

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 наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр

(назва освітнього ступеня)

на тему: Підвищення ефективності комп'ютерної мережі
на основі топології Mesh

Виконав: студент VI курсу, групи СНнм-61
спеціальності 122 Комп'ютерні науки
(шифр і назва спеціальності)

(підпис) Коваленко О.С.
(прізвище та ініціали)

Керівник _____
(підпис) Готович В.А.
(прізвище та ініціали)

Нормоконтроль _____
(підпис) Мацюк О.В.
(прізвище та ініціали)

Завідувач кафедри _____
(підпис) Боднарчук І.О.
(прізвище та ініціали)

Рецензент _____
(підпис) Михайлишин Р.І.
(прізвище та ініціали)

Тернопіль
2021

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 наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

«__» _____ 2021 р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

на здобуття освітнього ступеня _____ Магістр
(назва освітнього ступеня)

за спеціальністю _____ 122 Комп'ютерні науки
(шифр і назва спеціальності)

Студенту _____ Коваленко Олегу Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Підвищення ефективності комп'ютерної мережі на основі топології Mesh

Керівник роботи _____ Готович Володимир Анатолійович, доц. кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «__» _____ 2021 року № _____

2. Термін подання студентом завершеної роботи _____ 2021р.

3. Вихідні дані до роботи _____ Наукові літературні джерела

4. Зміст роботи (перелік питань, які потрібно розробити)

Вступ. 1 Аналіз наукових публікацій. 2. Загальні принципи проектування та технічні вимоги до обладнання безпроводних Mesh мереж 3. Розробка проекту Mesh-мережі. 4. Безпека життєдіяльності та основи охорони праці. Висновки. Перелік джерел. Додатки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Стадник І. Я., професор		
Охорона праці	Дмитроца Л. П., доцент		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	21.10.2020 – 28.10.2020	<i>Виконано</i>
2.	Аналіз літературних джерел	22.12.2020 – 10.01.2021	<i>Виконано</i>
3.	Аналіз предмету дослідження та обґрунтування актуальності роботи	11.01.2021 – 21.02.2020	<i>Виконано</i>
5.	Оформлення розділу «Аналіз наукових публікацій»	22.02.2021 – 01.03.2021	<i>Виконано</i>
6.	Оформлення розділу «Загальні принципи проектування та технічні вимоги до обладнання безпроводних Mesh мереж»	02.03.2021 – 11.03.2021	<i>Виконано</i>
7.	Оформлення розділу «Розробка проекту Mesh-мережі»	02.03.2021 – 11.03.2021	<i>Виконано</i>
8.	Виконання завдання до підрозділу «Безпека життєдіяльності»	12.03.2021 – 20.03.2021	<i>Виконано</i>
9.	Виконання завдання до підрозділу «Основи хорони праці»	21.03.2021 – 28.03.2021	<i>Виконано</i>
10.	Нормоконтроль	30.04.2021 – 06.05.2021	<i>Виконано</i>
11.	Перевірка на плагіат	07.05.2021	<i>Виконано</i>
12.	Попередній захист кваліфікаційної роботи	10.05.2021	<i>Виконано</i>
13.	Захист кваліфікаційної роботи	25.05.2021	<i>Виконано</i>

Студент

_____ (підпис)

Коваленко О.С.

_____ (прізвище та ініціали)

Керівник роботи

_____ (підпис)

Готович В.А.

_____ (прізвище та ініціали)

АНОТАЦІЯ

Підвищення ефективності комп'ютерної мережі на основі топології Mesh // Кваліфікаційна робота освітнього рівня «Магістр» // Коваленко Олег Сергійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНм-61// Тернопіль, 2021 // С. , рис. , табл. , кресл. , додат. , бібліогр. .

Ключові слова: КОМП'ЮТЕРНІ МЕРЕЖІ, MESH МЕРЕЖА, ПРОТОКОЛ OLSR, ТОПОЛОГІЯ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ FREIFUNK, DD-WRT.

Кваліфікаційна робота присвячена розв'язання задач для підвищення ефективності доступу споживачів до інформації за рахунок використання комп'ютерної мережі, побудованої на основі топології Mesh.

Основним завданням кваліфікаційної роботи є проектування та налаштування конкретної Mesh-мережі.

У розділі охарактеризовано поняття Mesh-мережі та її роль в суспільстві.

В першому розділі кваліфікаційної роботи розглянуто наукові публікації по темі дослідження. Охарактеризовано поняття Mesh-мережі та її роль в суспільстві. Розглянуто найбільш розповсюджені технічні засоби реалізації Mesh-мережі.

В другому розділі розглянуто загальні принципи проектування та технічні вимоги до безпроводних Mesh-мереж. Сформульовано вимоги до програмного та апаратного забезпечення.

В третьому розділі розроблено проект конкретної Mesh-мережі. Здійснено вибір типу топології, розподіл каналів, розподіл IP адрес. Проведено налаштування Mesh-мережі.

В четвертому розділі опрацьовано питання охорони праці та безпеки життєдіяльності.

ANNOTATION

Efficiency increase of topology Mesh-based computer network // Diploma thesis Master degree // Kovalenko Oleh Sergiyovych // Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science, group SNnm-61 // Ternopil, 2020 // P. , Fig. – , Tables , References , Annexes .

Keywords: COMPUTER NETWORKS, MESH NETWORK, OLSR, TOPOLOGY, INDICATORS, FREIFUNK, DD-WRT.

Qualification work is devoted to solving problems to improve the efficiency of consumer access to information through the use of a computer network based on the Mesh topology.

The main task of the qualification work is the design and configuration of a specific Mesh-network.

The section describes the concept of Mesh-network and its role in society.

In the first section of the qualification work scientific publications on the research topic are considered. The concept of Mesh-network and its role in society is described. The most widespread technical means of realization of Mesh-network are considered.

The second section discusses the general principles of design and technical requirements for wireless Mesh networks. Requirements for software and hardware are formulated.

In the third section the project of a concrete Mesh-network is developed. The choice of topology type, channel distribution, IP address distribution is made. Mesh network settings have been set up.

The fourth section deals with the issues of labor protection and life safety.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

BSSID – (англ. Basic Service Set Identifier) – Ідентифікатор базового набору послуг.

COPM – (англ. Canadian Occupational Performance Measure) комплекс технічних засобів.

DHCP – (англ. Dynamic Host Configuration Protocol) – протокол динамічної конфігурації хосту.

DNS – (англ. Domain Name System) – система доменних імен.

ESSID – (англ. Service Set Identifier) – Розширений ідентифікатор набору послуг.

GPS – (англ. Global Positioning System) – система глобального позиціонування.

IP – (англ. Internet Protocol) – інтернет протокол.

IEEE 802.11 – мережевий протокол.

LAN – (англ. Local Area Network) – локальна мережа.

MAC – (англ. Media Access Control) – керування доступом.

OLSR – (англ. Optimized Link State Routing) – протокол маршрутизації.

PC – (англ. Personal Computer) – персональний комп'ютер.

RFC – (англ. Request for comment) – інформаційний документ.

SSH – (англ. Secure SHell) – безпечна оболонка.

SSID – (англ. Service Set Identifier) – найменування бездротової мережі.

VSAT – (англ. Very small aperture terminal) – мала супутникова наземна станція.

VoIP – (англ. Voice over internet protocol) – технологія передачі медіа-даних.

WAN – (англ. Wide Area Network) – глобальна мережа.

WAP – (англ. Wireless Access Point) – точка бездротового доступу.

WMN – (англ. Wireless Mesh Network) – безпроводна меш мережа.

WiMAX (англ. Worldwide Interoperability for Microwave Access) - стандарт бездротового зв'язку.

ЗМІСТ

ВСТУП.....	9
1 АНАЛІЗ НАУКОВИХ ПУБЛІКАЦІЙ.....	11
1.1 Загальні поняття та роль Mesh-мережі в суспільстві майбутнього.	11
1.2 Актуальність Mesh-мереж.....	12
1.3 Протокол 802.11	13
1.4 Область застосування Mesh-мереж	16
1.5 Протоколи для організації Wi-Fi Mesh	18
1.6 Ad Hoc мережі	19
1.7 Мобільна Ad Hoc мережа	20
1.8 Застосування Ad Hoc мережі в домашніх умовах	21
1.9 Висновки до першого розділу.....	22
2 ЗАГАЛЬНІ ПРИНЦИПИ ПРОЕКТУВАННЯ ТА ТЕХНІЧНІ ВИМОГИ ДО ОБЛАДНАННЯ БЕЗПРОВІДНИХ MESH-МЕРЕЖ.....	23
2.1 Проблема підключення до інтернету в сільській місцевості.....	23
2.2 Загальні принципи проектування безпроводної Mesh-мережі.....	24
2.2.1 Mesh-мережа	24
2.2.2 Вузол безпроводної мережі.....	25
2.2.3 Точка безпроводного доступу	25
2.2.4 Переваги безпроводних мереж	25
2.2.5 Принципи функціонування безпроводної мережі	26
2.2.6 Особливості проектування Mesh-мережі.....	27
2.3 Необхідне апаратне та програмне забезпечення.....	28
2.3.1 Вимоги до апаратного забезпечення	28
2.3.2 Вимоги до програмного забезпечення	29
2.5 Проблеми проектування Mesh-мереж.....	30
2.5.1 Архітектурне проектування мережі	30
2.5.2 «Плоска» безпроводна мережа	30
2.5.3 Ієрархічна Mesh-мережа	31

2.5.4 Гібридна Mesh-мережа	32
2.6 Висновки до другого розділу	33
3 РОЗРОБКА ПРОЕКТУ MESH-МЕРЕЖІ	34
3.1 Складання карти мережі	34
3.2 Вибір типу топології мережі	35
3.3 Розподіл каналів для Mesh-мережі	38
3.4 Розподіл каналів для домашніх користувачів	39
3.5 Планування розподілу IP-адрес	40
3.6 Планування процесу побудови мережі Mesh	42
3.7 Підготовка вузла безпроводної мережі.....	43
3.8 Встановлення програмного забезпечення Freifunk, її оновлення та налаштування	45
3.9 Налаштування системи Freifunk	46
3.10 Налаштування LAN для Mesh-мережі	47
3.11 Протокол OLSR та його налаштування	49
3.12 Налаштування OLSR на приєднання до двох різних Mesh-мереж	50
3.13 Налаштування програмного забезпечення	50
3.14 WAN та його налаштування.....	52
3.15 Прив'язка вузла мережі та точки доступу «спиною до спини»	52
3.16 Оновлення програмного забезпечення до DD-WRT та налаштування ...	53
3.17 Обслуговування мережі	55
3.18 Висновок до третього розділу	56
4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ ТА ОСНОВИ ОХОРОНИ ПРАЦІ	58
4.1 Питання щодо безпеки життєдіяльності	58
4.2 Охорона праці	60
4.3 Висновки до четвертого розділу	64
ВИСНОВКИ.....	65
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ	66
ДОДАТКИ	

ВСТУП

Актуальність теми роботи. У сучасному світі інформація представляє величезну цінність, а її своєчасне отримання є завданням першорядної важливості. Для доступу до неї і створення глобального інформаційного простору використовуються комп'ютерні мережі передачі даних. В умовах постійно зростаючих вимог до мереж передачі даних, відбувається і розвиток засобів доступу до неї. Все частіше споживачі хочуть мати власну безпроводну мережу і бути максимально незалежними від провайдерів. Ряд мережевих проектів у всьому світі (експеримент Freifunk OLSR у Берліні, Німеччина, мережа Дхарамсала в Індії та долина Піблз у Південній Африці) продемонстрували, що громада може створити та підтримувати безпроводна Mesh-мережу та мати доступ до цілого ряду сучасних інформаційно-комунікаційних послуг. Ці послуги включають телефонію (протокол передачі голосу через Інтернет), обмін миттєвими повідомленнями, електронну пошту, доступ до Інтернету, мультимедійні послуги та надання послуг (наприклад електронне навчання). Необхідність розв'язання таких задач зумовлює актуальність даної роботи.

Метою дослідження є підвищення ефективності доступу споживачів до інформації за рахунок використання комп'ютерної мережі, побудованої на основі топології Mesh. Для досягнення поставленої мети потрібно виконати такі завдання:

1. Провести аналіз наукових публікацій по темі дослідження.
2. Проаналізувати загальні принципи проектування та технічні вимоги до апаратного забезпечення на основі Mesh-мереж.
3. Спроекувати та налаштувати конкретну Mesh-мережу.

Об'єкт дослідження: підвищення ефективності доступу споживачів до сучасних комунікаційних послуг.

Предмет дослідження: проектування та налаштування безпроводної комп'ютерної мережі, побудованої на основі топології Mesh.

Науковою новизною роботи є проектування та налаштування безпроводної мережі на основі топології Mesh для споживачів, які проживають на місцевості без доступу до комунікаційних послуг, з використанням сучасного апаратного та програмного забезпечення.

Апробація результатів кваліфікаційної роботи. Результати виконання роботи магістра представлено на двох наукових конференціях:

1. IX Міжнародна науково-технічна конференція молодих учених та студентів «Актуальні задачі сучасних технологій», на тему «Підвищення ефективності комп'ютерної мережі на основі топології Mesh»
2. VIII науково-технічна конференція «Інформаційні моделі, системи та технології», на тему «Побудова комп'ютерної мережі на основі топології Mesh»

1 АНАЛІЗ НАУКОВИХ ПУБЛІКАЦІЙ

1.1 Загальні поняття та роль Mesh-мережі в суспільстві майбутнього.

Mesh-мережі - перспективний клас широкосмугових бездротових мереж передачі мультимедійної інформації, який в найближчі роки знайде широке застосування в локальних і розподілених міських бездротових мережах, в мультимедійних сенсорних мережах і т.д.

Одним з основних недоліків в Mesh-мережі є затримка при надсиланні інформації в мережу. Проблема в тому, що вони використовують проміжні пункти передачі даних. Щоб підвищити ефективність, застосовано обмеження на кількість точок доступу в одному кластері. Також для підвищення ефективності налаштовано потужніший сигнал, ніж зазвичай, а також обмежено розмір пакету даних, щоб вони швидше передавались по мережі [1].

Один з головних принципів побудови Mesh-мережі - самоорганізація архітектури. Вона забезпечує такі можливості, як топологія мережі "кожен з кожним", стійкість при відмові окремих компонентів, масштабованість мережі, збільшення зони інформаційного покриття в режимі самоорганізації, динамічна маршрутизація трафіку, контроль стану мережі і т.д. [1, 2].

Mesh-мережі можуть бути стаціонарними або мобільними.

Вузлами мобільної мережі можуть бути кишенькові ПК, мобільні телефони і т.д. Mesh-мережі описує стандарт IEEE 802.11, зміни в якому практично не зачіпають фізичний рівень. Всі нововведення відносяться до MAC-підрівня каналного рівня.

Крім того, в стандарті 802.11 розглядаються питання маршрутизації пакетів в рамках Mesh-мережі (фактично мережевий і транспортний рівень моделі OSI), що виходить за рамки IEEE 802.11 [1, 2].

Mesh-мережі – це цілком осмислений наступний крок у розвитку бездротових мереж. В Mesh-мережі ви «сам собі провайдер», вас не можна відключити від цієї мережі, з вами не можна розірвати договір про користування

інтернетом. Також вас не можна прослухати СОРМ спецобладнанням [3].

Дана технологія вирішує наступні проблеми:

1. Дозволяє бути незалежною від провайдера.
2. Ви можете самі собі побудувати мережу з Wi-Fi роутерами і маршрутизацією.
3. Кожний новий клієнт в мережі підвищує ефективність Mesh-мережі.

Переваги і недоліки Mesh-мереж [3].

Переваги:

- при стихійних лихах дозволяє мати мережу на місці події, хоча можливо і відрізану від глобальної частини;
- деякі сучасні протоколи для будівництва Mesh-мереж гарантують шифрування всього трафіку який проходить через мережу;
- динамічна, авто-налаштовувана маршрутизація;
- можливість об'єднувати Mesh-мережі через звичайний інтернет.

Недоліки:

- Ефективна робота досягається тоді, коли в мережі багато користувачів;
- Негарантована ширина каналу.

Перейдемо до актуальності мережі на основі топології Mesh.

1.2 Актуальність Mesh-мереж

Mesh-мережі можуть інтегруватися в різні мережеві системи і радіотехнології. Найрозповсюдженіший на сьогоднішній день стандарт безпроводного з'єднання пристроїв - Wi-Fi. Тому і самі Mesh-мережі будуються в основному на цій технології. Використовуються такі мережі переважно для організації локальних (LAN) та міських (MAN) мереж [4]. Особлива актуальність Mesh-мереж визначається розвитком мікроелектроніки, появою багатьох різних пристроїв, здатних працювати автономно довгий час, а також мають особливість багатократної зміни режиму (Online - знаходження в мережі та offline - виходу з

мереж) та потребують обміну інформацією зі своїм оточенням, а можливо і з керуючим або інформаційним центром [5].

Таким чином, можна завжди залишатися на зв'язку в місцях, де відсутня мережева інфраструктура. Це може виявитись досить корисно в районах підвищеного ризику (де вимушені працювати спеціальні бригади), в місцях дикої або неосвоєної природи (де проводять дослідження вчені, археологи, геологи, туристи) та віддалених населених пунктів, де абсолютно кожний абонентський пристрій (наприклад, смартфон місцевого жителя або станція, встановлена в транспортному засобі участкового) може приймати участь у процесі передачі важливої інформації до адресата [7]. За замислом, у повноцінних Mesh-мережах неможна перехватити трафік і заборонити поширення інформації. Це, у свою чергу, може перечити державному закону конкретній країні або регіону. В той же час, державні структури та військові за цими ж самими причинами зацікавлені в освоєнні та організації подібних мереж [8].

1.3 Протокол 802.11

Даний протокол є найбільш підходящим для побудови Mesh-мережі. Саме його було використано в даній кваліфікаційній роботі.

Ця технологія використовується в таких областях, як безпроводний доступ в інтернеті, безпроводне телебачення. Різні стандарти сімейства Wi-Fi визначають фізичний рівень (PHY) та рівень управління доступом до середовища (каналу) MAC (Medium Access Control).

У існуючих мережах стандарту 802.11 термінальні (абонентські, кінцеві) станції (STA) пов'язані з точками доступу (Точка доступу - AP) і можуть взаємодіяти тільки з ними. AP має вихід у інші мережі (наприклад, Ethernet), але не можуть обмінюватися інформацією одне з одним (рисунок 1.1) [9].

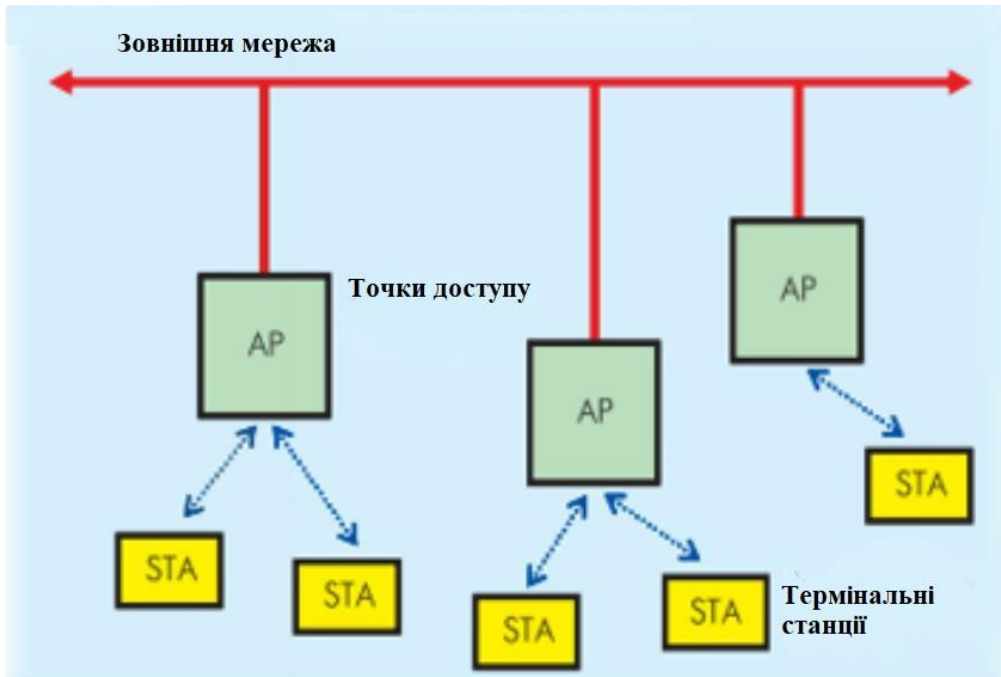


Рисунок 1.1 – Стандарт 802.11

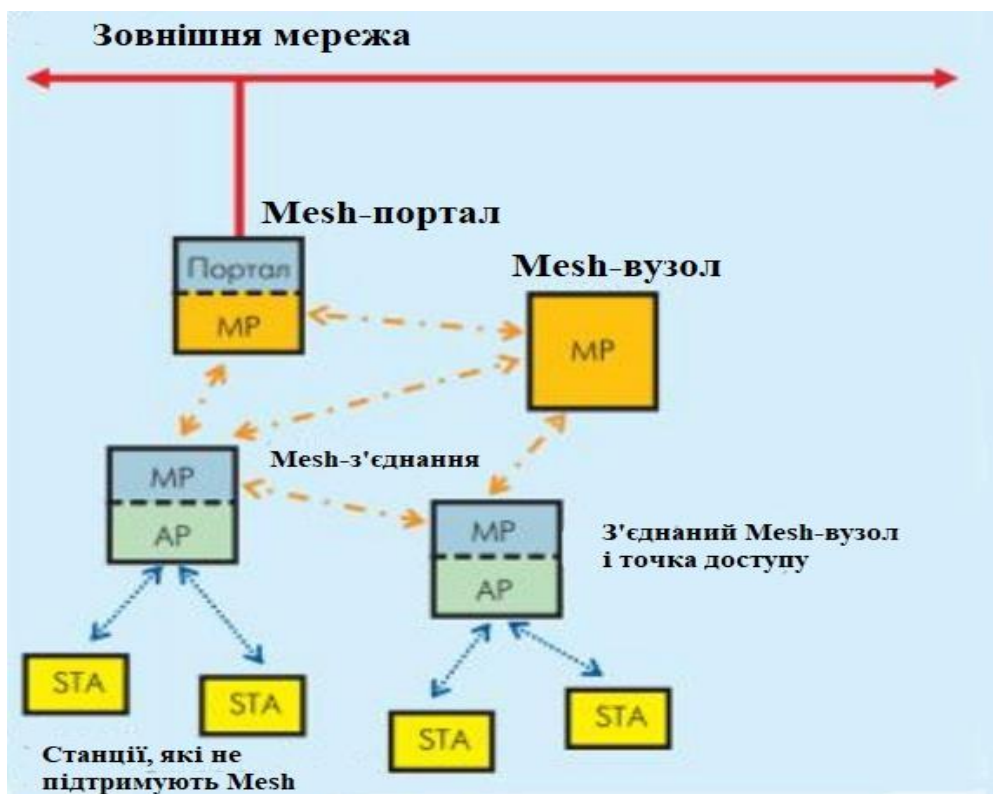


Рисунок 1.2 – Вузли Mesh-мережі

У Mesh-мережі, на відміну від термінальних станцій і точок доступу, є також особливі пристрої - вузли Mesh-мережі (Mesh Point - MP), здатні

взаємодіяти один з одним та підтримувати мережеві служби (рисунок 1.2) [9].

