.11.

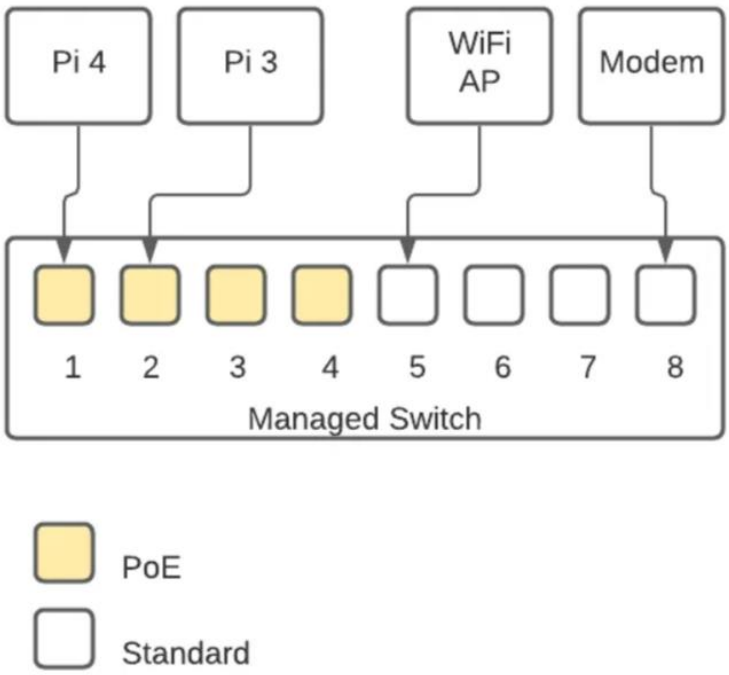

Рисунок 2.11 – Схема підключення до портів NetGear GS108PE

При налаштуванні параметрів комутатора можна скористатися веб-інтерфейсом, перейшовши у розділ VLAN, як продемонстровано на рис. 2.12. У даному випадку налаштовується два VLAN:

– VLAN 1 – порти 1-7;
– VLAN 2 – порти 1 та 8.

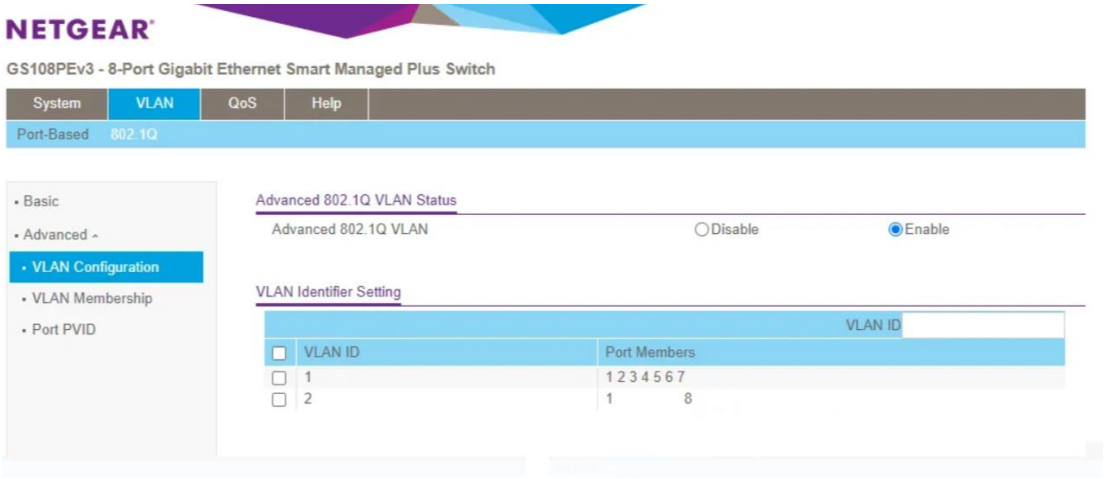

Рисунок 2.12 – Вікно налаштування VLAN

Для кожного з портів можна задати мітки або не задавати їх. Так, на рис. 2.13 показано налаштування VLAN з ідентифікатором 1, де портом з міткою є перший порт комутатора, а всі інші, які входять у нього, не позначені тегами. По аналогії на рис. 2.14 показано налаштування портів для VLAN2.

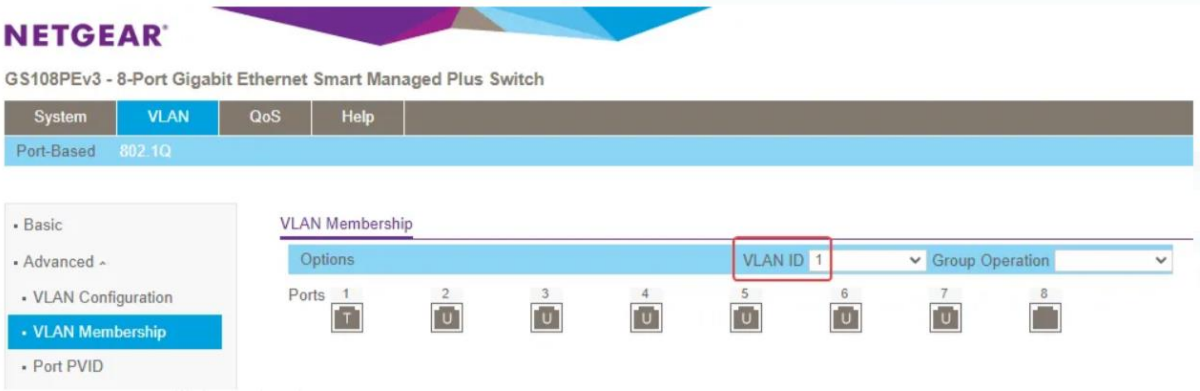

Рисунок 2.13 – Налаштування портів VLAN1

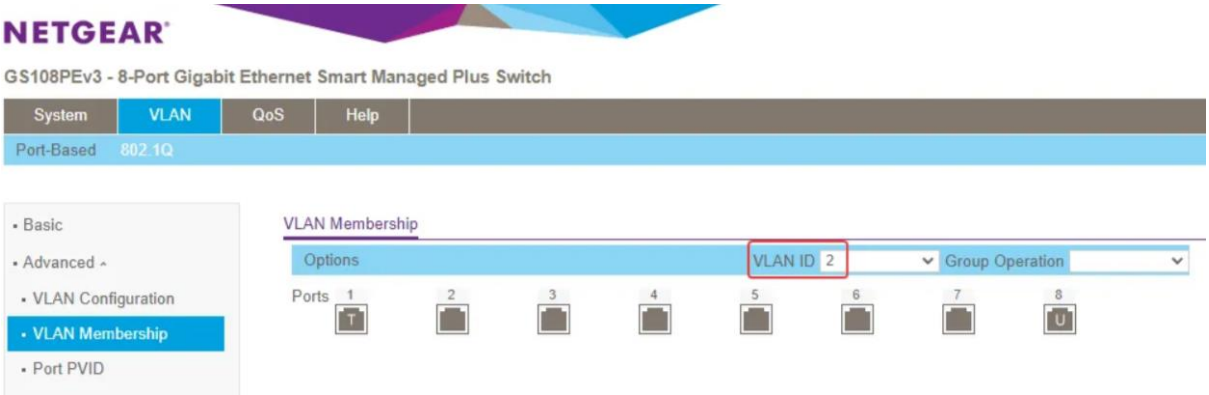

Рисунок 2.14 – Налаштування портів VLAN2

При такому налаштуванні потрібно звернути увагу і враховувати в подальших настройках маршрутизатора наступні речі:

Порти з мітками:

– VLAN 1: 1 порт;

– VLAN 2: 1 порт.

Порти без міток:

– VLAN 1: 2–7;

– VLAN 2: 8.

Стандартні порти:

– VLAN 1: 8;

– VLAN 2: 2–7.

Фрагмент налаштування інтерфейсів при визначених VLAN конфігурується так, як показано на рис. 2.15. Конфігураційний файл розташований за адресою – «/etc/config/network».

```
config interface 'loopback'
        option proto 'static'
        option ipaddr '127.0.0.1'
        option netmask '255.0.0.0'
        option device 'lo'

config interface 'lan'
        option proto 'static'
        option netmask '255.255.255.0'
        option ipaddr '192.168.0.1'
        option device 'eth0.1'

config interface 'wan'
        option proto 'dhcp'
        option device 'eth0.2'
```

Рисунок 2.15 – Налаштування конфігурації інтерфейсів мережі

При виконанні і збереженні таких налаштувань доцільно зробити резервну копію налаштувань, перш, ніж почати її використовувати. Для її створення використовується команда: «cp /etc/config/network /etc/config/network.bk»

Це практично всі процедури, які потрібно зробити, щоб налаштувати Pi на керованому комутаторі та маршрутизувати трафік із портів локальної мережі на порти 2 – 7.

Відкривши браузер і перейшовши по IP-адресі Raspberry Pi у локальній мережі, тобто 192.168.0.1, повинен відобразитися веб-інтерфейс Luci.

Виконавши перехід у меню Мережа -> Інтерфейси [Інтерфейси/Пристрої] можна побачити два інтерфейси і два відповідних пристрої, які показані нижче на рис. 2.16 та рис. 2.17 відповідно.

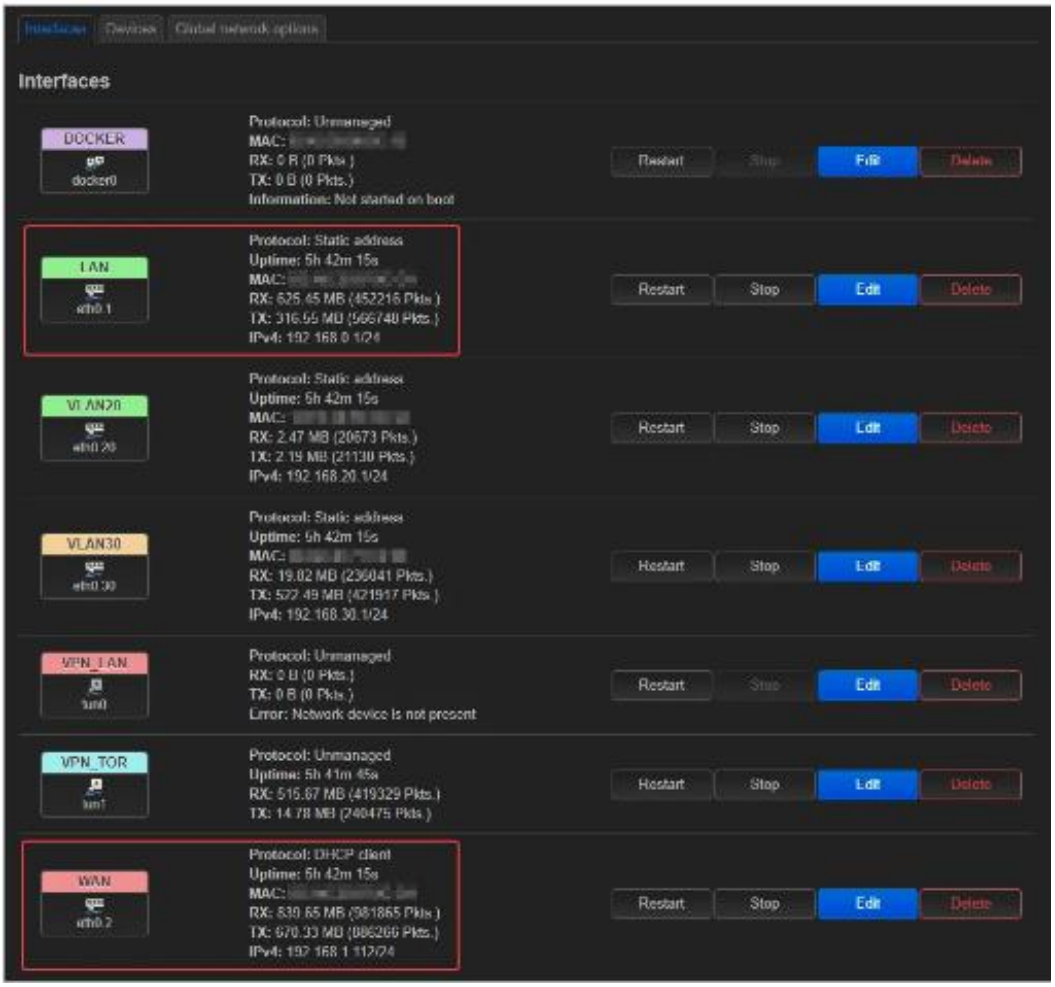

Рисунок 2.16 – Результат налаштування VLAN (інтерфейси)

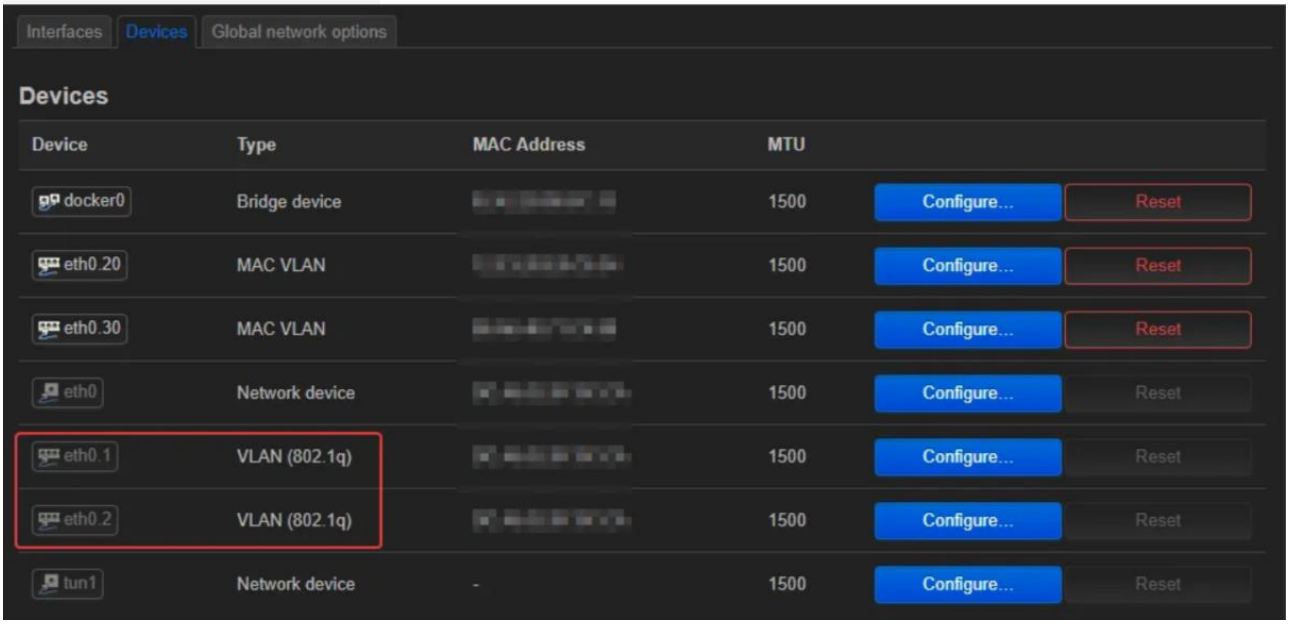

Рисунок 2.17 – Результат налаштування VLAN (пристрої)

Наступний крок полягає у формуванні і розгортанні Docker-контейнерів, налаштуванні точки доступу та інших сервісів.

