МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

першого (бакалаврського) рівня вищої освіти

на тему: **«Проектування безшовної Wi-Fi мережі з використанням контролерів точок доступу»**

Виконав: студент 4 курсу групи Іт-41

Спеціальності 126 «Інформаційні системи та технології»
(шифр і назва)

Дудко Богдан Олесьович
(Прізвище та ініціали)

Керівник: к.т.н., в.о. доцента Падюка Р.І.
(Прізвище та ініціали)

ДУБЛЯНИ-2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА
ІНФОРМАЦІЙНИХ ТЕХНЕОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Перший (бакалаврський) рівень вищої освіти
Спеціальність 126 «Інформаційні системи та технології»

«ЗАТВЕРДЖУЮ»

Завідувач кафедри_____

д.т.н., проф. А. М. Тригуба
«____» _____2024 р.

ЗАВДАННЯ

на кваліфікаційну роботу студенту

Дудко Богдану Олесьовичу

1. Тема роботи: «Проектування безшовної Wi-Fi мережі з використанням контролерів точок доступу»

Керівник роботи Падюка Роман Іванович, в.о. доцента
затверджені наказом по університету від 27.11.2023 року № 641/к-с.

2. Строк подання студентом роботи 10.06.2024 р.
3. Вихідні дані до роботи: *вимоги до проектування корпоративних мереж; методика проектування інформаційних систем; технічне завдання на проектування безшовної Wi-Fiмережі .*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)
Вступ.
1. Аналіз предметної області.
2. Постановка задачі та вибір технологій для проектування мережі
3 Проектування безшовної мережі з використанням контролера точок доступу.
4. Охорона праці та безпека в надзвичайних ситуаціях
Висновки та пропозиції.
Список використаної літератури.
5. Перелік ілюстраційного матеріалу (з точним зазначенням обов'язкових креслень): *Огляд і порівняння існуючих бездротових технологій; Особливості побудови і функціонування мереж IEEE 802.11; 2.2. Архітектура мереж з використанням безпровідної технології Wi-Fi; Проектування мереж з використанням контролерів бездротової локальної мережі; Проектування*

комплексної структурної та функціональної схеми для бездротової локальної мережі Wi-Fi; Налаштування бездротової мережі на контролері Cisco WLC 5508

6. Консультанти з розділів:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1, 2, 3	*Падюка Р.І., в.о. доцента кафедри ІТ*		
4	*Городецький І.М., доцент кафедри фізики, інженерної механіки та безпеки виробництва*		

7. Дата видачі завдання 30 листопада 2023 р.

Календарний план

№ з/п	Назва етапів дипломного проекту	Терміни виконання етапів роботи	Примітка
1	*Написання першого розділу*	*30.11.23-02.02.24*	
2	*Виконання другого розділу та аркушів ілюстраційного матеріалу до нього*	*03-28.02.24*	
3.	*Виконання третього розділу та аркушів ілюстраційного матеріалу до нього*	*01.03-30.04.24*	
4.	*Написання розділу «Охорона праці»*	*01-15.05.24*	
5.	*Завершення оформлення розрахунково-пояснювальної записки та аркушів ілюстраційного матеріалу*	*15-30.05.24*	
6.	*Завершення роботи вцілому*	*01 -10.06.24*	

Студент _____ Дудко Б.О
(підпис)

Керівник роботи _____Падюка Р.І.
(підпис)

УДК 004.9 : 631.1

Проектування безшовної Wi-Fi мережі з використанням контролерів точок доступу. Дудко Б.О. Кафедра ІТ – Дубляни, Львівський НУП, 2024. Кваліфікаційна робота: 73 с. текст. част., 15 рис., 4 табл., 10 арк. ілюстраційного матеріалу, 27 джерел.

Проаналізовано предметну область та здійснено огляд і порівняння існуючих бездротових технологій та особливості побудови і функціонування мереж IEEE 802.11. Описано основні концепції побудови локальних корпоративних мереж.

Проаналізовано архітектуру мереж з використанням безпровідної технології Wi-Fi та окреслено основні підходи до планування, проектування і масштабування цих мереж.

Досліджено особливості проектування мереж з використанням контролерів бездротової локальної мережі;

Розроблено технічне завдання на проектування бездротової мережі та структурну і функціональну схеми для бездротової локальної мережі. Здійснено вибір апаратних засобів для реалізації проекту;

Виконано налаштування бездротової мережі на основні контролера точок доступу та перевірено її функціонування шляхом моделювання.

Розроблено заходи щодо охорони праці.

ЗМІСТ

ВСТУП

Бездротові технології є однією з найбільш швидко і ефективно розвиваються сфер в IT. Основні переваги включають гнучкість архітектури мережі, широку зону покриття, швидкі періоди розгортання, низькі витрати на встановлення бездротових мереж і мобільність. На додаток до переваг, перерахованих раніше, бездротові технології також можуть похвалитися високою захищеністю завдяки розширенню спектру. Сучасні локальні мережі будуються з використанням різних технологій, які надають співробітникам безліч варіантів спілкування в одному середовищі для всієї компанії

Бездротові мережі сприяють доставці програм і ресурсів у режимі реального часу в різних офісах. З поширенням громадських бездротових послуг організації змушені гарантувати мобільність персоналу, тоді як окремі користувачі прагнуть досягти будь-якого одержувача з будь-якого місця. Глобальний попит на бездротове підключення зростає, особливо в бізнесі та IT-секторах, де кінцеві користувачі можуть використовувати інформацію бездротовим шляхом для значного підвищення продуктивності, не будучи прив'язаними до традиційних комунікаційних інфраструктур.

Оскільки бездротові мережі та Інтернет-технології продовжують набувати все більшого значення як основних бізнес-інструментів, організації звертають увагу на підвищення продуктивності співробітників. Технологія бездротової локальної мережі (WLAN) зараз широко поширена в усіх секторах, розглядається як засіб для посилення існуючих можливостей мережі. Гнучкість, яку пропонують бездротові технології для підключення будь-коли та будь-де в мережі, є важливою; він відповідає критичній потребі у підвищенні гнучкості робочої сили та перспектив мобільності.

Більше того, це веде до позитивного внеску під час вибору робочого простору та розгляду методів роботи — зрештою сприяє покращенню якості роботи, що діє як рушійна сила ефективності підприємства.

Зростаючий попит споживачів спонукає постачальників послуг надавати бездротові послуги, що підтримують багатосервісність через один або кілька пристроїв для обміну повідомленнями, телефонних дзвінків, доступу до корпоративної мережі та підключення до Інтернету.

Із зростанням популярності бездротових локальних мереж (WLAN) питання безпеки мережі стають все більш важливими для підприємств. Адміністратори мережі повинні забезпечити свободу та мобільність кінцевим користувачам, одночасно запобігаючи доступу зловмисників до самої WLAN або до інформації, що передається через бездротову мережу.

АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Огляд і порівняння існуючих бездротових технологій

В даний час очевидна поширеність технологій бездротового обміну даними, що супроводжується прогресом у розповсюдженні інформації та використанням інноваційних методів. Ці технології охоплюють створення віртуальних мереж шляхом впровадження точок входу, які сприяють відповідні пристрої. Протягом кількох років докладалися зусилля для стандартизації бездротової технології, що призвело до підвищення швидкості передачі даних. Отже, ці вдосконалення забезпечують підключення в ситуаціях, коли дротове з'єднання неможливо або коли повна мобільність є важливою.

Важливо визнати сумісність бездротових і кабельних мереж. Бездротові технології спеціально розроблені для бездротової передачі інформації між кількома об'єктами на різних відстанях [1-3]. Ця передача може бути досягнута за допомогою інфрачервоного випромінювання, радіохвиль, оптичних сигналів або лазерного випромінювання. З часом було розроблено та продано численні бездротові технології, включаючи Bluetooth, WiMAX, Wi-Fi та інші [4-7]. Кожна з цих технологій має унікальні характеристики, які визначають їх конкретні застосування.

Як режим ad-hoc, так і режим інфраструктури підтримуються всіма технологіями бездротової передачі даних. Це означає, що ви можете налаштувати мережу без використання точки доступу або підключитися через точку доступу. Гнучкість цих технологій дозволяє додавати нових користувачів і встановлювати мережеві вузли в будь-якому місці без необхідності використання мережевих шнурів. Незалежно від місця розташування точки доступу набір абонентів не обмежується конкретною комп'ютерною мережею. З робочою станцією, яка завжди в режимі онлайн, підключення мережевого кабелю стає необов'язковим. Ви маєте свободу пересування в межах зони покриття та завжди залишаєтесь на зв'язку з мережею [8-16].

Впровадження бездротових технологій призводить до фундаментальних змін у соціальній структурі суспільства, змінює моделі державного управління та економічні механізми, революціонізує оборонні пріоритети та повсякденне життя громадян. Згідно

Згідно з прогнозами Міжнародного союзу електрозв'язку [11], очікується, що до 2025 року кількість пристроїв, підключених до мережі, перевищить кількість користувачів більш ніж у шість разів: 25,5 мільярдів пристроїв порівняно з 4 мільярдами людей. Експоненціальне зростання бездротових технологій безпосередньо пов'язане з їх широким впровадженням.

Галузь телекомунікацій стрімко розвивається завдяки широкому використанню «ноутбуків», інструментів пошукового дзвінка та пристроїв на кшталт «персонального секретаря» (Personal Digital Assistant або PDA). Значно розширилися і функціональні можливості мобільних телефонів. Ці розробки очевидні у впровадженні нових стандартів і технологій. Прогрес у радіоелектроніці, мікропроцесорній техніці та алгоритмах цифрової обробки сигналів, а також використання перспективних телекомунікаційних технологій проклали шлях до створення систем бездротового зв'язку, які віддають перевагу високій пропускній здатності та стійкості до перешкод. Ці системи призначені для підтримки різноманітних завдань, таких як розрахунок часу, бізнес-планування, постійний зв'язок з віддаленими станціями та зберігання документів. Принцип бездротових технологій полягає в тому, щоб надавати послуги зв'язку в будь-який час і в будь-якому місці, не будучи обмеженими місцезнаходженням або часом.

ZigBee, Bluetooth і Wi-Fi наразі є найпоширенішими технологіями бездротового зв'язку. Однак важливо зазначити, що кожна з цих технологій є кращою в різних областях і обставинах. У цьому аналізі ми глибше розглянемо їхні сильні та слабкі сторони, а також визначимо конкретні сфери, у яких вони найбільш ефективні.

Піонерська технологія Wi-Fi, також відома як Radio Ethernet IEEE 802.11, зробила революцію у створенні бездротових локальних мереж (WLAN) у

обмеженому просторі. Цей інноваційний стандарт, розроблений в Інженерному інституті електротехніки та радіо, дозволяє кільком користувачам мати рівноправний доступ до спільного каналу передачі даних [2].

IEEE, також відомий як Інститут інженерів з електротехніки та електроніки, розробив стандарт WI-FI, який можна порівняти зі стандартом 802.3, який використовується для традиційних дротових мереж Ethernet. В основі мережі WI-FI лежить точка доступу, яка також називається точкою доступу, яка може встановлювати з'єднання з різними наземними мережевими інфраструктурами, такими як офісна мережа Ethernet, і сприяти передачі радіосигналів [3] .

З часом з'явилися численні версії стандарту IEEE 802.11, які позначалися різними літерними індексами, зокрема a, b, c, d, e, g, h, i, j, k, i, m, n, o, p, q , r, s, u, v і w. Однак найбільш поширені та улюблені версії серед виробників обладнання обмежені лише чотирма: a, b, g та n. Решта версій служать удосконаленнями, доповненнями або переглядами вже встановлених специфікацій. Початкова специфікація стандарту IEEE залишається незмінною. Прийняття 802.11 відбулося в 1997 році, ознаменувавши значну віху в галузі передачі даних. Цей стандарт запровадив швидкість передачі даних 1 і 2 Мбіт/с у неліцензованому діапазоні частот 2,4 ГГц. Крім того, він реалізував механізм керування доступом до фізичного середовища, зокрема радіоканалу, за допомогою методу множинного доступу з визначенням несучої з уникненням зіткнень (CSMA-CA). Для повного огляду основних стандартів IEEE 802.11 зверніться до таблиці 1.1, у якій наведено їхні ключові технічні характеристики.

Таблиця 1.1 - Ключові характеристики основних стандартів IEEE 802.11

Стандарт	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Рік ратифікації Wi-Fi альянсом	1999	1999	2003	2009

Продовження табл. 1.1

Частотний діапазон, ГГц	5.15-5.24 5.67-5.85	2.4-2.482	2.4-2.483	2.4-2.481 5.14-5.25 5.67-5.85
Доступ до радіоканалу	CSMA-,CA	CSMA-CA	CSMA-CA	CSMA-CA
Кількість абонентів на один канал	64	64	64	64
Максимальна швидкість обміну даними	54 Мбіт/с	11 Мбіт/с	54 Мбіт/сек	600 Мбіт/сек
Звичайна швидкість передачі даних	23 Мбіт/сек	4 Мбіт/с	20 Мбіт/сек	120 Мбіт/с
Ширина каналу	20 МГц	22 МГц	20 МГц	40 МГц
Метод модуляції	OFDM	BPSK, CCK	OFDM	BPSK, QPSK, 16-,QAM, 64-,QAM
Дальність дії в приміщенні	10-20	20-100	20-50	10-20

Водночас варто відзначити, що Міжнародний альянс Wi-Fi представив свіжий бездротовий стандарт, відомий як Wi-Fi 802.11ah, або «На Low». Цей новий стандарт працює на частоті 900 МГц, дозволяючи сертифікованим Wi-Fi пристроям встановлювати з'єднання на великій відстані, споживаючи мінімальну енергію. За радіусом дії Wi-Fi «HaLow» перевершує існуючі варіанти Wi-Fi приблизно в два рази. Крім того, використання діапазону 900 МГц пропонує важливі функції для таких додатків, як мобільні електронні пристрої та переносні датчики.

На відміну від встановлених на даний момент частот 2,4 ГГц і 5 ГГц, Wi-Fi 802.11ah пропонує розширений діапазон сигналу, який вдвічі довший. Ця технологія гарантує стабільне з'єднання, навіть коли радіохвилі мають проникати через перешкоди, як-от стіни (див. рис. 1.1).

Варто відзначити, що новий стандарт Wi-Fi 802.11ah стійкий до перешкод від побутової техніки, наприклад мікрохвильових печей, завдяки альтернативній частоті.

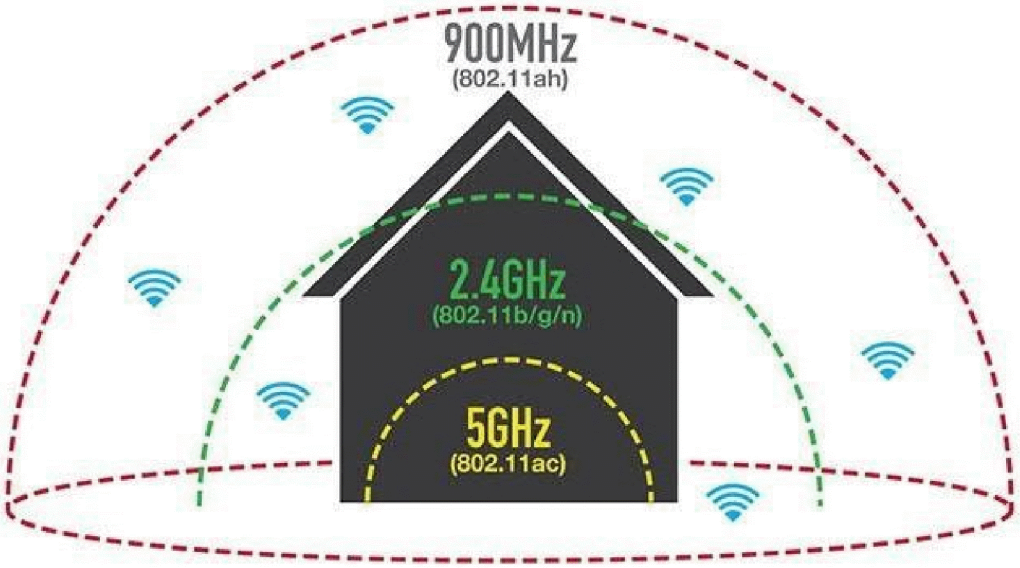


Рисунок 1.1 - Діапазон дії нового стандарту бездротового зв'язку Wi-Fi 802.11ah «HaLow».

Розробники запевняють, що Wi-Fi 802.11ah матиме всі переваги Wi-Fi, включаючи легку установку, сумісність з широким спектром пристроїв і надійний захист даних. Крім того, пристрої з підтримкою Wi-Fi «HaLow» зможуть працювати в діапазонах частот 2,4 і 5 ГГц, що дозволить їм легко інтегруватися в існуючу екосистему Wi-Fi, яка наразі складається з понад 7 мільярдів пристроїв. Подібно до пристроїв Wi-Fi, пристрої Wi-Fi «HaLow» підтримуватимуть IP-з'єднання, що дозволить їм працювати з хмарними сервісами, що є критично важливим для Інтернету та пов'язаних із ним сервісів. Ще однією істотною перевагою Wi-Fi «HaLow» є його здатність підключати численні пристрої до однієї точки доступу.

Поряд із новим стандартом Wi-Fi802.11ah, на горизонті є кілька важливих досягнень Wi-Fi. Одним із таких досягнень є розширення до діапазону 60 ГГц. WiGig Alliance зараз працює над розробкою технології Wi-Fi, яка працює в цьому частотному діапазоні, пропонуючи вражаючу максимальну швидкість

передачі 7 Гбіт/с. Ця розробка є особливо корисною для сценаріїв покриття picocell.