Один пристрій може з'єднувати між собою декілька функцій. Так, вузли Mesh-мережі, сумісні з точками доступу, називаються точками доступу Mesh-мережі (Точка доступу Mesh, MAP). Портали Mesh-мереж (Mesh Point Portal, MPP), що є MP, з'єднують Mesh-мережу з зовнішніми мережами. Таким чином, Mesh-мережа з точки зору інших пристроїв і протоколів більш високого рівня функціонально еквівалентна широкої Ethernet-мережі, усі вузли якої безпосередньо з'єднані на каналному рівні. Відмітимо, що зміни у стандартах IEEE 802.11 практично не зачіпають фізичний рівень. Всі нововведення відносяться до MAC-підрівня каналного рівня. Крім того, у стандартах 802.11 розглядають питання маршрутизації пакетів у рамках Mesh-мереж (фактично – мережевий та транспортний рівень моделей OSI), що виходить початкові рамки IEEE 802.11.

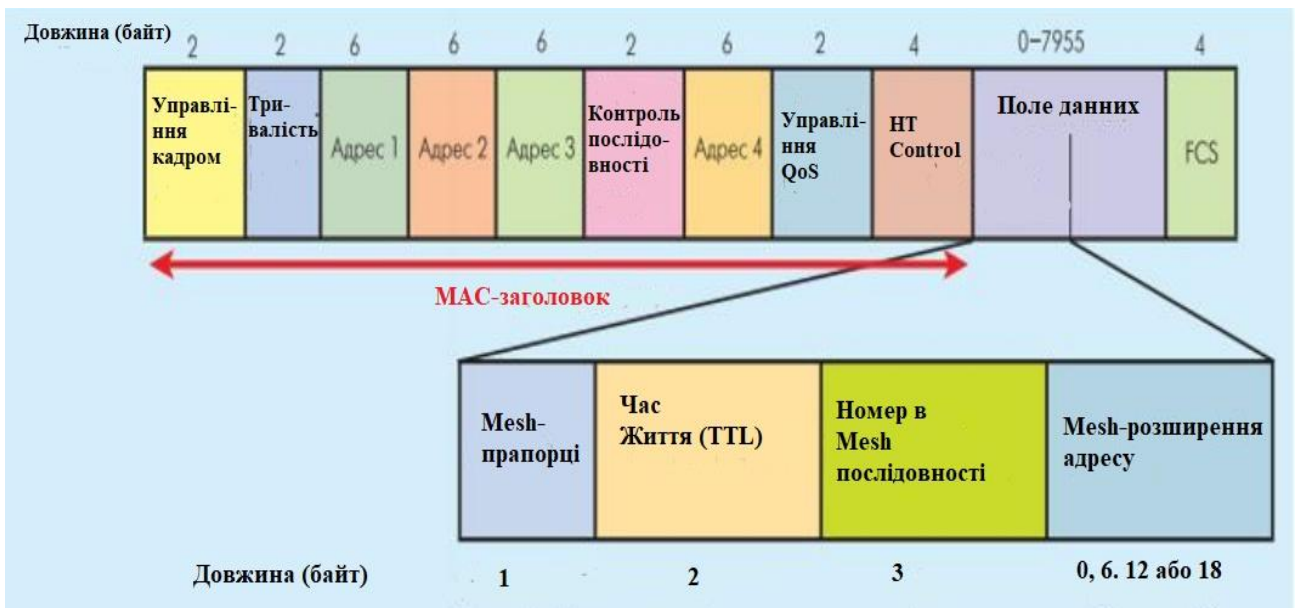


Рисунок 1.3 – Структура пакетів MAC-рівня в Mesh-мережі

Питання маршрутизації пакетів у Mesh-мережах ми роздивимось вище (рисунок 1.3), зосередившись на особливостях MAC-рівня [9].

1.4 Область застосування Mesh-мереж

Бездротові технології доступу дозволяють вирішити проблему доставки послуги абоненту. Ця задача може бути реалізована з використанням двох перспективних систем, система рівня району - Wi-Fi Mesh, система міського масштабу – WiMAX [10].

WiMAX є централізованою системою, заснованою на створенні базових станцій, які концентрують трафік з відповідного сектора в одній точці. Однак при використанні цієї технології мобільність абонентських пристроїв майже відсутня. Технологія Mesh (стандарт IEEE 802.11) дозволяє повністю децентралізувати архітектуру мережі та збільшити зону її дії. Ціль розробки стандарту IEEE 802.11 - забезпечення автоматичної маршрутизації між вузлами мережі Wi-Fi, в якій кожен вузол для передачі інформації, здатен задіяти з'єднання, використовуючи стрибучий (multi-hop) механізм перерозподілу трафіку і не більше 5% пропускної можливості каналу. Стандарт регламентування IEEE 802.11 – регламентує протоколи виявлення, ідентифікації та встановлення з'єднань між сусідніми пристроями.

Сукупність пристроїв, що працюють в мережах по стандарту IEEE 802.11, формує Mesh-мережу. Таким чином, реалізується концепція поступового росту та захоплення нових територій міста за допомогою розподільчої мережі. Почавши розвиток мережі в одній точці, в ідеалі можна безкінечно збільшувати зону її дії, просто додаючи нові пристрої. Прокладки додаткових комунікацій не потрібно.

Системи WiMAX і Wi-Fi Mesh мають різний підхід до побудови міської мережі - від глобального охоплення до поступового розвитку. Вони повинні доповнити один одного, а не конкурувати між собою. WiMAX призначена забезпечити транспорт даних у райони скупчення абонентів, а Wi-Fi Mesh має виконувати охоплення обладнаних, наприклад «спальних», мікрорайонів. Висока мобільність Mesh-мереж дозволяє використовувати їх у конкретних ситуаціях, наприклад для створення систем зв'язку між ключовими об'єктами міської

інфраструктури, розгортання мереж для екстрених служб у місцях, де немає вільного доступу до глобальної мережі. Плюси такої реалізації очевидні: всі мобільні об'єкти мають можливість бути на зв'язку незалежно від місцезнаходження, швидкості пересування і т.д. А швидке сповіщення в такій мережі забезпечить швидке реагування і відповідно більш високий рівень безпеки [11].

Приклад використання такої мережі показаний далі (рисунок 1.4).

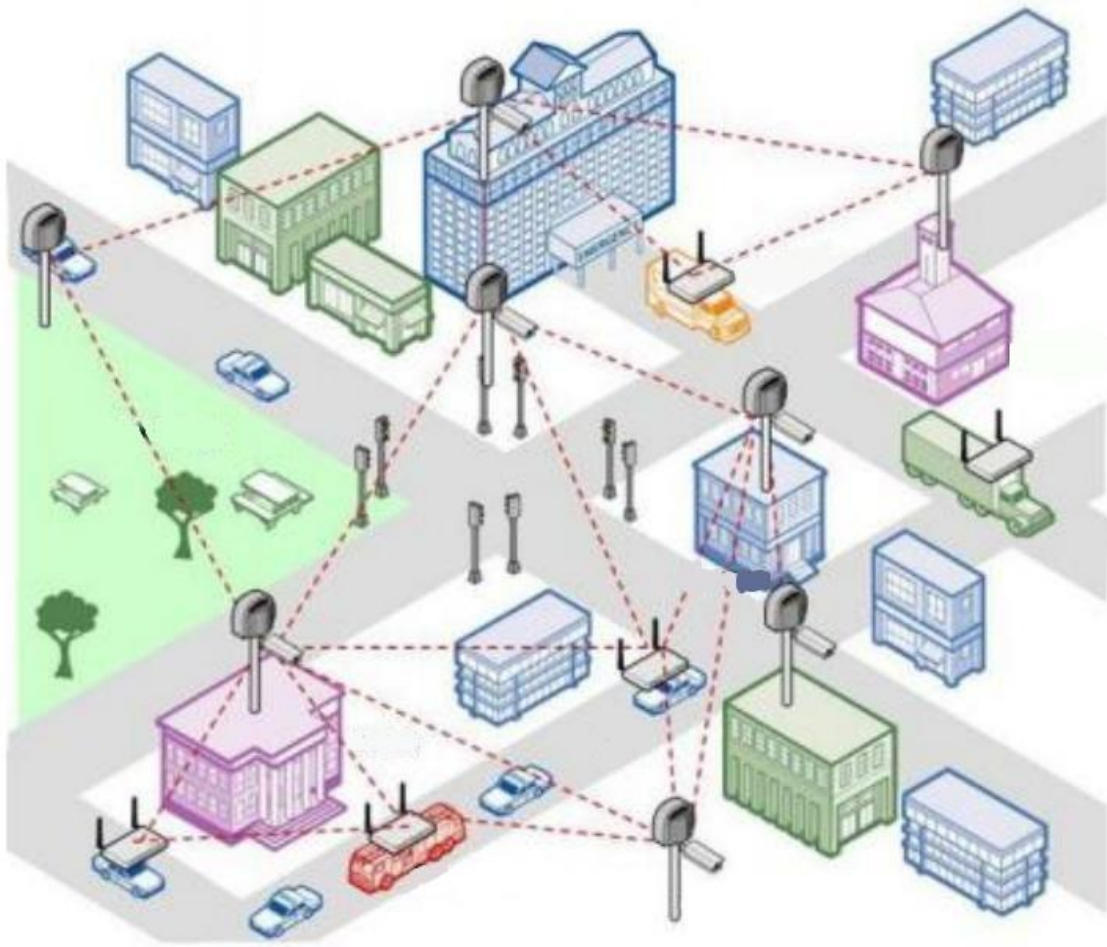


Рисунок 1.4 – Міська інфраструктура, з'єднана між собою Mesh-мережею

Ця мережа допоможе не тільки важливим структурам таким як пожежна, поліція, але й звичайним громадянам.

1.5 Протоколи для організації Wi-Fi Mesh

В теперішній час найпопулярніші протоколи для організації Wi-Fi Mesh мереж це:

- CJDNS

Cjdns - це зашифрована IPv6 мережа. У даній мережі використовуються ключі шифрування, щоб присвоїти публічні адреси. Це дає змогу створювати мережі з дуже простими налаштуваннями, які будуть захищені від потенційних проблем нині існуючих IPv4 і IPv6 мереж [11, 12].

- B.A.T.M.A.N.

B.A.T.M.A.N. - протокол маршрутизації, який є розробкою Freifunk, як заміна OLSR.

- DTN

Delay-tolerant networking (мережа стійка до розривів) - це новий підхід до мережевої архітектури комп'ютера, який спрямований на вирішення технічних питань у гетерогенних мережах, які не мають постійного підключення до мережі.

- Netsukuku

NETSUKUKU - проект створення розподіленої самоорганізованої тимчасової мережі, здатної забезпечити взаємодію великої кількості вузлів при мінімальному навантаженні на центральний процесор і пам'ять. У такій мережі можливо забезпечення підвищеної відмовостійкості, анонімності, неможливості цензури і повної незалежності від Інтернету.

- OSPF

OSPF - протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (link-state technology) і використовує для знаходження найкоротшого шляху алгоритм Дейкстри.

- FREIFUNK

Freifunk.net - некомерційне волонтерський бездротових мереж в Німеччині. Freifunk.net - частина міжнародного руху відкритих бездротових мереж [12].

1.6 Ad Hoc мережі

Ad Hoc - це децентралізована бездротова мережа. Ця мережа є спеціальною, оскільки вона не покладається на попередньо існуючу інфраструктуру, наприклад, дротові маршрутизатори мережі або точки доступу в керованій (інфраструктура) бездротовій мережі. Натомість кожен вузол бере участь у маршрутизації шляхом пересилання даних для інших вузлів. На основі цього ми можемо визначити, які вузли пересилають дані динамічно на основі підключення до мережі. Є також мобільна спеціальна мережа, яку також називають мобільною безпроводною мережею. Це самоконфігуруюча мережа мобільного зв'язку пристрої якої підключені за допомогою бездротового зв'язку[39].

На рисунку 1.5 показано роботу загальної спеціальної мережі (Ad Hoc).

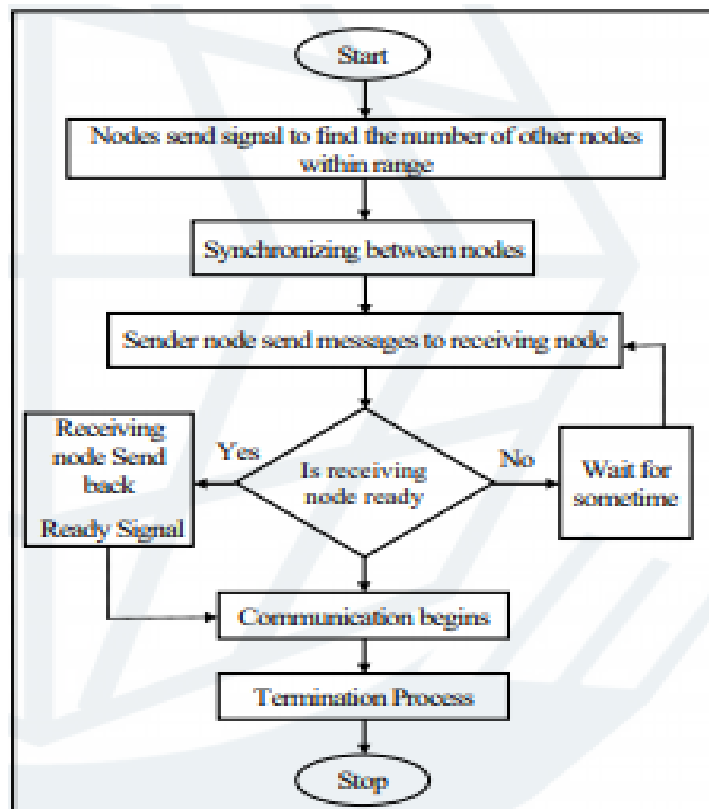


Рисунок 1.5 – Робота Ad Hoc мережі

Мережа складається з мережі з фіксованими і широкими шлюзами. Мобільні хости спілкуються з мостом у мережі (що називається базовою

станцією) в межах її радіус зв'язку. Відсутність інфраструктури представляє проблеми з централізованим контролем безпеки. Наприклад, контроль доступу, що є традиційним, підтримується центральним сервером.

Безпека механізмів, залучених довірених третіх сторін, може не бути життєздатними в спеціальних мережах [13].

1.7 Мобільна Ad Hoc мережа

З розвитком бездротового зв'язку, з'являється все більше бездротових мереж, наприклад, мобільних. Спеціальна мережа (MANET), бездротова мережа датчиків (WSN).

Мобільна мережа ad hoc (MANET) – це тимчасова настройка мережі для конкретної мети без допомоги будь-якої вже існуючої інфраструктури. На рисунку 1.6 зображено мобільну Ad Hoc мережу [14].

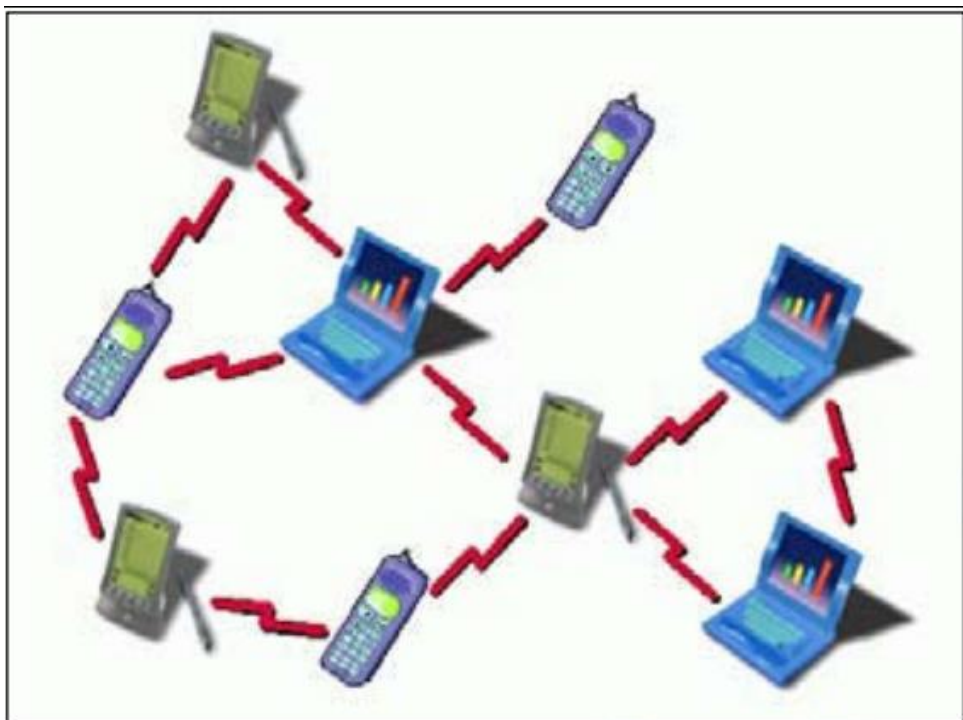


Рисунок 1.6 – Мобільна Ad Hoc мережа

Вузли в MANET наділені повноваженнями для обміну пакетами за допомогою радіоканалу. Вузли, що не знаходяться в зоні дії один біля одного

використовує свої проміжні вузли для пересилання пакетів. Тому існують загрози для мобільних пристроїв ad hoc мережі як із зовнішніх вузлів, несанкціонованих до участі у мобільних спеціальних мережах, так і від внутрішніх вузлів, які мають авторизацію посвідчення особи для участі в мобільній спеціальній мережі. Внутрішні вузли, що породжують загрози, можуть бути і надалі розділені відповідно до їх поведінки [14].

1.8 Застосування Ad Нос мережі в домашніх умовах

Розглянемо сценарій, завдяки якому бездротові комп'ютери стануть популярними в домі. На рисунку 1.7 зображено домашню Ad Нос мережу.

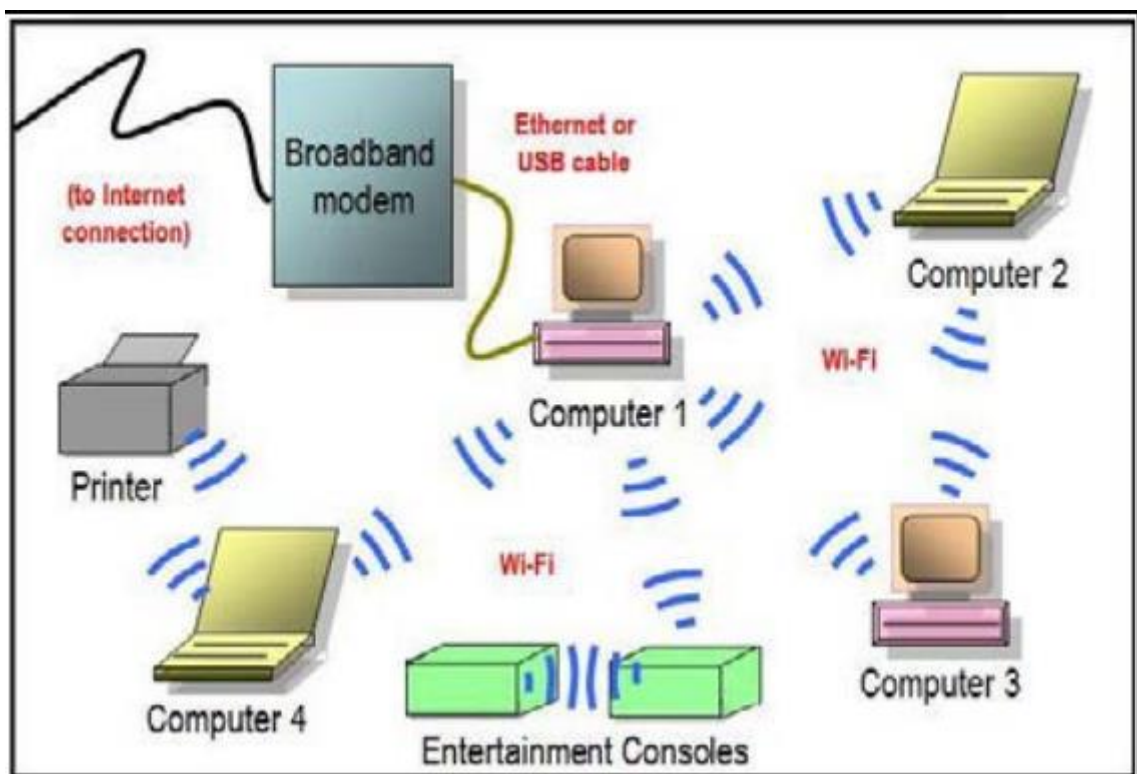


Рисунок 1.7 – Домашня Ad Нос мережа

Ці комп'ютери, ймовірно, будуть перенесені з офісного робочого середовища. Цілком можливо, що такі комп'ютери не будуть мати топологічно пов'язані IP-адреси, особливо якщо вони пов'язані в офісах кожного з батьків.