РОЗДІЛ 3 НАЛАШТУВАННЯ СЛУЖБ І СЕРВІСІВ МАРШРУТИЗАТОРА НА БАЗІ RASPBERRY PI

3.1 Налаштування параметрів точки доступу та спільних ресурсів

Налаштування точки доступу є доволі тривіальною задачею і передбачає лише програмного його увімкнення в режим «Access Point». Тут навіть не потрібно вмикати DHCP, оскільки опрацювання потоків пакетів покладається на Raspberry PI 4. Фізично точка доступу TL-WA1201 за допомогою кабель витої пари підключається до керованого комутатора, а саме до порта №5. Тобто точка доступу буде знаходитися у VLAN 1 – локальна мережа. Для успішного налаштування цього мережевого пристрою достатньо задати SSID і пароль. Вибір режиму роботи TL-WA1201 як точки доступу показано на рис. 3.1.

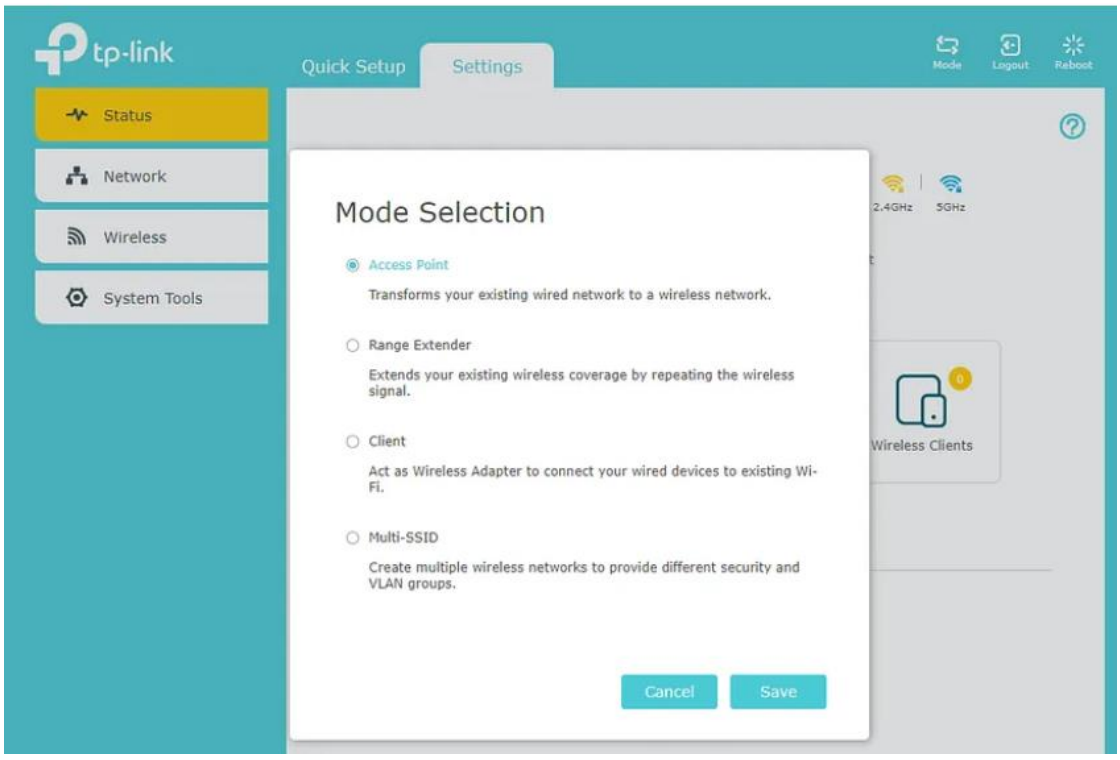

Рисунок 3.1 – Вибір режиму роботи точки доступу TL-WA1201

					КС КРБ 123.139.00.00 ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Яшнюк О.І.			Налаштування служб і сервісів маршрутизатора на базі Raspberry PI	Літ.	Арк. 44 / Аркушів
Перевірив.		Яцишин В.В.					
Консульт.		Гурик О.Я.				ТНТУ, каф. КС, гр. СІ-42	
Н. Контр.		Тиш Є.В.					
Затверд.		Осухівська Г.М.					

Щоб отримати віддалений доступ до 1 ТБ SSD-накопичувача (де зберігаються мультимедійні файли для Plex) з ПК під операційною системою Windows, потрібно встановити Samba та створити декілька спільних файлів.

Це буде встановлено з пакета всередині OpenWRT, який можна налаштувати для спільного доступу до папок у локальній мережі через IP-адресу Raspberry Pi.

Для того, щоб додати SSD-накопичувач з USB інтерфейсом потрібно встановити пакети, створити папку для монтування та визначити мітку диску, як показано на рис. 3.2

```
opkg update
opkg install ntfs-3g
mkdir -p /mnt/1TB && \
    ntfs-3g /dev/sda1 /mnt/1TB -o rw,lazytime,noatime,big_writes && \
    ls -la /mnt/1TB
```

Рисунок 3.2 – Монтування SSD-диску

З метою автоматичного монтування розділу під час запуску (з підключеним жорстким диском) треба відредагувати /etc/rc.local і додати такі рядки, які наведено на рис. 3.3. Процес монтування на Rapberry PI 4 проілюстровано на рис. 3.4.

```
sleep 1
ntfs-3g /dev/sda1 /mnt/1TB -o rw,lazytime,noatime,big_writes
exit 0
```

Рисунок 3.3 – Автоматичне монтування USB-диску

```
root@OpenWrt:~# cat /etc/rc.local
# Put your custom commands here that should be executed once
# the system init finished. By default this file does nothing.
sleep 1
ntfs-3g /dev/sda1 /mnt/1TB -o rw,lazytime,noatime,big_writes
exit 0
root@OpenWrt:~# _
```

Рисунок 3.4 – Процес монтування диску на Raspberry PI

Для того, щоб мати доступ до ресурсів SSD-диску з робочих станцій під операційної системою Windows необхідно встановити Samba. Для її інсталяції виконується команда, яка представлена на рис. 3.5

```
opkg install samba4-server samba4-client luci-app-samba4
```

Рисунок 3.5 – Інсталяція Samba

Після встановлення служби забезпечення спільного використання ресурсів потрібно перезавантажити Raspberry PI 4 або принаймні скинути службу після завершення. Окрім цього, для більш детального налаштування параметрів ресурсів спільного використанням можна використовувати Luci, зокрема: Luci -> Служби ->Мережні спільні ресурси.

3.2 Формування та налаштування докер-контейнерів у мережі маршрутизатора

В якості докер-контейнерів будуть використовуватися:

– PiHole – служба блокування реклами;
– Plex – медіа сервер;
– Transmission – служба торент-клієнт.

Для управління наведеними вище контейнерами застосовується Portainer. Ці служби варто використовувати у більш контрольованому середовищі через розділені мережі та маршрутизацію.

Для початку потрібно проінсталювати сам Docker з використанням пакетів, які показані на рис. 3.6.

```
opkg update
opkg install dockerd docker-compose luci-app-dockerman kmod-macvlan
```

Рисунок 3.6 – Інсталяція Docker

Особливої уваги потребує kmod-macvlan, це те, що знадобиться пізніше, щоб розділити мережу для Docker MACVLAN.

На даний момент налаштування Plex досить просте. Насправді його можна було не встановлювати, оскільки він був відокремлений від будь-якої іншої мережі. Дана служба може просто працювати на Raspberry PI та підключатися через міст Docker.

На твердотільному накопичувачі 1 ТБ знаходиться підпапка під назвою docker, для якої потрібно зіставити всі конфігурації контейнера і це допоможе уникнути проблем при відтворенні медіа.

Окрім цього на SSD-диску наявні деякі папки, які використовуються для розміщення музики та інших медіафайлів. Наразі команда Docker проста, і, можливо, дійсно її варто колись перетворити на сценарій YAML для створення докерів. У даному випадку використано образи linuxserver для Plex (рис. 3.7).

```
docker run --detach \
    --name plex \
    --net=host \
    --restart unless-stopped \
    -e PGID=1000 \
    -e PUID=1000 \
    -e UMASK=022\
    -e VERSION=docker \
    -v /mnt/1TB/dMusic:/data/dmusic \
    -v /mnt/1TB/docker/plex:/config \
    -v /mnt/1TB/docker/plex:/transcode \
    -v /mnt/1TB/Music:/data/music \
    linuxserver/plex
```

Рисунок 3.7 – Створення Docker-контейнера

Для того, щоб перейти до Docker-контейнера потрібно у браузері вказати IP-адресу і порт – http://192.168.0.1:32400, щоб завершити його налаштування.

Наступна частина інсталяції PiHole є дійсно цікавою, оскільки буде використовуватися VLAN з Docker, щоб розділити мережу та значно спростити налаштування DNS.

У більшості випадків при використанні блокувальників реклами на Open WRT встановлюється деяке програмне забезпечення, що виконує дивну переадресацію/маршрутизацію портів тим самим формуючи проблеми маршрутизації. У кваліфікаційній роботі пропонується запускати блокувальник реклами з контейнера.

Дотримуючись рекомендацій, які наведені у документації Open WRT було створено не лише мережу MACVLAN, а й мережу мосту на Docker, для якої контейнер підключився. MACVLAN у Docker насправді є лише розширенням будь-якої існуючої мережі, у якій наявні Ethernet, або VLAN. Тому тут не потрібне жодне перемикання та не потрібна жодна маршрутизація. Типово маршрутизація задана як показано на рис. 3.7

```
config route
        option interface 'macvlan'
        option target '192.168.30.3'
        option netmask '255.255.255.255'
```

Рисунок 3.7 – налаштування маршрутизації macvlan

Крім того, не потрібно створювати 10-fixroutes.sh всередині контейнера, оскільки він не використовує мережу Docker bridge «поверх» існуючої VLAN (рис. 3.8).

```
#!/usr/bin/with-contenv bash
set -e

echo "fixing routes"
ip route del default
ip route add default via 172.18.0.1
```

Рисунок 3.8 – Налаштування маршрутів всередині контейнера

Далі потрібно внести зміни у налаштування VLAN в OpenWRT. Виходячи з вище проведених процедур /etc/config/network, розширений і включає конфігурацію, яка представлена на рис. 3.9.

```
config interface 'vlan20'
        option proto 'static'
        option ipaddr '192.168.20.1'
        option netmask '255.255.255.0'
        option device 'eth0.20'

config device
        option type 'macvlan'
        option ifname 'eth0'
        option mode 'bridge'
        option name 'eth0.20'
        option acceptlocal '1'
        option ipv6 '0'
```

Рисунок 3.9 – Доповнена конфігурація VLAN

Тепер при розширенні конфігурації у веб-інтерфейсі можна побачити мережеві інтерфейси, як показано на рис. 3.10. Для того, щоб подивитися налаштування інтерфейсів потрібно пройти по шляху: «Luci -> Network -> Interfaces [Інтерфейси]».