Удосконалена технологія Wi-Fi Direct забезпечує пряме з'єднання між різними клієнтськими пристроями на звичайній швидкості Wi-Fi без використання традиційних точок доступу чи бездротових маршрутизаторів. Крім того, є розширена підтримка передових рішень VoIP через оновлений набір стандартів WFA.

Процес створення конкурентоспроможних альтернативних послуг передбачає встановлення протоколів для розвитку стільникових (Mesh) мереж Wi-Fi. Ці мережі побудовані з використанням доступних модулів, які з'єднані з сусідніми пристроями через радіоканали в межах їхнього діапазону видимості.

- Покращення радіоінтерфейсу Wi-Fi для досягнення ще кращої продуктивності.

- Оптимізація взаємодії між клієнтами Wi-Fi і точками доступу для покращення загального досвіду для користувачів.

Завершуючи розгляд технології бездротової передачі даних Wi-Fi, важливо виділити її основні переваги, до яких належать: зручність використання готових модулів, повна інтеграція з існуючими дротовими мережами (LAN), швидка передача інформації, незначна вищі витрати на обладнання порівняно з іншими бездротовими мережами, відносно вище споживання енергії порівняно з іншими бездротовими мережами, потенційні перешкоди від інших пристроїв, що працюють у діапазоні частот 2,4 ГГц (наприклад, адаптери Bluetooth), робочі обмеження та частотні обмеження, характерні для кожної країни, і неадекватність стандарту шифрування WEP, що використовується для захисту доступу до мережі. Розширюючи різні застосування технології бездротової передачі даних Wi-Fi, стає очевидним, що вона широко використовується в багатьох галузях промисловості. Інтернет-провайдери, зокрема, прийняли цю технологію завдяки її здатності усувати потребу у великих кілометрах проводки.

Ігрова індустрія також використовує цю технологію: такі популярні бренди, як Sony і Nintendo, встановлюють пристрої Wi-Fi у свої ігрові консолі для доступу до Інтернету. Крім того, комерційні організації використовують Wi-Fi для підключення до Інтернету. У випадку великих компаній і корпорацій Wi-Fi віддають перевагу дротовим мережам Ethernet через його економічну ефективність.

1.2. Особливості побудови і функціонування мереж IEEE 802.11

Впроваджуючи технологію бездротового широкосмугового доступу, яка відповідає серії IEEE 802.11 (широко відомої як Wi-Fi), користувачі можуть задовольнити свої вимоги щодо доступу до Інтернету та передачі даних. Важливо відзначити, що Wi-Fi також надає можливість створювати конкретні мережі, що зрештою призводить до збільшення клієнтури та впровадження інноваційних послуг для користувачів. Однак успіх цих починань значною мірою залежить від правильної та ефективної побудови самої мережі.

Зростаюча поширеність досліджень у сфері бездротових технологій 802.11 стає очевидною при аналізі наукової та спеціальної літератури з цього питання. Цей сплеск досліджень можна пояснити новизною та швидким прогресом апаратного забезпечення та протоколів, які є основою цих мереж.

Відомі гравці у галузі виробництва радіоелектронних компонентів, такі як Digi, Freescale, Semiconductor, Ember і Texas, надають пріоритет аналізу та вирішенню проблем, пов'язаних зі створенням надійних бездротових мереж, що включає стандарт IEEE 802.11, поряд із розробкою програмні та апаратні рішення.

На даний момент дослідження в цій галузі зосереджені на розробці нових протоколів зв'язку, включаючи різні інструменти та інші пов'язані компоненти.

Помітні досягнення в галузі науки включають дослідження бездротових систем, які охоплюють повне розуміння їхніх ключових атрибутів і

формулювання універсального рівняння для кількісної оцінки потужності прийнятого сигналу.

Окрім поточних досліджень стандартів 802.11, також проводяться дослідження стандарту 802.16. Ці стандарти мають схожість і на обидва впливають подібні типи перешкод у середовищі передачі. У статтях розглянуто причини міжканальних перешкод для багатопозиційних сигналів і запропоновано методи боротьби з ними. Висновки показали, що використання більшого обсягу даних призводить до збільшення швидкості передачі в каналі, а також до більш високих вимог до параметру сигнал/шум. У цьому контексті важливо враховувати тип модуляції як важливий фактор.

Щоб забезпечити ефективну передачу інформації, стандарт 802.11 використовує дві різні методи модуляції. Низькошвидкісна передача використовує MPSK, тоді як високошвидкісна передача покладається на QPSK. Дослідження показали, що підтримка належного співвідношення сигнал/шум є вирішальним фактором для досягнення оптимальної передачі інформації.

Пропускна здатність, безсумнівно, є вирішальним фактором, який визначає будь-який канал передачі. Ефективність каналу визначається забезпеченням цього параметра в конкретних межах і потенціалом його розширення. І навпаки, досліджуючи бездротові канали стандарту 802.11 Wi-Fi, можна спостерігати обмежений частотний ресурс, який вміщує численні мережі, які використовують ті самі канали для передачі даних. Особливо це помітно в густонаселених і високорозвинених районах, де кількість мереж може перевищувати 50. У таких випадках, коли частотні канали перекриваються, інформаційні пакети кожної мережі займають часові інтервали між пакетами інших мереж. Ці обставини неминуче призводять до перешкод і подальшого зменшення параметра корисної смуги пропускання.

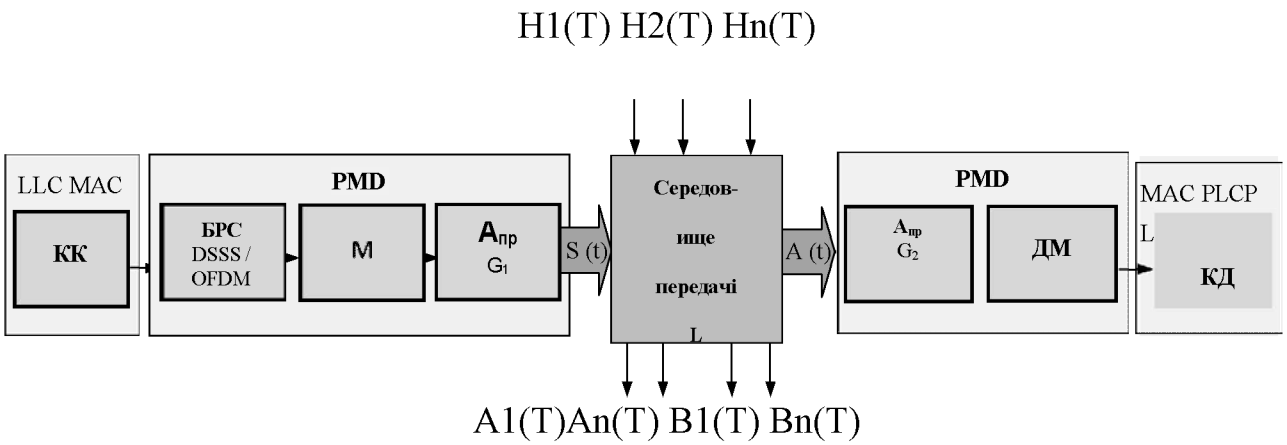
Враховуючи вищезазначені фактори, видається доцільним розглянути ці аспекти, щоб встановити ефективні принципи побудови та формалізації структури мережі.

Вивчаючи безліч факторів, які впливають на характеристики передачі, бездротовий канал у рамках стандарту 802.11 служить основою для наступних специфікацій. Подібно до інших стандартів у комітеті IEEE 802, документ IEEE 802.11 зосереджений на фізичному та канальному рівнях моделі OSI, причому останній далі поділено на два підрівні. Верхній підрівень, відомий як Logical Link Control (LLC), детально описаний у стандарті IEEE 802.2. Однак стандарт IEEE 802.11 конкретно стосується нижнього підрівня, контролю доступу до середовища (MAC), який керує доступом до середовища передачі. По суті, стандарт визначає протоколи взаємодії із середовищем передачі, включаючи швидкість і методи модуляції на фізичному рівні, а також принципи підключення пристроїв, автентифікації та механізмів захисту даних на рівні MAC.

Намір створення стандарту IEEE 802.11 полягав у створенні бездротової версії Ethernet, що дозволяє передавати пакети з використанням 48-розрядних адрес пакетів, що відображає структуру традиційних мереж Ethernet. Комітет IEEE 802 приділив велику увагу забезпеченню бездоганної сумісності всіх своїх стандартів, у результаті чого дротові та бездротові мережі під егідою IEEE 802 будучи легко сумісними один з одним.

При побудові бездротових мереж Wi-Fi аналіз каналів передачі можна візуалізувати у вигляді точок доступу та абонентських адаптерів, які служать інтерфейсами. Ці пристрої оснащені як передавачами, так і приймачами, що полегшує передачу радіосигналів через середовище та функціонує як перетворювачі, які перетворюють інформацію між мережевими інтерфейсами та радіосигналами.

На малюнку 1.2 показано базове налаштування бездротового каналу передачі, що складається з передавача та приймача. У каналі перешкодостійке кодування здійснюється на підрівнях LLC і MAC, а також на підрівні PLCP за допомогою канального кодера (CC). Цей процес передбачає створення кадру PPDU, який включає як службову, так і важливу інформацію для передачі.



B1 (t), ..., Bn (t) -перешкоди, які мають природний характер, перешкоди від пристроїв інших систем передачі і побутових приладів;

A1(T),..., An(T) - перешкоди, які вносять інші передавачі стандарту Wi-Fi;

H1(T), ..., Hn(T) - інтерференційні перешкоди.

Рисунок 1.2 - Структура бездротового каналу стандарту Wi-Fi.

Використовуючи квадратурний модулятор (M) і блок розширення спектру (SWB), PMD підрівня на рівні каналу перетворює двійкову послідовність у модульоване радіочастотне коливання. Для вищих стандартів, таких як 802.11n, використовується OFDM, тоді як для нижчих стандартів використовується DSSS. Передавальна антена (Apr) генерує сигнал S(t), який потім надсилається в середовище передачі. Потужність сигналу передавача дотримується заданого значення 100 мВт для стандарту Wi-Fi. Внутрішній шум від електричних кіл передавача незначний і ним можна знехтувати. Зміни та ослаблення сигналу в основному викликані перешкодами в середовищі передачі.

При розгляді радіотракту на наступному етапі необхідно приділити належну увагу першочерговому аспекту - частотному спектру. Стандарт IEEE 802.11 тісно пов'язаний із встановленими неліцензійними діапазонами частот у різних країнах, включаючи Сполучені Штати. Спочатку він був розроблений для роботи в діапазоні 2,400-2,4835 ГГц, пропонуючи широку смугу пропускання 83,5 МГц. Рисунок 1.3 ілюструє спектральну маску, передбачену

стандартом для одного каналу, з вимірюваннями потужності на основі піків функції Sin(x)/x. При -30 дБ ширина каналу охоплює 22 МГц, що дозволяє існувати три канали, що не перекриваються, у смузі частот 83,5 МГц [5].

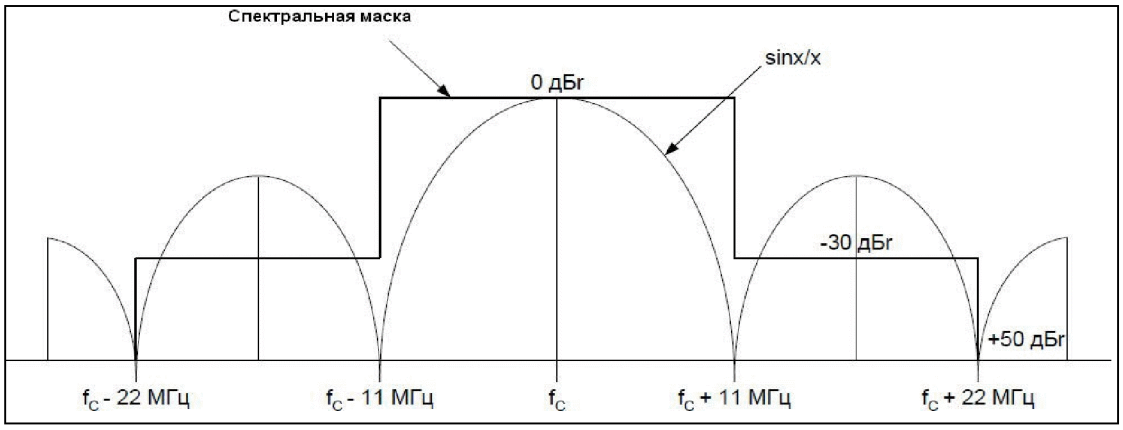


Рисунок 1.3 - Спектральна маска каналу мережі 802.11.

У стандарті IEEE802.11 існує два основні методи організації локальної мережі: принцип «одноранговий», який охоплює спеціальні мережі, як показано на малюнку 1.4, а), і структурована мережа, зображена на малюнку 1.6, б).

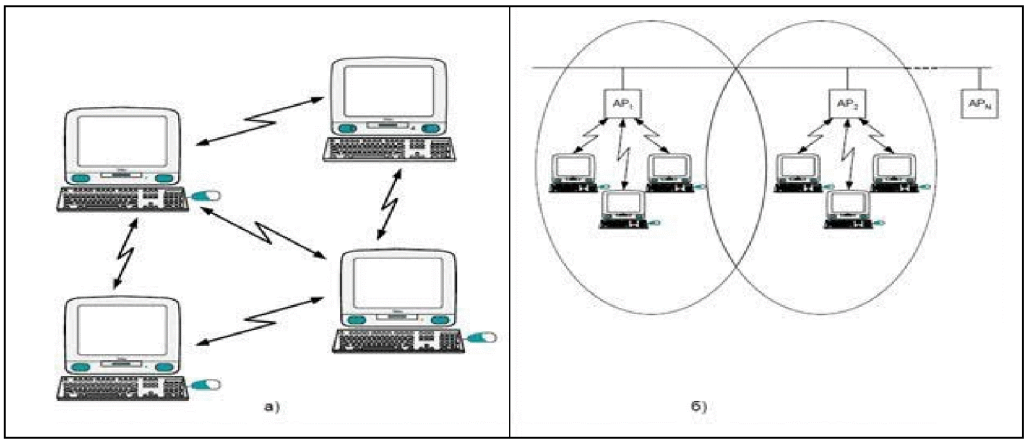


Рисунок 1.4 - Архітектура мережі 802.11: а - Ad-hoc-мережа; б - Структуровані мережі.

При встановленні зв'язку між двома станціями перший сценарій передбачає пряме з'єднання без будь-якого адміністративного втручання. Однак

у структурованих мережах, які зазвичай використовуються в мережах IEEE 802.11, точка доступу (AP) вводиться як додатковий компонент. Як правило, точка доступу стаціонарна і працює на певному каналі. Пристрої в мережі спілкуються виключно через точку доступу, яка служить шлюзом до зовнішніх дротових мереж.

Дротова мережа Ethernet з'єднує кілька точок доступу (AP) у мережі IEEE 802.11. По суті, цей тип мережі складається з набору базових станцій, розділених на окремі зони.

Можливість роумінгу між різними зонами точок доступу є ключовою особливістю стандарту IEEE 802.11, що дозволяє пристроям підтримувати зв'язок під час руху. Щоб вирішити проблеми з енергоспоживанням мобільних станцій, стандарт включає спеціальний протокол для керування використанням енергії. Під час передачі даних пристрій, що передає, має можливість перемикати приймач у режим очікування, оптимізуючи ресурси елемента живлення. Це забезпечує ефективне споживання енергії мобільними пристроями.

При побудові мережі IEEE 802.11 необхідно враховувати кілька важливих факторів. Перший – це вибір стандарту бездротової мережі, який можна порівняти в таблиці 1.1. Ця таблиця наочно демонструє незаперечні переваги стандарту IEEE 802.11n, включаючи підвищену швидкість передачі даних, розширену зону покриття, підвищену надійність передачі сигналу та збільшену пропускну здатність. Фізичний рівень цього стандарту містить удосконалення в обробці сигналу та модуляції, а також здатність передавати сигнали одночасно через чотири антени. На рівні мережі було досягнуто більш ефективне використання доступної смуги пропускання. У сукупності ці вдосконалення призводять до теоретичної швидкості передачі даних 600 Мбіт/с, перевищуючи 54 Мбіт/с стандарту 802.11a/g більш ніж у десять разів.

Далі важливо визначити підхід до інтеграції всіх компонентів бездротової мережі. Мета полягає в тому, щоб гарантувати безперебійну передачу та прийом даних із бездротової мережі на всіх мобільних пристроях у визначеній

зоні. Водночас важливо дотримуватися принципу, згідно з яким користувачі не повинні помічати жодних збоїв під час переміщення своїх мобільних пристроїв із однієї зони покриття Wi-Fi в іншу, усуваючи необхідність повторного підключення та введення пароля вручну.

Точка доступу Wi-Fi працює в кількох режимах, включаючи режим точки доступу (AP), режим бездротового мосту, режим AP/мост (AP + міст), режим ретранслятора (міст/ретранслятор), режим роумінгу (роумінг) і WDS (Бездротова система розподілу).