Маючи на увазі зручність, яку надає незмінна IP-адреса користувачеві, було б непогано дозволити різні мобільні комп'ютери для управління спеціальною мережею вдома, навіть якщо будинок підтримує власну підмережу з більшою кількістю вузлів [14].

1.9 Висновки до першого розділу

У розділі охарактеризовано поняття Mesh-мережі та її роль в суспільстві. Зроблено порівняння двох безпроводних мереж Ad Hoc та Mesh-мереж. Розглянуто найбільш розповсюджені технічні засоби Mesh-мережі.

Наведено деталі основних протоколів Mesh-мережі. Також виділено один найбільш ефективний протокол, на якому і була побудована Mesh-мережа. На основі даної інформації можна надати рекомендації безпосередньо щодо правильного розміщення точок Mesh-мережі та ефективного застосування саме цієї мережі. Було також розглято вузли мережі, а також структури пакетів MAC-рівня.

Огляд літератури свідчить про те, що мережа Mesh, ефективна як для служб миттєвого реагування так і для жителів місцевості, на якій побудована мережа.

2 ЗАГАЛЬНІ ПРИНЦИПИ ПРОЕКТУВАННЯ ТА ТЕХНІЧНІ ВИМОГИ ДО ОБЛАДНАННЯ БЕЗПРОВІДНИХ MESH-МЕРЕЖ

2.1 Проблема підключення до інтернету в сільській місцевості

У сільських місцевостях Тернопільської області рівень проникнення телекомунікаційних послуг, наприклад, телефонії та доступу до Інтернету, є низьким, а в деяких регіонах відсутній. Оператори зв'язку вважають цю місцевість неекономічною через природу цих регіонів - віддалених, часто недоступних, не мають інфраструктури, малонаселені, з низьким рівнем доходів та людей з низьким рівнем кваліфікації. Проте надійний, доступний та простий доступ до телекомунікаційних послуг для всіх визначено ключовим фактором соціального та економічного розвитку [15].

Самозабезпечення та володіння громадою, низькою вартістю розподіленої інфраструктури стає життєздатною альтернативою збільшенню проникнення телекомунікаційних послуг у селах.

Поява технології бездротових мережевих мереж (заснована на стандартах IEEE 802.11 a / b / g) може допомогти покращити надання телекомунікаційних послуг у цих регіонах.

Дизайн мережі для Mesh-мережі залежатиме від географічного ландшафту та відстані між точками, що підключаються. Поєднання точкових міжміських ліній зв'язку (з використанням спрямованих антен) та локальних точок до багатоточкових (з використанням всеспрямованих антен) між вузлами може створити надійну безпроводну мережу.

Ряд мережевих проєктів у всьому світі (експеримент Freifunk OLSR у Берліні, Німеччина, мережа Дхарамсала в Індії та долина Піблз у Південній Африці) продемонстрували, що громада може створити та підтримувати бездротову мережеву мережу та мати доступ до цілого ряду сучасні інформаційно-комунікаційні послуги [15].

Ці послуги включають телефонію (протокол передачі голосу через Інтернет), обмін миттєвими повідомленнями, електронну пошту, доступ до Інтернету, мультимедійні послуги та надання послуг (наприклад електронне навчання) [15].

2.2 Загальні принципи проектування безпроводної Mesh-мережі

2.2.1 Mesh-мережа

Мережа безпроводна мереж (WMN) складається з вузлів, що становлять магістраль мережі. Вузли можуть налаштовуватись автоматично та динамічно переконфігурувати, щоб підтримувати зв'язок. Це надає сітці характеристики її «самоутворення» та «самовідновлення». Цей самодостатній взаємозв'язок між вузлами знімає необхідність централізованого управління [16].

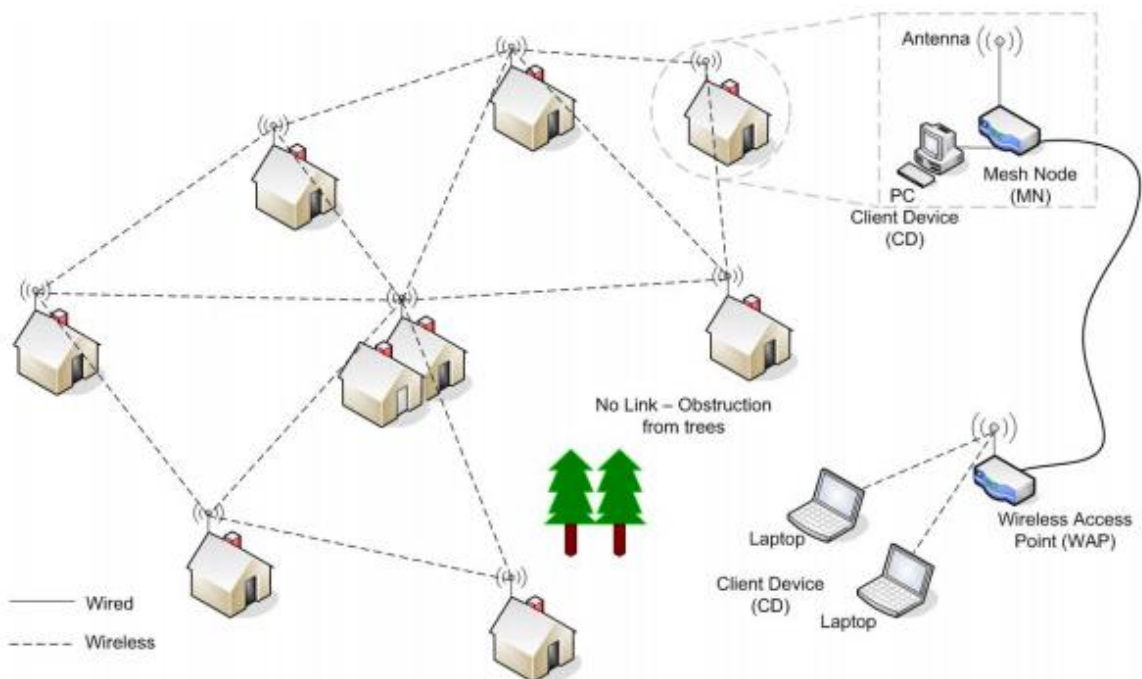


Рисунок 2.1 – Розгорнута безпроводна мережа

Інтелектуальна маршрутизація дозволяє мережевим вузлам маршрутизувати пакети даних для вузлів, які можуть знаходитися не в безпосередній зоні безпроводна зв'язку (рисунок 2.1).

Таким чином, інформація може бути спрямована від джерела до пункту призначення за допомогою кількох стрибків. Це має потенційну перевагу з точки зору надійності мережі над традиційними мережами з одним стрибком, особливо для зворотного зв'язку [16].

2.2.2 Вузол безпроводної мережі

Вузол безпроводної мережі складається з безпроводного маршрутизатора та антени. Мережевий вузол можна встановити всередині приміщення або в атмосферостійкому приміщенні на відкритому повітрі. Антена може бути стандартною всенаправленою антеною, а може бути зовнішньо встановленою спрямованою антеною. Мережий вузол спілкується лише з іншими безпроводними мережевими вузлами [17].

2.2.3 Точка безпроводного доступу

Точка безпроводного доступу складається з безпроводного маршрутизатора та антени. Безпроводну точку доступу можна встановити всередині приміщення або у атмосферостійкому приміщенні на відкритому повітрі. Антена може бути стандартною антеною, а може бути зовнішньо встановленою всенаправленою антеною. Точка безпроводного доступу створює точку доступу, де будь-який пристрій із підтримкою Wi-Fi може підключитися до безпроводної точки доступу [17].

2.2.4 Переваги безпроводних мереж

Однією з переваг Mesh-мережі є те, що вона самоформується. Це означає, що безпроводна мережа формується автоматично після налаштування та активації вузлів.

Також важливою перевагою є відмовостійкість. Якщо в мережі існують зайві маршрути, потік інформації не переривається в решті мережі, коли один вузол виходить з ладу. Мережа буде динамічно перенаправляти інформацію наступним доступним маршрутом [18].

Вагомою перевагою є те, що Mesh-мережа належить безпосередньо громаді. Тобто право власності на мережу є спільним, тому тягар підтримки мережі не покладається на одну людину.

Одним з фактів, чому Mesh-мережа є актуальною в встановленні є низька вартість інфраструктури. Безпроводні вузли можна будувати з недорогого, загальнодоступного обладнання. Також додаткові витрати на розширення мережі є низькими. З додаванням одного додаткового вузла, при граничних витратах на цей вузол, охоплення та значення мережі збільшується.

І завершальною перевагою є те, що Mesh-мережа проста в розгортанні. За невеликої підготовки члени громади можуть будувати власні вузли, налаштовувати та розгортати їх у мережі [18].

2.2.5 Принципи функціонування безпроводної мережі

Розглянемо основні пункти безпроводної Mesh-мережі. По-перше зв'язок між мережевими вузлами базується на радіостанціях Wi-Fi (IEEE 802.11 a / b / g / s), приєднаних до спрямованих або всенаправлених антен. Також для всіх радіостанцій встановлено режим ad hoc (не режим клієнта або режим інфраструктури (точка доступу)). Кожен вузол у мережі WMN має однакові ESSID (ім'я) та BSSID (номер) - BSSID повинен бути виправлений, щоб запобігти розділенню безпроводної мережі [19].

Усі вузли в мережі WMN працюватимуть на одному каналі (частоті). В ідеальній WMN кожен вузол повинен мати можливість "бачити" принаймні два інших вузли в WMN. Це дозволяє здійснити повний збій у випадку, якщо який-небудь вузол виходить з експлуатації (наприклад, через відмову обладнання або збій живлення).

Протокол Mesh-маршрутизації, як OLSR, буде спрямовувати IP-трафік між безпроводними інтерфейсами вузлів мережі. Він дізнається потенційні маршрути, прослуховуючи інформацію про маршрутизацію, якою обмінюється в мережі, і динамічно підтримує таблиці маршрутизації. Ця функція забезпечує відмовостійкість маршрутизації, забезпечуючи альтернативний маршрут, коли

вузол виходить з ладу, якщо такий є.

Жоден безмережний безпроводний пристрій не підключається безпосередньо до безпроводного сітчастого вузла (сітчасті вузли забезпечують безпроводну зворотну кістку). Ця інфраструктура вважається критичною інфраструктурою, і нею слід керувати з максимальною доступністю, оскільки решта мережі залежить від доступності кожного вузла. Логін на Mesh-вузлах повинен бути доступний лише технічній групі, а не всім користувачам Mesh-мережі.

Кожна IP-адреса в Mesh-мережі повинна бути унікальною, щоб будь-який комп'ютер в мережі підключався до будь-якого іншого комп'ютера в мережі. Комп'ютер може під'єднуватися до Mesh-мережі за допомогою кабелів локальної мережі, підключених до вузла, або через безпроводне підключення до окремої точки доступу, підключеної до локальної сторони вузла мережі.

Варто зауважити, що один або кілька вузлів можуть бути підключені до спеціально підготовленого вузла, що з'єднується у віддалену мережу. Цей вузол також може бути вузлом мережі, але не буде налаштований так само, як локальні вузли [20].

2.2.6 Особливості проектування Mesh-мережі

Розглянемо особливості проектування Mesh-мережі до яких належать:

1. Вартість планування та вартість підтримки безпроводної мережі

Існує компроміс між вартістю планування та підтримки побудова мережі на початок проекту та витрати на утримання спроектованої мережі. Варто докласти зусиль, щоб ретельно спланувати, отримати відповідне обладнання та створити надлишкові маршрути в безпроводні мережі, де це можливо [21].

2. Комунікації

У кожній країні є регулюючий орган, який регулює використання безпроводного обладнання. Зверніться до місцевого регулятора щодо будь-яких конкретних норм щодо обладнання Wi-Fi, використання діапазонів 2,4 ГГц та 5,8 ГГц та максимальної вихідної потужності для безпроводного обладнання.

3. Планування безпроводної мережі (канали)

У стандартах IEEE 802.11 b / g є лише три смуги, що не перекриваються (не втручаються), і це канали 1, 6 і 11.

4. Планування мережі Ethernet (підмережі)

Приймаються адреси IP4, але також можливий IPv6.

5. Wi-Fi - це технологія прямої видимості Різні перешкоди можуть заважати сигналам, і їх слід враховувати:

а) Дерева та рослини - вода на листі негативно впливає на силу сигналу.

б) Будівельні матеріали - металеві предмети, такі як дахи або армування в бетонних стінах, впливають на силу сигналу.

6. Джерела перешкод

Мікрохвильові печі, кондиціонери та інше радіообладнання можуть заважати роботі обладнання Wi-Fi. Краще уникати цих перешкод, щоб забезпечити хороший зв'язок.

7. Блискавка

Електроніка сприйнятлива до ударів блискавки, і слід враховувати захист від блискавки, особливо для зовнішніх установок обладнання Wi-Fi [21].

2.3 Необхідне апаратне та програмне забезпечення

2.3.1 Вимоги до апаратного забезпечення

Тепер розглянемо, яке обладнання буде застосовуватись в побудові Mesh-мережі.

Почнемо з маршрутизаторів. Безпроводні маршрутизатори: Linksys WRT54G (до версії 4.0) або Linksys WRT54GL (версія 1.0 або 1.1). З WRT54G версії 5.0 флеш-пам'ять зменшено з 4 МБ до 2 МБ, і в результаті пам'яті вже не вистачає для Freifunk. На сьогоднішній день Linksys WRT54GL є одним з найпопулярніших пристроїв для безпроводних мереж.

Потрібно також ПК або ноутбук з картою LAN (для підключення ПК / ноутбука до Інтернету або офісної мережі). Для з'єднання вузлів потрібен стандартний мережевий кабель CAT5. Важливим елементом є адаптери Power-over-Ethernet (якщо ви маєте намір створити зовнішній мережевий вузол).

Одним з найважливіших пристроїв Mesh-мережі є направлені антени (для міжміських зв'язків) та всеспрямовані антени (для гарячих точок). І не варто забувати про захисні пристрої для освітлення (якщо обладнання буде встановлено під відкритим небом) [22].

2.3.2 Вимоги до програмного забезпечення

В налаштуванні нашої мережі буде використовуватись таке програмне забезпечення:

1. Freifunk версії 1.4.5 (доступне за посиланням:http://download-master.berlin.freifunk.net/ipkg/_g%2bgl/).
2. DD-WRT версії 2.3 (доступне за посиланням:<http://www.dd-wrt.com/dd-wrtv2/downloads.ph>).
3. Putty.exe

Це клієнт Windows SSH, необхідний для будь-якого ПК / ноутбука під управлінням Windows.

4. Tcprdump

(доступне

за посиланням:<http://downloads.openwrt.org/whiterussian/packages/>)

5. dot-draw (завантажте останню версію olsrd-mod-dot-draw пакет від <http://downloads.openwrt.org/whiterussian/packages>)

В результаті тестів зроблено висновок, що це програмне забезпечення є найбільш підходящим для Mesh-мережі.

2.5 Проблеми проектування Mesh-мереж

Є багато питань, які потребують розгляду, коли безпроводна мережа (WMN) є розроблена для певного застосування. Ці проблеми можуть широко класифікуватись на архітектурні питання та питання протоколу.

2.5.1 Архітектурне проектування мережі

WMN можуть бути розроблені у трьох різних мережевих архітектурах на основі топології мережі: «плоскі» WMN, ієрархічні WMN та гібридні WMN. Ці категорії коротко обговорюються нижче [25].

2.5.2 «Плоска» безпроводна мережа

На рисунку 2.2 зображено «плоску» безпроводну мережу.

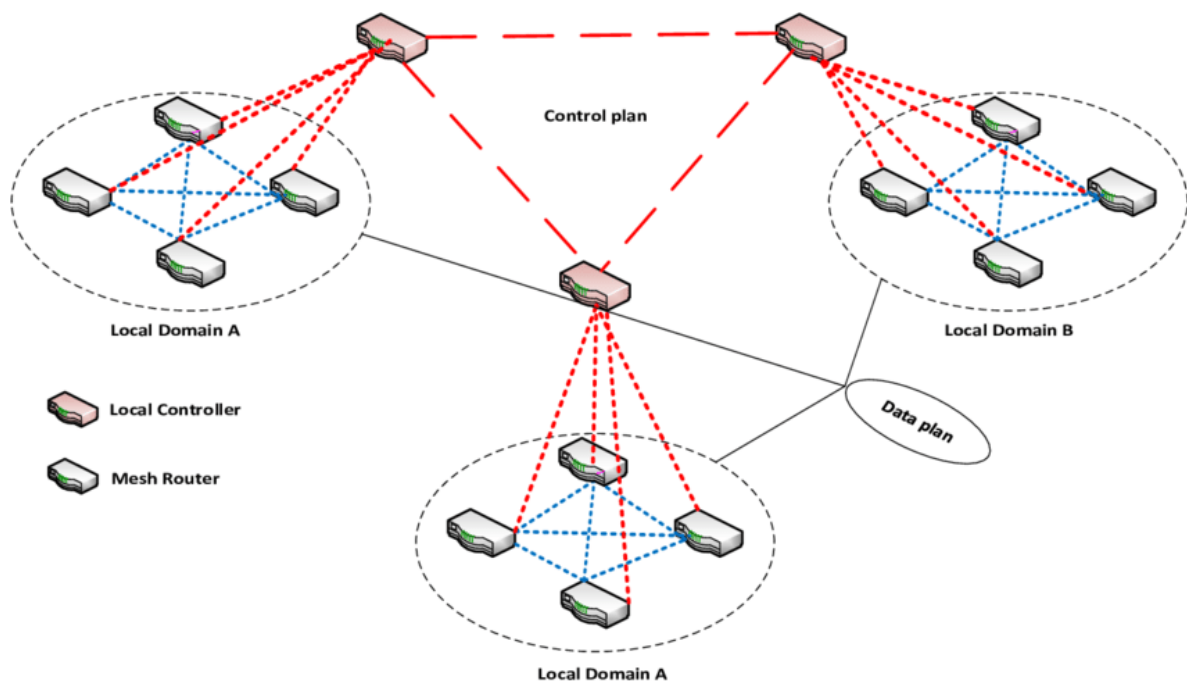


Рисунок 2.2 – «Плоска» безпроводна мережа

У «плоскій» мережі WMN мережу формують клієнтські машини, які діють як хости, так і маршрутизатори. Тут кожен вузол знаходиться на одному і тому ж рівні. Вузли бездротового клієнта координуються між собою та забезпечують

маршрутизацію, конфігурацію мережі, надання послуг та надання різних програм. Ця архітектура найближча до спеціальної бездротової мережі (Ad Hoc) і вона найпростіша серед трьох архітектур WMN.

Основною перевагою цієї архітектури є її простота, а її недоліки включають відсутність масштабованості мережі і високі обмеження ресурсів. WMN - це схема адресації, маршрутизації та виявлення послуг схеми. У плоскій мережі адресація є однією з проблем та може стати слабким місцем для масштабованості [26].

2.5.3 Ієрархічна Mesh-мережа

На рисунку 2.3 зображено приклад ієрархічної Mesh-мережі.