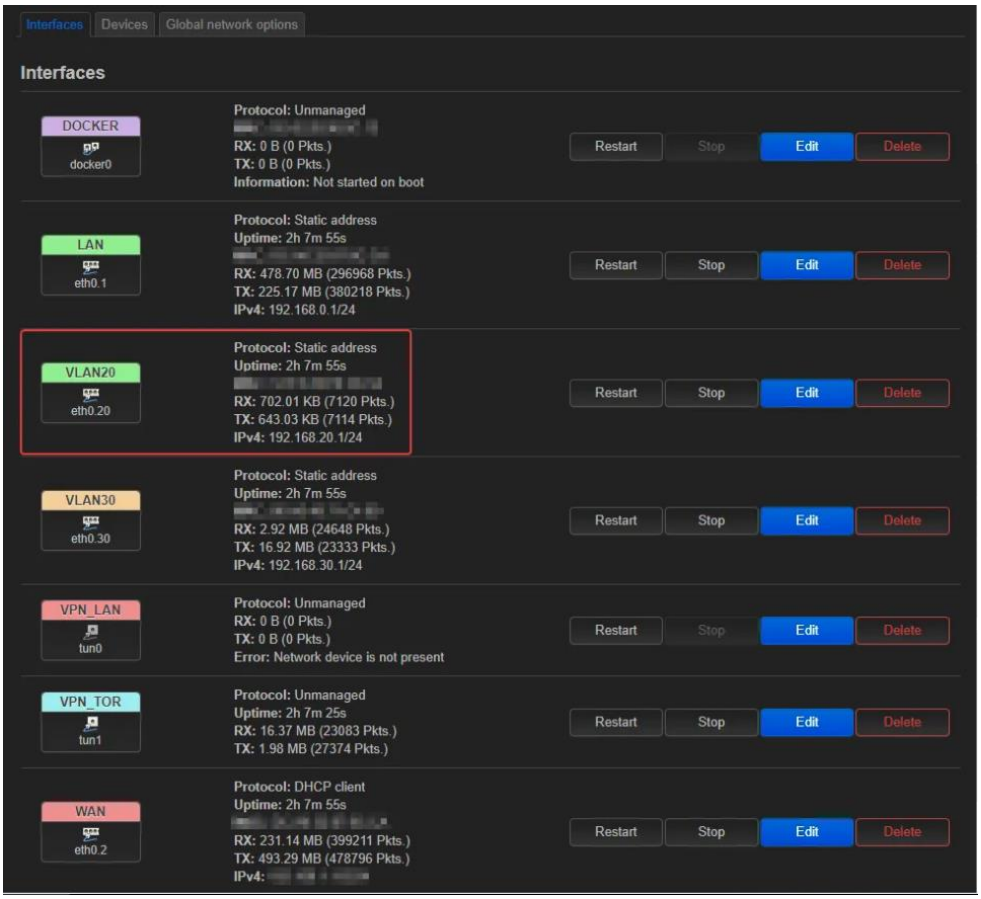

Рисунок 3.10 – Відображення розширеної конфігурації інтерфейсів мережі

Для більш детального перегляду та можливого налаштування інтерфейсів обравши VLAN20 можна побачити вміст, який показано на рис. 3.11.

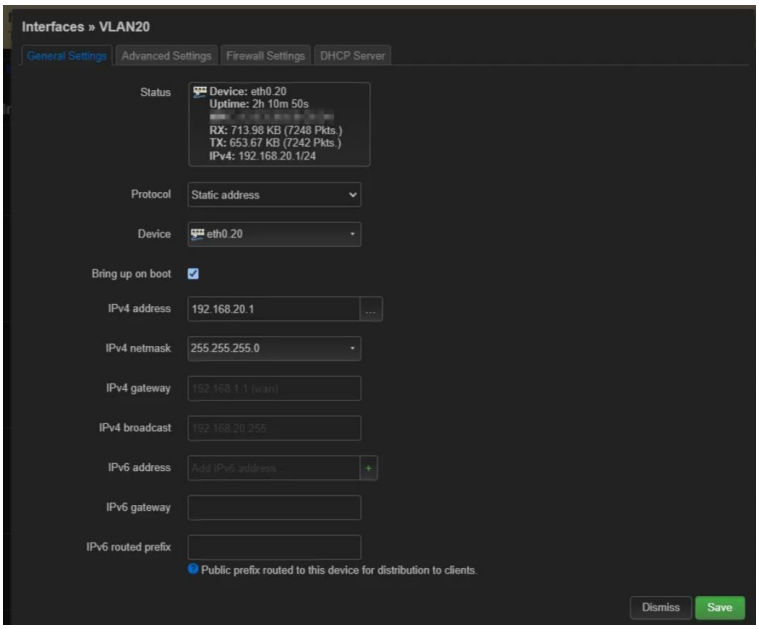

Рисунок 3.11 – Детальна конфігурація VLAN20

Перейшовши на вкладу «Advanced» можна задати шлюз за замовчуванням, як показано на рис. 3.12.

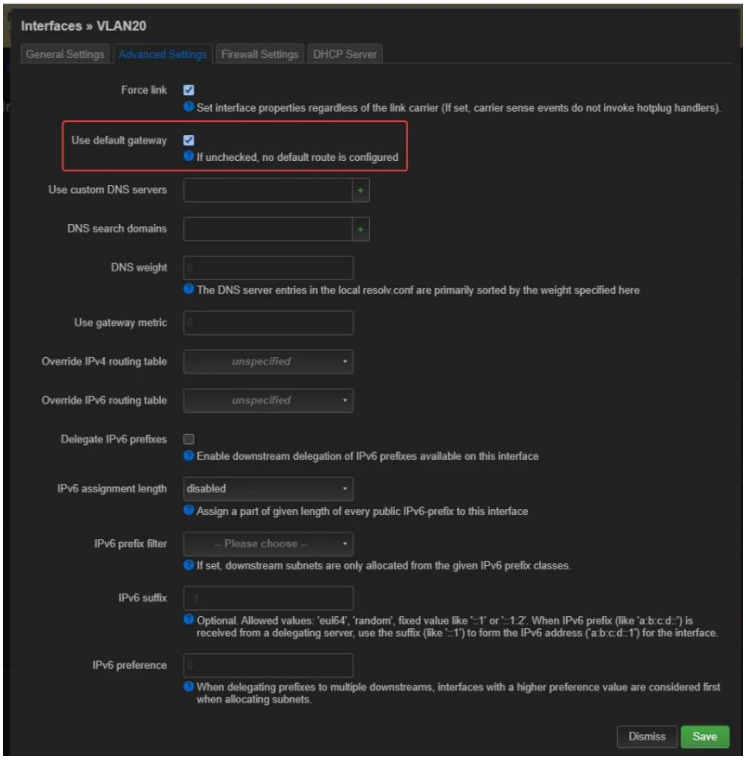

Рисунок 3.12 – Вибір шлюза за замовчуванням

Налаштування зон FireWall можна виконати на вкладці FireWall Settings, як показано на рис. 3.13.

Рисунок 3.13 – Налаштування зон FireWall

Налаштування DHCP-сервера виконується на однойменній вкладці, як представлено на рис. 3.14.

Рисунок 3.14 – Вкладка для налаштування параметрів FireWall

Якщо пройти по шляху Luci -> Мережа -> Інтерфейси [Пристрої] можна побачити та провести налаштування пристроїв, які наявні в ком'ютерній мережі.

Зокрема, у випадку реалізації маршрутизатора на основі Raspberry PI 4 та Open WRT доступними і налаштовуваними пристроями є:

– MAC VLAN;
– VLAN;
– мережевих пристроїв;
– пристроїв типу міст.

На рис. 3.15 наведено пристрої, які будуть використовуватися і маршрутизуватися за допомогою Raspberry PI 4.

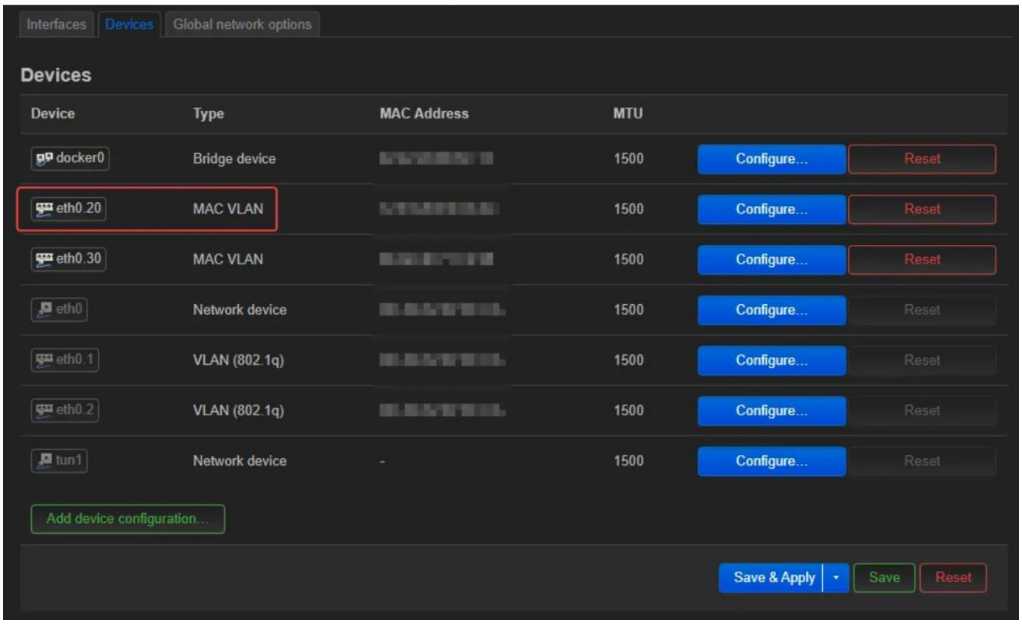

Рисунок 3.15 – Налаштування пристроїв мережі

При виборі MAC VLAN відображається вікно більш детальних його налаштувань (рис. 3.16).

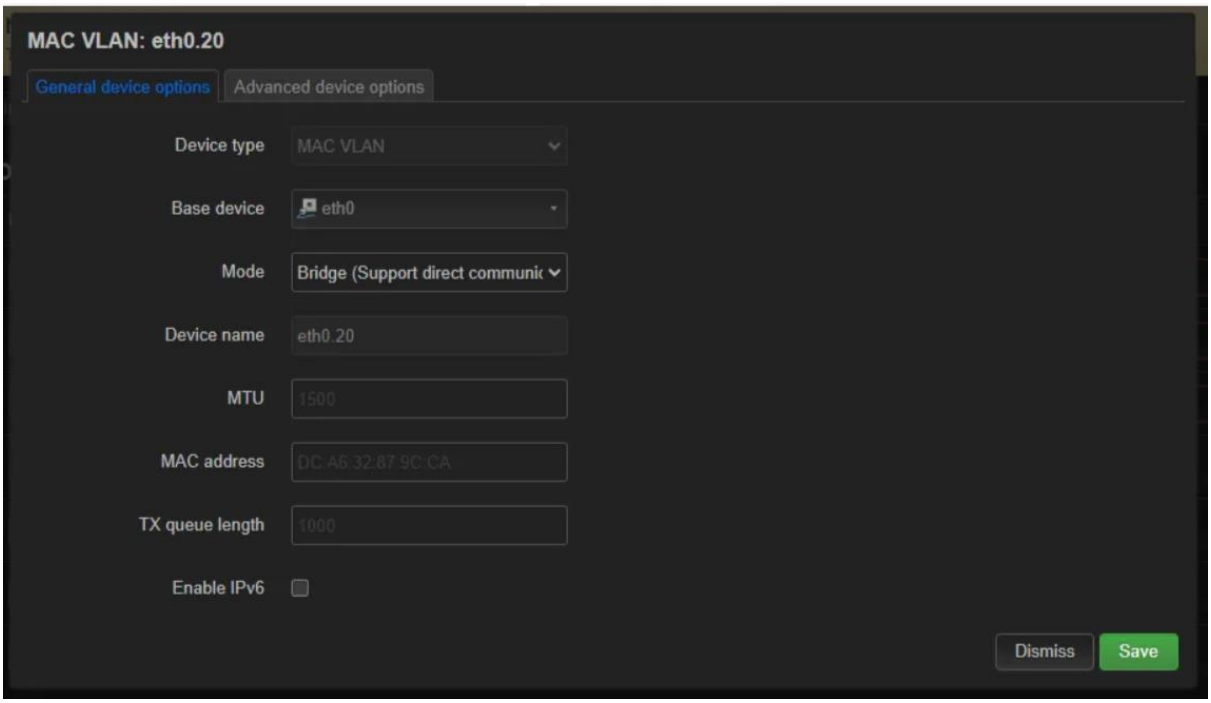

Рисунок 3.16 – Детальне налаштування MAC VLAN

На вкладці «Advanced» (рис. 3.17) вікна налаштувань пристроїв можна вказати також параметри безпеки, тобто налаштувань FireWall.

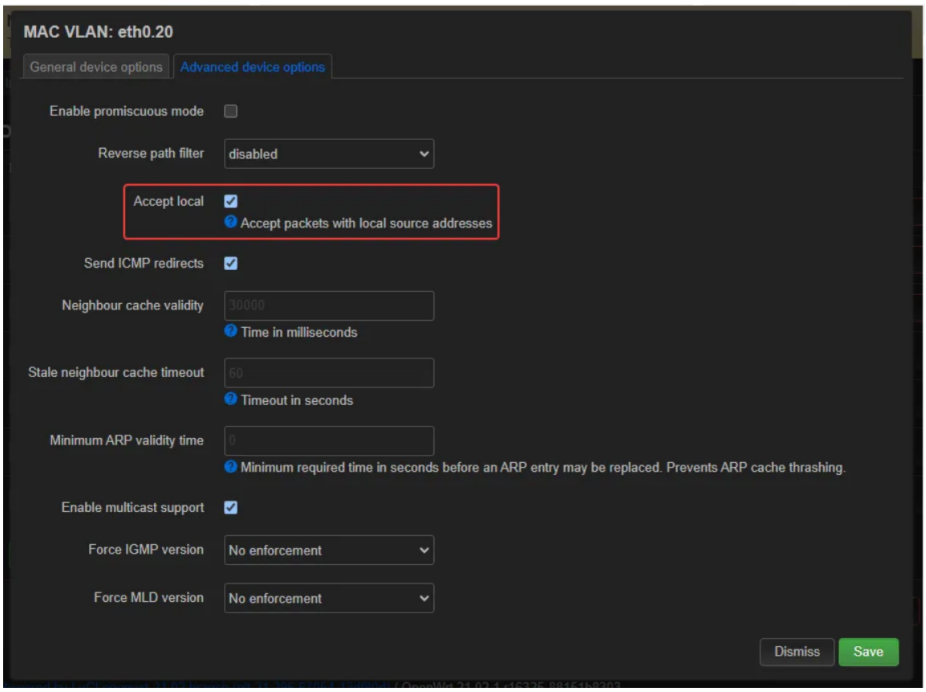

Рисунок 3.17 – Налаштування вкладки Advanced

Важливою частиною цього налаштування є додавання MACVLAN до тієї самої зони брандмауера, до якої належить локальна мережа. Можливо, це не обов'язково, оскільки можна додати його до іншої зони та дозволити маршрутизацію. Налаштовані параметри також можна побачити в налаштуваннях зони брандмауера для локальної мережі (рис. 3.18).