Вибір обладнання - ще один важливий аспект, який слід враховувати. З широким асортиментом виробників і брендів, доступних для мережевих бездротових пристроїв, дуже важливо встановити чіткі критерії вибору та зосередитися на ключових факторах. При виборі обладнання важливо звернути увагу на такі характеристики:

Розглядаючи пристрої Wi-Fi, необхідно враховувати кілька факторів, наприклад тип точки доступу (внутрішня чи зовнішня та придатна для використання в приміщенні чи на вулиці), тип антени (спрямована чи всеспрямована) , доступні порти та роз'єми на пристрої, підтримувані стандарти (зокрема IEEE 802.11), частотний діапазон, потужність бездротового сигналу, різні режими роботи та кількість користувачів, які можуть одночасно підтримуватися однією точкою доступу. Крім того, важливо зазначити, що можуть спостерігатися втрати ефективності сигналу Wi-Fi, коли він стикається з перешкодами. (див табл. 1.2.)

Таблиця 1.2 Втрата ефективності сигналу Wi-Fi при проходженні через різні середовища.

Перешкода	Додаткові втрати, Дб	Ефективна відстань,%
Відкритий простір	0	100
Вікно	3	70
Дерев'яна стіна	10	30

Продовження табл. 1.2

Міжкімнатні стіна завтовшки 15,2 см	15-20	15
Несуча стіна завтовшки 30,5 см	20-25	10
Бетонна підлога або стеля	15-25	10-15
Монолітне залізобетонне перекриття	20-25	10

При проектуванні бездротової мережі вкрай важливо враховувати кілька факторів: стандарт зв'язку, спосіб об'єднання точок доступу, тип обладнання і зону покриття «Корисного» сигналу. Нехтування будь-яким із цих моментів призведе до значного зменшення діапазону сигналу. Як наслідок, це може призвести до затримок і помилок під час доступу до послуг із високим трафіком. Тому важливо досліджувати нові методи та технології, які можуть мінімізувати вплив цих факторів. Одним із перспективних напрямів дослідження є вдосконалення математичних моделей для бездротових мереж та їхніх каналів, метою яких є точне відображення характеристик середовища передачі.

1.3. Основні концепції побудови локальних корпоративних мереж

Корпоративну мережу можна описати як складну комбінацію взаємопов’язаних програмних і апаратних елементів, які працюють разом, щоб полегшити обмін інформацією між різними програмами та системами, що використовуються в компанії. З кількома центрами обробки даних корпоративні мережі класифікуються як розподілені або децентралізовані обчислювальні системи [9]. Важливо розглянути корпоративну мережу з різних точок зору:

Корпоративну мережу можна проаналізувати з трьох різних точок зору:

- структурної,
- системної інженерії
- функціональної.

З точки зору функціональності, корпоративна мережа є високоефективною платформою для передачі важливої інформації, яка є ключовою для вирішення проблем корпорації.

З точки зору системної інженерії, корпоративна мережа — це комплексна структура, що складається з кількох взаємопов'язаних рівнів. Ці рівні включають спеціалізовані програми, системні служби, такі як веб-перегляд, електронна пошта, обмін файлами та мережевий друк, а також системи керування базами даних, мережеві операційні системи, системи транспортування даних, центри зберігання та системи оплати даних.

Корпоративну мережу, розглядаючи через призму системної інженерії, можна розуміти як комплексну систему, яка пропонує користувачам і програмам ряд цінних послуг. Ця система охоплює як загальносистемні, так і спеціалізовані додатки та має набір корисних якостей. Додатково до складу корпоративної мережі входять сервіси, що забезпечують безперебійну роботу мережі. Компоненти, які складають корпоративну мережу, як показано на малюнку 1.1, зазвичай складаються з наступних етапів [3].

Початковий етап підключення передбачає підключення пристроїв користувачів до мережі. Цей процес передбачає поділ користувачів на віртуальні підмережі (VLAN), впровадження основних заходів безпеки, таких як блокування невикористаних портів, фільтрація MAC-адрес або аутентифікація 802.1x [14]. Крім того, пріоритетність трафіку досягається шляхом призначення міток для класифікації якості обслуговування (QoS). Комутатори рівня доступу також забезпечують живлення IP-телефонів і бездротових точок доступу через технологію Power over Ethernet (PoE). Для забезпечення стійкості підключення до рівня розповсюдження встановлюється через два незалежні канали. Ця архітектура мережі ефективно обмежує вплив збоїв, оскільки лише користувачі в межах певної VLAN не зможуть отримати

доступ до корпоративних ресурсів, тоді як решта мережі залишатиметься повністю функціональною [1].

Рівень доступу виконує кілька важливих функцій, зокрема керування мережевим трафіком, контроль доступу до мережі та виконання різноманітних завдань, пов'язаних із прикордонними пристроями. Переходячи до рівня розподілу, цей рівень відповідає за три основні завдання.

На цьому рівні увага зосереджена на різних аспектах, таких як ізоляція ефектів зміни топології, контроль розміру таблиці маршрутизації та агрегування мережевого трафіку. Це передбачає маршрутизацію між різними мережами VLAN, впровадження заходів безпеки, пріоритетність передачі трафіку та використання відмовостійких протоколів для забезпечення стабільності мережі [17].

Основний рівень, третій рівень мережі, відіграє вирішальну роль у забезпеченні ефективної комутації пакетів між комутаторами рівня розподілу, серверною фермою та модулем EDGE. Існує два типи базових рівнів: вироджений тип ядра та ядро на основі базової мережі. У невеликих корпоративних мережах використовується вироджене ядро, яке складається з одного маршрутизатора. Однак цей тип ядра має свої недоліки, включаючи обмежену масштабованість і надійність. З іншого боку, це пропонує перевагу спрощеного адміністрування. На відміну від цього, ядро базової мережі складається з групи маршрутизаторів, з'єднаних між собою високошвидкісними каналами зв'язку. Цей тип ядра пропонує такі переваги, як гнучкість, масштабованість і надійність. Однак він має недолік, пов'язаний із вищими витратами на впровадження.

Зв'язок між корпоративною мережею та зовнішнім середовищем забезпечує Edge-Module. У межах Edge-Module є різні компоненти, які забезпечують зв'язок із низкою постачальників послуг, включаючи Інтернет-модуль, WAN-модуль і голосовий модуль.

Модуль підключення до Інтернету забезпечує безперебійне підключення до всесвітньої павутини. Його основні функції включають захист мережі,

забезпечення безпечного зв'язку з філіями та віддаленими користувачами через зашифровані канали (VPN), а також налаштування публічних серверів для веб-хостингу, служб електронної пошти та керування DNS.

Основною функцією модуля WAN є полегшення зв'язку та підключення між різними офісами та філіями в корпоративній мережі. Його головна мета – встановити надійне з'єднання, яке забезпечує високу якість обслуговування і постійну затримку. Ця можливість дозволяє розробляти розподілені корпоративні системи, які можуть ефективно підтримувати різні додатки, такі як IP-телефонія та відеоконференції.

Голосовий модуль забезпечує безперебійне з'єднання між внутрішньою телефонною мережею компанії та зовнішніми публічними мережами. Це дозволяє надавати послуги телефонії як традиційним операторам, так і операторам VoIP.

Ієрархічна структура корпоративної мережі дозволяє ефективно проектувати розгалужені мережі, забезпечуючи якість обслуговування на всіх рівнях, інформаційну безпеку, впровадження інтелектуальних послуг, систем IP-телефонії та відеоконференцзв'язку.

Проектування корпоративних мереж передбачає вирішення унікальних аспектів. Основною метою є встановлення відповідної комбінації апаратного та програмного забезпечення, а також структури та організації мережі з урахуванням специфічних характеристик інформаційних потоків підприємства. Вкрай важливо враховувати параметри як споживачів інформації, так і виробників, щоб відповідати фундаментальним вимогам до якості інформаційних послуг, що надаються мережею. Все це має бути виконано в рамках заданих обмежень щодо проектування, реалізації та витрат на обслуговування [7].

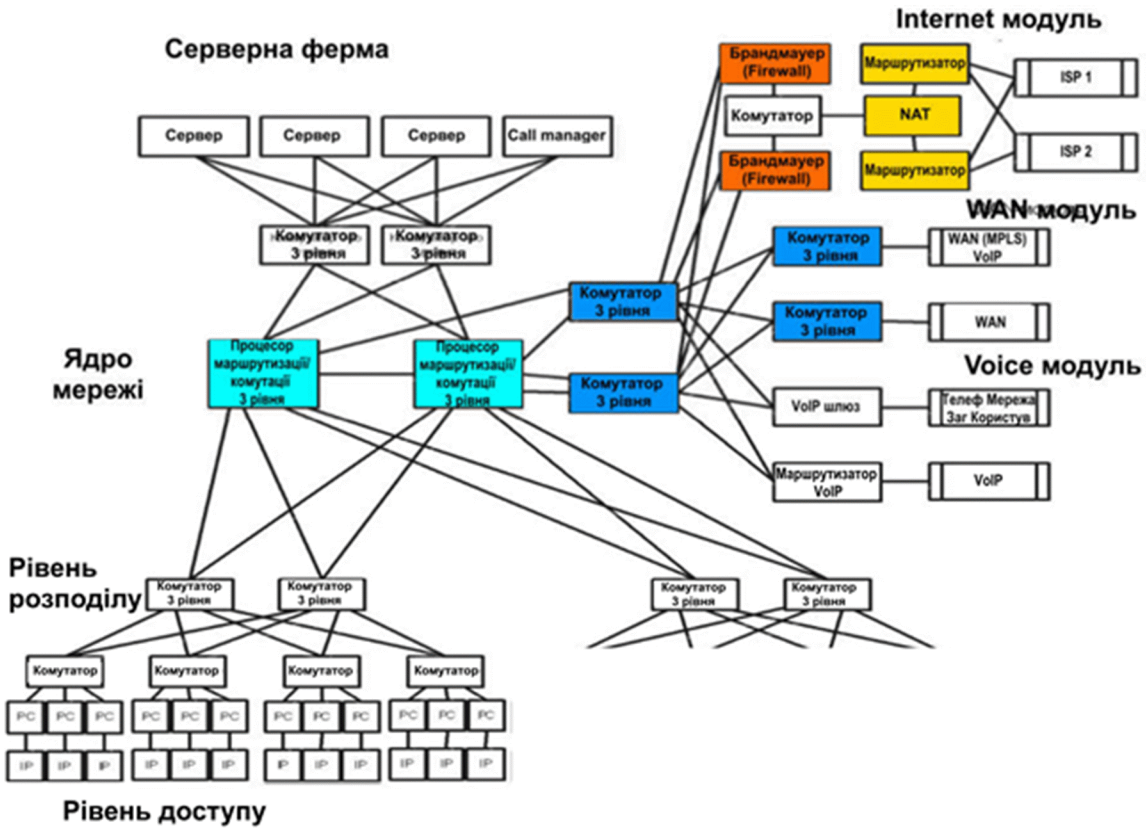


Рисунок 1.5 Загальна архітектура корпоративних мереж

При проектуванні корпоративної мережі мережеві інтегратори та адміністратори відповідають за дотримання кількох вимог. Вони включають розширюваність, що дозволяє легко інтегрувати мережеві компоненти, такі як користувачі, комп'ютери, програми та служби. Крім того, вирішальною є масштабованість, яка дозволяє мережі розміщувати все більшу кількість вузлів, довші з'єднання та підвищення продуктивності мережевого обладнання. Продуктивність є ще одним ключовим аспектом, який забезпечує відповідність мережевих вузлів і каналів зв'язку необхідним параметрам продуктивності, таким як час реакції, швидкість передачі даних, затримка передачі та варіація. Керованість також є важливою, забезпечуючи централізоване управління, моніторинг мережі та планування розвитку. Крім того, першорядним є надійність, яка гарантує безперебійну роботу мережевих вузлів і каналів зв'язку, а також цілісність, послідовність і неспотворену доставку даних до вузла призначення. Нарешті, безпека відіграє життєво важливу роль, захищаючи дані від несанкціонованого доступу.

2 ПОСТАНОВКА ЗАДАЧІ ТА ВИБІР ТЕХНОЛОГІЙ ДЛЯ ПРОЕКТУВАННЯ МЕРЕЖІ

2.1 Мета та задачі проекту

Метою проектування безшовної Wi-Fi мережі з використанням контролерів точок доступу є забезпечення стабільного та безперервного підключення до мережі для користувачів, незалежно від їхнього місця розташування в межах покриття мережі. Безшовність мережі означає, що користувачі можуть переміщатися між зонами покриття різних точок доступу (ТД) без втрати з'єднання чи переривання зв'язку. Це особливо важливо для корпоративних середовищ, навчальних закладів, лікарень та інших великих об'єктів, де користувачі постійно переміщуються. Контролери точок доступу відіграють ключову роль у цьому процесі, оскільки вони централізовано керують всіма ТД, забезпечуючи координацію передачі з'єднань між точками доступу, управління спектром частот, балансування навантаження та запобігання інтерференції.

Другим важливим аспектом є підвищення ефективності управління мережею та зменшення витрат на її обслуговування. Використання контролерів точок доступу дозволяє адміністраторам мережі централізовано налаштовувати та моніторити всі аспекти функціонування Wi-Fi інфраструктури. Це включає налаштування параметрів безпеки, управління пропускною здатністю, оновлення програмного забезпечення та діагностику проблем. Таким чином, контролери точок доступу забезпечують більш високу надійність і безпеку мережі, зменшують час простою і підвищують продуктивність користувачів, що, в свою чергу, призводить до зростання загальної ефективності роботи організації.

Для виконання цього проекту потрібно виконати наступні завдання:

- Проаналізувати предметну область, а саме здійснити огляд і порівняння існуючих бездротових технологій та особливості

побудови і функціонування мереж IEEE 802.11. Описати основні концепції побудови локальних корпоративних мереж

- Проаналізувати архітектуру мереж з використанням безпровідної технології Wi-Fi та окреслити основні підходи до планування, проектування і масштабування цих мереж ;
- Дослідити особливості проектування мереж з використанням контролерів бездротової локальної мережі;
- Розробити технічне завдання на проектування бездротової мережі та структурну та функціональну схеми для бездротової локальної мережі. Вибрати апаратні засоби для реалізації проекту;
- Здійснити налаштування . бездротової мережі на основні контролера точок доступу та перевірити її функціонування.

2.2 Архітектура мереж з використанням безпровідної технології Wi-Fi

Розробку та використання архітектурних рішень Wi-Fi можна розділити на дві основні тенденції: автономна архітектура та централізована/керована архітектура. Ці архітектурні підходи є основою для більшості проектів мереж Wi-Fi [8].

Коли йдеться про автономну архітектуру, рішення передбачає використання окремих точок доступу, які індивідуально налаштовуються та обслуговуються. Як наслідок, складність керування мережею, побудованою таким чином, зростає лінійно або навіть експоненціально зі збільшенням кількості пристроїв. Як правило, інженери уникають проектування великомасштабних мереж з автономною архітектурою, обмежуючи їх лише 3-5 пристроями. Однак є деякі винятки, які дозволяють використовувати трохи більші мережі, наприклад технологія кластеризації точок доступу. Важливо зазначити, що це не є повністю керованою архітектурою. Крім того, автономна архітектура створює проблеми, коли мова йде про впровадження системи безпеки бездротової мережі, оскільки стає майже неможливим виконати

кореляцію атак на всіх точках доступу в зоні покриття без централізованого концентратора. Кожна точка доступу має свій унікальний погляд на навколишнє середовище, сприймаючи ефір по-своєму. Щоб повністю зрозуміти подію нападу, вкрай важливо враховувати різні масштаби сприйняття та розуміння динаміки нападу. Це ж явище виникає, коли виникають проблеми з перешкодами, що перешкоджає координації керування радіоресурсами (RRM) між кількома точками доступу. Відсутність централізованого хабу для збору інформації з усіх точок доступу перешкоджає ефективним процесам прийняття рішень.

Слід підкреслити, що були задокументовані випадки автономних мереж, що складаються з багатьох точок доступу. Однак ключ до забезпечення безперебійного функціонування такої інфраструктури полягає в досвіді інженерів WLAN у IT-службі. Ці кваліфіковані фахівці розробляють індивідуальні сценарії для ефективного керування всіма точками доступу у великому масштабі.

Керування доступом, контроль SNMP і збір статистики є складною та ризикованою роботою. Цей підхід не слід сприймати легковажно, особливо враховуючи потенційні проблеми, які можуть виникнути під час підтримки цього рішення, якщо інженер-розробник, відповідальний за його створення, піде.

Контролер WLAN бере на себе відповідальність за керування всією інфраструктурою мережі радіодоступу в централізованій архітектурі. Cisco називає цю архітектуру CUWN (уніфікована бездротова мережа Cisco). У централізованому рішенні контролер виконує такі завдання, як завантаження та зміни програмного забезпечення, модифікація конфігурації, динамічне керування радіоресурсами (RRM) і встановлення мережевих з'єднань WLAN із зовнішніми серверами (AAA, DHCP, LDAP тощо). Крім того, контролер керує автентифікацією користувачів, профілями якості обслуговування QoS і спеціальними функціями. Щоб забезпечити безперебійний роумінг для клієнтів між різними точками доступу в межах зони покриття, контролери можна

згрупувати разом. Наприклад, рішення Cisco Systems дозволяє об'єднати кілька контролерів в один мобільний домен, що підтримує десятки тисяч точок доступу. Це забезпечує плавне перемикання або роумінг між точками доступу, керованими одним контролером, і тими, що контролюються різними. Успішно розгорнуто мережі з майже 100 000 точок доступу. Така масштабованість досяжна лише за допомогою керованої архітектури [2, 9].