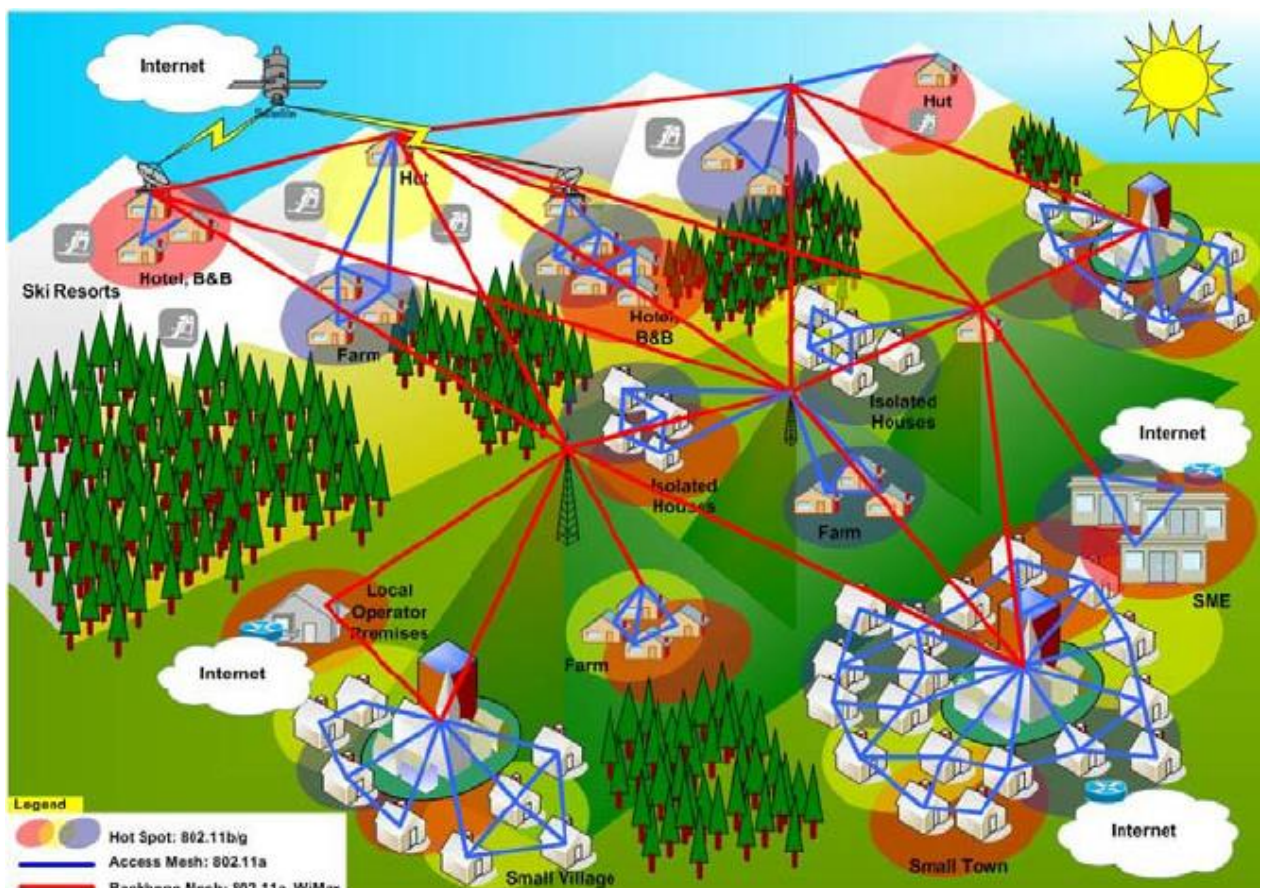


Рисунок 2.3 – Ієрархічна Mesh-мережа

В ієрархічній мережі WMN, мережа має кілька рівнів або ієрархічних рівнів, на яких вузли клієнта WMN формують найнижчі в ієрархії. Ці клієнтські

вузли можуть взаємодіяти з магістральною мережею WMN, сформованою маршрутизаторами.

У більшості випадків вузли WMN є виділеними вузлами, які утворюють магістральну мережу. Це означає, що магістральні вузли не можуть створювати або припиняти трафік даних, як вузли клієнта WMN. Відповідальність за самоорганізацію та підтримку магістральної мережі покладається на маршрутизатори WMN, деякі з яких у магістральній мережі можуть мати зовнішній інтерфейс до Інтернету, і такі вузли називаються шлюзовими вузлами [27].

2.5.4 Гібридна Mesh-мережа

На рисунку 2.4 зображено гібридну Mesh-мережу.

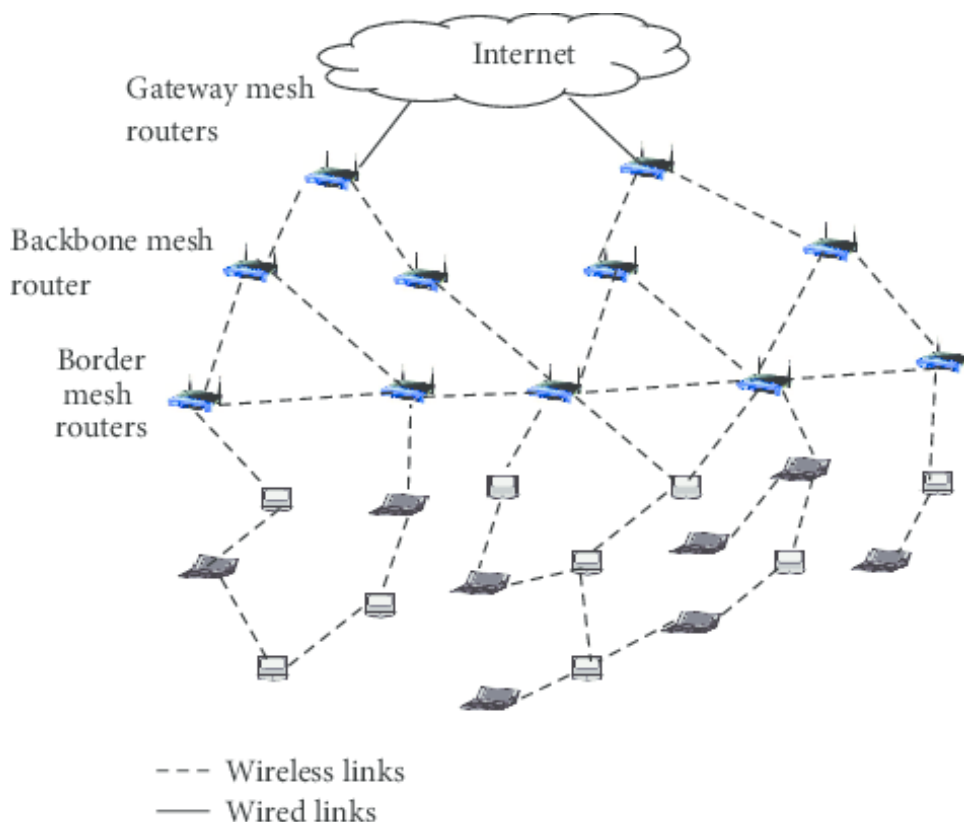


Рисунок 2.4 – Гібридна Mesh-мережа

Це особливий випадок ієрархічних WMN, де WMN використовує інші бездротові мережі для зв'язку. Наприклад, використання інших мереж WMN на

основі інфраструктури, таких як стільникові мережі, мережі WiLL, мережі WiMAX або супутникові мережі. Приклади таких гібридних WMN включають багатопрофільні стільникові мережі, покращену пропускну здатність у бездротових мережах локальної петлі (TWiLL) та уніфіковані стільникові спеціальні мережі. Практичним рішенням такої гібридної WMN для реагування на надзвичайні ситуації є платформа CalMesh. Ці гібридні WMN можуть використовувати різні технології для обох WMN [28].

2.6 Висновки до другого розділу

У другому розділі кваліфікаційної роботи розглянуто загальні принципи проектування та технічні вимоги до обладнання безпроводних Mesh-мереж. Наведено поняття та описано вузол безпроводної мережі та точку безпроводного доступу.

Також було наведено переваги безпроводних мереж та описано принципи безпроводної мережі. Розглянуто всі тонкощі проектування Mesh-мережі. Зокрема вартість, комунікації, планування та джерела перешкод. Проаналізовано види та проблеми проектування Mesh-мереж.

Описано апаратне та програмне забезпечення, яке потрібне для безпроводної Mesh-мережі.

3 РОЗРОБКА ПРОЕКТУ MESH-МЕРЕЖІ

Мережі Mesh легко побудувати, коли у вас є кілька локальних вузлів для налаштування. Однак масштаби мереж зростають досить швидко. Це може стати причиною численних проблем. Розглянемо поетапно сукупність задач по плануванню Mesh-мережі.

3.1 Складання карти мережі

Будувати мережу ми будемо будувати на території села Карашинці Тернопільської області (рисунок 3.1). Потрібно визначити та скласти ділянку (будинків / офісів), які отримають Mesh вузол (Linksys).

Зазвичай можна отримати координати GPS цих об'єктів, щоб побудувати їх на Google Earth. Координати GPS також можуть бути використані при плануванні радіозв'язку за допомогою спеціалізованих інструментів, які можуть дати "цифрову модель висоти місцевості" кожного об'єкта. Як мінімальна вимога слід мати принаймні схематичний сюжет. Положення кожного вузла не повинно бути дуже точним, хоча положення вузлів відносно один одного є корисним при призначенні каналів та IP-адрес. На рисунку 3.6 зображено карту Mesh-мережі.

Наступним кроком буде планування безпроводної мережі.

Тепер сайти можна пов'язати між собою за допомогою сюжету. Кожне посилення визначається як пряма лінія між двома безпроводної вузлами. Довжина кожного посилення повинна відображати відстань між об'єктами. У Mesh-мережі існує багато можливих посилень — малювати всі можливі комбінації не потрібно. Також потрібно намалювати місце розташування сайту Інтернет-шлюзу [29].



Рисунок 3.1 – Карта Mesh-мережі с. Карашинці

Основна мета макету - отримати загальну картину мережі. Зображення дасть інформацію про топологію мережі та кількість стрибків між сайтами та інтернет-шлюзом.

3.2 Вибір типу топології мережі

Mesh - це найпростіша топологія для налаштування в безпроводних мережах. Сайти досить рівномірно розподілені, і кожен вузол може бачити кожен інший вузол. Якщо область стає занадто великою, деякі веб-сайти можуть бути занадто далеко від інтернет-шлюзу, тому їм потрібно "перестрибнути" через багато інших вузлів, перш ніж дістатися до шлюзу. Це сповільнить їх зв'язок [30].

Одним із рішень було б додати шлюзи по всій mesh. Недоліком є висока вартість, пов'язана з інтернет-шлюзом. Тому найкращим рішенням було б побудувати так звану магістраль, що простягається від шлюзу по всій mesh мережі.

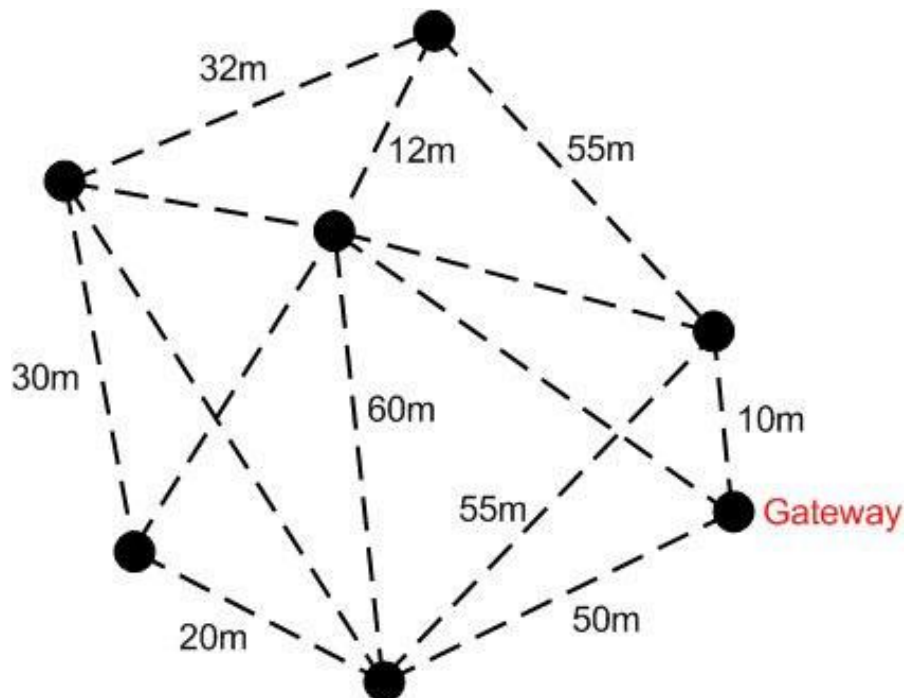


Рисунок 3.2 – Графічне представлення простої Mesh-мережі

Якщо шлюз знаходиться посередині, може знадобитися кілька магістралей (наприклад, топологія зірок), щоб гарантувати, що всі отримують однакову пропускну здатність. На рисунку 3.2 наведено приклад «простого» графічного графіку мережі, що не вимагає магістралі. На рисунку 3.3 наведено приклад «прямокутної» Mesh-мережі, яка в ідеалі потребує магістральної мережі по всій сітчастій мережі [31].

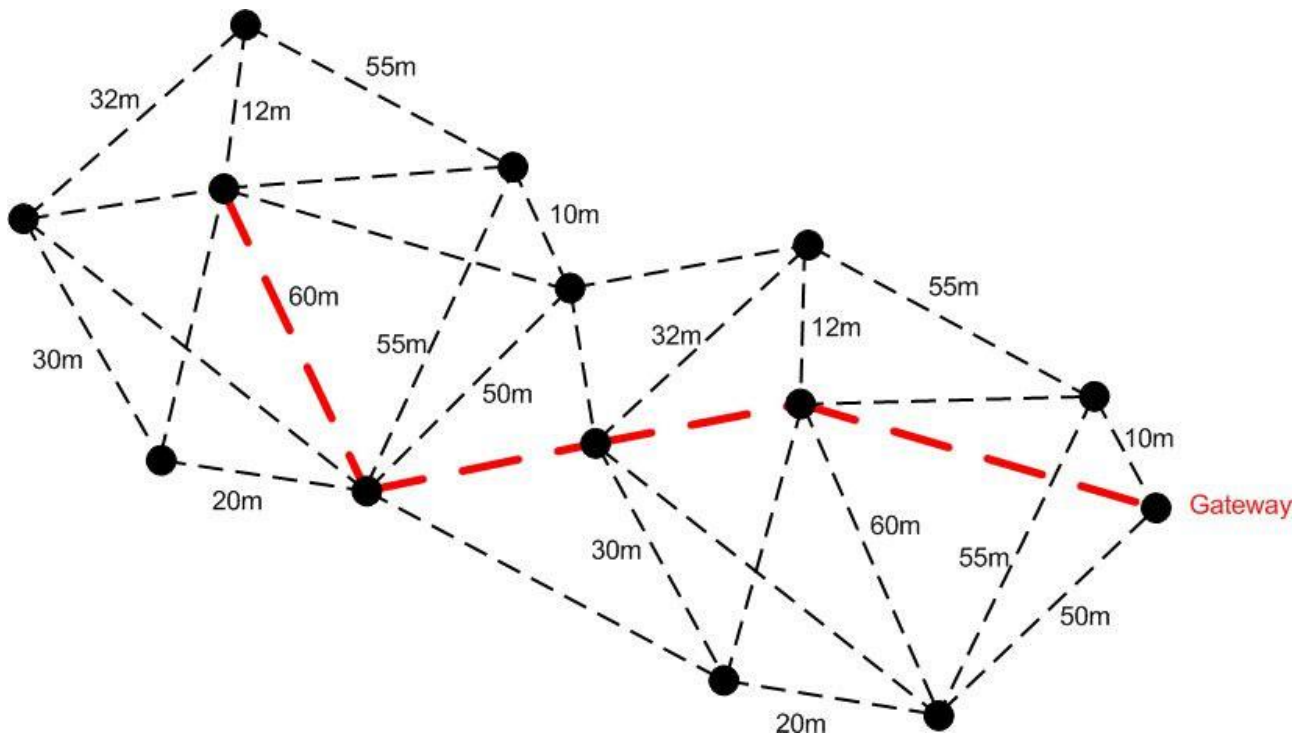


Рисунок 3.3 – Діаграма Mesh-мережі з магістраллю

Кластери: Чи сформовані в мережі кластери? Наскільки далекі ці скупчення один від одного?

Якщо кластери знаходяться занадто далеко один від одного (беручи до уваги, чи використовується один із внутрішніх / зовнішніх антен, розмір зовнішніх антен), можливо, знадобиться магістраль для з'єднання кластерів між собою [32].

Також слід враховувати розташування інтернет-шлюзу. Як і у випадку з топологією мережі вище, магістраль з'єднає шлюз (шлюзи) з усіма кластерами, гарантуючи, що всі отримують однакову пропускну здатність [33].

На рисунку 3.4 показано графік мережі з трьома кластерами, які з'єднані разом з магістраллю.

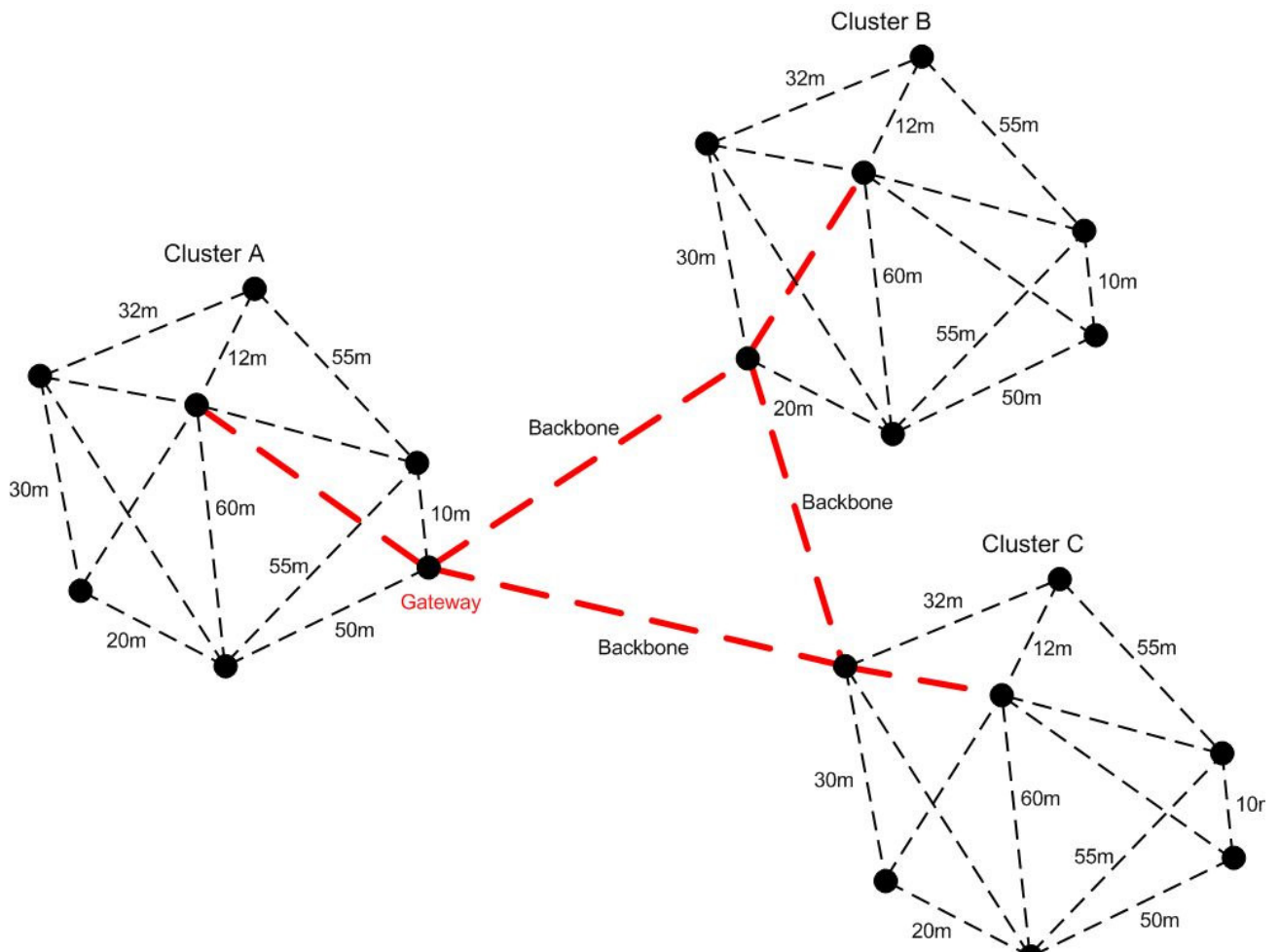


Рисунок 3.4 – Кластерна мережа з магістраллю

Звернемо увагу, що шлюз є частиною магістральної мережі, щоб забезпечити швидше підключення до Інтернету.

3.3 Розподіл каналів для Mesh-мережі

Два типи вузлів вже були визначені в розділі 3.2: «нормальний» вузол мережі та магістральний вузол. Розподіл каналів на сітчастому вузлі, як правило, дуже проста справа. Можна вибрати один із трьох каналів (1, 6 або 11). Коли кожен вузол у сітці встановлений на один і той же канал, вони можуть «розмовляти» між собою [34].

Додаючи магістральний вузол, потрібен буде інший канал. Додавання магістралі ефективно додає іншу безпроводну мережу, яка повинна працювати незалежно від іншої сітчастої мережі. Отже, «нормальна» мережа працюватиме

на каналі 6, а магістраль на каналі 11. Це забезпечить, щоб дві мережі не перешкоджали одна одній. Менше перешкод призведе до кращої роботи.

Повертаючись до рисунку 3.4, можна налаштувати вузли в кластерах А, В і С для використання каналу 6. Магістральні вузли будуть налаштовані на використання каналу 11. У цьому контексті ми припускаємо, що основний вузол складається з двох радіостанцій (або двох блоків Linksys): один буде обслуговувати магістраль на частоті 11, а інший буде обслуговувати сітчасту мережу на каналі 6. Дві радіостанції (або бокси Linksys) з'єднані між собою за допомогою кабелю локальної мережі (витою парою) [35].

3.4 Розподіл каналів для домашніх користувачів

У розділі 3.3 вже було виділено два канали для магістральної та сітчастої мереж. У цих рамках можлива третя безпроводна мережа: гаряча точка.

Точка доступу зазвичай потрібна вдома або в офісі, коли потрібно створити локальну безпроводну мережу для підключення ноутбуків та іншого безпроводного обладнання. Точка доступу потребуватиме підключення безпроводної точки доступу (Linksys) до сітчастого вузла. Два коробки Linksys з'єднані між собою за допомогою кабелю локальної мережі (через порти комутатора Ethernet) [36].

Точка доступу не може використовувати той самий канал, що і сітчасті або магістральні вузли. Це може спричинити перешкоди та погіршити роботу мережі. У нашому прикладі, коли канали 6 і 11 вже використовуються, єдиним варіантом буде призначення каналу 1 точці доступу.

У точці доступу локальна мережа та безпроводні інтерфейси з'єднані між собою. Linksys, що створює точку доступу, повинен мати спеціальне програмне забезпечення, щоб легко налаштувати точку доступу. Найкращим варіантом буде використовувати DD-WRT [37].

3.5 Планування розподілу IP-адрес

Адреси розподіляються згідно з RFC 1918, який містить деталі приватного адресного простору. RFC можна знайти за адресою <http://www.ietf.org/rfc.html>.