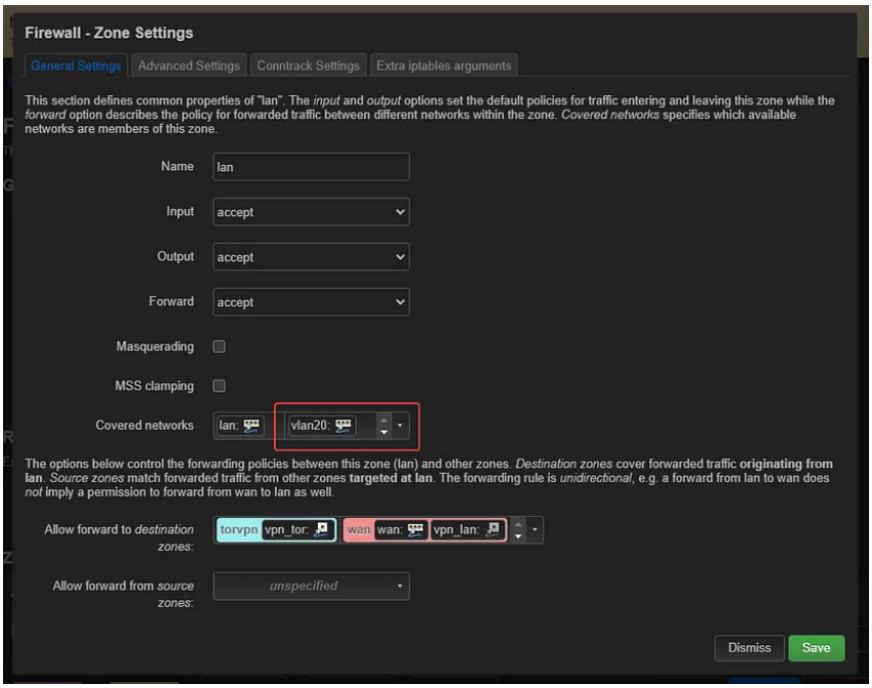

Рисунок 3.18 – Параметри FireWall для локальної мережі

3.3 Налаштування Docker

Тепер, коли MACVLAN/VLAN налаштовано, можна розгорнути контейнер. Використовуючи файл docker-compose.yml, який наведений на рис. 3.19 нижче, виконано запуск docker-compose up -d pihole.

```
version: "3.3"
services:
  pihole:
    container_name: pihole
    image: pihole/pihole:latest
    hostname: pihole.lan
    environment:
      TZ: 'Europe/London'
      WEBPASSWORD: 'asdf'
    volumes:
      - '/mnt/1TB/docker/pihole/pihole/:/etc/pihole/'
      - '/mnt/1TB/docker/pihole/dnsmasq.d/:/etc/dnsmasq.d/'
    cap_add:
      - NET_ADMIN
    restart: unless-stopped
    networks:
      lan20:
        ipv4_address: 192.168.20.3

networks:
  lan20:
    name: lan20
    driver: macvlan
    driver_opts:
      parent: eth0.20
    ipam:
      config:
        - subnet: 192.168.20.0/24
          gateway: 192.168.20.1
```

Рисунок 3.19 – Запуск Docker-контейнера блокувальника реклами

У випадку успішного розгортання контейнера, зайшовши в Luci можна побачити налаштування параметрів, які показано на рис. 3.20 та рис. 3.21.

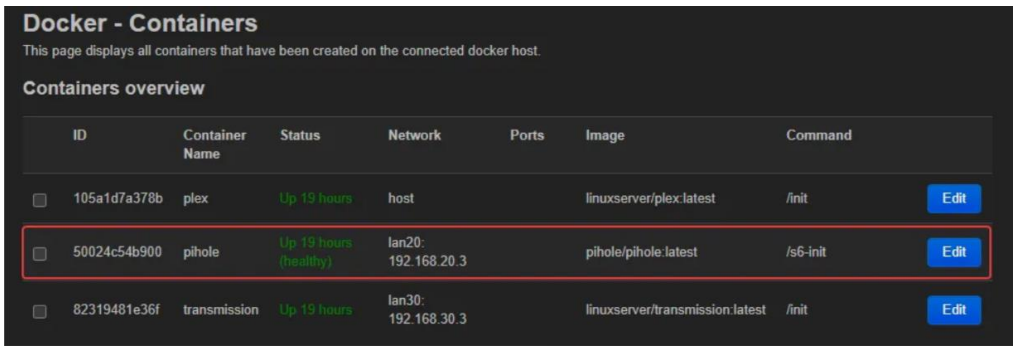

Рисунок 3.19 – Результат успішного розгортання контейнера блокувальника реклами

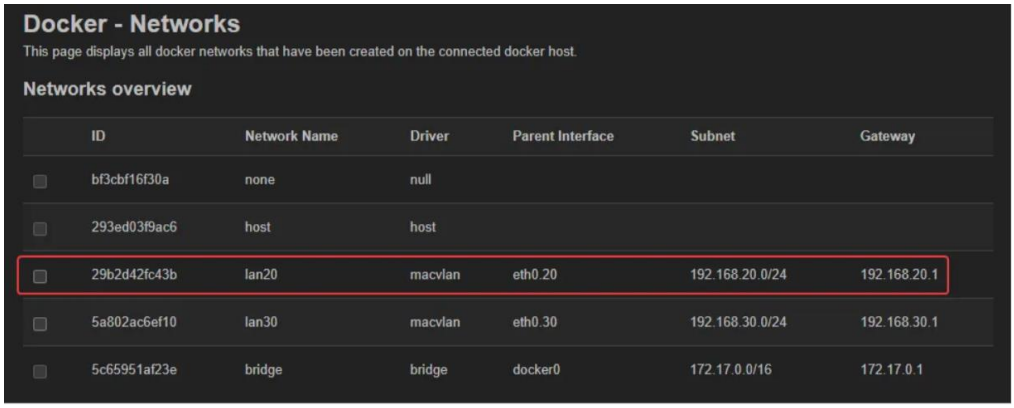

Рисунок 3.20 – Результат розгортання контейнера MAC VLAN

Наступний крок полягає у налаштуванні OpenWRT DNS. Для цього потрібно пройти по шляху: Luci -> Мережа -> DHCP і DNS, щоб вказати на щойно створений PiHole (рис. 3.21).

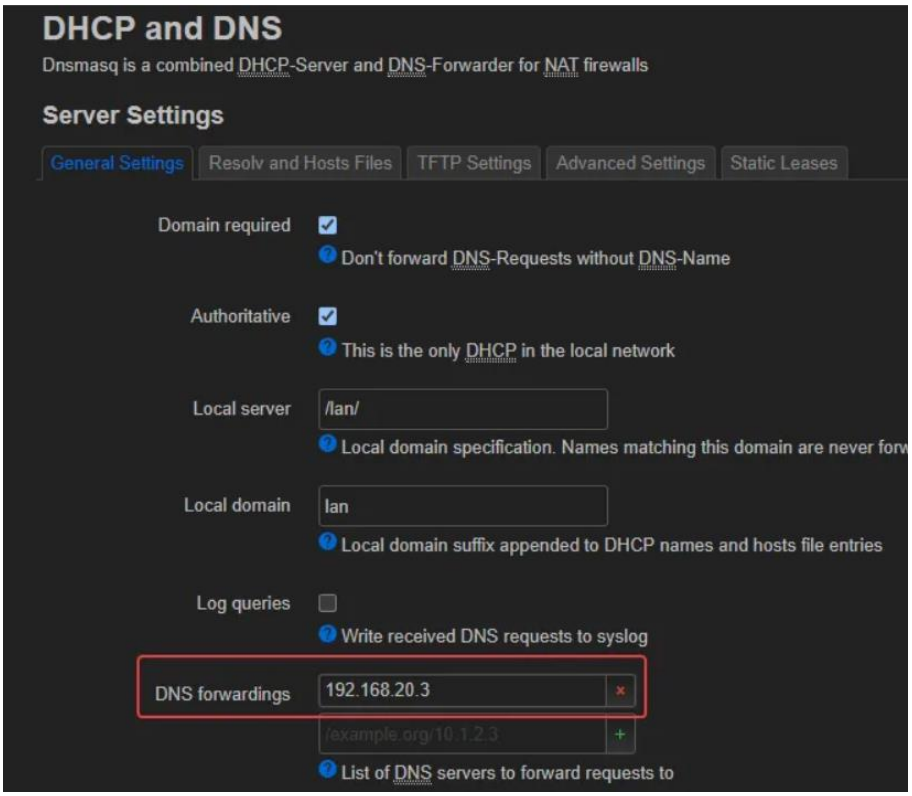

Рисунок 3.21 – Налаштування DNS та DHCP

Завершальним етапом є змусити всі пристрої у мережі проходити через PiHole; інакше вони можуть використовувати власний DNS і уникати списку блокувань або навіть мати витік DNS.

Для цього треба додати правило PREROUTING у розділ спеціальних правил брандмауера, пройшовши за шляхом Luci -> Мережа -> Брандмауер [Користувацькі правила] (рис. 3.22).

```
iptables -t nat -A PREROUTING -i eth0 -p udp --dport 53 -j DNAT --to
192.168.20.3
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 53 -j DNAT --to
192.168.20.3
```

Рисунок 3.22 – Задання правила PREROUTING

У даному розділі можна здійснити налаштування власних DNS-серверів Upstream. Проте більш раціонально налаштувати DNS через HTTPS.

3.4 Налаштування DNS через HTTPS

Налаштування DNS через HTTPS виконується для вихідного сервера, до якого PiHole звернеться, коли домен не існує в його списку блокувань. Дані, надіслані на цей пристрій розпізнавання, будуть зашифровані та повернуті назад до PiHole, і, потім надсилаються назад до оригінального абонента (рис. 3.22).

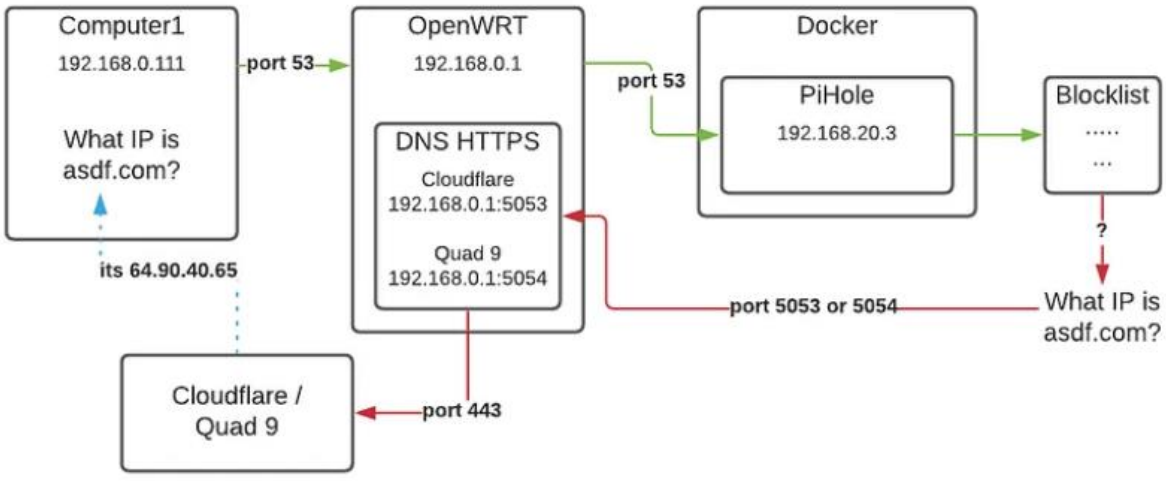

Рисунок 3.22 – Організація DNS через HTTPS

Першим кроком при налаштуванні є інсталяція проксі DNS поверх HTTPS/ для виконання цієї команди використовується скрипт, який показаний на рис. 3.23.

```
opkg update
opkg install https-dns-proxy luci-app-https-dns-proxy
```

Рисунок 3.23 – Встановлення DNS проксі через HTTPS

Після успішної інсталяції та виконання команд (рис. 3.23), потрібно перейти по шляху – «Luci -> Сервіси -> DNS HTTPS Proxy Settings» та увімкнути/запустити службу. У цьому випадку рекомендується виконати повне перезавантаження пристрою і оновити конфігурацію, як показано на рис. 3.24.

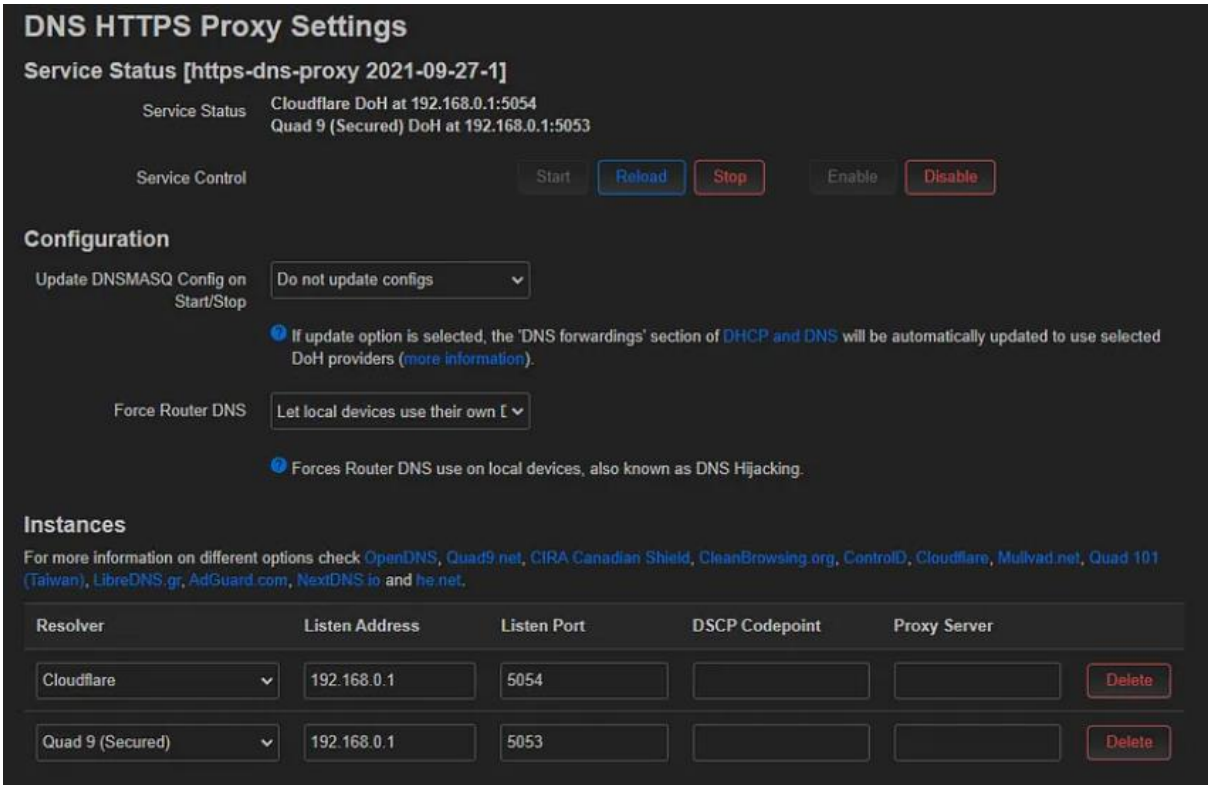

Рисунок 3.24 – Налаштування DNS HTTPS Proxy

Завершальним етапом є вказання параметрів PiHole на використання сервера для пошуку DNS (рис. 3.25).