Коли мова йде про пристрої з підтримкою Wi-Fi, такі як точки доступу або маршрутизатори, важливо віддавати перевагу тим, які підтримують 802.11n. Тепер давайте заглибимося в різні типи мереж, побудованих на основі технології Wi-Fi.

Забезпечення з'єднання Wi-Fi у житлових приміщеннях може бути досягнуто шляхом використання компактних маршрутизаторів Wi-Fi, таких як ті, що виробляються Cisco Linksys, D-Link, Netgear та іншими подібними брендами.

Як правило, у квартирі встановлюється один домашній маршрутизатор з підтримкою Wi-Fi (бажано з частотами 2,4 ГГц і 5 ГГц). Цей маршрутизатор підключений до мережі провайдера через дротовий інтерфейс, що дозволяє пропонувати бездротове з'єднання користувачам удома. Процес встановлення цього маршрутизатора вимагає використання простого програмного забезпечення.

Як користувач Android, ви можете використовувати Wi-Fi Analyzer, щоб перевірити частотні канали, які використовують сусідні пристрої. Досить часто ці пристрої працюють на однакових або тісно перекриваються каналах, що може призвести до перешкод. Проводячи спектральний аналіз, ви можете визначити незайняті канали або канали з найслабшою силою сигналу, дозволяючи вам оптимізувати продуктивність вашого пристрою. З точки зору безпеки мережі, більшість мереж покладаються на WPA2, зокрема WPA2-personal із PSK.

Щоб забезпечити доступ до Wi-Fi для невеликого офісу, рекомендується використовувати маленькі роутери, спеціально призначені для цієї мети. Ці

маршрутизатори, такі як Cisco WAP, WET, AP і Cisco ISR з модулями Wi-Fi, є більш ефективними та універсальними порівняно з домашніми маршрутизаторами. Крім того, існують інші подібні пристрої, які пропонують подібні функції, включаючи точки доступу, які можуть працювати в автономному режимі. [21]

Зіткнувшись із таким сценарієм, доцільно вибрати єдиний пристрій, який є одночасно універсальним і ефективним. Доступний простір обмежений, але робоче навантаження значно вище, ніж у квартирі, а вимоги до стабільності неперевершені. Тому найоптимальнішим вибором буде спеціальний пристрій, спеціально призначений для виконання цих завдань.

Для невеликих корпоративних мереж Wi-Fi, наприклад тих, що охоплюють один поверх або невеликий будинок, рекомендується використовувати централізовану архітектуру. Однак через обмежену кількість точок доступу, які зазвичай містяться в цих налаштуваннях (зазвичай не більше 10-20), ідеальним вибором є компактний і сучасний контролер. Це може бути автономний пристрій, наприклад Cisco 2500 або Aruba 3000, або його можна інтегрувати як модуль у багатофункціональний маршрутизатор, наприклад модуль SRE у маршрутизаторі Cisco ISR.

Коли справа доходить до керування великими корпоративними мережами доступу Wi-Fi, такими як університетські кампуси, корпоративні кампуси, офісні кампуси, заводські території та порти, централізована архітектура з надійними контролерами є найефективнішим підходом. Настійно рекомендується використовувати сучасні контролери, такі як Cisco 5508, Aruba A6000 або HP Pcm-Server, які розгортаються в центрі обробки даних мережі. У випадках, коли виробник пропонує модульні рішення для комутаторів або маршрутизаторів, наприклад Cisco WiSM або WiSM2, їх також можна використовувати.

Трирівнева модель включає можливість використання цього рішення на кордоні мережі. Впровадивши централізовану архітектуру, ви можете легко масштабувати свою мережу до будь-якого розміру та ефективно контролювати

її з одного централізованого місця, зменшуючи навантаження на ваш IT-персонал.

5. Надання зв'язку Wi-Fi для невеликих віддалених офісів, також відомих як мережі «філій», є звичайною практикою в різних галузях, таких як банківська справа. Ці мережі забезпечують централізований контроль і з'єднують безліч невеликих віддалених офісів із головним офісом. Як правило, зв'язок між цими віддаленими офісами та центральним офісом встановлюється через орендовані канали, надані операторами зв'язку, а іноді через супутникові канали.

Основна проблема в цьому сценарії полягає в тому, що в результаті типових заходів зі скорочення витрат у діловому світі бракує виділених, обширних і надійних каналів зв'язку між головним офісом і малими офісами. Як правило, з'єднання між цими віддаленими офісами встановлюється через

Що стосується доступу до Інтернету, більшість людей обирають найближчого та найдоступнішого провайдера, не беручи до уваги необхідність угоди про рівень обслуговування (SLA) або якщо провайдер навіть пропонує такі послуги. Для підключення до корпоративної мережі використовується VPN. Однак такий підхід часто призводить до таких проблем, як розірвання з'єднань або перевантаження мережі у віддаленому офісі або на стику, де мережа провайдера з'єднується зі штаб-квартирою. Незважаючи на ці проблеми, бажання мати бездротову мережу у віддалених офісах залишається сильним, особливо в банках, де потрібно обслуговувати кілька офісів. Однак утримання IT-персоналу в кожному офісі є нерентабельним, а відправка інженера з центру для вирішення проблем з мережею потребує багато часу та витрат. Тому рішення має вирішити ці проблеми.

Управління всією колекцією віддалених мереж Wi-Fi у різних віддалених офісах з одного центрального місця є важливим. Крім того, це управління має бути незалежним від будь-яких зовнішніх залежностей.

Канали, що з'єднують віддалені офіси зі штаб-квартирою, мають різні характеристики. Однак важливо переконатися, що існують параметри

централізованого моніторингу, усунення несправностей і налаштування віддалених пристроїв. Крім того, послуга Wi-Fi повинна надаватися у віддалених офісах із можливістю автентифікації клієнтів Wi-Fi та адаптації до тимчасової втрати з'єднання з центральним сайтом, що забезпечує плавний вхід і вихід клієнтів Wi-Fi.

Існує потенціал як для центрального, так і для локального перемикання трафіку користувачів, що передбачає спрямування трафіку з віддаленого сайту в центральне місце розташування або у віддалений офіс. Щоб полегшити це, потрібне спеціалізоване рішення, таке як хмарні контролери, які пропонують Cisco серії 7500 [10].

Міські мережі Wi-Fi, які пропонують точки доступу, розташовані на вулицях, забезпечуючи цілорічне обслуговування міських служб, жителів і відвідувачів.

У цьому сценарії основна увага приділяється повністю підключеним мережам Wi-Fi, також відомим як Mesh-мережі, де кінцевим користувачам надається послуга через один радіоінтерфейс точки доступу (зазвичай 2.4 ГГц), тоді як транспортний радіоканал встановлюється з сусідніми точками доступу через інший інтерфейс (зазвичай 5 ГГц). Mesh-мережі зазвичай складаються з двох типів TD: Mesh (відомий як MAP у Cisco) і Root (відомий як RAP у Cisco), причому RAP підключається до дротової мережі, а бездротова частина мережі будується на MAP. У мережі Mesh формуються дерева з коренем, розташованим у RAP, і ці дерева будуються за допомогою спеціалізованих протоколів (IAPP у Cisco). Як правило, гілки дерев не повинні перевищувати 8 стрибків, хоча це залежить від профілю трафіку та конструкції TD. Наприклад, якщо є лише один радіомодуль у діапазоні 5 ГГц, пропускна здатність зворотного зв'язку зменшується майже вдвічі на кожному стрибку, тоді як якщо є два незалежних радіомодуля 5 ГГц, зменшення пропускної здатності є мінімальним. Управління інфраструктурою Mesh зазвичай здійснюється контролером WLAN. В ідеалі програмне забезпечення WLAN Controller має бути здатне одночасно керувати як точками доступу в звичайному режимі, так і

точками доступу в Mesh Mode, оскільки це забезпечує гнучкість у введенні та налаштуванні проектів мережі, а також зв'язування зовнішніх і внутрішніх доменів для забезпечення безперебійної мобільності в межах мережі. мережі.

Варто зазначити, що подібні перехрестя часто використовуються для різних «вуличних/зовнішніх» проектів, таких як покриття кар'єрів, заводських територій, залізничних транспортних ліній тощо. 7. Унікальні сценарії вимагають різних підходів (ангари, склади, фабричні цехи, залізничні рішення (надземні та підземні – кожне потребує окремих підходів), рішення повітряного транспорту, рішення великих торгових центрів, стадіонів і великих об'єктів (з високою щільністю користувачів) , лікарняні розчини тощо). У всіх цих випадках оптимальним вибором є централізована архітектура, і рішення має бути адаптоване до конкретних вимог завдання.

Важливо визнати, що впровадження рішень Wi-Fi у різних умовах середовища призвело до розробки та використання трьох основних типів структур точок доступу [9]. По-перше, це кімнатні телевізори або «офісні» версії, які відомі своїм привабливим дизайном, вбудованими антенами та температурним діапазоном 0 - +40 °C. По-друге, є ТД, призначені для внутрішнього використання або варіанту «ангар-склад», які часто бувають у металевому корпусі, мають зовнішні антени та мають більший температурний діапазон від -20 до +55 °C. Нарешті, є ТД, спеціально розроблені для використання на вулиці, або «вулична» версія, яка зазвичай має посилений зовнішній корпус, зовнішні або вбудовані антени, захист від вологи та широкий температурний діапазон від -40 до +55 °C.

2.3 Основні підходи до планування, проектування і масштабування мережі Wi-Fi

Ґрунтуючись на емпіричних даних, очевидно, що Wi-Fi часто розглядають як просту та нескладну технологію в практичних ситуаціях.

Переважний метод зазвичай передбачає суб'єктивну оцінку необхідних точок доступу, розміщення замовлення та подальшу побудову мережі з нуля.

На жаль, результати використання цього методу є незадовільними, і навіть з найсучаснішою технологією ви можете стати свідками надзвичайно нестабільної та нерівної мережевої служби. Навпаки, вимоги до бездротового підключення постійно зростають із зростаючим набором ресурсомістких послуг, які тепер можна ефективно передавати через Wi-Fi або надавати через Wi-Fi. Зараз багато проектів потребують зосередження на потужності, а не на охопленні. Вкрай важливо обслуговувати пристрої з низьким споживанням енергії, такі як смартфони або RFID-мітки [11].

Оманлива простота проектування мереж Wi-Fi створює унікальний виклик для інженерів, на відміну від простої природи мереж 2G, 3G і WiMAX. Як наслідок, у будь-якому бездротовому проекті стає критично важливим приділяти значну увагу польовому радіодослідженню об'єкта (Site Survey).

Основні аспекти, які слід враховувати під час початкової оцінки проекту:

1. На яких частотах розчин буде ефективним?
2. Які фактори визначають, коли очікується розгортання? (такі міркування, як планування приміщення, характеристики будівлі, висота стелі тощо)
3. У випадках, коли очікується, що робота буде проходити у складних радіообстановках, наприклад, у машинобудівних цехах з численними перешкодами, необхідно провести ретельне радіообстеження місця.
4. Скільки осіб, особливо тих, хто активно користується послугою принаймні один раз, очікується, що будуть частиною мережі?
5. Важливим фактором, який слід враховувати, є розподіл користувачів по мережі.
6. Зони концентрації та прогнозована кількість користувачів у цих зонах є факторами, які необхідно враховувати.

7. Запуск мережі зумовлює необхідність надання певних послуг користувачам, а також окреслення планів щодо подальшого розширення, наприклад:

- Доступ до Інтернету включає такі міркування, як швидкість на користувача та мінімальні вимоги до пропускної здатності на краю сокета.
- Крім того, доступ до локальних ресурсів передбачає визначення того, які ресурси доступні та з якою швидкістю до них можна отримати доступ.
- Однією з доступних послуг є голос через Wi-Fi, також відомий як VoIP.
- Можливість потокової передачі відео за допомогою багатоадресної технології є також дуже цінною функцією.
- Одним з основних завдань включають також визначення місцезнаходження клієнтів Wi-Fi та/або RFID-міток у приміщеннях, а також встановлення передової системи безпеки для радіомовлення.
- Типи клієнтських пристроїв, що використовуватимуться в мережі, наприклад ноутбуки, планшетні комп'ютери, смартфони, сканери штрих-кодів, RFID-мітки тощо.

8. Які існуючі вимоги до автентифікації користувачів і які методи найбільше підходять для різних сценаріїв? Наприклад, які параметри доступні для автентифікації другого рівня, як-от 802.1x, або автентифікації третього рівня, як-от веб-портал?

9. Чи є необхідність пропонувати гостьовий доступ і які фактори слід враховувати в цьому відношенні (наприклад, можливість гнучкого керування гостьовими обліковими записами та можливість максимальної простоти чи максимальних можливостей під час створення нових облікових записів тощо)?

10. Чи є якісь міркування щодо зовнішнього вигляду приміщення, де буде працювати мережа Wi-Fi? Це має вирішальне значення для визначення того, чи достатньо внутрішніх антен, чи слід використовувати зовнішні антени, і якщо так, то які антени будуть більш естетично привабливими.

Плануючи встановити нову точку доступу, слід врахувати низку моментів. Не можна просто розмістити точку доступу в будь-якому місці будівлі і очікувати, що вона буде працювати оптимально. Перше, про що вам слід подумати, це розташування користувачів, яких точка доступу буде обслуговувати в цій будівлі. Користувачам потрібен доступ до бездротової мережі, коли вони знаходяться за своїми робочими столами, але їм також може знадобитися доступ до мережі Wi-Fi, коли вони знаходяться в конференц-залах або інших приміщеннях для зустрічей. У цьому випадку точки доступу слід розміщувати ближче до цих частин приміщення або поверху.

Також варто подумати про розташування внутрішніх стін у кожній конкретній частині будівлі. Потрібно намагатися уникати металевих і бетонних стін між точками доступу і користувачами, оскільки ці матеріали часто блокують або послаблюють бездротовий сигнал. Необхідно проаналізувати і прийняти рішення про тип антен, які потрібно використовувати у проектованому бездротовому середовищі. Крім того, потрібно переконатися, що використовується достатньо потужна антена з високим коефіцієнтом підсилення, щоб вона могла пробиватися крізь стіни, які можуть перешкоджати сигналу від точки доступу та досягати користувачів.

Можна використовувати кілька точок доступу, залежно від кількості користувачів і розміру будівлі. Рекомендується перекривати сигнал від точок доступу у співвідношенні 20-25%, щоб користувачі могли переходити від однієї точки доступу до іншої. Потрібно переконатися, що частоти, які використовуються точками доступу, не перекриваються, оскільки не бажано, щоб одна з точок доступу створювала перешкоди для частот іншої точки доступу. На рисунку 2.1 нижче показано приклад перекриття каналів, коли використовуються канали 1, 6 і 11 без жодної точки перекриття між точками доступу, які використовують певний номер каналу (мінімізація перешкод):

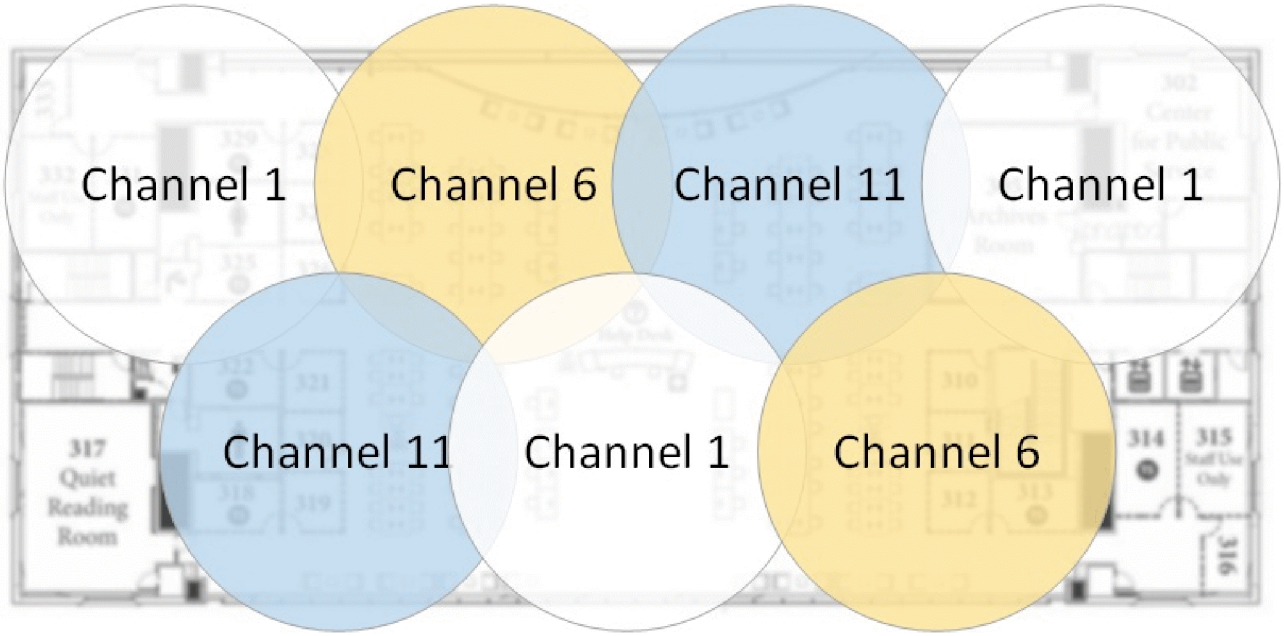


Рисунок 2.1 - Перекриття каналів точки доступу

Перед встановленням точок доступу слід провести відповідне обстеження ділянки, щоб забезпечити правильне розміщення з урахуванням розподілу сигналу, який вам знадобиться. Постачальники часто допомагають з цим процесом або дають експертні поради.