RFC 1918 - це меморандум Інженерної робочої групи (IETF) про методи призначення приватних IP-адрес у мережах TCP / IP. Поряд з NAT (тунелювання мережевих адрес), RFC 1918 сприяє розширенню корисної кількості IP-адрес, доступних під IPv4, як зупиняюче рішення для запобігання вичерпанню загальнодоступних IP, доступних до прийняття IPv6. Не потрібно реєструвати приватні IP-адреси в Регіональному реєстрі Інтернету (RIR), що спрощує налаштування приватних мереж.

Схема IP-адресації повинна забезпечувати унікальні адреси для кожного вузла та ПК у мережі. Перше, що потрібно вибрати, це доступна підмережа. RFC 1918 містить інформацію про те, які приватні підмережі доступні [38].

Відповідно до RFC 1918, доступними підмережами для приватних IP-мереж, які не будуть підключені до Інтернету, є:

10.0.0.0	-	10.255.255.255	(Префікс 10/8)
172.16.0.0	-	172.31.255.255	(Префікс 172.16 / 12)
192.168.0.0	-	192.168.255.255	(Префікс 192.168 / 16)

Рисунок 3.5 – Метод присвоєння номерів IP

Після вибору підмережі можна випадковим чином присвоїти IP-номери вузлам з'єднання та ПК. Пропоную вибрати спосіб присвоєння номерів IP і дотримуватися його дуже суворо [38].

Приклад методу присвоєння номерів IP показаний на рисунку 3.5. Приклад реалізації методу показаний на рисунку 3.6.

Тип	Бездротовий	Ethernet
Вузол магістралі	10.0.1. x де $1 \leq x < 255$	
«Звичайний» сітчастий вузол	10.1.1. x де $1 \leq x < 255$	
Точка доступу (точка доступу)	10.2.x. y де $1 \leq y < 255$	

Рисунок 3.6 – Метод присвоєння номерів IP (безпроводний інтерфейс)

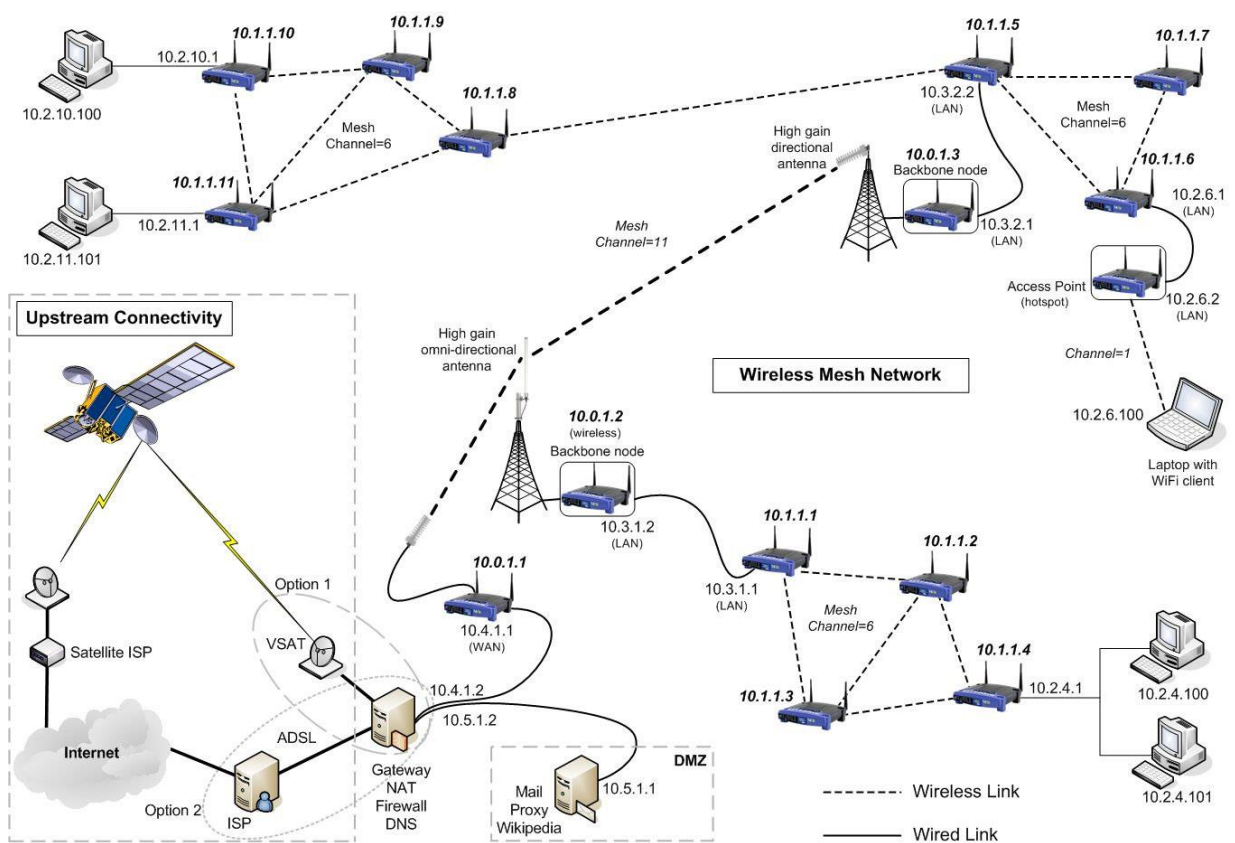


Рисунок 3.7 – Приклад макета безпроводної Mesh-мережі

Вузол магістралі:

1. Інтерфейс безпроводного зв'язку: 10.0.1. x / 24 де $1 \leq x < 255$
2. Інтерфейс Ethernet: 10.3.x. y / 24 де $1 \leq y < 255$

«Звичайний» Mesh-вузол:

1. Інтерфейс безпроводного зв'язку: 10.1.1. a / 24 де $1 \leq a < 255$
2. Інтерфейс Ethernet: 10.2.a. б / 24 де $1 \leq b < 255$.

Зверніть увагу, що вузли Linksys будуть знаходитися в нижньому діапазоні, але інші ПК та ноутбуки, підключені до вузла, будуть нумеруватися від 100 відповідно до налаштувань DHCP.

Точка доступу:

Можна підключити безпроводну точку доступу Linksys (DD-WRT) взаємно до “звичайного” сітчастого вузла Linksys. Таким чином, підмережа, призначена безпроводній локальній мережі або точці доступу, буде такою ж, як і у локальній мережі Ethernet, підключеної до вузла.

10.0.1. x / 24 позначення перекладається на: IP-адреса:	10.0.1. x де $1 \leq x < 255$, та
Маска підмережі:	255.255.255.0

Очевидно, що кожен метод розподілу IP матиме обмеження на розмір підмережі. Щоб подолати обмеження розміру підмережі та зробити можливим автоматичне розподіл IP-адрес, альтернативою є використання IPv6.

3.6 Планування процесу побудови мережі Mesh

Почнімо будувати безпроводну мережу, налаштувавши всі вузли та точки безпроводного доступу в центральному місці відповідно до проекту мережі. Позначте кожен сітчастий вузол та точку безпроводного доступу деталями конфігурації, написаними на аркуші паперу та приклеєними до пристрою. Таким чином, подальші кроки налаштування стануть набагато простішими. Також хорошою практикою є ведення журналу з деталями конфігурації та розташуванням кожного вузла та записуванням історії вузла. [39].

Перебуваючи в центральному місці, протестуємо все обладнання, щоб переконатися, що все працює правильно. Підключіть ПК до сітчастого вузла за допомогою кабелю локальної мережі. Переконайтеся, що ПК запитує IP-адресу через DHCP. Пінгувати кожен другий вузол. Якщо пінг пройшов успішно, то сітчастий вузол, приєднаний до ПК, та інші вузли працюють. Якщо це не вдалося, перевірте конфігурації.

Почнімо встановлювати Mesh-вузли з шлюзу - точки, де Інтернет буде підключений до Mesh-мережі. Таким чином ми можемо підтвердити, що мережа все ще працює, встановлюючи кожен новий вузол. Підключіть ПК до Mesh-вузла за допомогою кабелю локальної мережі. Спершу перевіримо пінг шлюзу, і якщо це вдається, проведемо пінг будь-якого веб-сайту в Інтернеті, щоб забезпечити доступ ПК до Інтернету [39].

3.7 Підготовка вузла безпроводної мережі

Відкриваючи пакет Linksys, вміст зображений на рисунку 3.8 нижче:



Рисунок 3.8 – Linksys WRT54GL та вміст упаковки

Це стандартна комплектація роутера. На рисунку 3.9 ми бачимо його вид ззаду.



Рисунок 3.9 – Безпроводний широкосмуговий маршрутизатор Linksys
WRT54GL

Для підготовки вузла безпроводної мережі потрібні наступні кроки:

- Оновлення мікропрограми - це буде зроблено для всіх магістральних та «звичайних» вузлів мережі
- Налаштування системи
- Налаштування безпроводного зв'язку
- Налаштування локальної мережі
- Налаштування OLSR

Для кожного з чотирьох розділів конфігурації (налаштування системи, безпроводної мережі, локальної мережі та OLSR), що впливають, існує потреба перезапустити Linksys після завершення налаштування кожного розділу. Проте, ви можете виконати всі чотири налаштування розділу, пропустивши перезапуск після кожного розділу, перш ніж перезапустити Linksys. Хоча пропускати перезапуск після кожного розділу недоцільно, якщо ви не знаєте, що робите, це економить значну кількість часу, оскільки вам доведеться чекати кілька хвилин, щоб Linksys щоразу перезапускався [40].

3.8 Встановлення програмного забезпечення Freifunk, її оновлення та налаштування

Наступним кроком є оновлення Linksys за допомогою програмного забезпечення Freifunk. Цього досягають, дотримуючись наведених нижче кроків.

Завантажуємо Freifunk. Далі підключаємо кабель локальної мережі (синій кабель, що міститься на упаковці Linksys) до ПК / ноутбука та до задньої панелі Linksys на одному з портів, позначених 1-4. Дивимось уважно, щоб НЕ підключити в порт з написом "Інтернет". Переконайтеся, що ваш апарат налаштований на автоматичне отримання IP-адреси. Підключаємо Linksys до кабелю живлення (знаходиться в упаковці Linksys) і вмикаємо джерело живлення. Залежно від того, який LAN-порт Linksys ми використали, передній світлодіод, що відповідає номеру порту ззаду, повинен бути світло-зеленим. Тобто, якщо ви використовували порт 1, тоді світлодіод 1 повинен світитися. Налаштовуємо підключення до локальної мережі так, щоб ми отримали 192.168.1. x IP-адреса [41].

Щоб перевірити, чи є у нас 192.168.1.x IP-адреса: У вікні Мережні підключення: клацаємо правою кнопкою миші на «Місцевий зв'язок» → вибираємо «Статус» → натискаємо на «Підтримка». Ми повинні побачити IP-адресу 192.168.1.x, (де $1 \leq x < 255$).

Відкриваємо веб-браузер і переконаймося, що наш браузер НЕ налаштований на встановлення веб-з'єднань через проксі. У полі адреси веб-браузера введемо: 192.168.1.1 і натискаємо [Enter]. Це перенесе нас на сторінку налаштування маршрутизатора Linksys. Натискаємо на «Адміністрація» → «Оновлення мікропрограми» натиснемо на «Перегляньте» та за допомогою вікна «Вибрати файл» виберіть Freifunk (openwrt-g-freifunk-1.4.5-en.bin), який ми завантажили → натисніть на «Оновлення». Натискаємо «Продовжити» і готово.

Після оновлення Linksys до програмного забезпечення Freifunk ми можемо розпочати конфігурацію Mesh-вузла (рисунок 3.10).

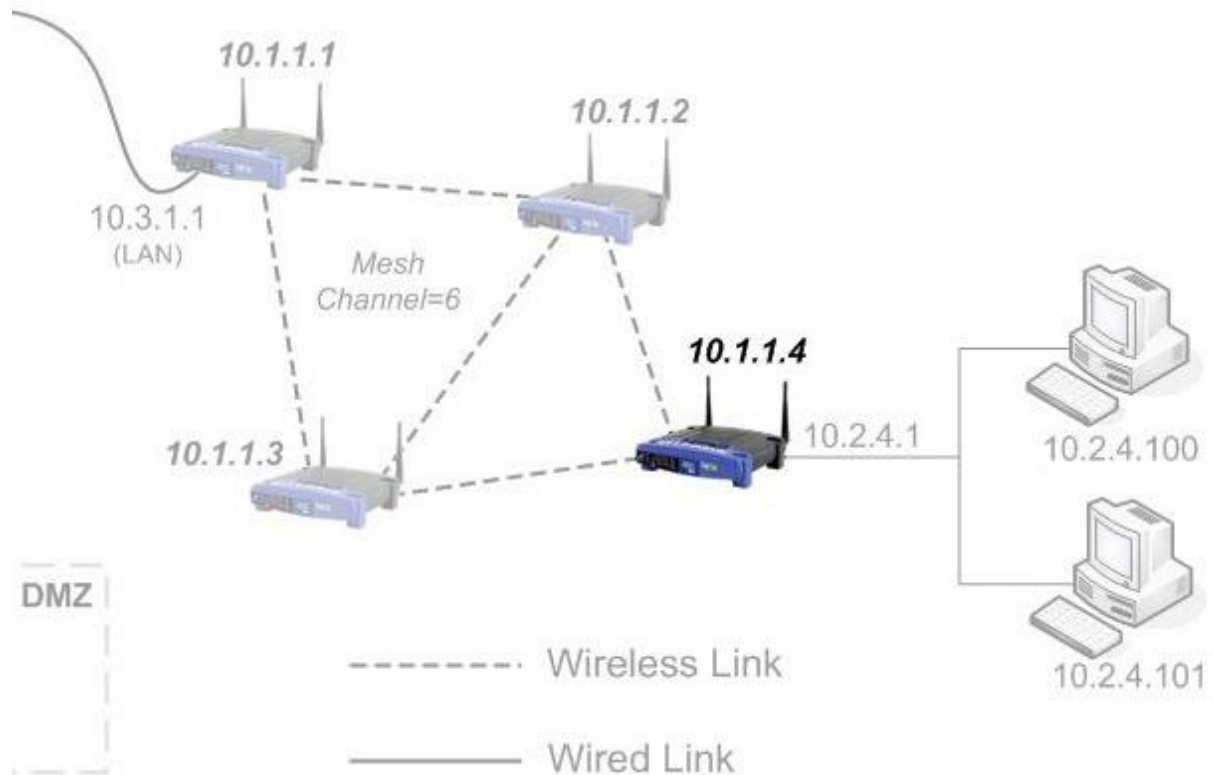


Рисунок 3.10 – Конфігурація Mesh-вузла

Вузол мережі з безпроводною IP-адресою 10.1.1.4, як показано на рисунку 3.15 (уривок з рисунка 3.7), використовується як приклад.

3.9 Налаштування системи Freifunk

Для початку розглянемо що таке Freifunk, його налаштування та функції.

Freifunk (безкоштовна безпроводна мережа) - це рішення для підтримки, реалізації та розвитку інструментів для безкоштовних Mesh-мереж. Крім того, вона підтримує громади, що розробляють ноу-хау для створення власних мереж.

Спільнота freifunk є частиною мережі проектів, що розробляють інструменти для безпроводних мереж, включаючи проекти програмного забезпечення Freifunk та OpenWrt, протоколи маршрутизації, такі як OLSR та BATMAN, інструменти, такі як карти для мереж (наприклад, freimap), інструменти сканування, такі як інструмент horst та багато інших. Нещодавно

люди також почали розробляти відкрите обладнання, таке як Mesh Potato (безпроводна картопля) для villagetelco.

За допомогою мікропрограми freifunk відносно легко створювати нові безпроводні мережі, використовуючи спеціальну маршрутизацію рівнів 2 та 3 рівня безпроводної локальної мережі, використовуючи протоколи OLSR, BATMAN та інші.

Freifunk створений у Німеччині. Він успішно впроваджений у багатьох країнах. Проект OLPC в Афганістані використовує freifunk для розгортання мереж для розповсюдження цифрових книг, новин та освітніх засобів масової інформації. У Гані freifunk використовується для подолання цифрового розриву в селах. У В'єтнамі freifunk використовується для підключення до інтернету на безкоштовних та відкритих програмах, таких як FOSSASIA. У Європі та Америці міські та сільські мережі знижують витрати на громади та малі та середні компанії, які мають спільні інтернет-з'єднання, ADSL, телефонні або супутникові лінки у віддалених регіонах [42].

Детальніше про Freifunk для Mesh-мережі, поетапне встановлення програмного забезпечення та налаштування описано в додатку А.

3.10 Налаштування LAN для Mesh-мережі

LAN складається з кабелів, точок доступу, комутаторів, маршрутизаторів та інших компонентів, що дозволяють пристроям підключатися до внутрішніх серверів, веб-серверів та інших локальних мереж через глобальні мережі (рисунок 3.11).

Зростання віртуалізації також сприяло розвитку віртуальних локальних мереж, які дозволяють адміністраторам логічно групувати мережеві вузли та розділяти свої мережі без необхідності серйозних змін інфраструктури.

Наприклад, в офісі з декількома відділами, такими як бухгалтерія, ІТ-підтримка та адміністрування, комп'ютери кожного відділу можуть бути логічно

підключені до одного і того ж комутатора, але сегментовані, щоб поводитися так, ніби вони окремі.



Рисунок 3.11 – Локальна мережа (LAN)

Переваги локальної мережі такі ж, як і у будь-якої групи пристроїв, об'єднаних у мережу. Пристрої можуть використовувати одне підключення до інтернету, обмінюватися файлами один з одним, друкувати на спільних принтерах, а також мати доступ та навіть керувати один одним [43].

LAN були розроблені в 1960-х роках для використання коледжами, університетами та дослідницькими установами (такими як NASA), насамперед для підключення комп'ютерів до інших комп'ютерів. Лише з розвитком технології Ethernet (1973, на Xerox PARC), її комерціалізацією (1980) та стандартизацією (1983), локальні мережі почали широко застосовуватися.

Незважаючи на те, що переваги підключення пристроїв до мережі завжди добре розумілися, лише після широкого розгортання технології Wi-Fi, локальні мережі стали звичним явищем майже в усіх типах середовища. Сьогодні не тільки підприємства та школи використовують локальну мережу, але й ресторани, кав'ярні, магазини та будинки.

Безпроводне підключення також значно розширило типи пристроїв, які можна підключити до локальної мережі. Зараз майже все, що можна собі уявити, можна «підключити», починаючи від ПК, принтерів та телефонів, до смарт-телевізорів, стереосистем, динаміків, освітлення, терморегуляторів, віконних панелей, дверних замків, камер безпеки - і навіть кавоварок, холодильників та іграшок [44].

Детальніше про налаштування LAN для Mesh-мережі розписано у додатку Б.

3.11 Протокол OLSR та його налаштування

Оптимізований протокол маршрутизації стану зв'язку (OLSR) розроблений для мобільних спеціальних мереж. Він працює як табличний проактивний протокол, тобто обмінюється інформацією про топологію регулярно з іншими вузлами мережі. Кожен вузол вибирає набір сусідніх вузлів як "багатоточкові реле" (MPR). У OLSR відповідають лише вузли, вибрані як MPR для переадресації управління, призначеного для розподілу по всій мережі. MPR надають ефективний механізм керування кодуванням, шляхом зменшення кількості передач. Вузли, вибрані як MPR, також несуть особливу відповідальність при оголошенні стану зв'язку інформація в мережі. Дійсно, єдина вимога до OLSR забезпечити найкоротший шлях до всіх пунктів призначення. Крім того, протокол використовує MPR для полегшення ефективного кодування контролю повідомленнями в мережі.

OLSR розроблений для роботи незалежно від інших протоколів. Він успадковує концепцію переадресації та ретрансляції від HIPERLAN (рівень MAC протокол), який стандартизований ETSI. Протокол розроблений в IPANEMA проекту (частина програми Евкліда) та в проекті PRIMA (частина програми RNRT) [45]. Детальніше про налаштування OLSR для Mesh-мережі описано в додатку В.

3.12 Налаштування OLSR на приєднання до двох різних Mesh-мереж

У цьому випадку ми маємо дві нез'єднані Mesh-мережі, обидві під управлінням OLSR. Ми використовуємо два вікна Linksys для з'єднання двох мереж. На рисунку 3.12 нижче ми посилаємось на вузли з адресами Ethernet 10.3.1.2 та 10.3.1.1.

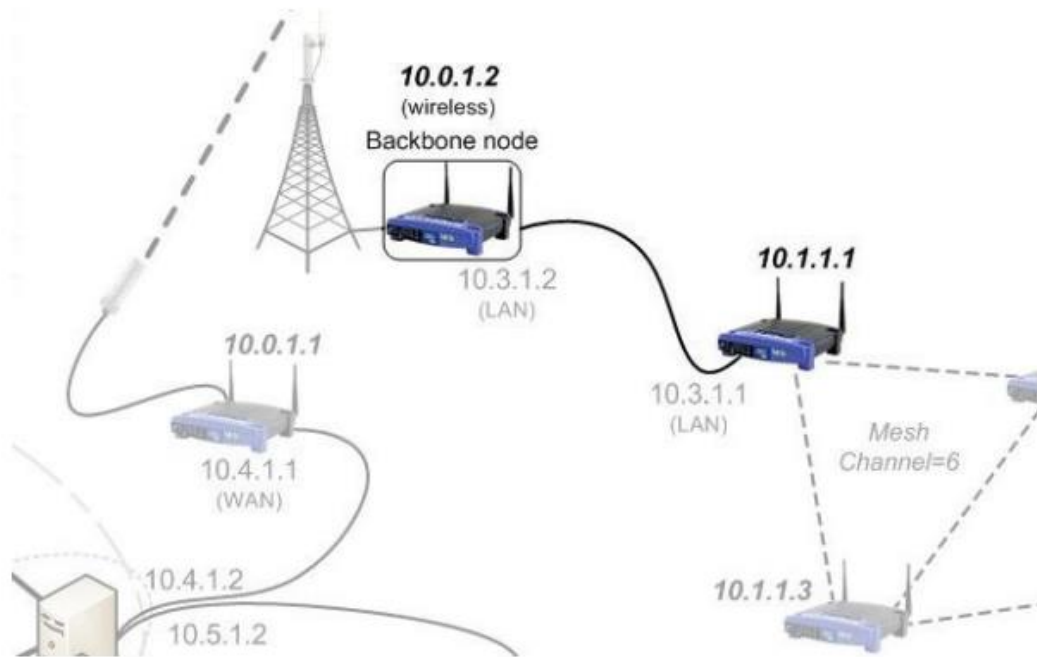


Рисунок 3.12 – Приєднання двох різних безпроводних мереж

Припускаємо, що дві мережі мають унікальні IP-адреси (інакше їх не можна приєднати). В MOST одна з мереж має Інтернет-шлюз (пізніше ми обговоримо, як забезпечити, щоб вузол mesh з доступом до Інтернету рекламував свій стандартний інтернет-маршрут до решти мережі mesh).