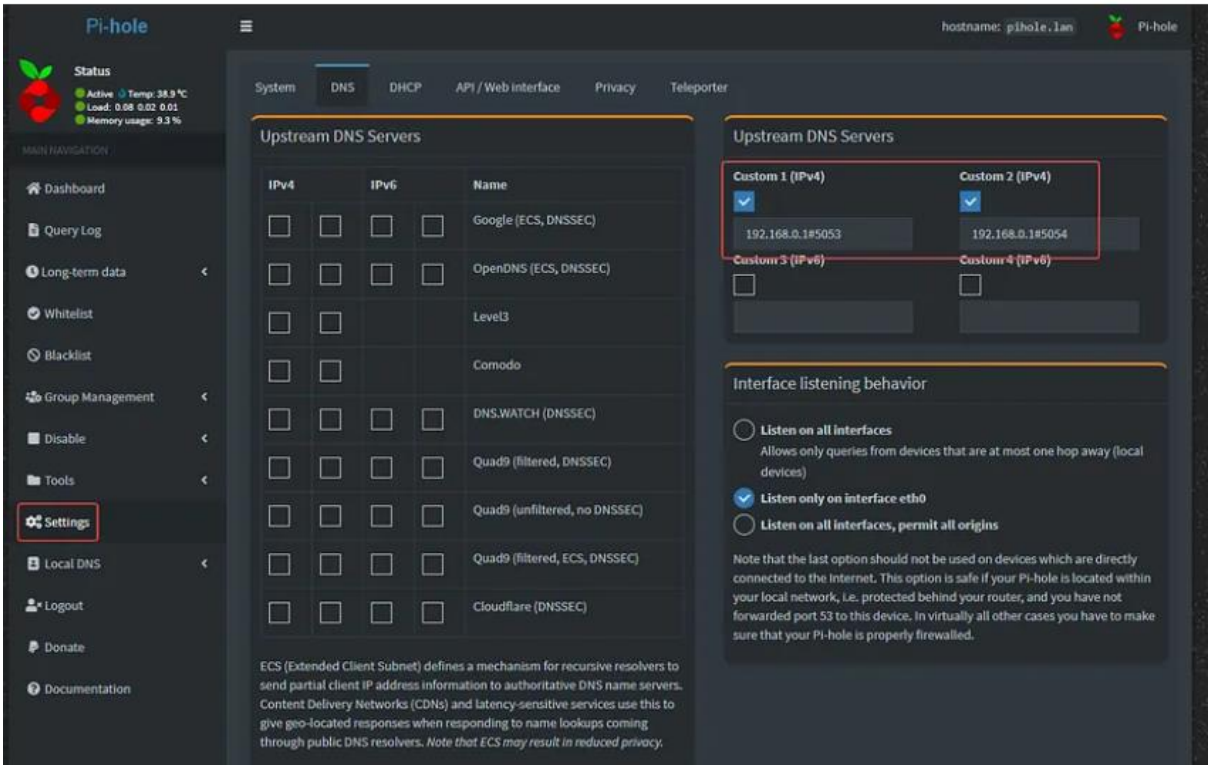

Рисунок 3.25 – Налаштування PiHole

Як видно з рис. 3.25, особливу увагу варто звернути на використання IP-адреси та «хешу» для позначення порту.

Встановлення та налаштування торент-клієнта

До цього часу було успішно проінстальовано та налаштовано Docker, MACVLAN і VLAN. Тепер потрібно створити Docker торрент-контейнер, відокремлений від решти мережі. Серед його налаштувань потрібно передбачити і виконати перевірку того, що він підключається через VPN, а не через звичайну глобальну мережу, яка показує домашню IP.

Для цього доцільно використовувати ті самі налаштування MACVLAN/VLAN, що й для PiHole, але цього разу його необхідно помістити в тій самій зоні брандмауера, що й локальна мережа. Проблема з цим, звісно, полягає в тому, що локальна мережа налаштована на вихід у глобальну мережу, тож як контейнер повинен виходити у мережу через VPN.

Для початку треба створити інтерфейс і пристрій, як було зазначено раніше при налаштуванні інших сервісів, зокрема з PiHole. Ці процедури показано відповідно на рис. 3.26 та рис. 3.27.

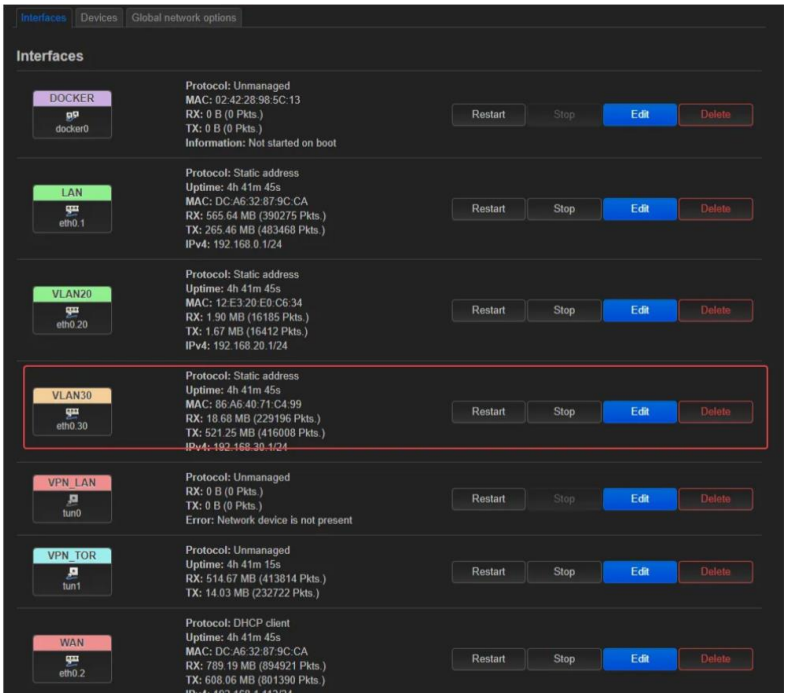

Рисунок 3.26 – Налаштування інтерфейсу торент-клієнта

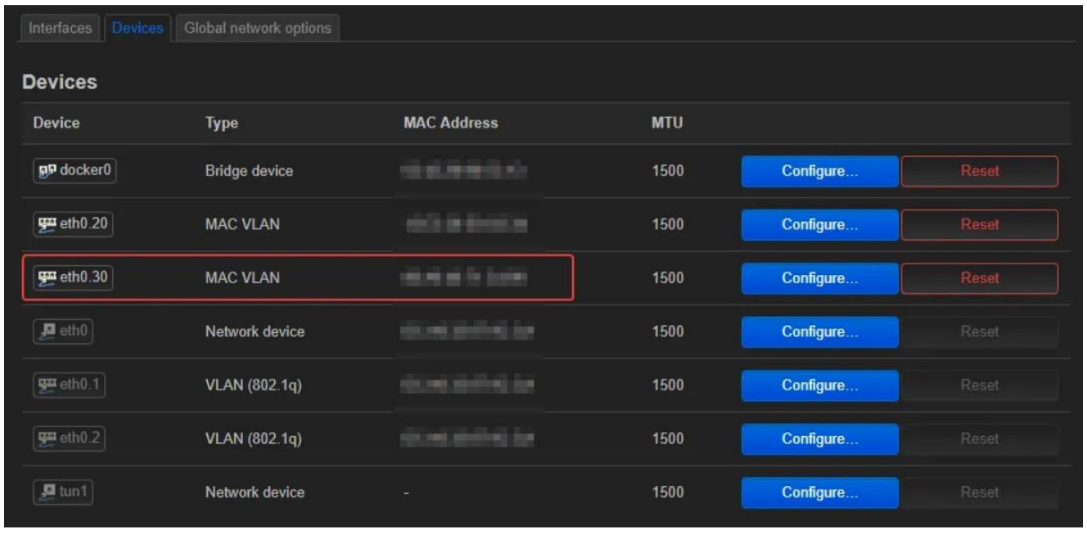

Рисунок 3.27 – Налаштування пристрою для торент-клієнта

Далі створюється Docker-контейнер і відповідна мережу, як показано на рис. 3.28.

```
version: "3.3"
services:
  transmission:
    container_name: transmission
    image: linuxserver/transmission:latest
    hostname: transmission.lan
    environment:
      TZ: 'Europe/London'
    volumes:
      - '/mnt/1TB/docker/transmission/config/:/config'
      - '/mnt/1TB/docker/transmission/downloads/:/downloads'
      - '/mnt/1TB/docker/transmission/watch/:/watch'
    cap_add:
      - NET_ADMIN
    restart: unless-stopped
    networks:
      internal:
      lan30:
        ipv4_address: 192.168.30.3

networks:
  internal:
    name: transmission_internal
    driver: bridge
  lan30:
    name: lan30
    driver: macvlan
    driver_opts:
      parent: eth0.30
    ipam:
      config:
        - subnet: 192.168.30.0/24
```

Рисунок 3.28 – Створення Docker-контейнера для троент-клієнта

Існує багато настанов, які пояснюють, як налаштовувати OpenVPN на OpenWRT. Тому цей процес можна не описувати, оскільки він є доволі простим. Після налаштування OpenVPN в розділі інтерфейсів повинно з’явитися інформація, як показано на рис. 3.29.

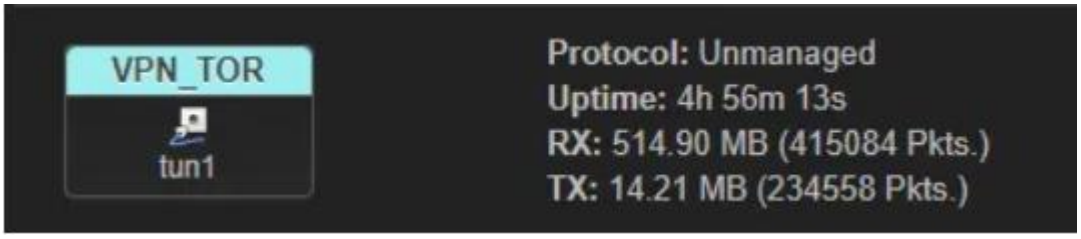

Рисунок 3.29 – Інтерфейс для роботи через OpenVPN

Очевидно, що назва інтерфейсу VPN_TOR, яка дає змогу ідентифікувати декілька VPN, чітко розрізняючи їх призначення.

Варто також зазначити, що повинен бути вказаний тунельний пристрій у файлі конфігурації OpenVPN. Таким чином можна налаштувати багато

інтерфейсів/пристроїв VPN і примусово виводити певний трафік через певні віртуальні мережі, як показано на рис. 3.30.

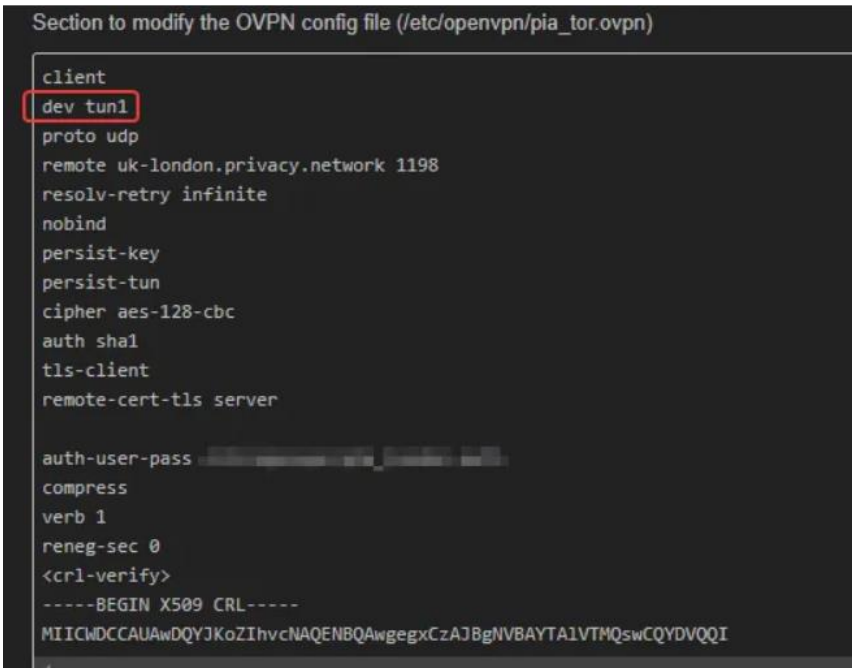

Рисунок 3.30 – Вибір VPN

Варто відмітити і той факт, що не обов’язково створювати пристрій, щоб використовувати його, оскільки OpenVPN створює його на льоту. Коли запускається OpenVPN, можна помітити, що пристрій відображається на вкладці пристроїв, і коли це станеться, можна завершити його налаштування інтерфейсу, вказавши пристрій tunX, який з’явився.