2.4 Особливості проектування мереж з використанням контролерів бездротової локальної мережі

Як відомо, будь-який дизайн — це дуже спрощена симуляція реальності, яка ще попереду. Тому передбачити всі можливі фактори з урахуванням усіх вимог, які можуть виникнути в майбутньому, практично неможливо.

Проте все ще можна сформулювати загальний підхід до проектування локальних комп'ютерних мереж, і деякі корисні принципи для таких проектів були запропоновані та успішно використані. Їх не слід розглядати лише як придатні для будь-якої практичної ситуації та враховувати всі можливі обставини [30].

Стадія архітектурного проектування. Важливість цього етапу пов’язана як з необхідністю спрощення вимог до проекту що впроваджується, та його до

окремих складових для забезпечення можливості прийняття зважених конкретних рішень у майбутньому, так і з його раціональністю [3].

Створюючи нову мережу для будь-якого бізнесу, слід враховувати такі фактори:

- необхідний розмір мережі (поточний, найближчий і заснований на прогнозах у майбутньому);
- структура, ієрархія та основні частини мережі (за відділами підприємства та за приміщеннями, поверхами та будівлями підприємства);
- основний напрямок та інтенсивність інформаційного потоку в мережі (зараз, у найближчому майбутньому та у віддаленому майбутньому), характер інформації, що передається через мережу (дані, цифрова мова, зображення), безпосередньо впливає на необхідну швидкість передачі ;
- технічні характеристики обладнання (комп'ютери, адаптери, кабелі, повторювачі, концентратори, комутатори) та їх вартість;
- можливість прокладки кабельних систем всередині і між приміщеннями, а також заходи щодо забезпечення цілісності кабелю;
- обслуговувати мережу та контролювати її надійність і безпеку;
- вимоги до програмних засобів щодо прийнятного розміру мережі, швидкості, гнучкості, розподілу прав доступу, вартості та можливостей контролю обміну інформацією;
- необхідність підключення до глобальної або інших локальних мереж.

Етап телекомунікацій означає вибір розміру та структури мережі [11]. У цьому випадку розмір мережі відноситься до кількості підключених до мережі комп'ютерів і відстані між ними. Необхідно чітко уявляти собі, скільки комп'ютерів (мінімум і максимум) необхідно підключити до мережі. При цьому слід залишити осторонь можливість подальшого зростання кількості комп'ютерів у мережі, хоча б на 20-50%.

В ідеалі структура мережі повинна відповідати структурі будівлі підприємства або будівельного комплексу. Робоче місце групи працівників, які

працюють над одним завданням (наприклад, бухгалтерія, відділ продажів, інженерна група), повинно бути розташоване в одній або суміжних кімнатах. Потім ви можете об'єднати комп'ютери цих співробітників у сегмент мережі, робочу групу та встановити сервер біля кімнати, де вони працюють, разом із концентратором або комутатором, який з'єднує всі комп'ютери.

При виборі мережевого обладнання слід враховувати багато факторів, особливо [5,16]:

- ступінь стандартизації обладнання та його сумісність з найбільш часто використовуваними програмними засобами;
- швидкість передачі інформації та потенціал її подальшого вдосконалення;
- можливі топології мережі та їх комбінації (шина, пасивна зірка, пасивне дерево);
- спосіб управління комутацією мережі (CSMA/CD, повнодуплексний або тегований метод);
- дозволені типи мережевих кабелів, максимальна довжина, захист від перешкод;
- вартість і технічні характеристики конкретного обладнання (мережеві адаптери, трансивери, повторювачі, хаби, комутатори).

Наступний етап – оптимізація та усунення несправностей працюючої мережі. Можливі причини цих проблем [19]:

- недоліки використовуваного програмного та апаратного забезпечення;
- мережева операційна система налаштована неправильно;
- несправність кабельної системи;
- збій на рівні мережевого протоколу через несумісність або збій мережевого обладнання або його неправильну конфігурацію;
- неправильна організація локальної мережі, наприклад, недостатня сегментація в мережі типу Ethernet, що може призвести до виникнення додаткових колізій пакетів.

Що стосується саме контролерів бездротової локальної мережі (рис. 2.2), то вони складаються з наступних компонентів:

- Бездротова локальна мережа - (тобто ім'я SSID)
- Інтерфейси - логічні інтерфейси, які відображаються на мережеву VLAN
- Порт розподілу - фізичне підключення до комутатора, точки доступу або маршрутизатора

Рисунок 2.2 - Фізичний вигляд CISCO WLC 5508

Іспити CCNA Wireless та Cisco Design дуже детально розглядають питання проектування бездротових мереж. При проектуванні бездротової мережі слід ретельно проаналізувати надмірність контролерів. Радіоканали вимагають обстеження радіочастотного поля та управління сертифікованими фахівцями з бездротового зв'язку.

Однією з головних особливостей рішення WLAN є можливість доступу користувачів до мережевих ресурсів з різних зон, в тому числі з тих, де важко прокласти кабель. Ще однією причиною використання WLAN є політика організації, яка дозволяє гостьовий доступ тільки через бездротову мережу. Іноді рішення WLAN будується як перехідна мережа, поки не буде впроваджена повноцінна дротова мережа.

Враховуючи вищезгадані сценарії, кінцеві користувачі, швидше за все, будуть переїжджати з одного місця в інше. Вирішенням цієї проблеми є функції роумінгу та мобільності, які дають користувачам можливість доступу до мережі з різних місць. Роумінг відбувається, коли бездротові клієнти змінюють свою асоціацію з однієї точки доступу до іншої без втрати зв'язку. Проектувальники

мережі повинні ретельно масштабувати бездротову мережу, щоб уможливити процес роумінгу клієнтів. Бездротовий роумінг можна розділити на дві категорії:

- Внутрішньоконтролерний роумінг
- Міжконтролерний роумінг (рівень 2 або рівень 3)

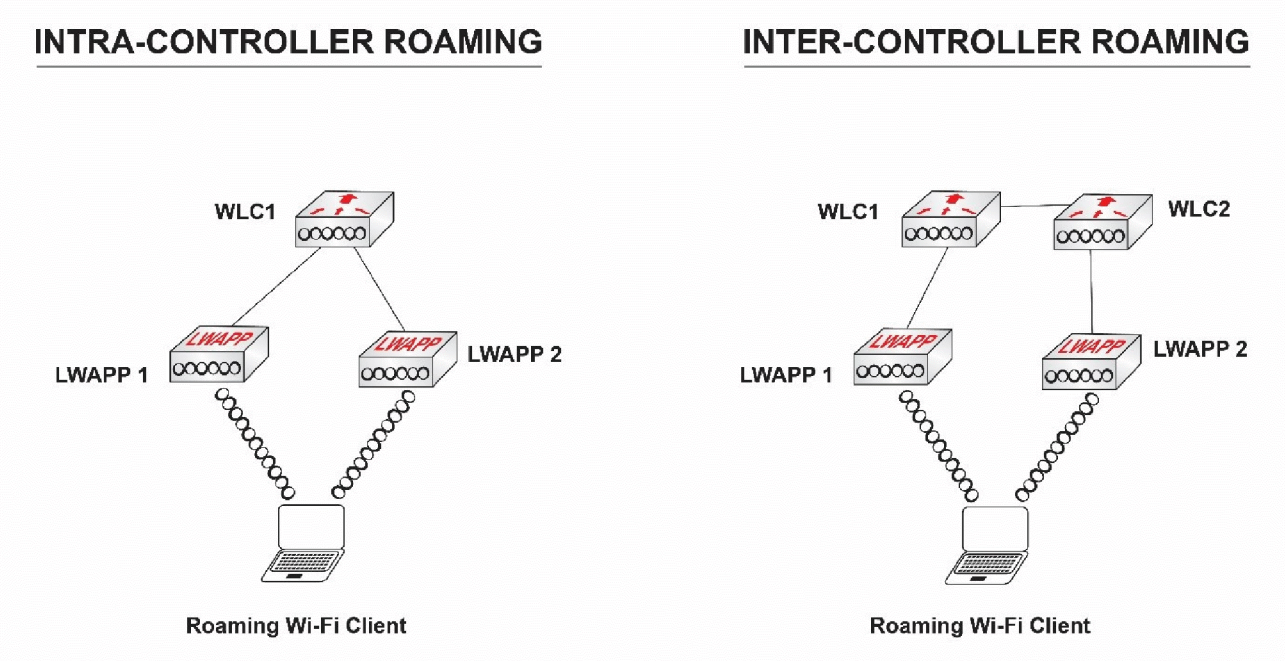


Рисунок 2.3. Мобільність бездротової локальної мережі [21]

Як показано на рисунку 2.3 вище, внутрішньоконтролерний роумінг відбувається, коли клієнт переходить від однієї точки доступу до іншої точки доступу, контрольованої тим самим WLC. У цей момент WLC оновлює базу даних клієнтів новою асоціацією, але не змінює IP-адресу клієнта. Міжконтролерний роумінг може працювати як на рівні 2, так і на рівні 3. У міжконтролерному роумінгу 2-го рівня користувачі переміщуються від точки доступу до точки доступу і від WLC до WLC, залишаючись в одній підмережі. При роумінгу між контролерами 3-го рівня користувачі переміщуються від точки доступу до точки доступу, від WLC до WLC і від підмережі до підмережі. Цей сценарій ускладнює реалізацію міжконтролерного роумінгу, і WLC повинні бути налаштовані з групами мобільності, щоб тісно взаємодіяти і обмінюватися інформацією про статус роумінгового користувача.

Дуже важливою перевагою міжконтролерного роумінгу 3-го рівня є те, що користувачі можуть зберегти свою початкову IP-адресу. Два WLC з'єднуються через IP-з'єднання, а трафік перенаправляється в іншу IP-підмережу. Коли клієнти асоціюються з новою точкою доступу, новий WLC обмінюється інформацією про мобільність зі старим WLC. Оригінальна база даних клієнтів не переміщується до нового WLC. Замість цього старий WLC позначить клієнтів у своєму записі бази даних (якірний запис), і цей запис буде скопійовано до запису бази даних нового WLC (зовнішній запис). Бездротові клієнти зберігають свою оригінальну IP-адресу, яка повторно аутентифікується, як тільки встановлюється новий сеанс безпеки.

WLC призначаються групам мобільності для динамічного обміну повідомленнями про мобільність і тунелювання даних через IP-з'єднання. Групи мобільності використовують такі порти для обміну даними:

- Управління LWAPP: UDP 12223
- Дані LWAPP: UDP 12222
- WLC обмінюються незашифрованими повідомленнями: UDP 16666
- WLC обмінюються зашифрованими повідомленнями: UDP 16667

LWAPP дозволяє перенести інтелектуальні функції з точки доступу і поділитися ними з WLC. WLC керують політиками бездротового зв'язку, контролюють налаштування обміну повідомленнями, автентифікацію та бездротові операції. WLC також можна вважати мостом між бездротовими та дротовими мережами. Пристрої WLC можуть керувати декількома точками доступу, надаючи інформацію про конфігурацію, а також оновлення мікропрограми на спеціальній основі.

LWAPP - це проект стандарту IETF для обміну повідомленнями керування бездротовою мережею між точками доступу та WLC. Він може працювати як на рівні 2, так і на рівні 3, але рівень 3 LWAPP набагато популярніший.

Функції LWAPP рівня 2 включають в себе:

- 11 маячків та відповідей на зонди
- Контроль пакетів
- Підтвердження та передача пакетів
- Черга кадрів і пріоритетність пакетів
- Шифрування та дешифрування даних на рівні MAC-адреси

Функції WLC рівня 2 включають

- Управління MAC адресами
- Резервування ресурсів
- Автентифікація та управління ключами

Тунелі LWAPP рівня 3 використовуються між точками доступу і контролерами бездротової мережі для передачі керуючих повідомлень. Він використовує UDP-порт 12223 для керування і UDP-порт 12222 для передачі даних. Cisco LWAP може працювати в шести різних режимах:

- Локальний режим
- Режим віддаленої точки доступу (REAP)
- Режим монітора
- Режим Rogue Detector (RD)
- Режим сніфферу
- Мостовий режим

Локальний режим - це режим роботи за замовчуванням у LWAP. Кожні 180 секунд точки доступу витрачають 60 мс на канали, на яких вони не працюють. Протягом цих 60 мс точки доступу проводять вимірювання шуму і перешкод, а також сканування на предмет виявлення вторгнень.

Режим REAP дозволяє точці доступу LWAP перебувати через лінію LAN і при цьому мати можливість зв'язуватися з WLC та забезпечувати функціональність звичайної точки доступу LWAP. Режим REAP підтримується не всіма моделями LWAP.

Режим моніторингу - це спеціальна функція, яка дозволяє точкам доступу з підтримкою LWAPP не брати участь в обробці трафіку даних між клієнтами

та інфраструктурою. Замість цього ці точки доступу діють як спеціальні датчики для сервісів на основі визначення місцезнаходження, виявлення несанкціонованих точок доступу та систем виявлення вторгнень. Точки доступу в режимі монітора не можуть обслуговувати клієнтів, і вони безперервно циклічно перебирають всі доступні канали, прослуховуючи кожен канал приблизно 60 мс.

У режимі RD точка доступу LWAP відстежує несанкціоновані точки доступу. Мета точки доступу RD - бачити всі VLAN в мережі, оскільки несанкціоновані точки доступу можуть бути підключені до будь-якої з цих VLAN. Комутатор надсилає всі списки MAC-адрес клієнтів несанкціонованих точок доступу точці доступу RD, яка пересилає їх до WLC для порівняння з MAC-адресами легальних клієнтів. Якщо MAC-адреси збігаються, контролер знає, що несанкціонована точка доступу, яка працює з цими клієнтами, знаходиться в дротової мережі.

Режим сніффера дозволяє LWAP перехоплювати і пересилати всі пакети на певному каналі на віддалений комп'ютер, на якому запущено програмне забезпечення для перехоплення і аналізу пакетів. Ці пакети містять мітки часу, розмір пакета та інформацію про рівень сигналу.

Режим моста зазвичай працює на зовнішніх точках доступу, які функціонують у комірчастій топології. Це економічно ефективний механізм бездротового мостового з'єднання з високою пропускною здатністю, який

CAPWAP, який базується на LWAPP, є стандартним, сумісним протоколом, який дозволяє контролеру керувати колекцією бездротових точок доступу. Точки доступу LAP можуть виявляти контролер CAPWAP і приєднуватися до нього. Єдиним винятком є розгортання рівня 2, які не підтримуються CAPWAP. Крім того, контролери CAPWAP і LWAPP можуть бути розгорнуті в одній мережі. Програмне забезпечення з підтримкою CAPWAP дозволяє точкам доступу приєднуватися до контролера, який використовує CAPWAP або LWAPP.

Коли LAP приєднується до контролера, він завантажує програмне забезпечення контролера, якщо версії на LAP і контролері не збігаються. Після цього LAP повністю перебуває під контролем контролера і не може функціонувати незалежно від контролера.

LWAPP захищає зв'язок між LAP і контролером за допомогою безпечного розподілу ключів, що вимагає наявності цифрових сертифікатів X.509 як на LAP, так і на контролері. Сертифікати, встановлені на заводі, позначаються терміном "MIC", що є абревіатурою від Manufacturing Installed Certificate (сертифікат, встановлений на заводі).

3 ПРОЕКТУВАННЯ БЕЗШОВНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ КОНТРОЛЕРА ТОЧОК ДОСТУПУ

3.1 Технічне завдання на проектування бездротової мережі.

Щоб гарантувати послідовне та безперервне функціонування навчального закладу, вкрай необхідно створити та встановити бездротову мережу Wi-Fi на основі Cisco, яка пропонує як масштабованість, так і непохитну надійність. Нижче наведено основні передумови для проектування цієї мережі Wi-Fi:

1. Мережа має бути бездротовою та використовувати обладнання Cisco.

2. Мережа повинна бути розроблена на основі обладнання Cisco.

3. Мережа Wi-Fi має відповідати специфікаціям і вказівкам, встановленим Cisco.

4. Проект мережі повинен віддавати пріоритет масштабованості та здатності пристосуватися до майбутнього зростання.

5. Надійність є вирішальним фактором, і мережа має бути побудована таким чином, щоб забезпечити безперебійне з’єднання.

6. Мережа повинна бути здатна обробляти великі обсяги трафіку та вимоги користувачів.

7. Проект повинен включати заходи безпеки для захисту від несанкціонованого доступу та порушень даних.

8. Мережа Wi-Fi повинна бути сумісна з різними пристроями та операційними системами.

9. Проект мережі повинен враховувати конкретні потреби та вимоги навчального закладу.

10. Впровадження мережі повинно здійснюватися таким чином, щоб звести до мінімуму збої в роботі установи.

Розробка та реалізація цього проекту передбачатиме використання сучасних технологічних рішень, забезпечення дотримання чинних норм і стандартів, а також сумісність із сучасними технологіями.

Ключовим моментом є здатність швидко пристосовуватися до IT-ландшафту, що постійно розвивається, і підтримувати масштабованість без зміни фундаментальної концепції протягом усього операційного циклу, використовуючи при цьому стандартизовані компоненти та матеріали.

Функціональні вимоги до бездротової мережі включають можливість дистанційного моніторингу та як прямого, так і дистанційного керування мережею. Він також повинен забезпечувати можливість повідомляти відповідальний персонал у разі порушення параметрів навколишнього середовища або несправності в окремих модулях.