3.13 Налаштування програмного забезпечення

Щоб налаштування пройшли успішно підключаємо кабель локальної мережі (синій кабель, що міститься на упаковці Linksys) до ПК / ноутбука та до задньої панелі Linksys на одному з портів, позначених 1-4. Потім потрібно увійти

до Linksys за допомогою ssh або Putty (якщо використовується Windows).

PuTTY - це популярний SSH- і Telnet-клієнт (Telnet - той же SSH, лише без шифрованої передачі даних (пакетів)), тобто програма для безпечного підключення до віддаленого комп'ютера (або до сервера) та виконання на різних командах.

SSH або Secure Shell (що в перекладі означає «безпечна оболочка») - це мережевий протокол, що використовується для підключення до віддалених комп'ютерів та управління ними за допомогою технологій тунелювання. І в завершенні потрібно редагувати файл / etc / olsrd.conf, Тип vi /etc/olsrd.conf та змінити розділ інтерфейсів на такий: інтерфейс «eth1» «br0». Все це потрібно повторити наведені вище дії на другому Linksys. Прямий кабель і підключіть Linksys, тобто підключіть один кінець кабелю до одного з 4 мережевих портів з позначкою 1-4, а інший кінець до відповідного мережевого порту 1-4 на інших Linksys. Таким чином, з нашого прикладу нище підключіть один кінець кабелю локальної мережі до порту 1-4 вузла 10.3.1.2, а інший кінець - до порту 1-4 вузла 10.3.1.1 (рисунок 3.13) [46].

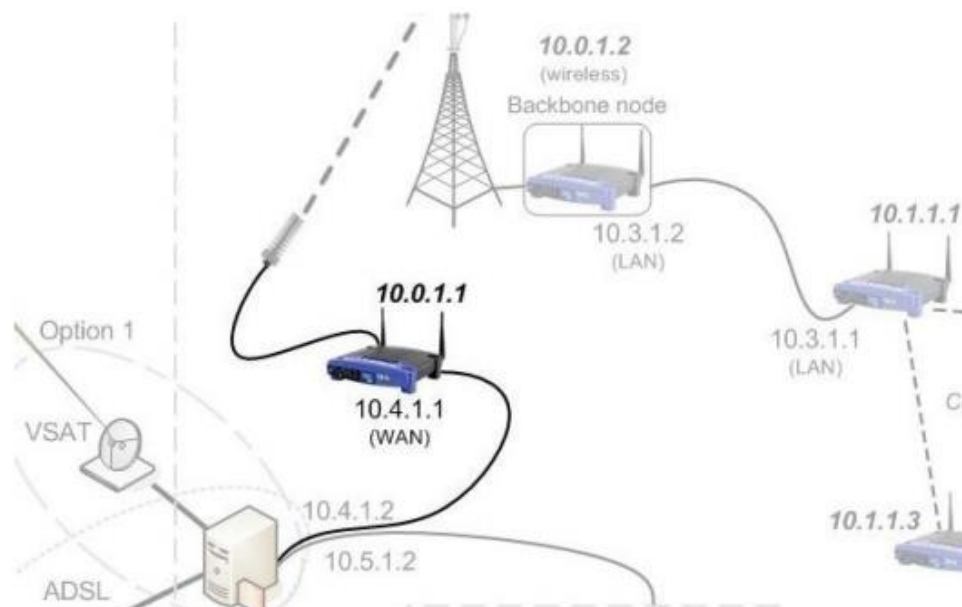


Рисунок 3.13 – Налаштування шлюзу

Після всіх налаштувань нам потрібно налаштувати WAN. Тому переходимо до наступного пункту кваліфікаційної роботи.

3.14 WAN та його налаштування

Широкополосна мережа (WAN) - це мережа пристроїв, локальних мереж (LAN) або міських мереж (MAN), які підключаються або через безпроводні, або через провідні лінії зв'язку. Віртуальна приватна мережа (VPN) з'єднує різні WAN-сайти.

Такі зв'язки охоплюють більші географічні райони і можуть рухатися між містами, регіонами та навіть країнами. WAN часто використовується найбільшими компаніями, які хочуть керувати та обмінюватися інформацією та ресурсами між філіалами. Цей тип мережі в основному використовується для підключення невеликих локальних мереж, і хоча він має більші можливості для передачі даних з локальних мереж, може підключити більш широкую зону покриття [47].

Детальніше про налаштування WAN для Mesh-мережі описано в додатку Д.

3.15 Прив'язка вузла мережі та точки доступу «спиною до спини»

Для підготовки точки безпроводного доступу необхідні наступні кроки:

1. Оновлення мікропрограми (DD-WRT)
2. Конфігурація

Потрібно звернути уваги на налаштування та плавне переведення програмного забезпечення на DD-WRT.

Першим кроком є оновлення Linksys до програмного забезпечення DD-WRT. Цього досягають, дотримуючись наведених нижче кроків.

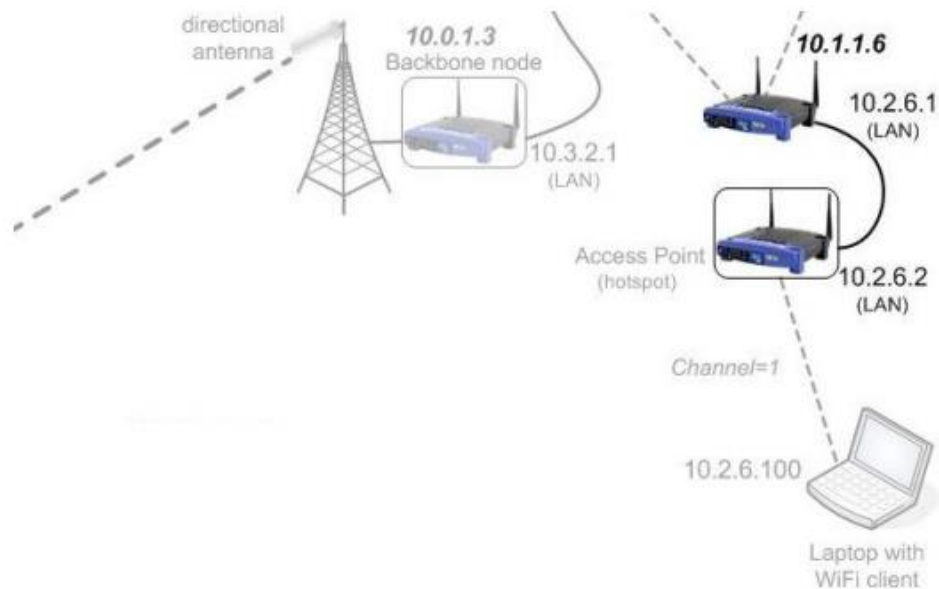


Рисунок 3.14 – Створення точки безпроводного доступу

На рисунку 3.14 вище зображено точки безпроводного доступу з з'єднанням «спина дог спини».

3.16 Оновлення програмного забезпечення до DD-WRT та налаштування

DD-WRT - це безкоштовна програмного забезпечення для багатьох безпроводних маршрутизаторів, заснована на чіпах BroadCom / Atheros / Xscale / PowerPC.

Першопочатково розроблена для серії маршрутизаторів Linksys WRT54G (включаючи WRT54GL і WRT54GS) і представляє собою мініатюрну операційну систему, засновану на ядрі Linux. Поширення під ліцензією GNU GPL v2 [48].

Версія DD-WRT до v22 була заснована на програмному забезпеченні від Sveasoft, яка в свою чергу була заснована на оригінальній програмного забезпечення фірм Linksys.

DD-WRT CONTROL PANEL Firmware: DD-WRT v23

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Setup | DDNS | MAC Address Clone | Advanced Routing | VLANs

Internet Setup

Internet Connection Type:

STP: Enable Disable (disable for COMCAST ISP)

Optional Settings (required by some ISPs)

Router Name:

Host Name:

Domain Name:

MTU:

Size:

Network Setup

Router IP

Local IP Address:

Subnet Mask:

Gateway:

Local DNS:

Network Address Server Settings (DHCP)

DHCP Type:

DHCP Server:

Time Setting

Automatically adjust clock for daylight saving changes:

Help [more...](#)

Automatic Configuration - DHCP:
This setting is most commonly used by Cable operators.

Host Name:
Enter the host name provided by your ISP.

Domain Name:
Enter the domain name provided by your ISP.

Local IP Address:
This is the address of the router.

Subnet Mask:
This is the subnet mask of the router.

DHCP Server:
Allows the router to manage your IP addresses.

Starting IP Address:
The address you would like to start with.

Maximum number of DHCP Users:
You may limit the number of addresses your router hands out.

Time Setting:
Choose the time zone you are in. The router can also adjust automatically for daylight savings time.

Рисунок 3.15 – Інтерфейс програмного забезпечення DD-WRT

Версії DD-WRT v23 та вище мають практично повністю переписаний код (рисунок 3.15).

Спеціальні функції, не включені в оригінальне програмне забезпечення, ми надали підтримку в DD-WRT. До нього відноситься мережа Kai, сервіси на основі демонів, IPv6, система безпроводного розподілу, RADIUS, можливості для розмови та підтримка апаратних модифікацій для SD-карт [49].

За допомогою даного програмного забезпечення ми будемо доналаштувати нашу Mesh-мережу. Детальніше про налаштування у додатку Е.

3.17 Обслуговування мережі

Запропоновані послуги залежатимуть від ряду факторів, таких як: вимога до пропускну здатності служби, технічні навички в спільноті, пам'ять, доступна в сітчастих вузлах, тощо. Деякі цінні послуги включають:

Шлюз / брандмауер (для формування смуги пропускання та управління): Це, як правило, сервер, що дозволяє спільне використання одного Інтернет-з'єднання. Зазвичай він підключається до VSAT на одному інтерфейсі, а безпроводна мережа - на іншому. Формування та управління пропускну здатністю також зазвичай знаходяться в шлюзі, щоб гарантувати, що кожен отримує пропускну здатність за те, за що заплатив (або щоб кожен отримав рівну частку пропускну здатності).

DNS (система доменних імен): система, що перетворює імена хостів та імена доменів на IP-адреси в Інтернеті або локальних мережах. Це може значно покращити час відгуку мережі.

Електронна пошта (заснована на Інтернеті або на сервері). Ця послуга дозволяє користувачам мережі спілкуватися, обмінюючись електронними повідомленнями, надісланими або отриманими через поштовий сервер. Найпростішим варіантом було б для всіх використовувати веб-систему електронної пошти, де сервер знаходиться десь в Інтернеті (наприклад, Gmail, Yahoo).

Чат / обмін миттєвими повідомленнями: це дозволяє здійснювати текстові розмови в режимі реального часу між користувачами комп'ютерів у мережевому середовищі, такому як Інтернет. Користувач набирає текстове повідомлення та натискає клавішу Enter. Текст одразу з'являється на комп'ютерах інших

користувачів, дозволяючи набрані розмови, які часто лише дещо повільніші, ніж звичайні розмови.

VOIP (на основі Asterisk): АТС (наприклад, Asterisk) потрібно налаштувати десь у мережі (близько до шлюзу було б зрозуміло), щоб можна було телефонувати між користувачами та мережею. Користувачеві потрібен звичайний телефон, підключений до аналогового телефонного адаптера (АТА), який знову підключається через Ethernet до сітчастого вузла Linksys.

Веб-проксі (для доступу до Інтернету): Мережева служба на основі сервера, яка дозволяє веб-браузерам встановлювати непрямі веб-з'єднання з загальнодоступними веб-сайтами. Це часто поєднується з кешем, щоб зберегти пропускну здатність, зберігаючи певний запитуваний вміст локально та розумно обслуговуючи локальну копію при наступному запиті.

Сервер спільноти: Веб-сервер може полегшити обмін інформацією між членами спільноти, наприклад, рекламні заходи, заплановані в спільноті, або послуги, пропонувані членами спільноти, та їх контактні дані. Він також може виступати як цифрова бібліотека, де можна отримати доступ до цінних для громади ресурсів, таких як медична інформація, сільськогосподарська інформація чи освітня інформація (наприклад, електронна енциклопедія) [50].

3.18 Висновок до третього розділу

У даному розділі описана безпосередньо побудова Mesh-мережі та підвищення її ефективності. Розроблена в Google Earth карта мережі с. Карашинці. Був розроблений розподіл каналів Mesh.

Зроблене також планування IP – адрес. Було детально показано встановлення програмного забезпечення Freifunk, налаштування кожного вузла. За допомогою OLSR було реалізовано безпроводну мережу. Також було детально описано налаштування LAN та WAN.

Описано встановлення програмного забезпечення DD-WRT та за допомогою неї налаштовано маршрутизатори та ціленаправлені антени для

створення Mesh- мережі.

Детально описані послуги та обслуговування даної безпроводної мережі.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ ТА ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Питання щодо безпеки життєдіяльності

Оскільки тема кваліфікаційної роботи пов'язана з галуззю ІТ, де люди працюють у приміщеннях, то розглянемо вплив виробничого середовища на здоров'я та працездатність людини.

Нормальна життєдіяльність людини вагомо залежить від умов зовнішнього середовища, зокрема виробничого. Адже в процесі трудової діяльності на організм людини чиниться своєрідний “тиск” несприятливими виробничими факторами, що прямо чи опосередковано впливають на її здоров'я та працездатність. Серед виробничих факторів прийнято розрізняти небезпечні та шкідливі [51].

Всі фактори на будь-якому підприємстві можуть мати різне походження. Часто можна стикатися з несприятливими умовами праці, які виникають з вини керівництва. Це питання потребує особливої уваги з боку перевіряючих органів. Хочеться сподіватися, що велика частина небезпечних факторів має природне походження, і людині просто необхідно вжити всі заходи, щоб їх вплив був мінімальним. Всі шкідливі виробничі фактори ГОСТ поділяє на наступні групи:

- Фізичні.
- Хімічні.
- Біологічні.
- Психофізіологічні, до яких можна віднести важкі та напружені умови праці.

Можна відзначити, що немає чіткої межі між шкідливими та небезпечними факторами, вона завжди умовна і у будь-який момент може бути зруйнована.

Небезпечний виробничий фактор – виробничий фактор, дія якого за певних умов може призвести до травм або іншого раптового погіршення здоров'я працівника.

Шкідливий виробничий фактор – виробничий фактор, вплив якого може призвести до погіршення стану здоров'я, зниження працездатності працівника.

Небезпечні та шкідливі виробничі фактори за природою дії поділяються на такі групи: фізичні, хімічні, біологічні та психофізіологічні [52].

До фізичних небезпечних та шкідливих виробничих факторів належать: рухомі машини та механізми; пересувні частини виробничого устаткування; підвищена запиленість та загазованість повітря робочої зони; підвищена чи понижена температура поверхонь устаткування, матеріалів чи повітря робочої зони; підвищений рівень шуму, вібрацій, інфразвукових коливань, ультразвуку, іонізуючих випромінювань, статичної електрики, електромагнітних випромінювань, ультрафіолетової чи інфрачервоної радіації; підвищені чи понижені барометричний тиск, вологість, іонізація та рухомість повітря; небезпечне значення напруги в електричному колі; підвищена напруженість електричного чи магнітного полів; відсутність чи нестача природного світла; недостатня освітленість робочої зони; підвищена яскравість світла; пряме та відбите випромінювання, що створює засліплюючу дію [53].

До хімічних небезпечних та шкідливих виробничих факторів належать хімічні речовини, які за характером дії на організм людини поділяються на:

- загальнотоксичні, що викликають отруєння всього організму;
- подразнюючі, що викликають подразнення дихального тракту та слизових оболонок;
- сенсibiliзуючі, що діють як алергени;
- канцерогенні, що викликають ракові захворювання;
- мутагенні, що призводять до змін наслідкової інформації;
- такі, що впливають на репродуктивну (дітонароджувальну) функцію.

До біологічних небезпечних та шкідливих виробничих факторів належать патогенні мікроорганізми (бактерії, віруси, мікроскопічні грибки та ін.) та продукти їх життєдіяльності, а також макроорганізми (рослини та тварини).

До психофізіологічних небезпечних та шкідливих виробничих факторів належать фізичні (статичні та динамічні) і нервово-психічні перевантаження

(розумове перенапруження, перенапруження органів чуття, монотонність праці, емоційні перевантаження) [54].

Один і той же небезпечний і шкідливий виробничий фактор за природою своєї дії може належати одночасно до різних груп.

Залежно від наслідків впливу на працюючих шкідливих та небезпечних виробничих факторів розрізняють виробничі травми, професійні захворювання та професійні отруєння, внаслідок яких може відбутись зниження або втрата працездатності (тимчасова чи постійна, повна чи часткова), можливий і фатальний кінець.

Виробнича травма – порушення анатомічної цілісності організму людини або його функцій внаслідок дії виробничих факторів.

Професійне захворювання – патологічний стан людини, обумовлений роботою і пов'язаний з надмірним напруженням організму або несприятливою дією шкідливих виробничих факторів.

Професійне отруєння – це порушення стану здоров'я в результаті дії шкідливих речовин при їх проникненні в організм людини у виробничих умовах. Довготривалий вплив незначних доз шкідливих речовин (однак дещо вищих за ГДК) призводить до хронічних отруєнь. Проникнення в організм великої кількості шкідливих речовин за короткий час (не більше доби) спричинює гострі отруєння [54].

4.2 Охорона праці

У кваліфікаційній роботі описано побудову та методи ефективності Mesh-мережі, які в свою чергу використовують мережеве обладнання, зокрема: маршрутизатори, комутатори, повторювачі, сервери, тому при роботі з даною технікою є необхідним дотримання правил охорони праці, техніки безпеки та протипожежної безпеки.

Згідно з законом України, нормативно-правові акти з охорони праці є обов'язковими для виконання у виробничих майстернях, лабораторіях, цехах, на

дільницях та в інших місцях трудового і професійного навчання, облаштованих у будь-яких навчальних закладах [55].

Всі пристрої мережевої взаємодії потребують живлення від електромереж, при цьому електромагнітні поля, які створюються цими пристроями, особливо негативно впливають на організм людини, яка безпосередньо працює з джерелом випромінювання. При дії випромінювання на людину можливі гострі та хронічні форми порушення фізіологічних функцій організму. Такі порушення виникають в результаті дії електричної складової випромінювання на нервову систему, а також на структуру кори головного та спинного мозку, серцево-судинної системи.

Приміщення, в яких планується установка та подальша робота з комп'ютеризованими приладами, за допомогою яких буде будуватися віртуальний макет комп'ютерної мережі, повинні відповідати проектній документації будинку, погодженій з уповноваженими державними органами. Крім того, повинні бути враховані санітарні нормативи освітлення, вимоги до параметрів мікроклімату (температура, відносна вологість), ступеня і сили вібрації, звукового шуму і вогнестійкості приміщення.

Конкретні показники зазначених санітарних норм знаходяться в Державних санітарних правилах і нормах роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98 [56].

Відповідне приміщення повинно бути укомплектоване системами центрального або індивідуального опалення, кондиціонування чи вентиляції повітря. При установці зазначених систем, необхідно переконатись, що батареї опалення, водопровідні труби, вентиляційні кабелі тощо, надійно сховані під захисними щитками, які перешкоджатимуть можливому потраплянню робітника під напругу.

У процесі роботи з модельованою комп'ютерною мережею, необхідно дотримувати правильний режим праці та відпочинку. В іншому випадку у робочого персоналу значно збільшується напруга зорового апарату, з'являються

скарги на незадоволеність роботою, головні болі, дратівливість, порушення сну, втому і хворобливі відчуття в очах, попереку, в області шиї і руках.

Робочі місця слід розташовувати так, щоб уникнути попадання в очі прямого світла. Джерела освітлення рекомендується розташовувати з обох боків екрану паралельно напрямку погляду. Для уникнення світлових відблисків екрану, клавіатури в напрямку очей користувача, від світильників загального освітлення або сонячних променів, необхідно використовувати антиполюсові сітки, спеціальні фільтри для екранів, захисні козирки, на вікнах - жалюзі.

Екран дисплея повинен бути розташованим перпендикулярно до напрямку погляду. Якщо він розташований під кутом, то стає причиною сутулості. Відстань від дисплея до очей повинна трохи перевищувати звичну відстань між книгою та очима.

Перед екраном монітора, особливо старих типів, повинен бути спеціальний захисний екран. При його відсутності треба сидіти на відстані витягнутої руки від монітора.

Фільтри з металевої або нейлонової сітки використовувати не рекомендується, тому що сітка спотворює зображення через інтерференцію світла. Найкращу якість зображення забезпечують скляні поляризаційні фільтри. Вони усувають практично всі відблиски, роблять зображення чітким і контрастним.