Наступний етап – це конфігурування зон брандмауера. Для виконання налаштувань потрібно перейти за шляхом: «Luci -> Network -> Firewall» і визначити кілька нових зон. Приклад налаштування зон показано на рис. 3.32.

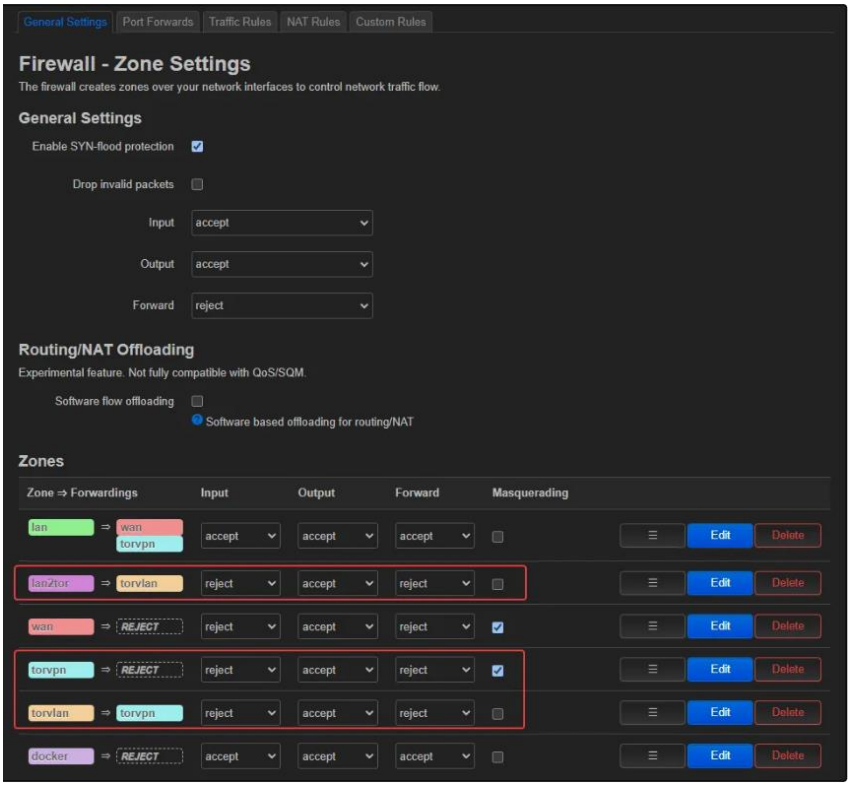

Рисунок 3.33 – Конфігурування зон FireWall

TorVLAN вказує мережу передачі (torrent/TORVLAN/VLAN30) для доступу до служби VPN (рис. 3.34).

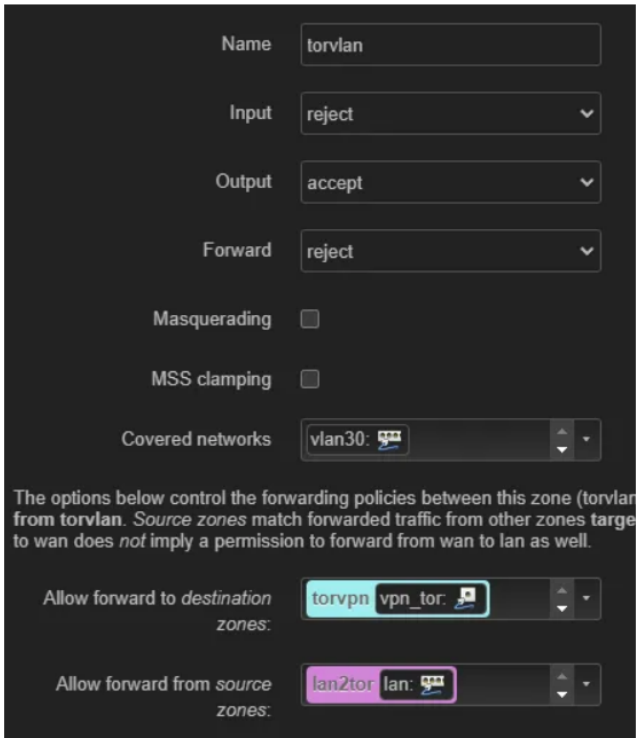

Рисунок 3.34 – Мережа TorVLAN

TorVPN вмикає службу VPN для використання локальною мережею та VLAN30 (рис. 3.35).

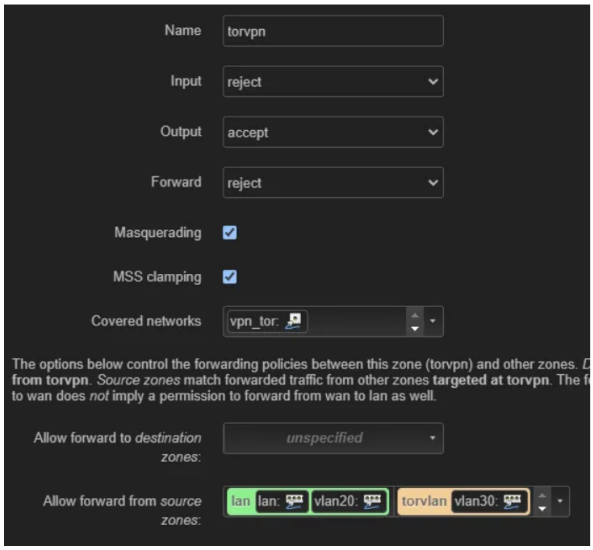

Рисунок 3.35 – TorVPN

LAN2TOR надає дозвіл локальній мережі отримувати доступ до VLAN30, але не навпаки. Налаштування показані на рис. 3.36

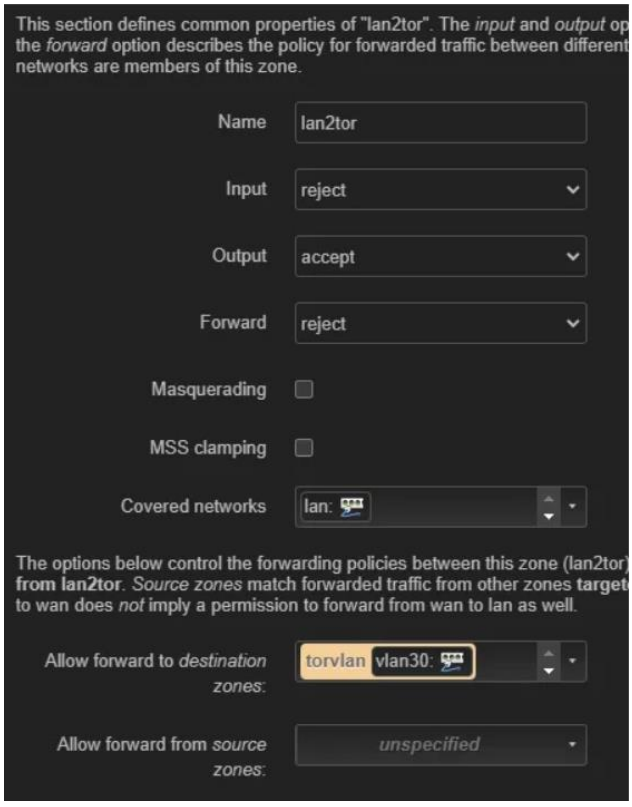

Рисунок 3.36 – LAN2TOR

Таким чином на основі Raspberry PI 4 та Open WRT реалізовано проект маршрутизатора, який виконує як прямі функції роутера, так і надає сервіси для авторизованого доступу ззовні до медіасервера, торента та забезпечує блокування реклами.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при ураженні електричним струмом

Дія електричного струму на організм людини має різносторонній характер і різносторонні прояви – від слабих подразнень до смертельних наслідків.

Електричний струм , що проходить через тіло людини, спричиняє термічну, хімічну, світлову, механічну та біологічну дію.

Біологічна дія є виключною властивістю живої тканини. Вона проявляється сильним збудженням нервової тканини, що призводить до порушення внутрішніх біоелектричних процесів, які пов'язані з життєвими функціями організму. Зовнішній струм при взаємодії з біоелектричними процесами людини може викликати судоми м'язів, життєво важливих органів, у тому числі серця і легенів, що призводить до зупинки дихання і кровообігу.

Електричне ураження організму струмом буває місцевим (електричні травми) і загальним(електричні удари) коли уражається весь організм.

Характерними видами місцевих електричних травм є:

- електричні опіки;
- електричні знаки;
- металізація шкіри;
- механічні ураження;
- електрофтальмія.

Залежно від умов виникнення опіки бувають трьох видів: струмовий (контактний), дуговий і змішаний, під дією струму і електричної дуги. "Ствол" електродуги має високу температуру – від 4000 до 15000^{0}С і вище. Людина, яка потрапляє у таку ситуацію, отримає опіки того чи іншого ступеню тяжкості.

Тканини, що лежать на шляху струму внаслідок великої кількості теплоти висушуються, обвуглюються і безслідно щезають.

Внаслідок контакту з електромережею виникають електричні знаки. Шкіра в місці контакту затвердіває подібно до мозоля.

Металізація шкіри виникає внаслідок короткого замикання і потрапляння в глибину шкіри газоподібних або розплавлених часток металу, які розлітаються у всі сторони.

Механічні ураження є наслідком судомних скорочень м'язів під дією струму, що призводить до розриву кровоносних судин, м'язів, сухожилків, вивиху суглобів або перелом кісток. Вони виникають тоді, коли людина тривало перебуває під напругою 380В.

При ураженні електричним струмом необхідно якомога швидше звільнити потерпілого від струмопровідних частин обладнання. Дотик до струмопровідних частин (мережі під напругою) у більшості випадків призводить до судом м'язів, тобто людина самостійно не в змозі відірватися від провідника. Тому необхідно швидко відключити ту частину електрообладнання, до якої доторкається людина. Будь-яке зволікання при наданні допомоги, а також невміння того, хто допомагає, надати кваліфіковану допомогу, призводить до загибелі людини, яка знаходиться під дією струму.

При звільненні потерпілих від струмопровідних частин або проводу в електроустановках напругою до 1000 В відключають струм, використовуючи сухий одяг, палицю, дошку, шапку, сухі рукавиці, рукав одягу, діелектричні рукавиці. Провідники перерізають інструментом з ізольованими ручками, перерубують сокирою з дерев'яним сухим топорищем [21].

Потерпілого можна також відтягнути від струмопровідних частин за одяг, уникаючи дотику до навколишніх металевих предметів та до відкритих частин тіла потерпілого. Відтягуючи потерпілого за ноги, не можна торкатися його взуття, оскільки воно може бути сирим і стає провідником електричного струму. Той, хто надає допомогу, повинен одягнути діелектричні рукавиці або обмотати їх шарфом, натягнути на них рукав піджака або пальта. Можна також ізолювати себе, ставши на гумовий килимок, суху дошку.

Після звільнення потерпілого від дії струму потрібно відразу ж надати йому необхідну медичну допомогу. Виділяють три стани людського організму внаслідок дії електроструму:

– I стан – потерпілий при свідомості. Слід забезпечити повний спокій, 2-3 годинне спостереження, виклик лікаря.

– II стан – потерпілий непритомний, але дихає. Людину покласти горизонтально, розстебнути комір і пасок, дати нюхати нашатирний спирт, викликати лікаря.

– III стан – потерпілий не дихає або дихає з перервами, уривчасто. Роблять штучне дихання і непрямий масаж серця.

Якщо потерпілий після звільнення від дії електричного струму і надання медичної допомоги прийшов до тями, його не слід одного відправляти додому або допускати до роботи. Такого потерпілого слід доставити в лікувальний заклад, де за ним буде встановлено спостереження, так як наслідки від впливу електричного струму можуть проявитися через кілька годин і привести до більш важких наслідків.

Системний адміністратор, який обслуговує маршрутизатор для уникнення небезпеки ураження електричним струмом при роботі з ПК повинен дотримуватись правил охорони праці та техніки безпеки, особливо електробезпеки.

4.2 Оцінка роботи адміністратора маршрутизатора щодо умов безпеки, втомлюваності та продуктивності праці

Маршрутизатор на основі Raspberry PI 4 та Open WRT є автоматизованим комплексом, що забезпечує автоматичну маршрутизацію та контроль пакетів у комп’ютерній мережі. Адміністратор системи орієнтується на графіки показників трафіку і час від часу проводить спостереження та їх аналіз.

Основним принципом при виборі системи робочих рухів при використанні даної системи є принцип “економії рухів”, який сприяє підвищенню

продуктивності праці і, у той же час, зменшенню стомлюваності, кількості помилок і травматизму.

Принципи “економії рухів” полягають у наступних положеннях: обидві руки повинні починати і закінчувати рух одночасно; руки не повинні бути бездіяльними, окрім періодів відпочинку; рухи рук повинні виконуватись одночасно у протилежних і симетричних напрямках; найкращою є така послідовність дій, яка вміщує найменше число елементарних рухів; руки слід звільняти від усякої роботи, яка може успішно виконуватись ногами чи іншими частинами тіла; при можливості об'єкт праці має закріплюватись за допомогою спеціальних пристроїв, щоб руки були вільні для виконання операцій.

Робота має організовуватись так, щоб ритм робочих операцій був, за можливості, чітким та природнім, а послідовність рухів такою, щоб один рух легко переходив у інші. Рух менш стомлюючий, якщо він відбувається у напрямку, що співпадає з напрямком сили тяжіння. Різкі коливання швидкості та невеликі перерви у русі мають бути виключені.