Безперервна та безперебійна організація роботи мобільних користувачів і робочих місць є основною метою розробки бездротової мережі Wi-Fi.

На етапі проектування вкрай важливо враховувати кількість користувачів і зону покриття бездротової мережі, щоб визначити відповідну кількість точок бездротового доступу та тип антен, які будуть використовуватися.

Центральні пристрої та засоби відображення інформації вимагають бездротової мережі, яка пропонує фізичний і транспортний рівень.

Інтерфейс RadioEthernet стандарту 802.11 b/g/n/ac має використовуватися бездротовим мережевим обладнанням для забезпечення комутації кадрів Ethernet. Крім того, ці пристрої повинні мати можливість підтримувати організацію VLAN, пріоритезувати трафік на основі технології QoS і пропонувати функцію віддаленого доступу для моніторингу та налаштування.

Конструкція системи повинна включати відмовостійкість, щоб забезпечити безперебійне надання послуг у разі збоїв або необхідності ремонту. Цього можна досягти шляхом впровадження запасних компонентів або процедур, які активуються негайно. Відмовостійкість може бути досягнута за допомогою програмного забезпечення, апаратного забезпечення або їх поєднання.

У таблиці 3.1 наведено опис проекту, який передбачає впровадження бездротової мережі Wi-Fi з використанням обладнання Cisco.

Таблиця 3.1. Технічне завдання на проектування мережі

Пункт завдання	Опис роботи
Призначення	Локальна бездротова мережа (Wi-Fi) у приміщенні вищого навчального закладу, що призначена для безперервної організації роботи мобільних користувачів (хостів), а також робочих місць
Замовник	Львівський національний університет природокористування
Розташування обєкту замовника	м. Дубляни, вул. Володимира Великого, 1
Вид робіт	Потрібно провести роботи з інсталяції та конфігурації активного мережевого обладнання та систем бездротового доступу до мережі на основі котролера та автономних точок доступу
Основні етапи побудови бездротової мережі	Перший етап: • Розробка плану сегментації мережі; • Розробка детальної схеми мережі; • Підготовка проектної документації; • Узгодження проектної документації та схеми мережі з відповідальнми представниками від Замовника

	Другий етап: Створення безротової (Wi-Fi) мережі: • Виконання монтажних робіт на обєкті; • Налаштування активнго обладнання; • Розміщення активного бездротового мережевого обладнання для покриття всіх приміщень на обєкті Замовника; • Приймально-здавальні випробування встановленого обладнання; • Здача обєкта в експуатацію. • Оформлення необхідної документації; • Замовник залишає за собою право вносити зміни у вимоги в процесі переговорів відповідно до змін бізнес-вимог та можливих техніко-економічних змін.

3.2 Проектування комплексної структурної та функціональної схеми для бездротової локальної мережі Wi-Fi

Проектування комплексної структурної та функціональної схеми для бездротової локальної мережі є вирішальним аспектом, який слід враховувати при її реалізації.

У наш час технології бездротової передачі даних стали невід'ємною частиною кожного бізнесу. Поява сучасних бездротових мереж забезпечила вирішення широкого кола проблем, від створення внутрішніх мереж у будівлі до створення гарячих точок і навіть розширення мереж у більшому масштабі, охоплюючи міста, регіони та цілі країни. Завдяки доступності, швидкому впровадженню та широким можливостям для передачі трафіку даних, IP-телефонії та відео бездротові технології стали одним із секторів телекомунікацій, що розвиваються найбільш швидко.

У процесі проектування архітектури WLAN для корпоративної мережі метою було створити добре збалансоване поєднання ключових мережевих характеристик і можливостей, таких як висока доступність, використовуючи сучасні методи, технології та пристрої [11, 19]. Мета полягала в тому, щоб мережа відповідала високим бізнес-вимогам і належним чином підтримувала бізнес-додатки.

Єдине в галузі рішення, відоме як уніфікована бездротова мережа Cisco [10], економічно ефективним способом усуває перешкоди безпеки, управління та контролю, з якими стикаються підприємства. Поєднуючи найкращі компоненти дротових і бездротових мереж, це рішення дозволяє створювати безпечні та масштабовані мережі WLAN з мінімальною загальною вартістю володіння.

Що стосується підтримки мережевої безпеки, Cisco Systems виділяється як найкращий гравець у галузі. Вони чудово забезпечують корпоративну безпеку WLAN, яка відповідає всім необхідним стандартам. Ось деякі з ключових функцій, які вони пропонують:

Нижче наведено основні компоненти безпечної мережі WLAN: 802.11i, 802.1X, захищений доступ Wi-Fi (WPA), WPA2, розширений стандарт шифрування (AES) і віртуальна приватна мережа (VPN).

Для підвищення безпеки вкрай важливо мати надійну систему запобігання вторгненням WLAN (IPS), яка може виявляти та зменшувати ризик

несанкціонованого доступу з пристроїв сторонніх виробників, незареєстрованих пристроїв клієнтів та інших мереж.

Cisco пропонує зручні рішення для керування мережами WLAN, які не тільки спрощують керування мережею, але й знижують витрати на експлуатацію та обслуговування. Ці служби керування бездоганно інтегровані в інфраструктуру WLAN, надаючи мережевим адміністраторам різноманітні можливості.

Стан радіообладнання можна візуально контролювати в режимі реального часу, пропонуючи розширені можливості для масштабування мережі та підвищення надійності, а також реалізовано розширені функції пошуку та діагностики, що надає покращені можливості для усунення несправностей.

Рішення Cisco Unified Wireless Network пропонує автоматичне налаштування, оптимізацію та усунення несправностей для бездротових мереж. Початкове покоління автономних WLAN на основі точки доступу забезпечувало зручне підключення до мережі. Однак з моменту появи мереж WLAN відбулися значні зміни. У наш час простого підключення до мережі вже недостатньо. Підприємствам потрібні мережі WLAN, які забезпечують безперебійне покриття всієї території. Ці мережі повинні підтримувати різноманітні мобільні послуги, такі як голосовий зв'язок, гостьовий доступ, позиціонування та надійні бездротові системи запобігання вторгненням (WIPS). Крім того, вони повинні мати спрощені механізми розгортання та адміністрування, а також мати високу масштабованість. По суті, компаніям потрібні мережі WLAN, які не обмежені обмеженнями [19].

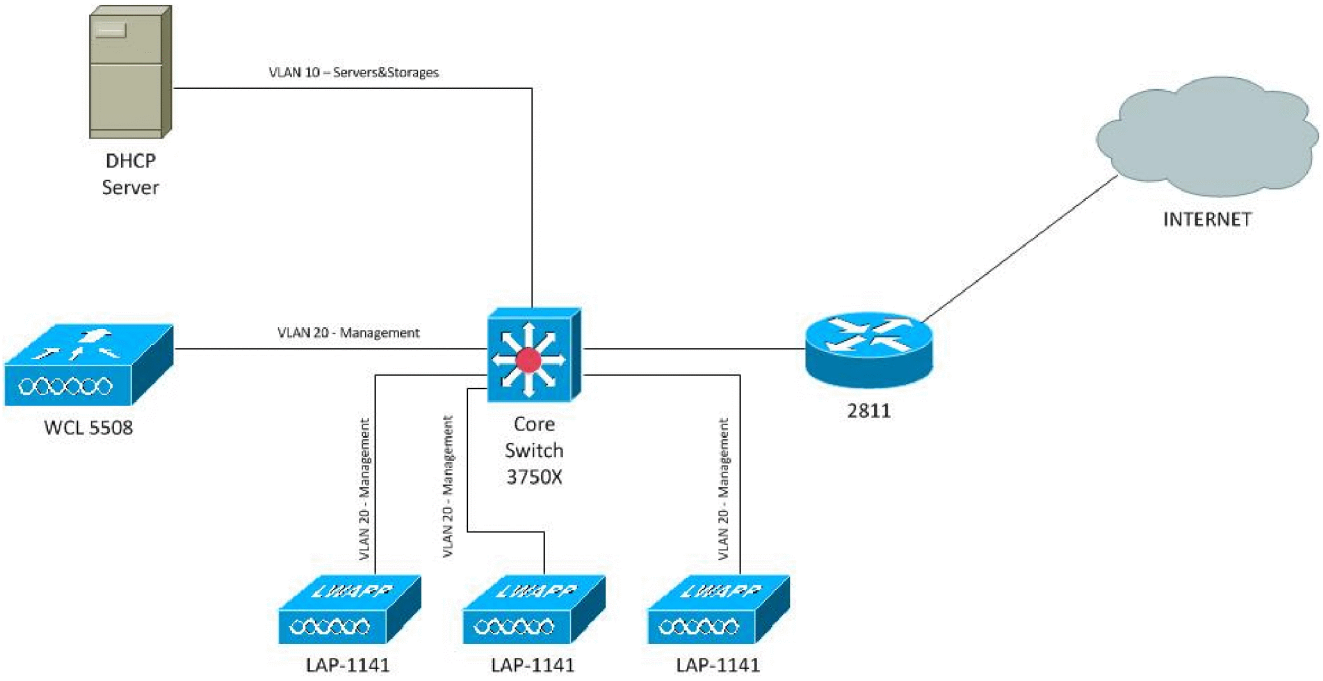


Рис. 3.1 Логічна схема мережі на базі контролера WLC5508 відповідно третьому рівню моделі OSI

Основна підмережа, 192.168.0.0/24, пов'язана з головним маршрутизатором Cisco 2811 і використовує статичну адресацію. Основна підмережа відповідає за підключення робочих станцій, портів керування комутаторами та контролера бездротової точки доступу. Кожна точка доступу підключена до контролера через власну підмережу. Ця мережева конфігурація була розроблена відповідно до вимог інформаційної безпеки та високої швидкості передачі даних. Для подальшого вдосконалення схеми на фізичному рівні буде реалізовано комутацію підмереж для точок доступу та агрегацію каналів.

3.3 Вибір апаратних засобів для реаліазації безшовної бездротової мережі з використанням контролерів точок доступу

Точками доступу, обраними для цієї бездротової мережі, є моделі LAP-AP1141N-X-K9, відомі своєю можливістю підключення зовнішніх антен. Ці точки доступу, що входять до серії Cisco Aironet 1140, вважаються «легкими»

та пропонують дводіапазонну функціональність, підтримуючи стандарт 802.11 a/b/g/n/ac. Однією з ключових переваг цих точок доступу є безперебійне налаштування та робота, яка не потребує втручання оператора. Вони забезпечують безпечне та економічно ефективне рішення для доступу до бездротових мереж, особливо в корпоративному середовищі. Завдяки розширеним радіочастотним можливостям і гнучким параметрам встановлення ці точки доступу підвищують продуктивність, безпеку, надійність і масштабованість бездротової мережі. Фактично, вони не тільки відповідають, але й перевершують вимоги продуктивності навіть для найвибагливіших корпоративних налаштувань.

Поєднання контролера бездротової локальної мережі Cisco та додаткової системи бездротового керування Cisco (WCS) дозволяє одночасно виконувати завдання пересилання даних і моніторингу для мережі Ethernet. Окрім можливостей доставки трафіку, ця точка доступу також забезпечує радіочастотний контроль у реальному часі та захист від вторгнень. Це інтегроване рішення усуває потребу в додаткових виділених вузлах моніторингу, що призводить до зниження витрат і спрощення архітектури мережі WLAN. Підтримка протоколів Wi-Fi Protected Access (WPA) і 802.11i/WPA2 серії Cisco Aironet 1140 забезпечує створення безпечної мережі WLAN корпоративного рівня, сумісної з різними пристроями.

У локальній мережі навчального закладу використовується контролер бездротової локальної мережі Cisco серії 5500 AIR-WLC5508-K9, а також інсталяція 12 точок від моделі AIR-LAP1141N-E-K9. Ці точки підключаються до наявних портів комутаторів.

Повна функціональність системи бездротової локальної мережі досягається завдяки взаємодії контролерів бездротової локальної мережі Cisco, точок доступу Cisco Aironet і системи бездротового керування Cisco (WCS). Будучи невід'ємною частиною об'єднаної бездротової мережі Cisco, серія Cisco 2100 надає адміністраторам можливість безпечно керувати мережами WLAN і покращувати мобільні послуги, такі як голосовий зв'язок, гостьовий доступ і

служби визначення місцезнаходження. Контролери бездротової локальної мережі Cisco серії 5500, розроблені для задоволення потреб роздрібної торгівлі, промисловості та малого та середнього бізнесу, підтримують різну кількість точок доступу (6, 12 або 25), залишаючись економічно ефективними. Завдяки восьми портам Ethernet ці контролери також пропонують зручність прямого живлення точок доступу Cisco (як зазначено в таблиці 3.2).

Сервер керування захищеним доступом (ACS) Cisco для Windows є цінним інструментом, який оптимізує керування користувачами та консолідує мережеву ідентифікацію на різних пристроях Cisco та програмах керування безпекою. Використовуючи Cisco Secure ACS, мережеві адміністратори можуть ефективно застосовувати призначені політики та ретельно контролювати такі аспекти:

- Особи, яким надано доступ до мережі, обмежені кількома обраними;
- Визначаються права доступу до мережі для кожного користувача;
- Записи перевірок безпеки або білінгову інформацію з облікових записів включено до даних, які аналізуються;
- Адміністратор кожної конфігурації має доступ до елементів керування та команд, які регулюють доступ до мережі.

У системах довіри та ідентифікації Cisco Cisco Secure ACS відіграє життєво важливу роль як фундаментальний елемент рішень мережевої безпеки. Завдяки інтеграції автентифікації, доступу користувачів і адміністратора, а також керування політикою, він покращує безпечний доступ. Це досягається за допомогою централізованої мережевої ідентифікаційної інфраструктури, яка не тільки додає гнучкості та мобільності, але й підвищує безпеку та підвищує продуктивність користувачів.

Коли справа доходить до вибору відповідного обладнання, бездротовий контролер Cisco серії 5500 пропонує рішення для малого та середнього бізнесу, а також для філій. Його основне призначення — полегшити бездротовий зв’язок у всій системі. Серія Cisco 5500, спеціально розроблена для підтримки

протоколу 802.11n/ac, служить бездротовим контролером початкового рівня, який оптимізує процес розгортання та керування точками доступу Cisco Aironet для безперебійного бездротового підключення.

Цей контролер, як частина об'єднаної бездротової мережі Cisco, пропонує централізовані політики безпеки для бездротових систем для запобігання несанкціонованим проникненням у мережу. Точки доступу Officeextend серії Cisco Aironet 600 функціонують на основі стандартів 802.11n в обох діапазонах 4 і 5 ГГц, розумно вибираючи менш перевантажений діапазон. Ці точки доступу мають можливість розрізняти корпоративні та приватні SSID, дозволяючи відокремити корпоративний і особистий трафік. У випадку віддалених працівників їхній особистий трафік направляється безпосередньо в Інтернет, не обтяжуючи корпоративних контролерів. Останні моделі цих точок доступу оснащені чотирма вбудованими портами Ethernet, що дозволяє підключати IP-телефони, принтери та інші мережеві пристрої. Для детальної розбивки специфікацій обладнання зверніться до Додатку А.

3.3 Налаштування бездротової мережі на контролері Cisco WLC 5508

Контролер і точки доступу знаходяться в керуючому VLAN, DHCP-сервер для клієнтів, що підключаються до бездротової мережі - в іншому VLAN. Самі клієнти, підключившись до мережі, потрапляють у свій окремий VLAN. Клієнти повинні під'єднатися до бездротової мережі, отримати необхідні налаштування зі стороннього DHCP-сервера і мати можливість виходу в Internet.

Параметри мереж:

VLAN 2 - WireLess_Users - 192.168.0.0/24

VLAN 10 - Servers&Storages - 172.16.0.0/24

VLAN 20 - Management - 10.10.0.0/24

DHCP-Server - 172.16.0.20/24

Мережа між ядром і маршрутизатором: 192.168.100.0/30

На проміжних пристроях будемо налаштовувати тільки те, що необхідно для вирішення завдання. Основний акцент на розгляд налаштувань контролера.

Налаштування комутатора ядра:

Створюємо необхідні VLAN:

*Core_SW(config)**#vlan 2***
*Core_SW(config-vlan)**#name WireLess_Users***
*Core_SW(config-vlan)**#vlan 10***
*Core_SW(config-vlan)**#name Servers&Storages***
*Core_SW(config-vlan)**#vlan 20***
*Core_SW(config-vlan)**#name Management***
*Core_SW(config-vlan)**#exit***

Налаштуємо необхідні SVI (Switch Virtual Interface):

*Core_SW(config)**#interface vlan 2***
*Core_SW(config-if)**#ip address 192.168.0.253 255.255.255.255.0***
*Core_SW(config-if)**#exit***
*Core_SW(config)**#interface vlan 10***
*Core_SW(config-if)**#ip address 172.16.0.253 255.255.255.255.0***
*Core_SW(config-if)**#exit***
*Core_SW(config)**# interface vlan 20***
*Core_SW(config-if)**#ip address 10.10.0.253 255.255.255.255.0***
*Core_SW(config-if)**#ip helper-address 172.16.0.20***
*Core_SW(config-if)**#exit***

Додаємо адресу DHCP-Сервера, тому що ми повинні будемо перенаправляти запити DHCP від точок доступу на зовнішній DHCP. Вирішено

не використовувати окремий DHCP-Server для точок доступу безпосередньо на контролері. Нехай всі DHCP-сервери знаходяться на одному пристрої (для простоти управління і адміністрування).