При роботі з текстовою інформацією (в режимі введення даних та редагування тексту, читання з екрану даних про поточний стан мережі, зміна конфігурації мережевих пристроїв тощо) найбільш фізіологічним правильним є зображення чорних знаків на світлому (чорному) фоні.

Монітор повинен бути розташований на робочому місці так, щоб поверхня екрана знаходилась в центрі поля зору на відстані 400-700 мм від очей користувача.

Залежно від джерела світла виробниче освітлення може бути: природним, що створюється прямими сонячними променями та розсіяним світлом небосхилу; штучним, що створюється електричними джерелами світла, та

суміщеним, при якому недостатнє за нормами природне освітлення доповнюється штучним. Природне освітлення поділяється на: бокове (одно - або двостороннє), що здійснюється через світлові отвори (вікна) в зовнішніх стінах; верхнє - через ліхтарі та отвори в дахах і перекриттях; комбіноване - поєднання верхнього та бокового освітлення.

Штучне освітлення може бути загальним та комбінованим.

Окрім вищезазначеного, важливою складовою охорони праці є пожежна безпека приміщень. Основними напрямками забезпечення пожежної безпеки є усунення умов виникнення пожежі та мінімізація її наслідків. Об'єкти повинні мати системи пожежної безпеки, спрямовані на запобігання пожежі, дії на людей та матеріальні цінності небезпечних факторів пожежі, в тому числі їх вторинних проявів. До таких факторів, згідно з ГОСТ 12.1.004-91, належать [57]:

- полум'я та іскри;
- підвищена температура навколишнього середовища;
- токсичні продукти горіння й термічного розкладу матеріалів і речовин;
- знижена концентрація кисню;

Відповідно до ГОСТ 12.1.004-91, пожежна безпека об'єкта повинна забезпечуватися системою запобігання пожежі, системою протипожежного захисту і системою організаційно-технічних заходів.

Основними вихідними даними при розробці комплексу технічних і організаційних рішень щодо забезпечення потрібного рівня пожежної безпеки в кожному конкретному випадку є чинна законодавча і нормативно-технічна база з питань пожежної безпеки, властивості матеріалів і речовин, що застосовуються у виробничому циклі, матеріалів, речовин і особливості виробництва.

Згідно з Положенням про порядок розроблення, затвердження, перегляду, скасування та реєстрації нормативних актів з питань пожежної безпеки, створено Державний реєстр нормативних актів з питань пожежної безпеки (НАПБ), до якого включено близько 360 найменувань документів, які поділені на 8 груп різних рівнів та видів: загальнодержавні, міжгалузеві, галузеві нормативні акти, нормативні акти міністерств, інших центральних органів виконавчої влади,

міждержавні стандарти з питань пожежної безпеки, державні стандарти України (ДСТУ) з питань пожежної безпеки, галузеві стандарти з питань пожежної безпеки, нормативні документи в галузі будівництва з питань пожежної безпеки [58].

Окрім документів, що увійшли до вищезгаданого реєстру, існує низка нормативних актів спеціального призначення, окремі розділи яких регламентують вимоги пожежної безпеки, такі як ДНАОП 0.00-1.32-01 "Правила будови електроустановок. Електрообладнання спеціальних установок, який визначає вимоги до електрообладнання. На основі цих даних визначаються критерії небезпеки об'єкта, категорії приміщень і будівель за вибуховою і пожежною небезпекою, а також класи вибухонебезпечних і пожежонебезпечних зон [58].

4.3 Висновки до четвертого розділу

В даному розділі розглянуто питання щодо безпеки життєдіяльності. В ньому описано про фактори виробничого середовища, які впливають на роботу персоналу, їхню безпеку під час роботи. Тому потрібно приділяти надзвичайно багато уваги безпеці персоналу, щоб таких факторів було якнайменше.

В розділі також описано про охорону праці. Розглянуто умови при яких працівник досягає високої ефективності і при цьому отримує якнайменше шкоди для свого здоров'я. Отже робимо висновок, що слід дотримуватись всіх правил охорони праці, щоб зберегти своє здоров'я як для себе, так і для свої колег.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи магістра досягнуто поставленої мети, а саме побудовано Mesh-мережу, реалізоване налаштування та встановлення програмного забезпечення, а також проаналізовано всі переваги та недоліки Mesh-мережі.

У ході виконання даної роботи інстальовано два види програмних забезпечення Freifunk і DD-WRT. Саме вони на даний момент є ідеальним варіантом для побудови великої безпроводної мережі за відносно невеликі кошти. Маршрутизатори Linksys WRT54GL зарекомендували себе доволі непогано. Вони дають потужний сигнал та легко з'єднуються між іншими вузлами мережі.

Також розроблено макет точок (вузлів) на карті за допомогою сервісу Google Earth. Це дало змогу детальніше зрозуміти де і на якій відстані будуть знаходитись маршрутизатори один від одного.

Здійснено детальне планування IP адрес з метою зручності обслуговування даної мережі в майбутньому для зручного.

Підтримка та модернізація спроектованої мережі є предметом подальших досліджень.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «TELECOMMUNICATION: PROBLEMS AND INNOVATION 2020. URL: http://www.dut.edu.ua/uploads/p_1739_44635808.pdf – Дата звернення 05.11.2020.

2. Науково-технічна конференція «Сучасні інфокомунікаційні технології» 2019 URL: http://www.dut.edu.ua/uploads/n_7726_26577046.pdf – Дата звернення 08.11.2020.

3. ДИСЕРТАЦІЯ «МОДЕЛІ І МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПЕРЕДАЧІ ТРАФІКУ» URL: http://www.dut.edu.ua/uploads/p_1739_44635808.pdf – Дата звернення 10.11.2020.

4. Аналіз ефективності методів маршрутизації на основі OLSR і AODV з балансуванням навантаження трафіку мережі Wi-Fi URL: <https://openarchive.nure.ua/bitstream/document/12709/1/Kry2016predt.pdf> – Дата звернення 13.11.2020.

5. Mesh мережі [Електронний ресурс] // Mesh network. URL: <https://studfile.net/preview/9937489/page:3/> – Дата доступу 15.11.2020.

6. Стандарт локальних мереж ieee 802.11 wi fi URL: <https://beloshop.ru/uk/ethernet-standard-ieee-80211-wi-fi/> – Дата доступу 18.11.2020.

7. Адаптація багатоантенних систем до невизначених умов зв'язку в Mesh мережах URL: http://journals.khnu.km.ua/vestnik/pdf/tech/2011_1/31pos.pdf – Дата доступу 23.11.2020.

8. Технологія ieee 802.11. Підтримка потокових даних. Сумісність з іншими стандартами бездротового зв'язку [Електронний ресурс]. URL: <https://teploskat.ru/the-technology-ieee-80211/> – Дата доступу 02.12.2020.

9. Протокол 802.11 URL: http://www.irbisnbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Nzundiz_2015_6_3.pdf – Дата доступу

06.12.2020.

10. Дослідження показників якості обслуговування в локальних бездротових мережах [Електронний ресурс]. URL:<http://masters.donntu.org/2019/fkita/kolenikov/diss/indexu.htm> – Дата доступу 11.12.2020.

11. Технологія бездротового інтелектуальної мережі SmartMesh. Нашу мережу не здолати. Основні особливості побудови mesh мереж [Електронний ресурс]. URL:<https://socscan.ru/uk/virusy/tehnologiya-besprovodnoi-intellektualnoi-seti-smartmesh-nashu-set-ne-odolet.html> – Дата доступу 15.12.2020.

12. Безпроводова MESH-мережа з енергозбереженням та балансуванням мережного навантаження URL:<https://er.nau.edu.ua/bitstream/NAU/41948/.pdf> – Дата доступу 18.12.2020.

13. Бездротові ad hoc мережі [Електронний ресурс]. URL: <https://montazhtv.ru/uk/rezhim-ad-hoc-besprovodnoi-seti-harakterizuetsya-sleduyushchim-vvedenie-v-seti-adhoc/> – Дата доступу 21.12.2020.

14. Ad Hoc мережа [Електронний ресурс]. URL: <https://nettech.ua/news/ad-hoc/> – Дата доступу 25.12.2020.

15. Актуальні задачі сучасних технологій: зб. тез доповідей міжнар. наук.-техн. конф. Молодих учених та студентів. URL: https://tntu.edu.ua/storage/pages/00000828/book%202_2020.pdf – Дата доступу 29.12.2020.

16. «Підвищення ефективності комп'ютерної мережі на основі топології Mesh» URL:http://elartu.tntu.edu.ua/bitstream/lib/34682/2/AZST_2020v2_Kovalenko_O_S-Improving_the_efficiency_29.pdf – Дата доступу 02.01.2021.

17. Вишневский В. Mesh-мережі стандарта IEEE 802.11: протоколи маршрутизації // Перша Миля. 2009. Том 10, №1. С 16-21.

18. Олифер, В. Г. Комп'ютерні мережі. Принципи, технології, протоколи : підручник для вишів / В. Г. Олифер, Н. А. Олифер. - Санкт- Петербург, 2010. - 944 с.

19. Cisco Aironet 1500 [Електронний ресурс] // Univers system integration. URL:https://www.unisi.ru/products/cisco/wireless/cisco_aironet_1500.php. – Дата

доступу 10.01.2021.

20. Нові комп'ютерні засоби, обчислювальні машини та мережі: Збірник наукових праць. Т.2. - К.: НАНУ, Ін-т кіберн. ім. В.М. Глушкова, Наук. рада НАН з проблеми «Кібернетика», 2001. - 176 с. - 6.00

21. Network bridge [Електронний ресурс] // Мобільний зв'язок. – Режим доступу: <http://celnet.ru/bridge.php>– Дата доступу 15.01.2021.

22. A. Raniwala and T. Chiueh. Architecture and Algorithms for an IEEE 802.11-Based Multi Channel Wireless Mesh Network. In Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'05), vol. 3, pp. 2223–2234. IEEE Communications Society Press, 2005.

23. B. Hubert, T. Graf, G. Maxwell, R. van Mook, M. van Oosterhout, P. B. Schroeder, J. Spaans, and P. Larroy. LARTC – Linux Advanced Routing & Traffic Control. URL <http://lartc.org/> - Access date: 18.01.2021.

24. Carleton University. Wireless Mesh Networking. URL <http://kunz-pc.sce.carleton.ca/MESH/index.htm>. - Access date: 20.01.2021.

25. Purdue University. Purdue University Wireless Mesh Network Testbed. URL <https://engineering.purdue.edu/MESH>. – Access date: 21.01.2021.

26. Santhanam, L.; Xie, B. & Agrawal, D. (2008). Selfishness in mesh networks: wired multi-hop MANETs. IEEE Journal of Wireless Communications, Vol 15, No 4, pp. 16 – 23.

27. Zhu, S.; Xu, S.; Setia, S. & Jajodia, S. (2003). LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks. Proceedings of ICDCS International Workshop on Mobile and Wireless Network, pp. 749 – 755, Providence, Rhode Island.

28. Perrig, A.; Canetti, R.; Tygar, J. D. & Song, D. (2000). Efficient authentication and signing of multicast streams over lossy channels. Proceedings of the IEEE Symposium on Security and Privacy, pp. 56 – 73.

29. Mathis, M.; Mahdavi, J.; Floyd, S. & Romanow, A. (1996). TCP selective acknowledgment options. IETF RFC 2018, October 1996.

30. Ylonen, T. SSH Protocol Architecture [Електронний ресурс] // Network Working Group. – 2006. – С. 1-5. – Режим доступу:

<https://tools.ietf.org/html/rfc4251> – Дата доступу 22.02.2021.

31. Perkins C., Bhagwat P. Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers. // Computer Communication Review. – Дата доступу 24.02.2021.

32. Du, W.; Deng, J.; Han, Y. S. & Varshney, P. K. (2003). A pair-wise key pre-distribution scheme for wireless sensor networks. ACM Transactions on Information and System Security, Vol 8, No 2, pp. 228 – 258.

33. S. M. M. Rahman, A. Inomata, T. Okamoto, M. Mambo, and E. Okamoto, “Anonymous secure communication in wireless mobile ad-hoc networks”, in Proceedings of the 1st International Conference on Ubiquitous Convergence Technology(ICUCT’06), Jeju Island, Korea, December 2006. Lecture Notes in Computer Science, vol 4412, pp. 140-149, Springer-Verlag, Heidelberg, Germany, December 2006.

34. J. Sen, P. R. Chowdhury, and I. Sengupta, «A distrusted trust establishment scheme for mobile ad hoc networks», in Proceedings of the International Conference on Computation: Theory and Applications (ICCTA’07), Kolkata, India, pp. 51-57, March 2007.

35. S. Bansal and M. Baker, Observation-based Cooperation Enforcement in Ad hoc Networks, Research Report cs.NI/0307012, Stanford University, USA, 2003.

36. C. Gentry, A Fully Homomorphic Encryption Scheme, Doctoral Thesis, Department of Computer Science, Stanford University, USA, 2009.

37. A. Khalili, J. Katz, and W. A. Arbaugh, “Towards secure key distribution in truly ad-hoc networks“, in Proceedings of the IEEE Workshop on Security and Assurance in Ad hoc Networks in conjunction with the IEEE International Symposium on Applications and the Internet (SAINT’03), pp. 342-346, Orlando, Florida, USA, January 2003. IEEE Computer Society Press.

38. Діапазони приватних IP-адрес Azure URL: <https://uk.assassionista.com/711737-azure-vnet-private-ip-ranges-SKNGBV> – Дата доступу 15.03.2021.

39. XenSource, Inc. XEN – The Xen virtual machine monitor. URL <http://www.xensource.com/>. – Access date: 26.03.2021.
40. J. Bicket, D. Aguayo, S. Biswas, and R. Morris. Architecture and Evaluation of an Unplanned 802.11b Mesh Network. In Proceedings of the 11th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'05), pp. 31–42. ACM Press, 2005.
41. R. Bruno, M. Conti, and E. Gregori. Mesh networks: commodity multihop ad hoc networks. IEEE Communications Magazine, 43(3):123–131, 2005.
42. M. Carson and D. Santay. NIST Net: a linux-based network emulation tool. ACM SIGCOMM Computer Communication Review, 33(3):111–126, 2003.
43. T. Clausen and P. Jacquet. The Optimized Link State Routing Protocol (OLSR). RFC 3626, October 2003.
44. K. N. Ramachandran, K. C. Almeroth, and E. M. Belding-Royer. A Framework for the Management of Large-scale Wireless Network Testbeds. In Proceedings of the 1st Workshop on Wireless Network Measurements (WiNMee'05). 2005.
45. RWTH Aachen University. UMIC-Mesh.net – A hybrid Wireless Mesh Network Testbed. URL <http://www.unic-mesh.net>. – Access date: 10.04.2021.
46. The Olsr.org Project. OLSRd – The olsr.org OLSR daemon. URL <http://www.olsr.org/>. – Access date: 10.04.2021.
47. D. Kidston, L. Li, H. Tang, and P. Mason, Mitigating Security in Tactical Networks, Communications Research Center, Defence R&D Canada (DRDC) Publication, September 2010.
48. J. Sen, “A distributed trust management framework for detecting malicious packet dropping nodes in a mobile ad hoc network”, International Journal of Network Security and its Applications (IJNSA), vol 2, no 4, pp. 92-104, October 2010.
49. H. Petersen and P. Horster, “Self-certified keys-concepts, and applications”, in Proceedings of the 3rd International Conference on Communications and Multimedia Security, pp. 102-116, Athens, Greece, September 1997.
50. G. Gaubatz, J. P. Kaps, and B. Sunar, “Public key cryptography in sensor

networks-revisited”, in Proceedings of the 1st European Workshop on Security Ad-Hoc and Sensor Networks (ESAS’04). Lecture Notes in Computer Science vol 3313, pp. 2-18, Springer-Verlag, Heidelberg, Germany, 2005.

51. Ткачук К.Н. Охорона праці і промислова безпека / К.Н. Ткачук, В.В. Зацарний, Л.Д. Третьякова та ін. // К.: Лібра, 2010. – 425 с.

52. Третьяков О.В. Охорона праці / О.В. Третьяков, В.В. Зацарний, В.Л. Безсонний // Харків, УЦЗУ, 2009. – 436 с.

53. 3. Гогіташвілі Г. Г. Системи управління охороною праці. — Л.: Афіша, 2002. – 320 с.

54. Про затвердження Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/z0508-18#Text> – Дата доступу 15.04.2021.

55. Шевченко Л. С. Основи економічної теорії. Харків, 2008. 448 с.

56. Закон України «Про охорону праці». Відомості Верховної ради України (ВВР), 1992, №2694-ХІІ, ст. 1.

57. ДСанПіН 3.3.2.007-98. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин.

58. ГОСТ 12.1.004-91. Система стандартів безпеки праці. Пожежна безпека.

ДОДАТКИ

Налаштування програмного забезпечення Freifunk

Розберемо по кроках налаштування системи. Як приклад див. Рисунок нижче.

1. Клацніть на Admin
2. Клацніть на System - Посилання для налаштування системних налаштувань.
3. Введіть на ваш вибір "Host Name" (Будь-яка унікальна описова назва для ідентифікації цього Linksys)
4. Ми **ОБОВ'ЯЗКОВО** обираємо країну, де ми використовуємо Linksys, щоб можна було визначити прийнятний параметр країни (в нашому випадку Україна).
5. Залишаємо всі інші варіанти недоторканими. Натисніть на "Подати заявку". З'явиться таке повідомлення:

The changed settings are committed. The settings are active after the next [Restart](#).

6. Клацніть на "Перезавантажити".

The screenshot shows the 'Admin: System' configuration page in the Freifunk firmware interface. The page has a yellow header with 'Home | Admin' and 'freifunk.firmware'. A sidebar on the left lists menu items: Admin, Password, Contact info, System, OLSR, Wireless, LAN, WAN, Publish, Software 1, Software 2, Firmware, and Restart. The main content area is titled 'Admin: System' and contains the following fields and options:

- Host Name:
- Domain:
- DNS Server:
- Use mini_fo: Enable Disable
- IPK Source:
- Network start messages: Enable Disable
- Timezone:
- Country:

At the bottom of the form are 'Apply' and 'Cancel' buttons. Below the form is a tip: "Tip: To ensure a convenient network access, you should enter the **Host Name** (a single name without dots) and the internal **Domain** (multiple names separated by dots). Example: If you set **Host Name** to "mywrt" and **Domain** to "mynet.freifunk.net", it should be possible to call up the pages of this device with <http://mywrt.mynet.freifunk.net/>, as well as with <http://mywrt/>." The footer of the page shows 'Changed: 30.11.2006' and a 'Top of page' link.

Безпроводні налаштування

1. Клацніть на Admin
 2. Клацніть на Wireless «Посилання для налаштування бездротового інтерфейсу»
 3. Виберіть “ Статичні ” для “ Протокол WLAN ”
 4. Введіть на ваш вибір “ WLAN-IP-адреса ”
 5. Введіть на ваш вибір “ Маска мережі WLAN ”
 6. Введіть на ваш вибір “ Маршрут за замовчуванням WLAN ”(якщо є, за замовчуванням пусто)
 7. Виберіть «Спеціальна (однорангова)» для “ Режим WLAN ”
 8. Введіть ESSID на ваш вибір
 9. Введіть BSSID за вашим вибором. (Завжди блокуйте BSSID. Ви можете вибрати MAC-адресу одного Linksys і використовувати його для всіх інших Linksys (-ів) у Mesh-мережі. BSSID важливо вказати, щоб дозволити повторне приєднання до мережевих мереж, якщо мережа коли-небудь прорветься щонайменше до 2 мереж через зникнення з'єднання та згодом відновлення).
 10. Введіть обраний вами канал, як правило, цифри від 1-13, однак, доступні канали залежно від країни, вибраної в налаштуваннях системи. З обговорення це може бути 1, 6 або 11.
 11. Виберіть “ Авто RX антена ” і “ Антена TX ”.
 12. Залиште решта варіантів недоторканими і перезавантажте пристрій.
- Детальніше рисунок нижче:

v1.4.5

Admin

Password

Contact info

System

OLSR

Wireless

LAN

WAN

Publish

Software 1

Software 2

Firmware

Restart

Admin: Wireless

WLAN Protocol:	Static
WLAN-IP Address:	10.1.1.4
WLAN Netmask:	255.255.255.0
WLAN Default Route:	
WLAN Mode:	Ad Hoc (Peer to Peer)
ESSID:	ptamesh
BSSID:	02:02:6f:34:21:a0
Channel:	6
Card Type:	<input type="radio"/> 802.11a <input checked="" type="radio"/> 802.11b/g
RX Antenna:	<input checked="" type="radio"/> Auto <input type="radio"/> Antenna A <input type="radio"/> Antenna B
TX Antenna:	<input checked="" type="radio"/> Auto <input type="radio"/> Antenna A <input type="radio"/> Antenna B
TX Power:	
Distance (Meter):	
Radio Mode:	Mixed B/G
Broadcast (E)SSID:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Basic Rate:	Default
Transmission Rate:	Auto
CTS Protection Mode:	Disable
Frame Burst:	Disable
Beacon Interval:	100
DTIM Interval:	1
Fragmentation Threshold:	2346
RTS Threshold:	2347
MTU Value:	

Apply Cancel

Tip: For most devices, the setting **Antenna A** activates the left antenna (seen from the front).