Враховується ряд положень щодо швидкості руху рук людини: там, де вимагається швидка реакція, слід використовувати рух “до себе”; швидкість руху зліва направо для правої руки більша, ніж у зворотному напрямі; обертові рухи у 1,5 рази швидше, ніж поступальні; плавні криволінійні рухи рук швидші, ніж прямолінійні з миттєвою зміною напрямку; рухи з великим розмахом швидші; рухи, орієнтовані механізмами, швидші, ніж рухи, орієнтовані “на око”; рухи слід обмежувати обмежувачами скрізь, де це можливо.

Максимальна частота рухів руки (при згинанні та розгинанні) – біля 80; ноги – 45, корпуса – 30 раз на хвилину, а пальця – 6 раз і долоні – 3 рази на секунду [20].

Оснащення робочого місця. Оснащення та обладнання робочого місця залежить від виконуваної роботи (технологічних операцій), від характеру роботи (розумова, фізична, тяжка, монотонна) та від умов праці (комфортні, нормальні, несприятливі).

Робоче місце працівника характеризує два поля: інформаційне поле (простір із засобами відображення інформації) і моторне поле (простір з органами управління та об'єктом праці).

В інформаційному полі зорового спостереження виділяють три зони: у зоні 1 розміщують засоби відображення інформації, які використовуються дуже часто і вимагають точного та швидкого зчитування інформації; у зоні 2 – засоби інформації, які використовуються часто і вимагають менш точного і швидкого зчитування інформації; у зоні 3 – засоби відображення інформації, які використовуються рідко.

В моторному полі (рис. 4.1) теж виділяють три зони: 1 – зона оптимальної досяжності, в якій розміщують дуже важливі і дуже часто використовувані (більше 2 раз за хвилину) органи управління; 2 – зона легкої досяжності, в якій розміщують часто використовувані (2 рази за хвилину) органи управління; 3 – зона досяжності, в якій розміщують рідко використовувані (менше 2 раз за хвилину) органи управління.

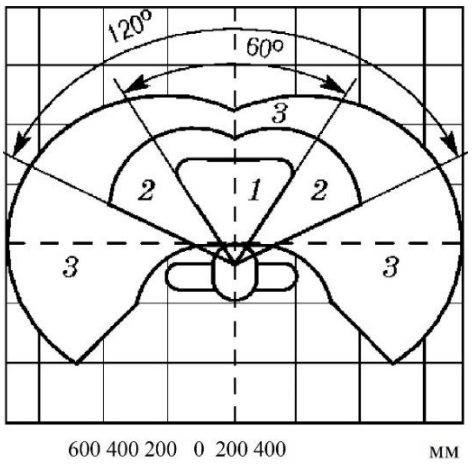

Рисунок 4.1 – Зона в моторному полі при виконанні ручних операцій та розміщення органів управління при робочій позі “сидячи”:
1 – зона оптимальної досяжності; 2 – зона легкої досяжності; 3 – зона досяжності

Вимоги виробничої санітарії до робочого місця. Кожне робоче місце повинно:

– обладнуватись необхідними засобами колективного захисту;

– укомплектовуватись необхідними засобами індивідуального захисту;

– мати достатнє природне та штучне освітлення;

– мати параметри мікроклімату відповідно до санітарних норм;

– мати вентиляцію;

– мати параметри інших санітарно-гігієнічних факторів такими, що не перевищують гранично допустимих значень відповідних нормативних документів.

Під час роботи від працівника вимагається підвищена увага, певна швидкість виконання окремих технологічних операцій, швидка переробка одержаної інформації, точна координація рухів, що може викликати перевантаження і перевтому організму та зниження працездатності. До таких же наслідків призводить і монотонна робота при виконанні спрощених одноманітних операцій у примусовому режимі та заданій позі. Таку перевтому можна зменшити створенням оптимального режиму праці і відпочинку.

Оптимальний режим праці і відпочинку досягається: паузами та перервами в роботі (для прийому їжі, обігрівання, охолодження), зміною форми роботи, зміною умов довкілля, усуненням монотонності в роботі, відпочинком у спеціальних кімнатах психологічного розвантаження і відпочинку, використанням психічного впливу музики.

Чергування праці і відпочинку встановлюють в залежності від зміни працездатності людини на протязі робочого дня. На початку зміни завжди має місце стадія наростаючої працездатності, коли відбувається відновлення робочих навичок. Тривалість цього періоду 0,5...1,5 години в залежності від характеру праці і тривалості попередньої перерви в роботі. Швидкість і точність дій у цей період невеликі. Потім настає стадія високої стійкої працездатності тривалістю до 3 годин в залежності від характеру роботи, ступеня підготовки та стану працівника. Після цього наступає стадія зменшення працездатності або стація розвитку втоми, рухи уповільнюються і увага розсіюється, сприйняття притупляється. В цей час, звичайно, роблять обідню перерву [20].

ВИСНОВКИ

У кваліфікаційній роботі розроблено проект маршрутизатора комп’ютерної мережі з використанням мінікомп’ютера Rapsberry PI 4 та прошивки Open WRT версії bcm2711.

У проекті передбачено:

– швидкість передачі даних на рівні 1 Гб/с;

– створено дві віртуальні локальні мережі;

– імплементовано сервіс блокування реклами;

– налаштовано доступ до медіа сервера;

– організовано торент-клієнт.

Усі перелічені служби і сервіси працюють у Docker-контейнерах, тобто ізольовано від інших мереж.

У роботі представлено базове налаштування Open WRT для Raspberry PI 4, визначено зони FireWall для різних віртуальних мереж і служб, що дало можливість підвищити рівень безпеки та якість надання послуг кінцевому користувачу у порівнянні з типовими маршрутизаторами серійного виробництва.

Реалізований проект маршрутизатора забезпечує високу гнучкість налаштування параметрів передачі даних, що задовольняє очікуванням користувача. Завдяки технічним характеристикам Raspberry PI 4 забезпечено високу продуктивність опрацювання та передачі даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гарасимчук О.І. Комплексні системи санкціонованого доступу: навч. посіб. Львів: Видавництво Львівської політехніки. 2010. 212 с.
2. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп’ютерні мережі. Книга 1. Львів : «Магнолія 2006», 2013. 256 с.
3. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп’ютерні мережі. Книга 2. Львів : "Магнолія 2006", 2014. 312 с.
4. Катренко А.В. Системний аналіз об’єктів та процесів комп’ютеризації Львів : Новий Світ-2000. 2013. 424 с.
5. Functional safety of electrical, electronic and programmable electronic safety related systems. International Electrotechnical Commission, IEC 61508. Parts 1 to 7. Geneva. Switzerland. 2015.
6. Safety management requirements for defence systems (part 1 and 2). Defence Standard 00-56. Ministry of Defence. Directorate of Standartization Glasgow. Issue 4. UK. June. 2007.
7. Городецька О.С., Гикавий О.В., Онищук В.А. Комп’ютерні мережі. Навчальний посібник. Вінниця: ВНТУ. 2015. 128 с.
8. Мельник І. Проектування та дослідження комп'ютерних мереж. К. : Університет «Україна», 2010. 362 с.
9. Kharchenko A., Bodnarchuk I., Yatcysyn V. The Method for Comparative Evaluation of Software Architecture with Accounting of Trade-offs. American Journal of Information Systems. 2014. Vol. 2. No. 1. P. 20-25.
10. Ткаченко В.А., Касілов О. В., Рябик В.А. Комп’ютерні мережі та телекомунікації: навч. посіб. Харків: НТУ “КПІ”. 2011. 224 с.
11. Царьов Р. Ю., Нікітюк Л.А., Царьов Р. Ю. Структуровані кабельні системи : навч. посіб. для студентів вищих навчальних закладів. Одеса : ОНАЗ ім. О.С. Попова. 2013. 260 с.
12. Raspberry Pi Access Point VPN. URL: https://forum.openwrt.org/t/raspberry-pi-access-point-vpn/45073 (дата звернення: 10.05.2024) .

13. Raspberry Pi 4B as a Router / Firewall / VPN Endpoint with OpenWRT: Success. URL: https://forums.raspberrypi.com/viewtopic.php?t=287915&sid=d7c0ed43953e8a9b41fa002d6aa6292e (дата звернення: 12.05.2024)

14. Securing Your Network with Raspberry Pi Firewalls. URL: https://www.nextpcb.com/blog/raspberry-pi-firewall (дата звернення: 18.05.2024).

15. The Ultimate Guide to Transforming Your Raspberry Pi into a Powerful Router. URL: https://www.sunfounder.com/blogs/news/the-ultimate-guide-to-transforming-your-raspberry-pi-into-a-powerful-router (дата звернення: 18.05.2024).

16. OpenVPN client using LuCI. URL: https://openwrt.org/docs/guide-user/services/vpn/openvpn/client-luci (дата звернення: 20.05.2024).

17. Паламар М.І., Стрембіцький М.О., Паламар А.М. Проектування комп'ютеризованих вимірювальних систем і комплексів. Навчальний посібник. Тернопіль: ТНТУ. 2019. 150 с.

18. IoT: від «розумних» лампочок до передових технологій виробництва / Новини / IT українською URL: http://it-ua.info/news/2016/06/21/iot-vd-rozumnih-lampochok-do-peredovih-tehnology-virobnictva.html (дата звернення 26.04.2024р.).

19. Осухівська Г.М., Тиш Є.В., Тиш Є.В., Паламар А.М. Методичні вказівки до виконання кваліфікаційних робіт здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 123 «Комп'ютерна інженерія» усіх форм навчання. Тернопіль, ТНТУ. 2022. 28 с.

20. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями». Київ. 2018.

21. Катренко Л.А., Катренко А.В. Охорона праці в галузі комп'ютинґу. Львів: Магнолія-2006. 2012. 544 с.

22. Бедрій Я. Основи охорони праці користувачів персональних комп'ютерів: навчальний посібник для студентів ВНЗ та інженерів-практиків. Навчальна книга-Богдан. 2014. 144 с.

Додаток А

Технічне завдання

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії

Кафедра комп'ютерних систем та мереж

"Затверджую"

Завідувач кафедри КС

_____ Осухівська Г.М.

"___" _____2024 р

КОМП'ЮТЕРНА СИСТЕМА ОБЛІКУ ВОДОПОСТАЧАННЯ
НА ОСНОВІ ІОТ ПРИСТРОЇВ

ТЕХНІЧНЕ ЗАВДАННЯ

на _*10*_ листках

Вид робіт: Кваліфікаційна робота

На здобуття освітнього ступеня «Бакалавр»

Спеціальність 123 «Комп'ютерна інженерія»

«УЗГОДЖЕНО»	«ВИКОНАВЕЦЬ»
Керівник кваліфікаційної роботи	Студент групи СІ-42
_____ к.т.н., доц. Яцишин В.В.	_____ Яшнюк О.І.
«____» _____ 2024 р.	«____» _____ 2024 р.

Тернопіль 2024

1 Загальні відомості

1.1 Повна назва та її умовне позначення

Повна назва теми кваліфікаційної роботи: «Маршрутизатор пакетів комп’ютерної мережі на основі Raspberry PI та Open WRT».

Умовне позначення кваліфікаційної роботи: КС КРБ 123.139.00.00

1.2 Виконавець

Студент групи СІ-42, факультету комп’ютерно-інформаційних систем і програмної інженерії, кафедри комп’ютерних систем та мереж, Тернопільського національного технічного університету імені Івана Пулюя, Яшнюк Олександр Ігорович.

1.3 Підстава для виконання роботи

Підставою для виконання кваліфікаційної роботи є наказ по університету (№4/7-408 від 24.04.2024 р.)

1.4 Планові терміни початку та завершення роботи

Плановий термін початку виконання кваліфікаційної роботи – 24.04.2024 р.

Плановий термін завершення виконання кваліфікаційної роботи – 24.06.2024 р.

1.5 Порядок оформлення та пред’явлення результатів роботи

Порядок оформлення пояснювальної записки та графічного матеріалу здійснюється у відповідності до чинних норм та правил ISO, ЕСКД, ЕСПД та ДСТУ.

Пред’явлення проміжних результатів роботи з виконання кваліфікаційної роботи здійснюється у відповідності до графіку, затвердженого керівником роботи.

Попередній захист кваліфікаційної роботи відбувається при готовності роботи на 90% , наявності пояснювальної записки та графічного матеріалу.

Пред’явлення результатів кваліфікаційної роботи відбувається шляхом захисту на відповідному засіданні ЕК, ілюстрацією основних досягнень за допомогою графічного матеріалу.

2 Призначення і цілі створення системи

2.1 Призначення системи

Маршрутизатор пакетів на основі Raspberry Pi та OpenWRT є потужним інструментом для створення та управління комп'ютерною мережею. Його призначення можна звести до декількох ключових аспектів.

Маршрутизація пакетів. Маршрутизатор виконує функцію маршрутизації, що дозволяє передавати пакети даних між різними пристроями в мережі. Використовуючи OpenWRT, він може оптимізувати маршрутизацію, враховуючи різні параметри, такі як швидкість передачі даних та стан з'єднання.

Функції мережевого проксі. Маршрутизатор може виконувати роль проксі-сервера для фільтрації та обробки мережевого трафіку. Це може включати фільтрацію веб-запитів, керування доступом до веб-сайтів, а також прискорення передачі даних за рахунок кешування.

Забезпечення безпеки мережі. Використовуючи OpenWRT, маршрутизатор може надавати різноманітні функції безпеки, такі як файрвол, VPN-з'єднання та інші механізми захисту від несанкціонованого доступу до мережі.

Можливості розширення. Через використання Raspberry Pi як базової платформи, маршрутизатор може бути легко розширений за допомогою додаткових модулів та розширень. Це може включати підтримку додаткових інтерфейсів, таких як Wi-Fi або Bluetooth, а також розвиток власних програмних рішень для специфічних потреб мережі.

Моніторинг та управління мережею. Маршрутизатор може надавати інструменти для моніторингу та управління мережевим трафіком, включаючи статистику використання, журнали активності та інші корисні функції для адміністраторів мережі.