Налаштовуємо приналежність портів до відповідних VLAN. Особливу увагу звернемо на інтерфейс Gi1/0/1, підключений до контролера. Передбачається, що керуючий трафік буде інкапсулюватися в теги керуючого VLAN 20, а трафік користувачів буде йти з тегом VLAN 2:

*Core_SW(config)**#interface gigabitEthernet 1/0/1***
*Core_SW(config-if)**#switchport trunk encapsulation dot1q***
*Core_SW(config-if)**#switchport mode trunk***
*Core_SW(config-if)**#switchport trunk allow vlan 2,20***
*Core_SW(config-if)**#switchport trunk native vlan 20***
*Core_SW(config-if)**#description WLC***
*Core_SW(config-if)**#inter g1/0/2***
*Core_SW(config-if)**#switchport mode access***
*Core_SW(config-if)**#switchport access vlan 20***
*Core_SW(config-if)**#spanning-tree portfast***
*Core_SW(config-if)**#description LAP***
*Core_SW(config-if)**#interf g1/0/48***
*Core_SW(config-if)**#switchport mode access***
*Core_SW(config-if)**#switchport access vlan 10***
*Core_SW(config-if)**#spanning-tree portfast***
*Core_SW(config-if)**#description DHCPServer***

Для зв'язку з маршрутизатором створимо інтерфейс L3 і призначимо йому IP-адресу:

*Core_SW(config)**#int gi1/0/47***
*Core_SW(config-if)**#description To_Outside***

*Core_SW(config-if)**#no switchport***
*Core_SW(config-if)**#ip address 192.168.100.2 255.255.255.255.252***
*Core_SW(config-if)**#exit***

Маршрутизацію між VLAN будемо здійснювати на комутаторі. Вихід у зовнішню мережу через маршрутизатор:

*Core_SW(config)**#ip routing** // вмикаємо можливість маршрутизації на нашому L3-комутаторі*
*Core_SW(config)**#ip route 0.0.0.0 0.0 0.0.0.0 192.168.100.1***

DHCP-Server виконаний на комутаторі L3 Cisco 3750X. Команди для налаштування сервера наведено нижче:

Налаштовуємо інтерфейс (L3 інтерфейс з фіксованою адресою - IP DHCP-Сервера):

*DHCPServer(config)**#interface gigabitEthernet 2/0/24***
*DHCPServer(config-if)**#no switchport***
*DHCPServer(config-if)**#ip address 172.16.0.20 255.255.255.255.0***

Налаштовуємо DHCP-пул для мобільних користувачів:

*DHCPServer(config)**#ip dhcp pool WLess_Users***
*DHCPServer(dhcp-config)**#network 192.168.0.0 255.255.255.255.0***
*DHCPServer(dhcp-config)**#default-router 192.168.0.253***
*DHCPServer(dhcp-config)**#dns-server 8.8.8.8***
*DHCPServer(dhcp-config)**#exit***
*DHCPServer(config)**#ip dhcp excluded-address 192.168.0.253***

Створимо пул для точок доступу. А на самому контролері, як було сказано вище, ми відключимо DHCP-сервер:

*DHCPServer(config)**#ip dhcp pool AP***
*DHCPServer(dhcp-config)**#network 10.10.0.0 255.255.255.0***
*DHCPServer(dhcp-config)**#default-router 10.10.0.10** // вказали адресу контролера*
*DHCPServer(dhcp-config)**#exit***
*DHCPServer(config)**#ip dhcp excluded-address 10.10.0.10***
*DHCPServer(config)**#ip dhcp excluded-address 10.10.0.11 10.10.0.254***

Далі налаштуємо останній проміжний пристрій, який бере участь у функціонуванні нашої мережі - маршрутизатор. Тут необхідно налаштувати тільки NAT, більше ніяких функцій на цей пристрій покладати не будемо:

hostname GW
interface GigabitEthernet0/0
ip address 192.168.100.1 255.255.255.252
ip nat inside ip virtual-reassembly in
duplex auto
speed auto

interface GigabitEthernet0/1
ip address x.x.x.x.x 255.255.255.0 //зовнішня адреса
ip nat outside ip virtual-reassembly in
duplex auto
speed auto

ip nat inside source list NAT interface GigabitEthernet0/1 overload
ip route 0.0.0.0.0 0.0.0.0 x.x.x.y // зовнішня next-hop адреса
ip route 10.10.0.0 255.255.255.255.0 192.168.100.2
ip route 172.16.0.0 255.255.255.255.0 192.168.100.2

ip route 192.168.0.0 255.255.255.255.0 192.168.100.2

ip access-list standard NAT

permit 192.168.0.0 0.0.0.0.255 // дозволяємо транслювати тільки адреси мобільних користувачів.

end

Приступаємо до налаштування контролера WLC5508. Пропускаємо налаштування під час початкової ініціалізації, тому що там усе досить просто. Налаштовувати контролер будемо з графічного інтерфейсу. Зробимо один SSID, мережа буде відкрита, користувачі повинні будуть потрапляти в VLAN 2 і отримувати налаштування з DHCP-сервера, розташованого в мережі 172.16.0.0. Заходимо на контролер, підключившись до сервісного порту. Далі, після введення логіна і пароля, потрапляємо на сторінку налаштування, де переходимо у вкладку ***CONTROLLER***.

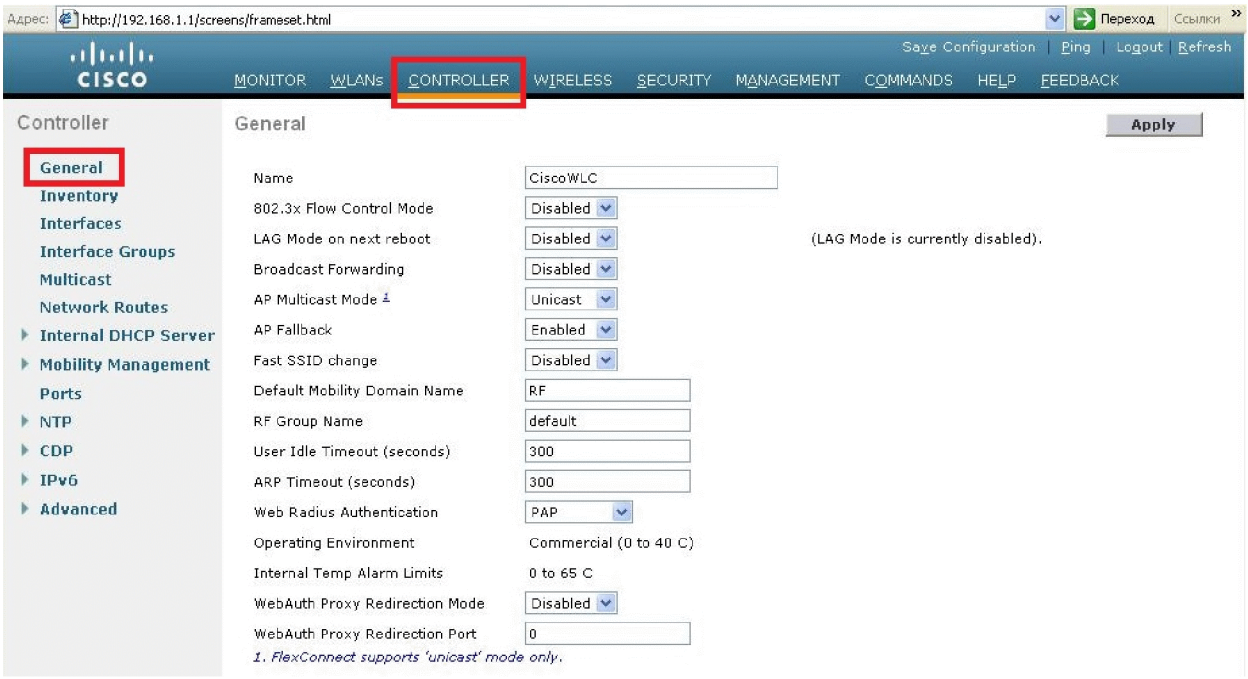


Рис. 3.2 Основне меню веб-інтерфейсу контролера WLC5508.

У меню зліва вибираємо пункт ***General***. Дивимося, що в нас є. Частину налаштувань ми зробили під час першого запуску (ім'я та доменне ім'я мобільної групи). Решту розглядати не будемо, оскільки це не потрібно для вирішення нашого завдання.

У меню зліва проходимо в пункт ***Interfaces***:

Рис. 3.3 Меню «Interfaces» веб-інтерфейсу контролера WLC5508

У цьому меню ми можемо налаштувати інтерфейси нашого контролера під необхідні цілі. Ми використовуватимемо один фізичний порт (Port 1), через який проходитиме як контрольний трафік (трафік management), так і трафік мобільних користувачів. Поділ буде існувати на рівні VLAN'ів. Отже, на малюнку вище вже створено два інтерфейси: management і user. Виконаємо налаштування першого інтерфейсу (management):

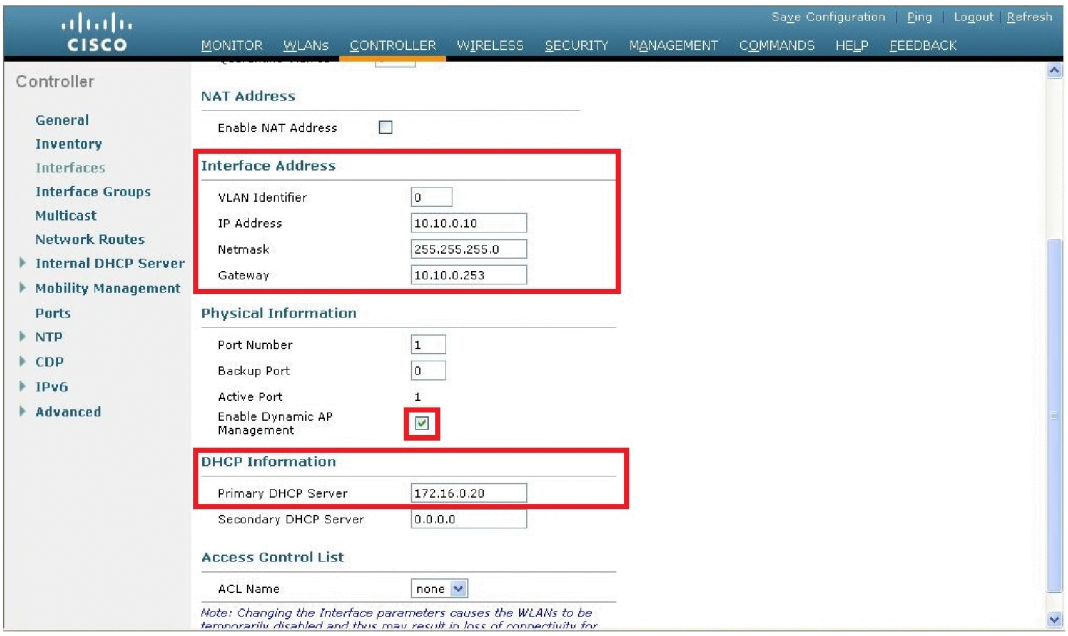


Рис. 3.4 Налаштування інтерфейсу management

Цей інтерфейс не тегується. Адреса призначена з Management-мережі. Встановлено галочку Enable dynamic AP Management, що свідчить про те, що

цей інтерфейс слугуватиме для управління точками доступу. Усі ці налаштування прив'язуються до першого фізичного порту.

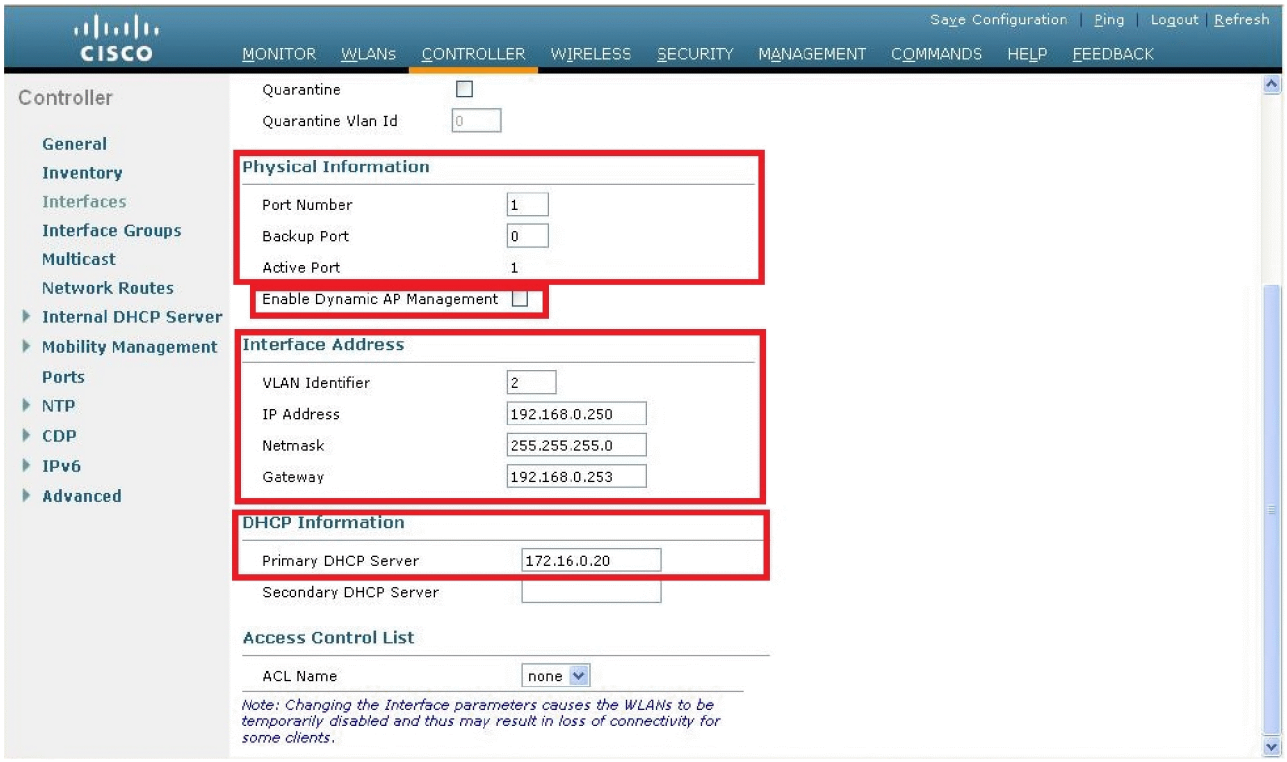


Рис. 3.5 Налаштування першого фізичного порту.

Інтерфейс User відрізняється від попереднього тим, що трафік цього інтерфейсу тегується призначеним для користувача VLAN 2, і трафік, що управляє, по ньому передаватися не буде. Саме цей інтерфейс буде використовуватися при налаштуванні WLAN..

Переходимо до налаштування WLAN. Для цього йдемо у вкладку WLAN's:

Рис. 3.6 Меню налаштування WLAN

Створюємо необхідні WLAN. У нашому випадку ми зробили всього одну бездротову мережу. Для перевірки її налаштувань необхідно натиснути на номер у колонці WLAN ID:

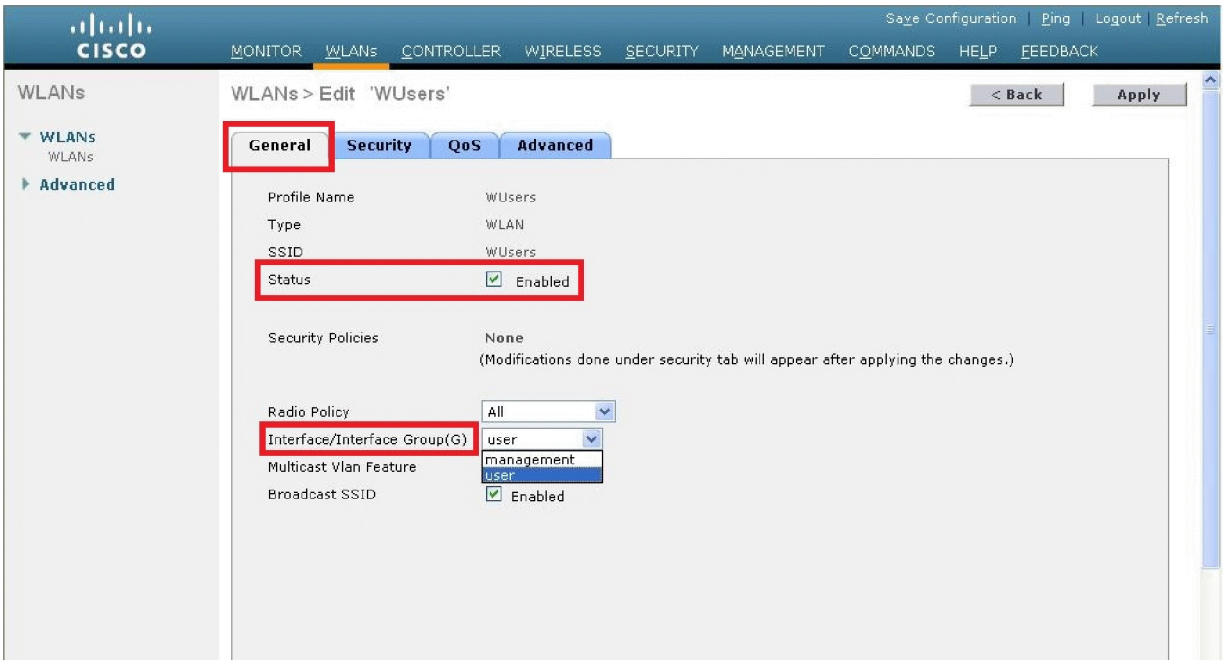


Рис. 3.7 Перевірка налаштувань мережі за її WLAN ID

У загальних налаштуваннях вказуємо, який інтерфейс буде асоційований з даними WLAN. У нашому випадку це інтерфейс під назвою User.