Changed: 18.11.2006

Top of page

Freifunk - Налаштування бездротового зв'язку

Налаштування LAN

1. Клацніть на Admin
2. Клацніть на LAN «Посилання для налаштування інтерфейсу локальної мережі»
3. Виберіть «Статичні» для «Протокол LAN»
4. Введіть на ваш вибір «LAN-IP»
5. Введіть на ваш вибір «Маска мережі» (Використання 255.255.255.0 якщо у вас немає «особливих» випадків для будь-якої іншої мережевої маски)
6. Введіть на ваш вибір «Маршрут за замовчуванням для локальної мережі»
7. Вимкнути «NAT», Встановивши прапорець біля нього
8. Вимкніть Брандмауер , Встановивши прапорець біля нього
9. Натисніть на Restart

Детальніше рисунок нижче:

Home | Admin

freifunk.firmware

Admin

Admin: LAN

LAN Protocol: Static

LAN IP: 10.2.4.1

LAN Netmask: 255.255.255.0

LAN Default Route:

Static Routes:

Disable NAT:

Disable Firewall:

DHCP Start IP: 192.168.1.100

DHCP Number of Users: 50 (DHCP off with "0")

DHCP Lease Time: seconds

Apply Cancel

Tip: These settings influence the configuration, which is sent to wired clients via DHCP. To ensure a convenient network access, you should enter the **Host Name** and the internal **Domain** (-> [System](#)).

Changed: 2.10.2006

Top of page

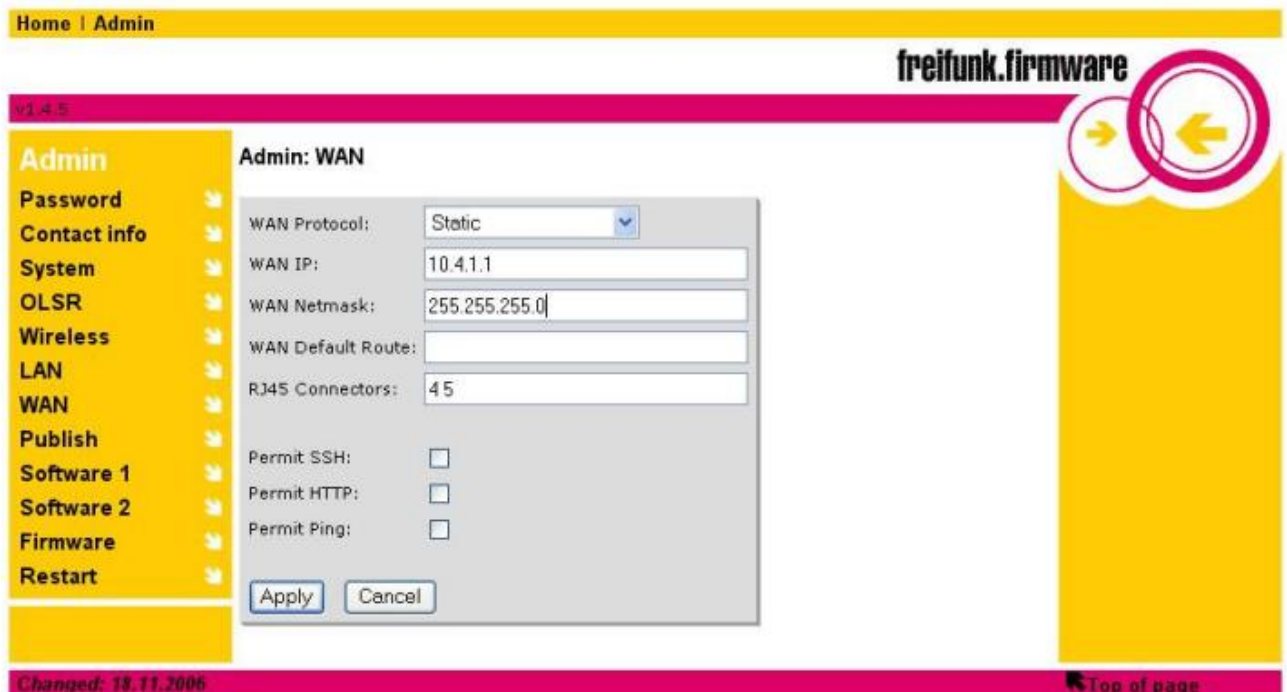
Налаштування OLSR

1. Клацніть на Admin
2. Клацніть на OLSR
3. Під " HNA4 " введіть текстове поле в перші три gjkz вашої IP-адреси локальної мережі, а потім - 0/24. (наприклад, якщо IP-адреса вашої локальної мережі - 10.2.4.1, введіть 10.2.4.0/24)
4. Якщо цей Linkys підключений до Інтернету, і ви хочете дозволити іншим вузлам доступ до Інтернету, натисніть " Увімкнути ", Щоб увімкнути динамічний шлюз“ DynGW "
5. Клацніть на Restart Процес перезапуску займе кілька хвилин і автоматично оновиться, коли Linksys закінчить процес перезапуску. ПРИМІТКА
ВАЖЛИВО: Незалежно від того, пропустили ви кроки перезапуску під час попереднього налаштування розділу чи ні, на даний момент ви ПОВИННІ ПЕРЕЗАВАНТАЖИТИ Linksys.

Налаштування WAN

Як приклад див. Рисунок нижче. Якщо на вашому сервері шлюзу (10.4.1.2 у наведеному вище прикладі) не запущено DHCP, виконайте кроки 1,2,3 (а), 4, 5. та 6. Якщо ваш сервер працює DHCP, виконайте лише кроки 1,2 та (b).

1. Клацніть на Admin
2. Клацніть на WAN
 - a. Виберіть “ Статичні ”Для“ Протокол WAN ”
 - b. Виберіть “ Динамічний ”Для“ Протокол WAN ”
3. Під WAN IP, введіть IP-адресу, яка знаходиться в діапазоні DHCP IP інших Linkys. З наведеного вище прикладу ви введете 10.4.1.1
4. Під WAN Мережева маска введіть 255.255.255.0
5. Під Маршрут за замовчуванням, Введіть IP-адресу брандмауера. З наведеного вище прикладу ви введете 10.4.1.2



Freifunk - налаштування WAN

Налаштування програмного забезпечення DD-WRT

1. Завантажте DD-WRT

2. Підключіть кабель локальної мережі (синій кабель, що міститься на упаковці Linksys) до ПК / ноутбука та до задньої панелі Linksys на одному з портів, позначених 1-4. Будь ласка НЕ скористайтеся портом із написом "Інтернет". Кабель локальної мережі не повинен бути кабелем, що постачається разом із Linksys, як і будь-який прямий (не перехресний) кабель локальної мережі.

3. Переконайтеся, що ваш апарат налаштований на автоматичне отримання IP-адреси. (Див. Додаток В - Етапи налаштування)

4. Підключіть Linksys до кабелю живлення (знаходиться на упаковці Linksys) і увімкніть джерело живлення.

5. Залежно від того, який LAN-порт Linkys ви використовували, передній світлодіод, що відповідає номеру порту ззаду, повинен бути світло-зеленим. Тобто, якщо ви використовували порт 1, тоді світлодіод 1 повинен світитися. Якщо світлодіод не світиться, перейдіть до Додатка С - Поширені запитання щодо усунення несправностей

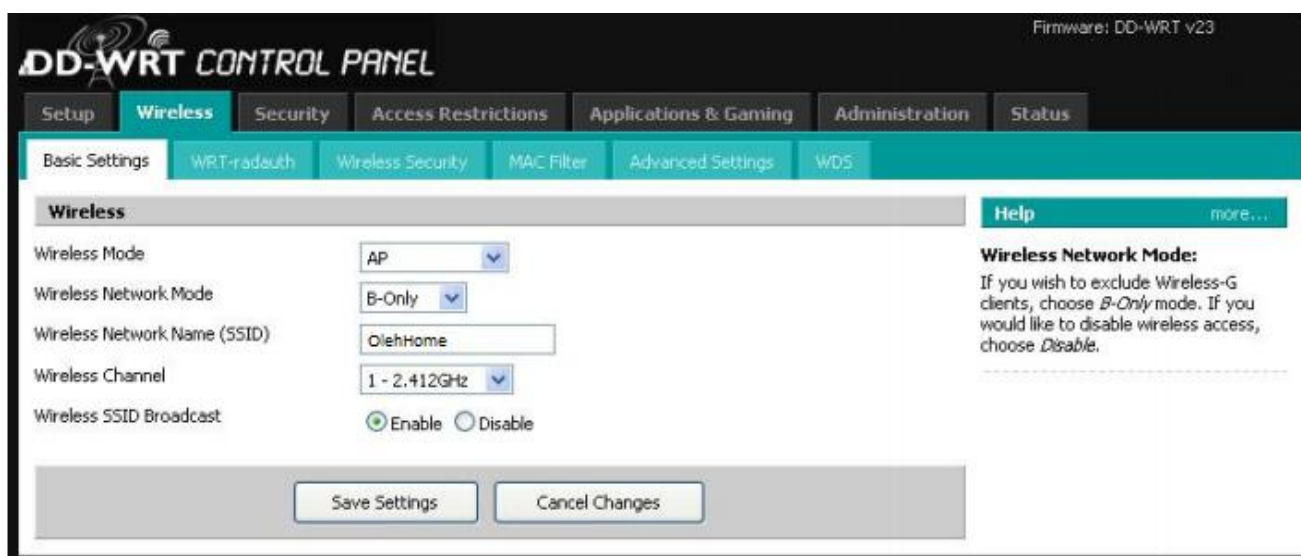
6. Відремонтуйте підключення до локальної мережі так, щоб ви отримали 192.168.1. x IP-адреса. (Див. Додаток В - Етапи налаштування) Щоб перевірити, чи є у вас 192.168.1. x IP-адреса: У вікні Мережні підключення: клацніть правою кнопкою миші на " Місцевий зв'язок " → виберіть " Статус " → натисніть на Підтримка ". Ви повинні побачити IP-адресу 192.168.1. x, (де $1 \leq x < 255$), ще перейдіть до Додатка С - Поширені запитання щодо усунення несправностей

7. Відкрийте веб-браузер і переконайтеся, що ваш браузер НЕ налаштований на встановлення веб-з'єднань через проксі. У полі адреси веб-браузера введіть: 192.168.1.1 і натисніть [Enter] Це перенесе вас на сторінку налаштування маршрутизатора Linksys Примітка: На запит про Ім'я користувача і Пароль використання: Ім'я користувача: корінь Пароль: адміністратор

8. Натисніть на "Адміністрація" → "Оновлення мікропрограми" → натисніть на "Перегляньте »Та у вікні« Вибрати файл »виберіть завантажену вами DD-WRT (ddwrt.v23_wrt54g.bin) → натисніть на "Оновлення". За цей час світлодіод живлення почне блимати. Примітка: ЗАЧЕКАЙТЕ для 4- 6 хвилин Переривання процесу оновлення може призвести до того, що Linksys стане непридатним для використання! Приблизно через 4-6 хвилин світлодіод живлення повинен постійно світитися (НЕ блимає) а світлодіод DMZ повинен постійно світитися ВИМК. Натисніть на "Продовжуйте" Це буде / має відкрити "WRT54GL - Налаштування"Сторінка

Налаштування бездротового зв'язку DD-WRT

1. Як приклад зверніться до рисунка нижче.
2. Натисніть на Wireless → натисніть на Basic Setting
3. У розділі Основні налаштування виберіть "AP" для "Wireless Mode"
4. Введіть SSID локальної точки доступу
5. Під "Wireless Channel" виберіть номер каналу
6. Решту налаштувань залиште за замовчуванням. Натисніть на "Save Setting"



Точка доступу - Налаштування бездротового зв'язку

Базові налаштування DD-WRT

Як приклад див. Рисунок нижче:

The screenshot displays the DD-WRT Control Panel interface. At the top, the title 'DD-WRT CONTROL PANEL' is visible on the left, and 'Firmware: DD-WRT v23' is on the right. Below the title bar, there are navigation tabs: 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. Under the 'Setup' tab, sub-tabs include 'Basic Setup', 'DDNS', 'MAC Address Clone', 'Advanced Routing', and 'VLANs'. The 'Internet Setup' section is active and contains the following fields:

- Internet Connection Type:** A dropdown menu set to 'Disable'.
- STP:** Radio buttons for 'Enable' (selected) and 'Disable (disable for COMCAST ISP)'.
- Optional Settings (required by some ISPs):**
 - Router Name:** Text input field containing 'WRT54G'.
 - Host Name:** Empty text input field.
 - Domain Name:** Empty text input field.
 - MTU:** A dropdown menu set to 'Auto'.
 - Size:** Text input field containing '1500'.
- Network Setup:**
 - Router IP:**
 - Local IP Address:** Four input fields containing '10', '2', '6', '2'.
 - Subnet Mask:** Four input fields containing '255', '255', '255', '0'.
 - Gateway:** Four input fields containing '0', '0', '0', '0'.
 - Local DNS:** Four input fields containing '0', '0', '0', '0'.
 - Network Address Server Settings (DHCP):**
 - DHCP Type:** A dropdown menu set to 'DHCP Forwarder'.
 - DHCP Server:** Four input fields containing '10', '2', '6', '1'.
 - Time Setting:**
 - Time Zone:** A dropdown menu set to '(GMT+02:00)'.
 - Automatically adjust clock for daylight saving changes:** An unchecked checkbox.

At the bottom of the page, there are two buttons: 'Save Settings' and 'Cancel Changes'. On the right side of the page, there is a 'Help' section with a 'more...' link. The help text includes:

- Automatic Configuration - DHCP:** This setting is most commonly used by Cable operators.
- Host Name:** Enter the host name provided by your ISP.
- Domain Name:** Enter the domain name provided by your ISP.
- Local IP Address:** This is the address of the router.
- Subnet Mask:** This is the subnet mask of the router.
- DHCP Server:** Allows the router to manage your IP addresses.
- Starting IP Address:** The address you would like to start with.
- Maximum number of DHCP Users:** You may limit the number of addresses your router hands out.
- Time Setting:** Choose the time zone you are in. The router can also adjust automatically for daylight savings time.

Основне налаштування точки доступу

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Національна академія наук України
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Шауляйська державна колегія (Литва)
Жешувський політехнічний університет ім. Лукасевича (Польща)
Білоруський національний технічний університет (Республіка Білорусь)
Міжнародний університет цивільної авіації (Марокко)
Національний університет біоресурсів і природокористування України (Україна)
Наукове товариство ім. Шевченка
ГО «Асоціація випускників Тернопільського національного технічного
університету імені Івана Пулюя»

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

Том II

**IX Міжнародної науково-технічної
конференції молодих учених та студентів
25-26 листопада 2020 року**



**УКРАЇНА
ТЕРНОПІЛЬ – 2020**

УДК 004.7

О.С. Коваленко

Тернопільський національний технічний університет імені Івана Пулюя, Україна

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ НА ОСНОВІ ТОПОЛОГІЇ MESH

O.S. Kovalenko

IMPROVING THE EFFICIENCY OF A COMPUTER NETWORK BASED ON TOPOLOGY

Бездротові мережі (Mesh мережі) відіграють сьогодні важливу роль в житті людини. Вони заповнюють все більше ніш в нашому житті і використовуються, насамперед, для доступу в Internet, а також для передачі звуку та відео з камер і мікрофонів, метео-даних для прогнозування погоди, активно застосовується в системах безпеки, платіжних терміналах, банкоматах. В процесі побудови мережі завжди виникають важливі питання. Як побудувати мережу? Як зробити її ефективною в офісі або ж на певній території? В даній доповіді буде описано, наскільки комп'ютерна мережа на основі топології Mesh ефективніша за звичайну мережу та коротко описано, що потрібно для побудови бездротової мережі. Розглянемо переваги бездротової мережі над звичайною. По-перше, звичайну мережу ми не реалізуємо без великої кількості кабелів. Mesh дозволяє бездротово покрити великі зони та має стійкість до втрат окремих елементів, що дає нам колосальний плюс. Наступною перевагою є те, що вузли мережі можна будувати недорого, з загальнодоступного обладнання. Бездротова мережа формується автоматично після налаштування та активації вузлів. Чим більше вузлів буде встановлено, тим швидша стане мережа. По-друге, якщо в мережі існують зайві маршрути, потік інформації не переривається в решті мережі, коли один вузол виходить з ладу. Мережа буде динамічно перенаправляти інформацію наступним доступним маршрутом. Ще можна виділити те, що право власності на мережу є спільним, тому тягар підтримки мережі не покладається на одну людину. З mesh немає проблеми єдиної точки відмови, яка є проблемою в зіркових топологіях. І головне, що відключення мережі неможливе, якщо не існує будь-якої всесвітньої катастрофи, яка знищує всі електронні пристрої в світі.[1]. Перед нами стоїть задача побудувати мережу в невеличкому селі під Тернополем. Нажаль, в даному селищі немає провайдера. Тому організувати звичайну мережу ми не зможемо. Але є вихід завдяки Mesh мережі. Mesh мережа (сітчаста мережа) – це топологія комп'ютерної мережі, в котрій кожен вузол виконує роль комутатора та передає дані по мережі.[2]. Для побудови мережі було обрано діаграмний тип мережі з магістраллю. Завдяки цьому можна уникнути сповільнення зв'язку, коли область мережі буде занадто великою. Також уникаємо різних перешкод: дерева, рослини тощо. Було зроблено два типи вузлів: "нормальний" та магістральний. "Нормальна" мережа працюватиме на каналі 6, а магістраль на каналі 11. Це забезпечить, щоб дві мережі не перешкоджали одне одній. Менше перешкод призведе до кращої роботи. Далі плануємо розподіл IP-адрес між бездротовою, локальною мережами та точками доступу. [2] Вся мережа буде побудована на маршрутизаторах Linksys WRT54GL та направлених антенах. Все це налаштовується на програмному забезпеченні Freifunk та DD-WRT.

Висновок: Топологія Mesh дозволяє нам побудувати велику безшовну мережу без кабелів і тому подібному, що притаманне звичайній комп'ютерній мережі. Дана мережа не є дорогою по обладнанню та налаштуванню, але вона дуже ефективна і допоможе людям в селищах, де неможливо прокласти кабелі від провайдера, користуватись інтернетом з доволі хорошою швидкістю.

Література

1. Аналіз роботи Mesh технологій [Електронний ресурс] - http://www.dut.edu.ua/uploads/p_421_42783021.pdf
2. Mesh сеть [Електронний ресурс] - https://wifi-solutions.ru/mesh_seti/

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ**

МАТЕРІАЛИ

VIII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

**«ІНФОРМАЦІЙНІ МОДЕЛІ,
СИСТЕМИ ТА ТЕХНОЛОГІЇ»**



9–10 грудня 2020 року

**ТЕРНОПІЛЬ
2020**

УДК 004.7

О.С. Коваленко

(Тернопільський національний технічний університет імені Івана Пулюя)

ПОБУДОВА КОМП'ЮТЕРНОЇ МЕРЕЖІ НА ОСНОВІ ТОПОЛОГІЇ MESH

UDC 004.7

O.S. Kovalenko

CONSTRUCTION OF A COMPUTER NETWORK BASED ON MESH TOPOLOGY

Mesh мережі (бездротові мережі) відіграють сьогодні важливу роль в житті людини. Вони заповнюють все більше ніш в нашому житті і використовуються, насамперед, для доступу в Internet, а також для передачі звуку та відео з камер і мікрофонів, метео-даних для прогнозування погоди, активно застосовується в системах безпеки, платіжних терміналах, банкоматах. В даній доповіді буде описано, як побудувати мережу на основі топології Mesh.

Насправді, бездротові мережі мають досить багато переваг порівняно зі звичайною мережею. А саме: побудова мережі без кабелів, стійкість до втрат окремих елементів. Також однією з переваг є те, що вузли мережі можна побудувати недорого [1].

Була поставлена задача побудувати мережу в невеличкому селі під Тернополем. Нажаль, в даному селищі немає провайдера. Тому організувати звичайну мережу ми не зможемо. Але є вихід завдяки Mesh мережі. Mesh мережа (бездротова мережа) – це топологія комп'ютерної мережі, в котрій кожен вузол виконує роль комутатора та передає дані по мережі [2].

Для побудови мережі було обрано діаграмний тип мережі з магістраллю. Завдяки цьому можна уникнути сповільнення зв'язку, коли область мережі буде занадто великою. Для того, щоб зв'язок був максимально стабільний, уникаємо природні (дерева, рослини) та електронні (мікрохвильова піч, тощо) перешкоди. Планування бездротової мережі було зроблено на основі стандартів IEEE 802.11 b/g. В даних стандартах є лише 3 смуги, що не перекиваються. Це канали 1, 6 і 11. Було зроблено два типи вузлів: "нормальний" та магістральний. "Нормальна" мережа працюватиме на каналі 6, а магістраль на каналі 11. Цей поділ на два канали забезпечить, щоб дві мережі не перешкоджали одне одній. Менше перешкод призведе до кращої роботи. Далі плануємо розподіл IP-адрес між бездротовою, локальною мережами та точками доступу. [2] Вся мережа буде побудована на маршрутизаторах Linksys WRT54GL та направлених антенах. Саме маршрутизатори Linksys WRT54GL найбільш підходять для побудови mesh мережі. Все це налаштовується на програмному забезпеченні Freifunk та DD-WRT. Freifunk – прошивка для маршрутизатора, що дає змогу створити вільну радіомережу, яка складається з самокерованих локальних комп'ютерних мереж. DD-WRT – прошивка, яка дозволяє якісно налаштувати направлені антени.

Дана розробка дозволяє побудувати велику бездротову мережу без кабелів та іншого додаткового обладнання, яке притаманне звичайній мережі. Мережа на основі топології Mesh не є дорогою по обладнанню та налаштуванню, тому є доволі доступною. Завдяки їй ми зможемо дати людям можливість вільно користуватися мережею Internet там, де інтернету не було ніколи. Я вважаю, що завдяки цій розробці люди зможуть подолати проблему мережевого зв'язку.

Література

1. Аналіз роботи Mesh технологій. URL: http://www.dut.edu.ua/uploads/p_421_42783021.pdf.
2. Mesh сеть. URL: https://wifi-solutions.ru/mesh_seti/.