Загалом, маршрутизатор на основі Raspberry Pi та OpenWRT є універсальним засобом для створення, управління та захисту комп'ютерних мереж з рядом додаткових можливостей розширення.

2.2 Мета створення системи

Мета створення маршрутизатора на основі Raspberry PI та Open WRT полягає у забезпеченні гнучкості функціонування комп’ютерної мережі із можливістю налаштування правил безпеки, авторизованого доступу до медіасервера, визначених правил функціонування блокувальника реклами та торент-сервісу, а також розподілу на віртуальні мережі.

Для досягнення поставленої мети потрібно розв’язати наступні задачі:

– дослідження принципів організації і типів комп’ютерних мереж;

– аналіз існуючих рішень щодо налаштування типових маршрутизаторів;

– аналіз особливостей технічних характеристик мінікомп’ютерів Raspberry PI;

– обґрунтування вибору прошивки Open WRT для функціонування на Raspberry PI як маршрутизатора;

– розробка архітектурного рішення до реалізації функцій маршрутизатора на Raspberry PI;

– налаштування базової конфігурації Open WRT;

– створення віртуальних мереж для локальної і глобальної мереж;

– налаштування маршрутизації пакетів та правил безпеки у комп’ютерній мережі;

– розробка схема підключення портів як для зовнішніх так і для віртуальних пристроїв;

– налаштування та розгортання Docker-контейнерів з блокувальником реклами, торент-сервісом та медіа-сервером.

2.3 Характеристика об'єкту

Маршрутизатор на базі Raspberry Pi 4 з використанням операційної системи OpenWRT пропонує низку переваг та характеристик, які роблять його привабливим в якості рішення для створення мережі.

Висока продуктивність: Raspberry Pi 4 має потужний 4-ядерний процесор ARM Cortex-A72 з тактовою частотою до 1,5 ГГц та можливість розширення оперативної пам'яті до 8 ГБ. Це забезпечує швидку обробку мережевого трафіку та виконання різноманітних мережевих завдань.

Підтримка бездротового зв'язку: Raspberry Pi 4 має вбудований модуль Wi-Fi 802.11ac та можливість підключення антен для покращення прийому сигналу. Це дозволяє використовувати його як точку доступу Wi-Fi або розширювати бездротову мережу.

Розширені можливості зв'язку: Завдяки наявності гігабітних Ethernet-портів, USB-портів та роз'ємів GPIO, Raspberry Pi 4 може бути легко підключений до різних мережевих пристроїв, таких як маршрутизатори, комутатори, модеми тощо.

Гнучкість та розширюваність: Використання OpenWRT надає широкі можливості конфігурації та налаштування маршрутизатора згідно з потребами

користувача. Також, завдяки відкритому джерелу, можливість розробки власних програмних рішень та додатків для розширення функціоналу.

Безпека: OpenWRT відомий своєю активною спільнотою та швидкими оновленнями безпеки. Це дозволяє забезпечувати високий рівень захисту для мережі, включаючи FireWall, VPN, механізми виявлення вторгнень та інші засоби захисту.

Енергоефективність: Raspberry Pi 4 має низьке споживання енергії, що дозволяє економити кошти на електроенергії при постійному використанні.

В цілому, маршрутизатор на базі Raspberry Pi 4 з OpenWRT - це потужне та гнучке рішення для створення та управління комп'ютерною мережею з високим рівнем продуктивності та безпеки.

3 Вимоги до системи

3.1 Вимоги до системи в цілому

Вимоги до маршрутизатора пакетів комп’ютерної комп’ютерної мережі на основі Raspberry PI та Open WRT можуть бути сформульовані наступним чином:

Блокування реклами:

– забезпечення можливості фільтрації трафіку для блокування рекламних матеріалів на різних пристроях у мережі.

– підтримка списків доменів для блокування реклами за допомогою відомих інструментів, таких як Pi-hole або AdGuard.

Торент-клієнт:

– можливість встановлення торент-клієнта для завантаження та обміну файлами через протокол BitTorrent.

– інтеграція з іншими мережевими сервісами та можливість планування завантажень.

Медіасервер:

– підтримка створення медіасервера для зберігання та потокової передачі мультимедійного контенту по мережі.

– відтворення мультимедійних файлів на різних пристроях, таких як смартфони, планшети, телевізори тощо.

Підтримка VLAN:

– можливість налаштування та управління віртуальними локальними мережами для ізоляції трафіку між різними частинами мережі.

– підтримка тегування та розмітки пакетів для ефективного управління VLAN.

Інтерфейс користувача:

– наявність зручного веб-інтерфейсу для конфігурування та управління всіма функціями маршрутизатора.

– можливість легкого доступу до налаштувань служб блокування реклам, торент-клієнта, медіасервера та VLAN.

Безпека:

– забезпечення захисту мережі від потенційних загроз та несанкціонованого доступу.

– підтримка механізмів шифрування та аутентифікації для забезпечення конфіденційності та цілісності даних.

Ці вимоги дозволять створити маршрутизатор, який буде не лише забезпечувати потрібні функції мережі, але й буде гнучким та легко налаштовуваним під потреби користувача.

3.1.1 Вимоги до способів та засобів зв’язку між компонентами системи

Вимоги до способів та засобів зв'язку між компонентами маршрутизатора на базі Raspberry Pi 4 та OpenWRT можуть бути наступними:

Підтримка Ethernet з'єднання – забезпечення можливості підключення до локальної мережі за допомогою Ethernet-кабелю для передачі даних між маршрутизатором та іншими пристроями.

Підтримка бездротового з'єднання – підтримка Wi-Fi для створення бездротової мережі та підключення до неї різних пристроїв, що дозволить розширити зону покриття мережі.

Наявність USB-інтерфейсів – використання USB-портів для підключення додаткових мережевих пристроїв, таких як модеми, адаптери Wi-Fi або зовнішні сховища даних.

Внутрішня шина даних (Internal Data Bus) – абезпечення ефективної внутрішньої комунікації між компонентами маршрутизатора, такими як процесор, оперативна пам'ять та різні модулі обробки даних.

SPI, I2C, GPIO – використання протоколів SPI (Serial Peripheral Interface), I2C (Inter-Integrated Circuit) та GPIO (General Purpose Input/Output) для зв'язку з різними периферійними пристроями та розширення функціоналу маршрутизатора.

Підтримка мережевих протоколів – забезпечує обмін даними з іншими пристроями у мережі з використанням протоколів TCP/IP, UDP, HTTP, HTTPS тощо.

Внутрішні мережеві інтерфейси (Internal Network Interfaces) – наявність внутрішніх мережевих інтерфейсів для забезпечення комунікації між різними компонентами програмного забезпечення маршрутизатора та службами.

Ці вимоги забезпечують необхідну гнучкість та ефективність у забезпеченні зв'язку між різними компонентами маршрутизатора, що дозволяє йому ефективно виконувати свої функції у мережі.

3.1.2 Вимоги по діагностуванню системи

Діагностика маршрутизатора пакетів комп’ютерної мережі на основі Raspberry PI та Open WRT повинна здійснюватися у відповідності до графіку регламентних робіт та у випадку збою функціональності або відсутності комунікації між

пристроями. Діагностичні процедури при цьому передбачають проведення перевірки працездатності апаратної і програмної складової системи.

На апаратному рівні проводяться перевірки щодо встановлення відповідності технічних характеристик Raspberry PI. При цьому можуть застосовуватися зовнішні вимірювальні пристрої.

На програмному рівні доцільно проводити тестування кожного окремого компоненту, а також перевірку системи в цілому.

3.1.3 Перспективи розвитку, модернізація системи

Перспективи розвитку та модернізації маршрутизатора на базі Raspberry Pi 4 та OpenWRT можуть бути наступними:

Підвищення продуктивності: з розвитком технологій можна очікувати випуску більш потужних версій Raspberry Pi або оптимізації програмного забезпечення, що дозволить підвищити загальну продуктивність маршрутизатора.

Розширення функціональності: можливість додати нові функції та сервіси до маршрутизатора, такі як додаткові мережеві протоколи, захист від DDoS-атак, підтримка мережевих стандартів нового покоління тощо.

Підвищення безпеки: інтеграція нових механізмів безпеки для захисту мережі від нових загроз та атак, таких як мережеві вразливості, вторгнення та шкідливе програмне забезпечення.

Підтримка нових технологій зв'язку: інтеграція підтримки нових стандартів бездротового зв'язку, таких як Wi-Fi 6 або 5G, для підвищення швидкості та ефективності бездротової мережі.

Розширення можливостей VLAN та мережевого сегментації: покращення можливостей управління мережевими сегментами та підтримка більшої кількості VLAN для підвищення безпеки та ефективності мережі.

Оптимізація споживання енергії: розвиток ефективних методів управління енергоспоживанням для зменшення впливу на довкілля та зниження витрат на електроенергію.

Підтримка IoT та домашніх мереж: інтеграція засобів для підтримки Інтернету речей (IoT) та розвиток функцій для управління домашньою мережею, включаючи підтримку розумних пристроїв та автоматизацію.

Розвиток маршрутизатора на основі Raspberry Pi 4 та OpenWRT залежить від швидкості розвитку апаратних та програмних технологій, а також від потреб користувачів у нових функціях та можливостях.

3.1.4 Вимоги до надійності системи

Надійність маршрутизатора на основі Raspberry Pi 4 та OpenWRT є критично важливою для забезпечення безперебійної роботи комп'ютерної мережі. Ось деякі вимоги до надійності:

Стійкість до відмов (Fault Tolerance): маршрутизатор повинен мати механізми автоматичного відновлення в разі виникнення помилок апаратного та програмного забезпечення. Окрім цього, повинна бути можливість забезпечити резервування ключових компонентів, таких як жорсткий диск або карта пам'яті, для запобігання втраті даних.

Стабільність роботи (Stability): зниження ймовірності виникнення системних збоїв шляхом підтримки стабільних версій програмного забезпечення та регулярного оновлення, а також тестування та валідація нових версій програмного забезпечення перед їх впровадженням у виробниче середовище.

Автоматизація відновлення (Automated Recovery): реалізація механізмів автоматичного відновлення роботи маршрутизатора після перебоїв у роботі, наприклад, перезавантаження системи або відновлення налаштувань за замовчуванням. Виявлення та автоматичне усунення помилок в мережі для забезпечення безперебійної роботи.

Резервне копіювання (Backup): можливість створення та відновлення резервних копій конфігурацій маршрутизатора для швидкого відновлення роботи після втрати даних або несправностей.

Моніторинг та журналювання (Monitoring and Logging): реалізація системи моніторингу та журналювання подій для виявлення відмов та аналізу причин їх виникнення. Також важлвим є формування повідомлень адміністратору про критичні події або відмови для оперативного реагування на проблеми.

Фізична безпека (Physical Security): забезпечення захисту маршрутизатора від фізичних впливів, таких як випадкові пошкодження або зловмисні вторгнення.

Надійність маршрутизатора на базі Raspberry Pi 4 та OpenWRT є ключовою у забезпеченні стабільної та безперебійної роботи мережі, особливо в критичних виробничих або бізнес-середовищах.

3.1.5 Вимоги до функцій та задач, які виконує система

Основними функціями до маршрутизатора пакетів у комп'ютерній мережі на основі Raspberry PI та Open WRT є надання послуг типового роутера, однак з можливістю налаштування VPN, поділу на VLAN, розгортанням Docker-контейнерів із сервісами та службами блокування реклами, торент-клієнта та медіа-сервера.

3.1.6 Вимоги до апаратного забезпечення

Апаратне забезпечення маршрутизатора базується лише на Raspberry PI 4 і використовує зовнішній пристрої локальної комп'ютерної мережі, зокрема:

– NetGear GS108PE – 8-ми портовий керований комутатор;

– TL-WA1201 – точка доступу від TP-Link, яка підключається до 5-го порта комутатора, що не є PoE портом;

– Модем – підключається як резервний пристрій доступу до мережі Internet.

3.1.7 Вимоги до програмного забезпечення

Вимогами до програмного забезпечення при реалізації маршрутизатора на основі Raspberry PI 4 та Open WRT є операція система Open WRT версії bcm2711, пакети Docker, PiHole, Transmission та Plex

4 Вимоги до документації

Документація повинна відповідати вимогам ЄСКД та ДСТУ

Комплект документації повинен складатись з:

– пояснювальної записки;

– графічного матеріалу:

1 Види і характеристика комп’ютерних мереж.

2 Типова організація VPN-мережі.

3 Структурна схема типового маршрутизатора

4 Інфраструктура мережі на основі Raspberry PI та Open WRT.

5 DNS через HTTPS при налаштуванні блокувальника реклами.

*Примітка: У комплект документації можуть вноситися міни та доповнення в процесі розробки.

5 Стадії та етапи проектування

Таблиця 1 – Стадії та етапи виконання кваліфікаційної роботи бакалавра

№ Етапу	Назва етапу виконання кваліфікаційної роботи	Термін виконання
1	Розробка і затвердження технічного завдання	24.04-28.04.2024
2	Аналіз технічного завдання	28.04-02.05.2024
3	Аналіз типів комп’ютерних мереж та ролі маршрутизаторів	02.05-05.05.2024
4	Проектування та налаштування маршрутизатора на Raspberry PI 4 з Open WRT	05.05-10.05.2024
5	Налаштування служб і сервісів маршрутизатора на базі Raspberry PI	10.05-25.05.2024
6	Розробка інструкцій щодо використання маршрутизатора	25.05-29.05.2024
7	Безпека життєдіяльності, основи охорони праці	01.06-05.06.2024
8	Оформлення кваліфікаційної роботи	05.06-12.06.2024
9	Попередній захист кваліфікаційної роботи	12.06-17.06.2024
10	Захист кваліфікаційної роботи	24.06-27.06.2024

6 Додаткові умови виконання кваліфікаційної роботи

Під час виконання кваліфікаційної роботи у дане технічне завдання можуть вноситися зміни та доповнення.