Переходимо в пункт ***Advanced/AP groups*** для того, щоб вказати, які саме точки доступу працюватимуть з тією чи іншою WLAN. Варто зазначити, що налаштовувати цю частину необхідно тоді, коли точки доступу вже пройшли процедуру асоціації з контролером.

На цьому налаштування завершено. Решта налаштувань – це підлаштування додаткових параметрів, які налаштовуються залежно від потреби та необхідності.

4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Структурно-функціональний аналіз виробничого процесу та розроблення моделі травмонебезпечних ситуацій

У зображеннях процесів формування, виникнення аварій та виробничих травм усі випадкові події, що утворюють конкретну аварійну ситуацію, пов'язані між собою причинно-наслідковими зв'язками.

Метод логічного моделювання потенційних аварій, травм та катастроф відкриває можливість розробити досконалу систему управління ОП виробництва, яка базується на оперативному пошуку виробничих небезпек, їх глибокому аналізі й терміновому прийнятті заходів для усунення потенційних небезпек ще до виникнення травмонебезпечних та катастрофічних ситуацій. Деякі небезпечні ситуації в табл. 4.1.

Працівники, що обслуговують електрообладнання вениляційної системи, зобов'язані знати Правила безпечної експлуатації електроустановок споживачів відповідно до займаної посади або роботи, як вони виконують, і мати відповідну групу з електробезпеки [26].

Працівники, що порушили вимоги Правил безпечної експлуатації електроустановок, усуваються від роботи і несуть відповідальність (дисциплінарну, адміністративну, кримінальну) згідно з чинним законодавством. Такі працівники не допускаються до робіт в електроустановках без позачергової перевірки знань вимог правил безпечної експлуатації електроустановок.

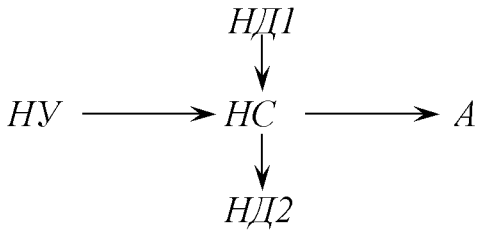
Забороняється допускати до роботи в електроустановках осіб, які не пройшли навчання і перевірку знань Правил безпечної експлуатації електроустановок.

Працівнику, який пройшов перевірку знань Правил безпечної експлуатації електроустановок, видається посвідчення встановленої форми.

Таблиця 4.1. Моделювання процесів формування та виникнення травмонебезпечних і аварійних ситуацій

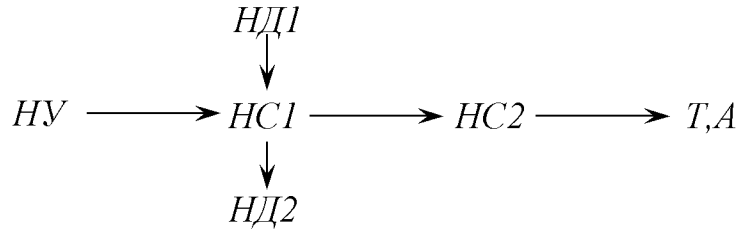
Вид робіт	Виробнича небезпека			Можливі наслідки	Заходи запобігання небезпечним ситуаціям
	Небезпечна умова (НУ)	Небезпечна дія (НД)	Небезпечна ситуація (НС)		
Використання механічної вентиляції	Оператор не перевірив обладнання НУ	Пошкоджений трубопровід мережі НД1 Закупорений трубопровід шланга НД2	Відмова вентиляційної системи (двигуна) НС	Аварія	Розвісити плакати, провести інструктажі із експлуатації обладнання системи

Модель процесу:



Використання електронних пристроїв регулювання	Пошкоджена ізоляція провідників з’єднання НУ	Пробій на корпус НД1 Коротке замикання НД2	Ураження людини електричним струмом НС1 Виведення обладнання із ладу НС2	Травма Аварія	Заміна провідників, установлення захисного обладнання (запобіжників, захист від ураження людини струмом) тощо

Модель процесу:



Посвідчення про перевірку знань працівника є документом, який засвідчує право на самостійну роботу в електроустановках на зазначеній посаді за фахом.

4.2. Вимоги техніки безпеки під час роботи обладнання та протипожежні заходи

Вимоги правил техніки безпеки перед початком роботи. Для початку роботи пов'язаної з вентиляцією вимикають рубильники або автоматичні вимикачі щита низької напруги, запирають шафу і вивішують попереджувальні плакати. Також повинні бути основні захисні засоби до яких належать такі, ізоляція яких надійно захищає від робочої напруги мережі і за допомогою яких можна дотикатися до струмопровідних частин, що перебувають під напругою, без небезпеки ураження електричним струмом (інструмент з ізольованими ручками, ізолюючі струмовимірювальні кліщі, діелектричні рукавиці).

Вимоги правил техніки безпеки під час роботи. Виконавши ці операції, надівають діелектричні рукавиці і за допомогою покажчика напруги перевіряють відсутність напруги на всіх фазах. Потім, приєднавши один кінець переносного заземлення до заземлюючого пристрою, накладають його на струмоведучі частини. Після цього остаточно приступають до роботи.

Вимоги правил техніки після закінчення роботи. Після закінчення роботи системи перед її вимиканням необхідно виконати такі технічні операції: перевірити надійність кріплення, зняти переносні тимчасові заземлення, відімкнути щит низької напруги і зняти плакати з техніки безпеки; якщо тимчасове переносне заземлення встановлене на лінії, його також треба зняти тощо [27].

Протипожежні заходи на об'єкті. Для запобігання пожеж на об'єкті розроблено організаційні, експлуатаційні, технічні режимного характеру,

пожежно-евакуаційні, профілактичні заходи. До організаційних заходів відносяться правила розміщення машин, що обслуговують приміщення, обладнання, матеріалів з дотримання певних проходів, не допускається захаращення приміщень, проходів і т.д.

4.3. Розрахунок штучного заземлення

Вибір штучного заземлення проводиться в залежності від характеру ґрунту і способу забивання стержнів [27]. Розраховуємо заземлюючий контур підстанції напругою 10/0,4 кВ з глухозаземленою нейтраллю. Характер ґрунту – чорнозем з $\rho=2\cdot10^4$ Ом·см. Кліматична зона – IV (K_c – 1,2, K_n – 1,5). Струм замикання на землю в мережі становить 50 А.

В відповідності з діючими правилами, опір заземлюючого пристрою повинен становити

$$R = \frac{125}{I_з} = \frac{125}{50} = 2,5 Ом, \qquad (4.1)$$

де $I_з$ – струм замикання на землю, А.

Приймаємо 3 Ом. Контур заземлення розміщуємо в ряд з а = 5 м, l = 2,5 м. В якості стержневого заземлювача приймаємо кутникові сталь 50х50х5 мм, а протяжного – пластинчасту сталь 40х4 мм.

Опір одиночного стержня становить:

$$R_o = 0.00318\rho \cdot K_c, Ом \qquad (4.2)$$

де K_c – коефіцієнт сезонності для стержневого заземлювача (K_c – 1,2).

$$R_o = 0.00318 \cdot 2 \cdot 10^4 \cdot 1.2 = 76.32 Ом.$$

Число стержнів приймаємо 15. При цьому коефіцієнт використання стержневих заземлювачів становить η_c = 0,7. Опір всіх стержнів розтікання струму становить:

$$R_c = \frac{R_o}{n \cdot \eta_c}, Ом \,, \tag{4.3}$$

де n – число стержнів, шт.

$$Rc = \frac{76.32}{15 \cdot 0.7} = 7.3 Ом \,.$$

Довжина протяжного заземлювача становить l = 35 м (3500 см); приймаємо t = 50 см, b = 0,4 см. Опір протяжного заземлювача становить:

$$R_{пр} = \frac{0,366}{l} \cdot \rho \cdot 2 \cdot \lg \frac{2 \cdot l^2}{t \cdot b}, Ом \tag{4.4}$$

$$R_{пр} = \frac{0,366}{3500} \cdot 1,2 \cdot 10^4 \cdot 2 \cdot \lg \frac{2 \cdot 3500^2}{0,4 \cdot 50} = 3,2 Ом$$

Коефіцієнт використання протяжного заземлювача η_n = 0,71. Дійсний опір протяжного заземлення становить:

$$R_n = \frac{R_{пр}}{\eta_n} = \frac{3,2}{0,71} = 4,5 Ом \tag{4.5}$$

Опір всього заземлюю чого пристрою становить:

$$R_u = \frac{R_c \cdot R_n}{R_c + R_n} = \frac{4.5 \cdot 7.3}{4.5 + 7.3} 2.78 < 3 Ом \tag{4.6}$$

Отже, число стержнів вибрано вірно.

4.4. Захист цивільного населення

Забезпечення захисту населення і території у разі загрози та виникнення надзвичайних ситуацій є одним з найважливіших завдань не лише підприємства, але й цілої держави. Актуальність проблеми забезпечення природо-техногенної безпеки населення і території зумовлена тенденціями зростання втрат людей і шкоди територіям, що спричиняються небезпечними природними явищами, промисловими аваріями і катастрофами.

Інженерний захист проводиться з метою виконання вимог ІТЗ із питань забудови міст, розміщення ПНО, будівлі будинків, інженерних споруд та інше.

Медичний захист проводиться для зменшення ступеня ураження людей, своєчасного надання допомоги постраждалим та їх лікування, забезпечення епідеміологічного благополуччя в районах надзвичайних ситуацій.

Біологічний захист включає своєчасне виявлення чинників біологічного зараження, їх характеру і масштабів, проведення комплексу адміністративно-господарських, режимно-обмежувальних і спеціальних протиепідемічних та медичних заходів.

Радіаційний і хімічний захист включає заходи щодо виявлення і оцінки радіаційної та хімічної обстановки, організацію і здійснення дозиметричного та хімічного контролю, розроблення типових режимів радіаційного захисту, забезпечення засобами індивідуального захисту, організацію і проведення спеціальної обробки.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

1 Проаналізовано предметну область та здійснено огляд і порівняння існуючих бездротових технологій та особливості побудови і функціонування мереж IEEE 802.11. Описано основні концепції побудови локальних корпоративних мереж.

2 Проаналізовано архітектуру мереж з використанням безпровідної технології Wi-Fi та окреслено основні підходи до планування, проектування і масштабування цих мереж.

3 Досліджено особливості проектування мереж з використанням контролерів бездротової локальної мережі, встановлено що використання контролерів точок доступу сприяє підвищенню ефективності управління мережею та зменшенню витрат на її обслуговування. А також дозволяє адміністраторам мережі централізовано налаштовувати та моніторити всі аспекти функціонування Wi-Fi інфраструктури.

4 Розроблено технічне завдання на проектування бездротової мережі та структурну і функціональну схеми для бездротової локальної мережі. Здійснено вибір апаратних засобів для реалізації проекту на основі сучасного активного мережевого обладнання Cisco ;

5 Виконано налаштування бездротової мережі на основні контролера точок доступу, що включало в себе налаштування комутатора ядра, DHCP сервера та власне контролера точок доступу.

6 Здійснене проектування та налаштування безшовної Wi-Fi мережі з використанням контролерів точок доступу забезпечить стабільне та безперервне підключення до мережі для користувачів, незалежно від їхнього місця розташування в межах покриття проектованої мережі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Комп'ютерні мережі [навчальний посібник] / А.Г. Микитишин, М.М. Митник, П.Д.Стухляк, В.В. Пасічник – Львів, «Магнолія 2006», 2017. – 256 с.

2. Комп'ютерні мережі [Текст]: 2-ге оновл. і доп. вид. / Є. Буров; ред. В.Пасічник. – Л.:БаК, 2016. – 584 с.

3. Організація комп'ютерних мереж [Електронний ресурс]: підручник: для студ.спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки»/ КПІ ім. Ігоря Сікорського; Ю.А. Тарнавський, І.М. Кузьменко. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259с

4. Stallings W. Data and Computer Communications 10th - Pearson, 2013. – 912 p.

5. Larry L. Peterson, Bruce S. Davie. Computer Networks: A Systems Approach / The MorganKaufman series in Networking – 2015 – 776 p.

6. David G. Messerschmitt. Networked Applications: A Guide to the New ComputingInfrastructure – The Morgan Kaufman series in Networking, 2012 –396p.

7. McCabe J. Network Analysis, Architecture, and Design. Third edition. Morgan Kaufmann, 2007. 495 p.

8. Яковина В.С. Основи безпеки комп'ютерних мереж: Навчальний посібник. Львів : НВФ "Українські технології", 2008. 396 с.

9. Демида Б.А. Обельовська К.М., Яковина В.С. Основи адміністрування LAN у середовищі MS Windows: навч. посіб. Львів : Видавництво Львівської політехніки, 2013. 488 с.

10. Документація з настройки обладнання фірми Cisco. : веб-сайт. URL: http://www.cisco.com (дата звернення: 12.03.2024).

11. Чистяков, В. А. Аналіз технологій бездротової передачі даних / В. А. Чистяков, Б. Є. Миктибаев, А. Б. Жанбеков // Журнал наукових і прикладних досліджень. - 2016. - №1. - С. 166-169.

12. Challoo, R. An overview and assessment of wireless technologies and co- existence of ZigBee, Bluetooth and Wi-Fi devices / R. Challoo, A. Oladeinde, N.

Yilmazer, S. Ozcelik, L. Challoo // Procedia Computer Science. - 2012. - T. 12. - C.386- 391.

13. Lee, JS "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi "/ JS Lee, YW Su, CCA Shen // Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE. - IEEE, 2007. - C.46-51.

14. Стрельников, А. Ю. Технологія бездротової передачі даних Wi-Fi / А. Ю. Стрельников, С. А. Страмоусова // Молодий вчений. - 2016.- №9-4 (113). - С. 67- 69.

15. Gerla, M. Multicluster, mobile, multimedia radio network / Mario Gerla, Jack Tzu-Chieh Tsai // Wireless networks. 1995. №1. - p. 255-265.

16. Gerla, M. Landmark Routing for Large Ad Hoc Wireless Networks / M. Gerla, X. Hong, and G. Pei // Proc. IEEE GLOBECOM. 2000. -№11.

17. Gupta, P. Capacity of wireless networks. / P. Gupta and PR Kumar // IEEE Transactions on Information Theory. 2000. - Volume 46, Issue 2.

18. Наміот, Д. Є. Розумні міста 2016 /Д.Е. Наміот // International Journal of Open Information Technologies. - 2016. - Т.4. - №.1. С. 1-3.

19. Li, J. Capacity of ad hoc wireless networks / Jinyang Li, Charles Blake, Douglas SJ De Couto, Hu Imm Lee, Robert Morris // Proceedings of the 7th annual International conference on Mobile computing and networking.- ACM, Rome. 2001. - C. 61-69.

20. Trends in Telecommunication Reform 2016: Regulatory Incentives to Achieve Digital Opportunities URL: http://www.itu.int/en/publications/ITU-D/Pages/default.aspx Sorensen, L. "Use scenarios 2020 року - a worldwide wireless future. Visions and research directions for the Wireless World. " Outlook / L. Sorensen, KE Skouby // Wireless World Research Forum. № 4. July 2009.

21. Osseiran, A. The foundation of the mobile and wireless communications system for 2020 and beyond: Challenges, enablers and technology solutions / A. Osseiran, V.Braun, H. Taoka, P. Marsch, H. Schotten, H. Tullberg, MAUusitalo, M.Schellman // Vehicular Technology Conference (VTC Spring), 2013 IEEE 77th. - IEEE, 2013. - C. 1-5.

22. Osseiran, A. Scenarios for 5G mobile and wireless communications: the vision of the METIS project / A. Osseiran, F. Boccardi, V. Braun, K. Kusume, P. Marsch, M.

23. Maternia, O. Queseth, M. Schellmann, H. Schotten, H. Taoka, H. Tullberg, MA Uusitalo, B. Timus and M . Fallgren // IEEE Communications Magazine. - 2014. - T.52. - №. 5. - C. 26-35.

24. Pei, Jie-fu Wireless sensor forest anti-fire network simulation based on NS2 / Pei Jiefu, Gao Lin, and Zhao Yan-dong. // In 2nd IEEE International Conference on Computer Science and Information Technology, 2009. ICCSIT 2009., 8-11 2009. doi: 10.1109 / ICCSIT.2009.5234944, PP. 300 -303.

25. Sarkar, NI Teaching Wireless Network Fundamentals Using Low-Cost Wi-Fi Devices / NI Sarkar // Revolutionizing Education through Веб- Based Instruction. - 2016. - C. 281.

26. Пістун І. П., Березовецький А. П., Тимочко В.О., Городецький І. М. Охорона праці (гігієна праці та виробнича санітарія): навч. посібн. / за ред. І.П. Пістуна. Ч. І. Львів: Тріада плюс, 2017. 620 с.

27. Пістун І. П., Тимочко В.О., Городецький І. М.. Березовецький А. П. Охорона праці (гігієна праці та виробнича санітарія): навч. посібн. / за ред. І.П. Пістуна. Ч. ІІ. Львів: Тріада плюс, 2011. 224 с.